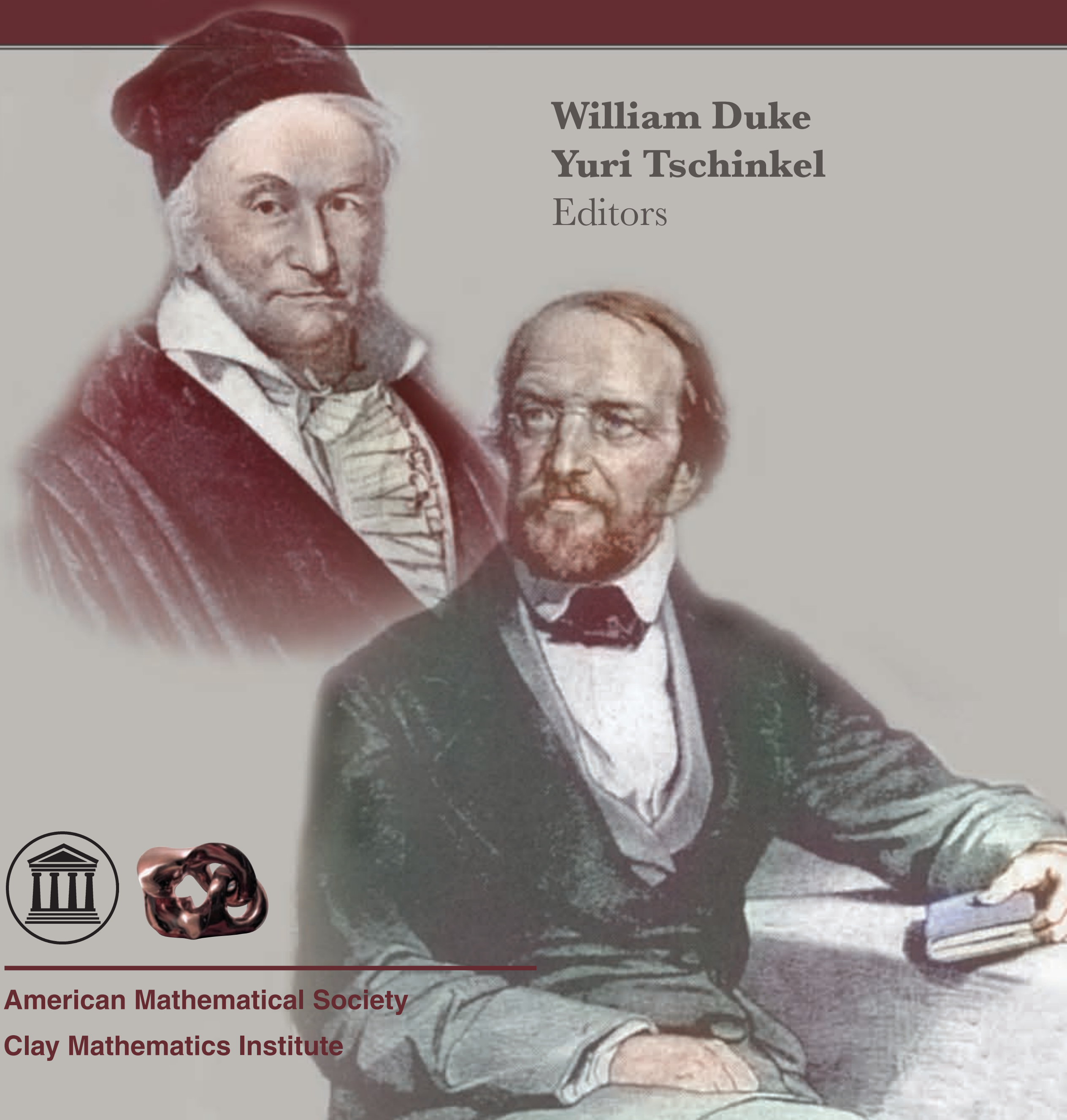
Clay Mathematics Proceedings
Volume 7

Analytic Number Theory

A Tribute to Gauss and Dirichlet

William Duke
Yuri Tschinkel
Editors



American Mathematical Society
Clay Mathematics Institute

Analytic Number Theory

A Tribute to Gauss and Dirichlet

Clay Mathematics Proceedings
Volume 7

Analytic Number Theory

A Tribute to Gauss and Dirichlet

William Duke
Yuri Tschinkel
Editors

American Mathematical Society
Clay Mathematics Institute

2000 *Mathematics Subject Classification.* Primary 01Axx, 11Dxx, 11Exx, 11Mxx, 11Nxx, 14Gxx.

The cover photo of Gustav-Peter Lejeune Dirichlet is courtesy of the Muhlenberg College Library.

Library of Congress Cataloging-in-Publication Data

Gauss-Dirichlet Conference (2005 : Göttingen, Germany)
Analytic number theory : a tribute to Gauss and Dirichlet : proceedings of the Gauss-Dirichlet Conference, Göttingen, Germany, June 20–24, 2005 / William Duke, Yuri Tschinkel, editors.
p. cm. — (Clay mathematics proceedings : v. 7)
Includes bibliographical references.
ISBN 978-0-8218-4307-9 (alk. paper)
1. Number theory—Congresses. I. Duke, William, 1958– II. Tschinkel, Yuri. III. Title.

QA241.G35 2005
512.7—dc22 2007060818

∞ The paper used in this book is acid-free and falls within the guidelines
established to ensure permanence and durability.
Visit the AMS home page at `http://www.ams.org/`
Visit the Clay Mathematics Institute home page at `http://www.claymath.org/`

10 9 8 7 6 5 4 3 2 1   12 11 10 09 08 07

Contents

Foreword

The year 2005 marked the 150th anniversary of the death of Gauss as well as the 200th anniversary of the birth of Dirichlet, who became Gauss's successor at Göttingen. In honor of these occasions, a conference was held in Göttingen from June 20 to June 24, 2005. These are the proceedings of this conference.

In view of the enormous impact both Gauss and Dirichlet had on large areas of mathematics, anything even approaching a comprehensive representation of their influence in the form of a moderately sized conference seemed untenable. Thus it was decided to concentrate on one subject, analytic number theory, that could be adequately represented and where their influence was profound. Indeed, Dirichlet is known as the father of analytic number theory. The result was a broadly based international gathering of leading number theorists who reported on recent advances in both classical analytic number theory as well as in related parts of number theory and algebraic geometry. It is our hope that the legacy of Gauss and Dirichlet in modern analytic number theory is apparent in these proceedings.

We are grateful to the American Institute of Mathematics and the Clay Mathematics Institute for their support.

William Duke and Yuri Tschinkel

November 2006

Gustav-Peter Lejeune Dirichlet

Courtesy of Niedersächsische Staats - und Universitätsbibliothek Göttingen, Sammlung Voit: Lejeune-Dirichlet, Nr. 2.

Clay Mathematics Proceedings
Volume 7, 2007

The Life and Work of Gustav Lejeune Dirichlet (1805–1859)

Jürgen Elstrodt

Dedicated to Jens Mennicke, my friend over many years

Contents

2000 *Mathematics Subject Classification.* Primary 01A55, Secondary 01A70.

Introduction

The great advances of mathematics in Germany during the first half of the nineteenth century are to a predominantly large extent associated with the pioneering work of C.F. Gauß (1777–1855), C.G.J. Jacobi (1804–1851), and G. Lejeune Dirichlet (1805–1859). In fact, virtually all leading German mathematicians of the second half of the nineteenth century were their disciples, or disciples of their disciples. This holds true to a special degree for Jacobi and Dirichlet, who most successfully introduced a new level of teaching strongly oriented to their current research whereas Gauß had "a real dislike" of teaching — at least at the poor level which was predominant when Gauß started his career. The leading role of German mathematics in the second half of the nineteenth century and even up to the fateful year 1933 would have been unthinkable without the foundations laid by Gauß, Jacobi, and Dirichlet. But whereas Gauß and Jacobi have been honoured by detailed biographies (e.g. [**Du**], [**Koe**]), a similar account of Dirichlet's life and work is still a desideratum repeatedly deplored. In particular, there exist in English only a few, mostly rather brief, articles on Dirichlet, some of which are unfortunately marred by erroneous statements. The present account is intended as a first attempt to remedy this situation.

1. Family Background and School Education

Johann Peter Gustav Lejeune Dirichlet, to give him his full name, was born in Düren (approximately halfway between Cologne and Aachen (= Aix-la-Chapelle)) on February 13, 1805. He was the seventh[1] and last child of Johann Arnold Lejeune Dirichlet (1762–1837) and his wife Anna Elisabeth, née Lindner (1768–1868(?)). Dirichlet's father was a postmaster, merchant, and city councillor in Düren. The official name of his profession was *commissaire de poste*. After 1807 the entire region of the left bank of the Rhine was under French rule as a result of the wars with revolutionary France and of the Napoleonic Wars. Hence the members of the Dirichlet family were French citizens at the time of Dirichlet's birth. After the final defeat of Napoléon Bonaparte at Waterloo and the ensuing reorganization of Europe at the Congress of Vienna (1814–1815), a large region of the left bank of the Rhine including Bonn, Cologne, Aachen and Düren came under Prussian rule, and the Dirichlet family became Prussian citizens.

Since the name "Lejeune Dirichlet" looks quite unusual for a German family we briefly explain its origin[2]: Dirichlet's grandfather Antoine Lejeune Dirichlet (1711–1784) was born in Verviers (near Liège, Belgium) and settled in Düren, where he got married to a daughter of a Düren family. It was his father who first went under the name "Lejeune Dirichlet" (meaning "the young Dirichlet") in order to differentiate from his father, who had the same first name. The name "Dirichlet" (or "Derichelette") means "from Richelette" after a little town in Belgium. We mention this since it has been purported erroneously that Dirichlet was a descendant of a

[1]Hensel [**H.1**], vol. 1, p. 349 says that Dirichlet's parents had 11 children. Possibly this number includes children which died in infancy.

[2]For many more details on Dirichlet's ancestors see [**BuJZ**].

French Huguenot family. This was not the case as the Dirichlet family was Roman Catholic.

The spelling of the name "Lejeune Dirichlet" is not quite uniform: Dirichlet himself wrote his name "Gustav Lejeune Dirichlet" without a hyphen between the two parts of his proper name. The birth-place of Dirichlet in Düren, Weierstraße 11, is marked with a memorial tablet.

Kummer [**Ku**] and Hensel [**H.1**], vol. 1 inform us that Dirichlet's parents gave their highly gifted son a very careful upbringing. This beyond doubt would not have been an easy matter for them, since they were by no means well off. Dirichlet's school and university education took place during a period of far-reaching reorganization of the Prussian educational system. His school and university education, however, show strong features of the pre-reform era, when formal prescriptions hardly existed. Dirichlet first attended an elementary school, and when this became insufficient, a private school. There he also got instruction in Latin as a preparation for the secondary school (Gymnasium), where the study of the ancient languages constituted an essential part of the training. Dirichlet's inclination for mathematics became apparent very early. He was not yet 12 years of age when he used his pocket money to buy books on mathematics, and when he was told that he could not understand them, he responded, anyhow that he would read them until he understood them.

At first, Dirichlet's parents wanted their son to become a merchant. When he uttered a strong dislike of this plan and said he wanted to study, his parents gave in, and sent him to the Gymnasium in Bonn in 1817. There the 12-year-old boy was entrusted to the care and supervision of Peter Joseph Elvenich (1796–1886), a brilliant student of ancient languages and philosophy, who was acquainted with the Dirichlet family ([**Sc.1**]). Elvenich did not have much to supervise, for Dirichlet was a diligent and good pupil with pleasant manners, who rapidly won the favour of everybody who had something to do with him. For this trait we have lifelong numerous witnesses of renowned contemporaries such as A. von Humboldt (1769–1859), C.F. Gauß, C.G.J. Jacobi, Fanny Hensel née Mendelssohn Bartholdy (1805–1847), Felix Mendelssohn Bartholdy (1809–1847), K.A. Varnhagen von Ense (1785–1858), B. Riemann (1826–1866), R. Dedekind (1831–1916). Without neglecting his other subjects, Dirichlet showed a special interest in mathematics and history, in particular in the then recent history following the French Revolution. It may be assumed that Dirichlet's later free and liberal political views can be traced back to these early studies and to his later stay in the house of General Foy in Paris (see sect. 3).

After two years Dirichlet changed to the Jesuiter-Gymnasium in Cologne. Elvenich became a philologist at the Gymnasium in Koblenz. Later he was promoted to professorships at the Universities of Bonn and Breslau, and informed Dirichlet during his stay in Bonn about the state of affairs with Dirichlet's doctor's diploma. In Cologne, Dirichlet had mathematics lessons with Georg Simon Ohm (1789–1854), well known for his discovery of Ohm's Law (1826); after him the unit of electric resistance got its name. In 1843 Ohm discovered that pure tones are described by purely sinusoidal oscillations. This finding opened the way for the application of Fourier analysis to acoustics. Dirichlet made rapid progress in mathematics under Ohm's guidance and by his diligent private study of mathematical treatises, such that he acquired an unusually broad knowledge even at this early age. He attended the Gymnasium in Cologne for only one year, starting in winter 1820, and then left with a school-leaving certificate. It has been asserted that Dirichlet passed the Abitur examination, but a check of the documents revealed that this was not the case ([**Sc.1**]). The regulations for the Abitur examination demanded that the candidate must be able to carry on a conversation in Latin, which was the *lingua franca* of the learned world for centuries. Since Dirichlet attended the Gymnasium just for three years, he most probably would have had problems in satisfying this crucial condition. Moreover he did not need the Abitur to study mathematics, which is what he aspired to. Nevertheless, his lacking the ability to speak Latin caused him much trouble during his career as we will see later. In any case, Dirichlet left the Gymnasium at the unusually early age of 16 years with a school-leaving certificate but without an Abitur examination.

His parents now wanted him to study law in order to secure a good living to their son. Dirichlet declared his willingness to devote himself to this bread-and-butter-education during daytime – but then he would study mathematics at night. After this his parents were wise enough to give in and gave their son their permission to study mathematics.

2. Study in Paris

Around 1820 the conditions to study mathematics in Germany were fairly bad for students really deeply interested in the subject ([**Lo**]). The only world-famous mathematician was C.F. Gauß in Göttingen, but he held a chair for astronomy and was first and foremost Director of the *Sternwarte*, and almost all his courses were devoted to astronomy, geodesy, and applied mathematics (see the list in [**Du**], p. 405 ff.). Moreover, Gauß did not like teaching – at least not on the low level which was customary at that time. On the contrary, the conditions in France were infinitely better. Eminent scientists such as P.-S. Laplace (1749–1827), A.-M. Legendre (1752–1833), J. Fourier (1768–1830), S.-D. Poisson (1781–1840), A.-L. Cauchy (1789–1857) were active in Paris, making the capital of France the world capital of mathematics. Hensel ([**H.1**], vol. 1, p. 351) informs us that Dirichlet's parents still had friendly relations with some families in Paris since the time of the French rule, and they let their son go to Paris in May 1822 to study mathematics. Dirichlet studied at the *Collège de France* and at the *Faculté des Sciences*, where he attended lectures of noted professors such as S.F. Lacroix (1765–1843), J.-B. Biot (1774–1862), J.N.P. Hachette (1769–1834), and L.B. Francœur (1773–1849). He also asked for permission to attend lectures as a guest student at the famous *École Polytechnique*. But the Prussian *chargé d'affaires* in Paris refused to ask for such a permission without the special authorization from the Prussian minister of religious, educational, and medical affairs, Karl Freiherr von Stein zum Altenstein (1770–1840). The 17-year-old student Dirichlet from a little provincial Rhenisch town had no chance to procure such an authorization.

More details about Dirichlet's courses are apparently not known. We do know that Dirichlet, besides his courses, devoted himself to a deep private study of Gauß' masterpiece *Disquisitiones arithmeticae*. At Dirichlet's request his mother had procured a copy of the *Disquisitiones* for him and sent to Paris in November 1822 (communication by G. Schubring, Bielefeld). There is no doubt that the study of Gauß' *magnum opus* left a lasting impression on Dirichlet which was of no less importance than the impression left by his courses. We know that Dirichlet studied the *Disquisitiones arithmeticae* several times during his lifetime, and we may safely assume that he was the first German mathematician who fully mastered this unique work. He never put his copy on his shelf, but always kept it on his desk. Sartorius von Waltershausen ([**Sa**], p. 21) says, that he had his copy with him on all his travels like some clergymen who always carry their prayer-book with themselves.

After one year of quiet life in seclusion devoted to his studies, Dirichlet's exterior life underwent a fundamental change in the summer of 1823. The General M.S. Foy (1775–1825) was looking for a private tutor to teach his children the German language and literature. The general was a highly cultured brilliant man and famous war hero, who held leading positions for 20 years during the wars of the French Republic and Napoléon Bonaparte. He had gained enormous popularity because of the circumspection with which he avoided unnecessary heavy losses. In 1819 Foy was elected into the Chamber of Deputies where he led the opposition and most energetically attacked the extreme royalistic and clerical policy of the majority, which voted in favour of the Bourbons. By the good offices of Larchet de Charmont, an old companion in arms of General Foy and friend of Dirichlet's parents, Dirichlet was recommended to the Foy family and got the job with a good salary, so that he no longer had to depend on his parents' financial support. The teaching duties were a modest burden, leaving Dirichlet enough time for his studies. In addition, with Dirichlet's help, Mme Foy brushed up her German, and, conversely, she helped him to get rid of his German accent when speaking French. Dirichlet was treated like a member of the Foy family and felt very much at ease in this fortunate position. The house of General Foy was a meeting-point of many celebrities of the French capital, and this enabled Dirichlet to gain self-assurance in his social bearing, which was of notable importance for his further life.

Dirichlet soon became acquainted with his academic teachers. His first work of academic character was a French translation of a paper by J.A. Eytelwein (1764–1848), member of the Royal Academy of Sciences in Berlin, on hydrodynamics ([**Ey**]). Dirichlet's teacher Hachette used this translation when he gave a report on this work to the Parisian *Société Philomatique* in May 1823, and he published a review in the *Bulletin des Sciences par la Société Philomatique de Paris*, 1823, pp. 113–115. The translation was printed in 1825 ([**Ey**]), and Dirichlet sent a copy to the Academy of Sciences in Berlin in 1826 ([**Bi.8**], p. 41).

Dirichlet's first own scientific work entitled *Mémoire sur l'impossibilité de quelques équations indéterminées du cinquième degré* ([**D.1**], pp. 1–20 and pp. 21–46) instantly gained him high scientific recognition. This work is closely related to Fermat's Last Theorem of 1637, which claims that the equation

$$x^n + y^n = z^n$$

cannot be solved in integers x, y, z all different from zero whenever $n \geq 3$ is a natural number. This topic was somehow in the air, since the French Academy of Sciences had offered a prize for a proof of this conjecture; the solution was to be submitted before January, 1818. In fact, we know that Wilhelm Olbers (1758–1840) had drawn Gauß' attention to this prize question, hoping that Gauß would be awarded the prize, a gold medal worth 3000 Francs ([**O.1**] pp. 626–627). At that time the insolubility of Fermat's equation in non-zero integers had been proved only for two exponents n, namely for $n = 4$ by Fermat himself, and for $n = 3$ by Euler. Since it suffices to prove the assertion for $n = 4$ and for all odd primes $n = p \geq 3$, the problem was open for all primes $p \geq 5$. Dirichlet attacked the case $p = 5$ and from the outset considered more generally the problem of solubility of the equation

$$x^5 \pm y^5 = Az^5$$

in integers, where A is a fixed integer. He proved for many special values of A, e.g. for $A = 4$ and for $A = 16$, that this equation admits no non-trivial solutions in integers. For the Fermat equation itself, Dirichlet showed that for any hypothetical non-trivial primitive integral solution x, y, z, one of the numbers must be divisible by 5, and he deduced a contradiction under the assumption that this number is additionally even. The "odd case" remained open at first.

Dirichlet submitted his paper to the French Academy of Sciences and got permission to lecture on his work to the members of the Academy. This must be considered a sensational event since the speaker was at that time a 20-year-old German student, who had not yet published anything and did not even have any degree. Dirichlet gave his lecture on June 11, 1825, and already one week later Lacroix and Legendre gave a very favourable report on his paper, such that the Academy decided to have it printed in the *Recueil des Mémoires des Savans étrangers*. However, the intended publication never materialized. Dirichlet himself had his work printed in 1825, and published it later on in more detailed form in the third volume of Crelle's Journal which — fortune favoured him — was founded just in time in 1826.

After that Legendre settled the aforementioned "odd case", and Dirichlet also subsequently treated this case by his methods. This solved the case $n = 5$ completely. Dirichlet had made the first significant contribution to Fermat's claim more than 50 years after Euler, and this immediately established his reputation as an excellent mathematician. Seven years later he also proved that Fermat's equation for the exponent 14 admits no non-trivial integral solution. (The case $n = 7$ was settled only in 1840 by G. Lamé (1795–1870).) A remarkable point of Dirichlet's work on Fermat's problem is that his proofs are based on considerations in quadratic fields, that is, in $\mathbb{Z}[\sqrt{5}]$ for $n = 5$, and $\mathbb{Z}[\sqrt{-7}]$ for $n = 14$. He apparently spent much more thought on the problem since he proved to be well-acquainted with the difficulties of the matter when in 1843 E. Kummer (1810–1893) gave him a manuscript containing an alleged general proof of Fermat's claim. Dirichlet returned the manuscript remarking that this would indeed be a valid proof, if Kummer had not only shown the factorization of any integer in the underlying cyclotomic field into a product of irreducible elements, but also the uniqueness of the factorization, which, however, does not hold true. Here and in Gauß' second installment on biquadratic residues we discern the beginnings of algebraic number theory.

The lecture to the Academy brought Dirichlet into closer contact with several renowned *académiciens*, notably with Fourier and Poisson, who aroused his interest in mathematical physics. The acquaintance with Fourier and the study of his *Théorie analytique de la chaleur* clearly gave him the impetus for his later epoch-making work on Fourier series (see sect. 8).

3. Entering the Prussian Civil Service

By 1807 Alexander von Humboldt (1769–1859) was living in Paris working almost single-handedly on the 36 lavishly illustrated volumes on the scientific evaluation of his 1799–1804 research expedition with A. Bonpland (1773–1858) to South and Central America. This expedition had earned him enormous world-wide fame, and he became a corresponding member of the French Academy in 1804 and a foreign member in 1810. Von Humboldt took an exceedingly broad interest in the natural sciences and beyond that, and he made generous good use of his fame to support young talents in any kind of art or science, sometimes even out of his own pocket. Around 1825 he was about to complete his great work and to return to Berlin as gentleman of the bedchamber of the Prussian King Friedrich Wilhelm III, who wanted to have such a luminary of science at his court.

On Fourier's and Poisson's recommendation Dirichlet came into contact with A. von Humboldt. For Dirichlet the search for a permanent position had become an urgent matter in 1825–1826, since General Foy died in November 1825, and the job as a private teacher would come to an end soon. J. Liouville (1809–1882) later said repeatedly that his friend Dirichlet would have stayed in Paris if it had been possible to find even a modestly paid position for him ([**T**], first part, p. 48, footnote). Even on the occasion of his first visit to A. von Humboldt, Dirichlet expressed his desire for an appointment in his homeland Prussia. Von Humboldt supported him in this plan and offered his help at once. It was his declared aim to make Berlin a centre of research in mathematics and the natural sciences ([**Bi.5**]).

With von Humboldt's help, the application to Berlin was contrived in a most promising way: On May 14, 1826, Dirichlet wrote a letter of application to the Prussian Minister von Altenstein and added a reprint of his memoir on the Fermat problem and a letter of recommendation of von Humboldt to his old friend von Altenstein. Dirichlet also sent copies of his memoir on the Fermat problem and of his translation of Eytelwein's work to the Academy in Berlin together with a letter of recommendation of A. von Humboldt, obviously hoping for support by the academicians Eytelwein and the astronomer J.F. Encke (1791–1865), a student of Gauß, and secretary to the Academy. Third, on May 28, 1826, Dirichlet sent a copy of his memoir on the Fermat problem with an accompanying letter to C.F. Gauß in Göttingen, explaining his situation and asking Gauß to submit his judgement to one of his correspondents in Berlin. Since only very few people were sufficiently acquainted with the subject of the paper, Dirichlet was concerned that his work might be underestimated in Berlin. (The letter is published in [**D.2**], p. 373–374.) He also enclosed a letter of recommendation by Gauß' acquaintance A. von Humboldt to the effect that in the opinion of Fourier and Poisson the young Dirichlet had a most brilliant talent and proceeded on the best Eulerian paths. And von Humboldt expressly asked Gauß for support of Dirichlet by means of his renown ([**Bi.6**], p. 28–29).

Now the matter proceeded smoothly: Gauß wrote to Encke that Dirichlet showed excellent talent, Encke wrote to a leading official in the ministry to the effect that, to the best of his knowledge, Gauß never had uttered such a high opinion on a scientist. After Encke had informed Gauß about the promising state of affairs, Gauß wrote on September 13, 1826, in an almost fatherly tone to Dirichlet, expressing his satisfaction to have evidence "from a letter received from the secretary of the Academy in Berlin, that we may hope that you soon will be offered an appropriate position in your homeland" ([**D.2**], pp. 375–376; [**G.1**], pp. 514–515).

Dirichlet returned to Düren in order to await the course of events. Before his return he had a meeting in Paris which might have left lasting traces in the history of mathematics. On October 24, 1826, N.H. Abel (1802–1829) wrote from Paris to his teacher and friend B.M. Holmboe (1795–1850), that he had met "Herrn Lejeune Dirichlet, a Prussian, who visited me the other day, since he considered me as a compatriot. He is a very sagacious mathematician. Simultaneously with Legendre he proved the insolubility of the equation

$$x^5 + y^5 = z^5$$

in integers and other nice things" ([**A**], French text p. 45 and Norwegian text p. 41). The meeting between Abel and Dirichlet might have been the beginning of a long friendship between fellow mathematicians, since in those days plans were being made for a polytechnic institute in Berlin, and Abel, Dirichlet, Jacobi, and the geometer J. Steiner (1796–1863) were under consideration as leading members of the staff. These plans, however, never materialized. Abel died early in 1829 just two days before Crelle sent his final message, that Abel definitely would be called to Berlin. Abel and Dirichlet never met after their brief encounter in Paris. Before that tragic end A.L. Crelle (1780–1855) had made every effort to create a position for Abel in Berlin, and he had been quite optimistic about this project until July, 1828, when he wrote to Abel the devastating news that the plan could not be carried out at that time, since a new competitor "had fallen out of the sky" ([**A**], French text, p. 66, Norwegian text, p. 55). It has been conjectured that Dirichlet was the new competitor, whose name was unknown to Abel, but recent investigations by G. Schubring (Bielefeld) show that this is not true.

In response to his application Minister von Altenstein offered Dirichlet a teaching position at the University of Breslau (Silesia, now Wrocław, Poland) with an opportunity for a *Habilitation* (qualification examination for lecturing at a university) and a modest annual salary of 400 talers, which was the usual starting salary of an associate professor at that time. (This was not too bad an offer for a 21-year-old young man without any final examination.) Von Altenstein wanted Dirichlet to move to Breslau just a few weeks later since there was a vacancy. He added, if Dirichlet had not yet passed the doctoral examination, he might send an application to the philosophical faculty of the University of Bonn which would grant him all facilities consistent with the rules ([**Sc.1**]).

The awarding of the doctorate, however, took more time than von Altenstein and Dirichlet had anticipated. The usual procedure was impossible for several formal reasons: Dirichlet had not studied at a Prussian university; his thesis, the memoir on the Fermat problem, was not written in Latin, and Dirichlet lacked experience in speaking Latin fluently and so was unable to give the required public disputation in Latin. A promotion *in absentia* was likewise impossible, since Minister von Altenstein had forbidden this kind of procedure in order to raise the level of the doctorates. To circumvent these formal problems some professors in Bonn suggested the conferment of the degree of honorary doctor. This suggestion was opposed by other members of the faculty distrustful of this way of undermining the usual rules. The discussions dragged along, but in the end the faculty voted unanimously. On February 24, 1827, Dirichlet's old friend Elvenich, at that time associate professor in Bonn, informed him about the happy ending, and a few days later Dirichlet obtained his doctor's diploma.

Because of the delay Dirichlet could not resume his teaching duties in Breslau in the winter term 1826–27. In addition, a delicate serious point still had to be settled clandstinely by the ministry. In those days Central and Eastern Europe were under the harsh rule of the Holy Alliance (1815), the Carlsbad Decrees (1819) were carried out meticulously, and alleged "demagogues" were to be prosecuted (1819). The Prussian *chargé d'affaires* in Paris received a letter from the ministry in Berlin asking if anything arousing political suspicion could be found out about the applicant, since there had been rumours that Dirichlet had lived in the house of the deceased General Foy, a fierce enemy of the government. The *chargé* checked the matter, and reported that nothing was known to the detriment of Dirichlet's views and actions, and that he apparently had lived only for his science.

4. Habilitation and Professorship in Breslau

In the course of the Prussian reforms following the Napoleonic Wars several universities were founded under the guidance of Wilhelm von Humboldt (1767–1835), Alexander von Humboldt's elder brother, namely, the Universities of Berlin (1810), Breslau (1811), and Bonn (1818), and the General Military School was founded in Berlin in 1810, on the initiative of the Prussian General G.J.D. von Scharnhorst (1755–1813). During his career Dirichlet had to do with all these institutions. We have already mentioned the honorary doctorate from Bonn.

In spring 1827, Dirichlet moved from Düren to Breslau in order to assume his appointment. On the long journey there he made a major detour via Göttingen to meet Gauß in person (March 18, 1827), and via Berlin. In a letter to his mother Dirichlet says that Gauß received him in a very friendly manner. Likewise, from a letter of Gauß to Olbers ([**O.2**], p. 479), we know that Gauß too was very much pleased to meet Dirichlet in person, and he expresses his great satisfaction that his recommendation had apparently helped Dirichlet to acquire his appointment. Gauß also tells something about the topics of the conversation, and he says that he was surprised to learn from Dirichlet, that his (i.e., Gauß') judgement on many mathematical matters completely agreed with Fourier's, notably on the foundations of geometry.

For Dirichlet, the first task in Breslau was to habilitate (qualify as a university lecturer). According to the rules in force he had
a) to give a trial lecture,
b) to write a thesis (*Habilitationsschrift*) in Latin, and
c) to defend his thesis in a public disputation to be held in Latin.
Conditions a) and b) caused no serious trouble, but Dirichlet had difficulties to meet condition c) because of his inability to speak Latin fluently. Hence he wrote to Minister von Altenstein asking for dispensation from the disputation. The minister

granted permission — very much to the displeasure of some members of the faculty ([**Bi.1**]).

To meet condition a), Dirichlet gave a trial lecture on Lambert's proof of the irrationality of the number π. In compliance with condition b), he wrote a thesis on the following number theoretic problem (see [**D.1**], pp. 45–62): Let x, b be integers, b not a square of an integer, and expand

$$(x + \sqrt{b})^n = U + V\sqrt{b}\ ,$$

where U and V are integers. The problem is to determine the linear forms containing the primes dividing V, when the variable x assumes all positive or negative integral values coprime with b. This problem is solved in two cases, viz.
(i) if n is an odd prime,
(ii) if n is a power of 2.
The results are illustrated on special examples. Of notable interest is the introduction in which Dirichlet considers examples from the theory of biquadratic residues and refers to his great work on biquadratic residues, which was to appear in Crelle's Journal at that time.

The thesis was printed early in 1828, and sent to von Altenstein, and in response Dirichlet was promoted to the rank of associate professor. A. von Humboldt added the promise to arrange Dirichlet's transfer to Berlin as soon as possible. According to Hensel ([**H.1**], vol. 1, p. 354) Dirichlet did not feel at ease in Breslau, since he did not like the widespread provincial cliquishness. Clearly, he missed the exchange of views with qualified researchers which he had enjoyed in Paris. On the other hand, there were colleagues in Breslau who held Dirichlet in high esteem, as becomes evident from a letter of Dirichlet's colleague H. Steffens (1773–1845) to the ministry ([**Bi.1**], p. 30): Steffens pointed out that Dirichlet generally was highly thought of, because of his thorough knowledge, and well liked, because of his great modesty. Moreover he wrote that his colleague — like the great Gauß in Göttingen — did not have many students, but those in the audience, who were seriously occupied with mathematics, knew how to estimate Dirichlet and how to make good use of him.

From the scientific point of view Dirichlet's time in Breslau proved to be quite successful. In April 1825, Gauß had published a first brief announcement — as he was used to doing — of his researches on biquadratic residues ([**G.1**], pp. 165–168). Recall that an integer a is called a biquadratic residue modulo the odd prime $p, p \nmid a$, if and only if the congruence $x^4 \equiv a \bmod p$ admits an integral solution. To whet his readers' appetite, Gauß communicated his results on the biquadratic character of the numbers ± 2. The full-length publication of his first installment appeared in print only in 1828 ([**G.1**], 65–92). It is well possible, though not reliably known, that Gauß talked to Dirichlet during the latter's visit to Göttingen about his recent work on biquadratic residues. In any case he did write in his very first letter of September 13, 1826, to Dirichlet about his plan to write three memoirs on this topic ([**D.2**], pp. 375–376; [**G.1**], pp. 514–515).

It is known that Gauß' announcement immediately aroused the keen interest of both Dirichlet and Jacobi, who was professor in Königsberg (East Prussia; now Kaliningrad, Russia) at that time. They both tried to find their own proofs of

Gauß' results, and they both discovered plenty of new results in the realm of higher power residues. A report on Jacobi's findings is contained in [**J.2**] amongst the correspondence with Gauß. Dirichlet discovered remarkably simple proofs of Gauß' results on the biquadratic character of ± 2, and he even answered the question as to when an odd prime q is a biquadratic residue modulo the odd prime $p, p \neq q$. To achieve the biquadratic reciprocity law, only one further step had to be taken which, however, became possible only some years later, when Gauß, in his second installment of 1832, introduced complex numbers, his Gaussian integers, into the realm of number theory ([**G.1**], pp. 169–178, 93–148, 313–385; [**R**]). This was Gauß' last long paper on number theory, and a very important one, helping to open the gate to algebraic number theory. The first printed proof of the biquadratic reciprocity law was published only in 1844 by G. Eisenstein (1823–1852; see [**Ei**], vol. 1, pp. 141–163); Jacobi had already given a proof in his lectures in Königsberg somewhat earlier.

Dirichlet succeeded with some crucial steps of his work on biquadratic residues on a brief vacation in Dresden, seven months after his visit to Gauß. Fully aware of the importance of his investigation, he immediately sent his findings in a long sealed letter to Encke in Berlin to secure his priority, and shortly thereafter he nicely described the fascinating history of his discovery in a letter of October 28, 1827, to his mother ([**R**], p. 19). In this letter he also expressed his high hopes to expect much from his new work for his further promotion and his desired transfer to Berlin. His results were published in the memoir *Recherches sur les diviseurs premiers d'une classe de formules du quatrième degré* ([**D.1**], pp. 61–98). Upon publication of this work he sent an offprint with an accompanying letter (published in [**D.2**], pp. 376–378) to Gauß, who in turn expressed his appreciation of Dirichlet's work, announced his second installment, and communicated some results carrying on the last lines of his first installment in a most surprising manner ([**D.2**], pp. 378–380; [**G.1**], pp. 516–518).

The subject of biquadratic residues was always in Dirichlet's thought up to the end of his life. In a letter of January 21, 1857, to Moritz Abraham Stern (1807–1894), Gauß' first doctoral student, who in 1859 became the first Jewish professor in Germany who did not convert to Christianity, he gave a completely elementary proof of the criterion for the biquadratic character of the number 2 ([**D.2**], p. 261 f.).

Having read Dirichlet's article, F.W. Bessel (1784–1846), the famous astronomer and colleague of Jacobi in Königsberg, enthusiastically wrote to A. von Humboldt on April 14, 1828: "... who could have imagined that this genius would succeed in reducing something appearing so difficult to such simple considerations. The name Lagrange could stand at the top of the memoir, and nobody would realize the incorrectness" ([**Bi.2**], pp. 91–92). This praise came just in time for von Humboldt to arrange Dirichlet's transfer to Berlin. Dirichlet's period of activity in Breslau was quite brief; Sturm [**St**] mentions that he lectured in Breslau only for two semesters, Kummer says three semesters.

5. Transfer to Berlin and Marriage

Aiming at Dirichlet's transfer to Berlin, A. von Humboldt sent copies of Bessel's enthusiastic letter to Minister von Altenstein and to Major J.M. von Radowitz (1797–1853), at that time teacher at the Military School in Berlin. At the same time Fourier tried to bring Dirichlet back to Paris, since he considered Dirichlet to be the right candidate to occupy a leading role in the French Academy. (It does not seem to be known, however, whether Fourier really had an offer of a definite position for Dirichlet.) Dirichlet chose Berlin, at that time a medium-sized city with 240 000 inhabitants, with dirty streets, without pavements, without street lightning, without a sewage system, without public water supply, but with many beautiful gardens.

A. von Humboldt recommended Dirichlet to Major von Radowitz and to the minister of war for a vacant post at the Military School. At first there were some reservations to installing a young man just 23 years of age for the instruction of officers. Hence Dirichlet was first employed on probation only. At the same time he was granted leave for one year from his duties in Breslau. During this time his salary was paid further on from Breslau; in addition he received 600 talers per year from the Military School. The trial period was successful, and the leave from Breslau was extended twice, so that he never went back there.

From the very beginning, Dirichlet also had applied for permission to give lectures at the University of Berlin, and in 1831 he was formally transferred to the philosophical faculty of the University of Berlin with the further duty to teach at the Military School. There were, however, strange formal oddities about his legal status at the University of Berlin which will be dealt with in sect. 7.

In the same year 1831 he was elected to the Royal Academy of Sciences in Berlin, and upon confirmation by the king, the election became effective in 1832. At that time the 27-year-old Dirichlet was the youngest member of the Academy.

Shortly after Dirichlet's move to Berlin, a most prestigious scientific event organized by A. von Humboldt was held there, the seventh assembly of the German Association of Scientists and Physicians (September 18–26, 1828). More than 600 participants from Germany and abroad attended the meeting, Felix Mendelssohn Bartholdy composed a ceremonial music, the poet Rellstab wrote a special poem, a stage design by Schinkel for the aria of the Queen of the Night in Mozart's *Magic Flute* was used for decoration, with the names of famous scientists written in the firmament. A great gala dinner for all participants and special invited guests with the king attending was held at von Humboldt's expense. Gauß took part in the meeting and lived as a special guest in von Humboldt's house. Dirichlet was invited by von Humboldt jointly with Gauß, Charles Babbage (1792–1871) and the officers von Radowitz and K. von Müffing (1775–1851) as a step towards employment at the Military School. Another participant of the conference was the young physicist Wilhelm Weber (1804–1891), at that time associate professor at the University of Halle. Gauß got to know Weber at this assembly, and in 1831 he arranged Weber's call to Göttingen, where they both started their famous joint work on the investigation of electromagnetism. The stimulating atmosphere in Berlin was compared by Gauß in a letter to his former student C.L. Gerling (1788–1864) in Marburg "to a move from atmospheric air to oxygen".

The following years were the happiest in Dirichlet's life both from the professional and the private point of view. Once more it was A. von Humboldt who established also the private relationship. At that time great salons were held in Berlin, where people active in art, science, humanities, politics, military affairs, economics, etc. met regularly, say, once per week. A. von Humboldt introduced Dirichlet to the house of Abraham Mendelssohn Bartholdy (1776–1835) (son of the legendary Moses Mendelssohn (1729–1786)) and his wife Lea, née Salomon (1777–1842), which was a unique meeting point of the cultured Berlin. The Mendelssohn family lived in a baroque palace erected in 1735, with a two-storied main building, side-wings, a large garden hall holding up to 300 persons, and a huge garden of approximately 3 hectares (almost 10 acres) size. (The premises were sold in 1851 to the Prussian state and the house became the seat of the Upper Chamber of the Prussian Parliament. In 1904 a new building was erected, which successively housed the Upper Chamber of the Prussian Parliament, the Prussian Council of State, the Cabinet of the GDR, and presently the German Bundesrat.) There is much to be told about the Mendelssohn family which has to be omitted here; for more information see the recent wonderful book by T. Lackmann [**Lac**]. Every Sunday morning famous Sunday concerts were given in the Mendelssohn garden hall with the four highly gifted Mendelssohn children performing. These were the pianist and composer Fanny (1805–1847), later married to the painter Wilhelm Hensel (1794–1861), the musical prodigy, brilliant pianist and composer Felix (1809–1847), the musically gifted Rebecka (1811–1858), and the cellist Paul (1812–1874), who later carried out the family's banking operations. Sunday concerts started at 11 o'clock and lasted for 4 hours with a break for conversation and refreshments in between. Wilhelm Hensel made portraits of the guests — more than 1000 portraits came into being this way, a unique document of the cultural history of that time.

From the very beginning, Dirichlet took an interest in Rebecka, and although she had many suitors, she decided for Dirichlet. Lackmann ([**Lac**]) characterizes Rebecka as the linguistically most gifted, wittiest, and politically most receptive of the four children. She experienced the radical changes during the first half of the nineteeth century more consciously and critically than her siblings. These traits are clearly discernible also from her letters quoted by her nephew Sebastian Hensel ([**H.1**], [**H.2**]). The engagement to Dirichlet took place in November 1831. After the wedding in May 1832, the young married couple moved into a flat in the parental house, Leipziger Str. 3, and after the Italian journey (1843–1845), the Dirichlet family moved to Leipziger Platz 18.

In 1832 Dirichlet's life could have taken quite a different course. Gauß planned to nominate Dirichlet as a successor to his deceased colleague, the mathematician B.F. Thibaut (1775–1832). When Gauß learnt about Dirichlet's marriage, he cancelled this plan, since he assumed that Dirichlet would not be willing to leave Berlin. The triumvirate Gauß, Dirichlet, and Weber would have given Göttingen a unique constellation in mathematics and natural sciences not to be found anywhere else in the world.

Dirichlet was notoriously lazy about letter writing. He obviously preferred to settle matters by directly contacting people. On July 2, 1833, the first child, the son Walter, was born to the Dirichlet family. Grandfather Abraham Mendelssohn Bartholdy got the happy news on a buisiness trip in London. In a letter he congratulated Rebecka and continued resentfully: “I don’t congratulate Dirichlet, at least not in writing, since he had the heart not to write me a single word, even on this occasion; at least he could have written: $2 + 1 = 3$” ([**H.1**], vol. 1, pp. 340–341). (Walter Dirichlet became a well-known politician later and member of the German Reichstag 1881–1887; see [**Ah.1**], 2. Teil, p. 51.)

The Mendelssohn family is closely related with many artists and scientists of whom we but mention some prominent mathematicians: The renowned number theorist Ernst Eduard Kummer was married to Rebecka’s cousin Ottilie Mendelssohn (1819–1848) and hence was Dirichlet’s cousin. He later became Dirichlet’s successor at the University of Berlin and at the Military School, when Dirichlet left for Göttingen. The function theorist Hermann Amandus Schwarz (1843–1921), after whom Schwarz’ Lemma and the Cauchy–Schwarz Inequality are named, was married to Kummer’s daughter Marie Elisabeth, and hence was Kummer’s son-in-law. The analyst Heinrich Eduard Heine (1821–1881), after whom the Heine–Borel Theorem got its name, was a brother of Albertine Mendelssohn Bartholdy, née Heine, wife of Rebecka’s brother Paul. Kurt Hensel (1861–1941), discoverer of the p-adic numbers and for many years editor of Crelle’s Journal, was a son of Sebastian Hensel (1830–1898) and his wife Julie, née Adelson; Sebastian Hensel was the only child of Fanny and Wilhelm Hensel, and hence a nephew of the Dirichlets. Kurt and Gertrud (née Hahn) Hensel’s daughter Ruth Therese was married to the professor of law Franz Haymann, and the noted function theorist Walter Hayman (born 1926) is an offspring of this married couple. The noted group theorist and number theorist Robert Remak (1888– some unknown day after 1942 when he met his death in Auschwitz) was a nephew of Kurt and Gertrud Hensel. The philosopher and logician Leonard Nelson (1882–1927) was a great-great-grandson of Gustav and Rebecka Lejeune Dirichlet.

6. Teaching at the Military School

When Dirichlet began teaching at the Military School on October 1, 1828, he first worked as a coach for the course of F.T. Poselger (1771–1838). It is a curious coincidence that Georg Simon Ohm, Dirichlet’s mathematics teacher at the *Gymnasium* in Cologne, simultaneously also worked as a coach for the course of his brother, the mathematician Martin Ohm (1792–1872), who was professor at the University of Berlin. Dirichlet’s regular teaching started one year later, on October 1, 1829. The course went on for three years and then started anew. Its content was essentially elementary and practical in nature, starting in the first year with the theory of equations (up to polynomial equations of the fourth degree), elementary theory of series, some stereometry and descriptive geometry. This was followed in the second year by some trigonometry, the theory of conics, more stereometry and analytical geometry of three-dimensional space. The third year was devoted to mechanics, hydromechanics, mathematical geography and geodesy. At first, the differential and integral calculus was not included in the curriculum, but some years later Dirichlet succeeded in raising the level of instruction by introducing so-called higher analysis and its applications to problems of mechanics into the program. Subsequently, this change became permanent and was adhered to even when Dirichlet left his post ([**Lam**]). Altogether he taught for 27 years at the Military School, from his transfer to Berlin in 1828 to his move to Göttingen in 1855, with two breaks during his Italian journey (1843–1845) and after the March Revolution of 1848 in Berlin, when the Military School was closed down for some time, causing Dirichlet a sizable loss of his income.

During the first years Dirichlet really enjoyed his position at the Military School. He proved to be an excellent teacher, whose courses were very much appreciated by his audience, and he liked consorting with the young officers, who were almost of his own age. His refined manners impressed the officers, and he invited them for stimulating evening parties in the course of which he usually formed the centre of conversation. Over the years, however, he got tired of repeating the same curriculum every three years. Moreover, he urgently needed more time for his research; together with his lectures at the university his teaching load typically was around 18 hours per week.

When the Military School was reopened after the 1848 revolution, a new reactionary spirit had emerged among the officers, who as a rule belonged to the nobility. This was quite opposed to Dirichlet's own very liberal convictions. His desire to quit the post at the Military School grew, but he needed a compensation for his loss in income from that position, since his payment at the University of Berlin was rather modest. When the Prussian ministry was overly reluctant to comply with his wishes, he accepted the most prestigious call to Göttingen as a successor to Gauß in 1855.

7. Dirichlet as a Professor at the University of Berlin

From the very beginning Dirichlet applied for permission to give lectures at the University of Berlin. The minister approved his application and communicated this decision to the philosophical faculty. But the faculty protested, since Dirichlet was neither habilitated nor appointed professor, whence the instruction of the minister was against the rules. In his response the minister showed himself conciliatory and said he would leave it to the faculty to demand from Dirichlet an appropriate achievement for his *Habilitation*. Thereupon the dean of the philosphical faculty offered a reasonable solution: He suggested that the faculty would consider Dirichlet — in view of his merits — as *Professor designatus*, with the right to give lectures. To satisfy the formalities of a *Habilitation*, he only requested Dirichlet

a) to distribute a written program in Latin, and
b) to give a lecture in Latin in the large lecture-hall.

This seemed to be a generous solution. Dirichlet was well able to compose texts in Latin as he had proved in Breslau with his *Habilitationsschrift*. He could prepare his lecture in writing and just read it — this did not seem to take great pains. But quite unexpectedly he gave the lecture only with enormous reluctance. It took Dirichlet almost 23 years to give it. The lecture was entitled *De formarum* *binarium secundi gradus compositione* ("On the composition of binary quadratic forms"; [**D.2**], pp. 105–114) and comprises less than 8 printed pages. On the title page Dirichlet is referred to as *Phil. Doct. Prof. Publ. Ord. Design.* The reasons for the unbelievable delay are given in a letter to the dean H.W. Dove (1803–1879) of November 10, 1850, quoted in [**Bi.1**], p. 43. In the meantime Dirichlet was transferred for long as an associate professor to the University of Berlin in 1831, and he was even advanced to the rank of full professor in 1839, but in the faculty he still remained *Professor designatus* up to his *Habilitation* in 1851. This meant that it was only in 1851 that he had equal rights in the faculty; before that time he was, e.g. not entitled to write reports on doctoral dissertations nor could he influence *Habilitationen* — obviously a strange situation since Dirichlet was by far the most competent mathematician on the faculty.

We have several reports of eye-witnesses about Dirichlet's lectures and his social life. After his participation in the assembly of the German Association of Scientists and Physicians, Wilhelm Weber started a research stay in Berlin beginning in October, 1828. Following the advice of A. von Humboldt, he attended Dirichlet's lectures on Fourier's theory of heat. The eager student became an intimate friend of Dirichlet's, who later played a vital role in the negotiations leading to Dirichlet's move to Göttingen (see sect. 12). We quote some lines of the physicist Heinrich Weber (1839–1928), nephew of Wilhelm Weber, not to be confused with the mathematician Heinrich Weber (1842–1913), which give some impression on the social life of his uncle in Berlin ([**Web**], pp. 14–15): "After the lectures which were given three times per week from 12 to 1 o'clock there used to be a walk in which Dirichlet often took part, and in the afternoon it became eventually common practice to go to the coffee-house 'Dirichlet'. 'After the lecture every time one of us invites the others without further ado to have coffee at Dirichlet's, where we show up at 2 or 3 o'clock and stay quite cheerfully up to 6 o'clock'[3]".

During his first years in Berlin Dirichlet had only rather few students, numbers varying typically between 5 and 10. Some lectures could not even be given at all for lack of students. This is not surprising since Dirichlet generally gave lectures on what were considered to be "higher" topics, whereas the great majority of the students preferred the lectures of Dirichlet's colleagues, which were not so demanding and more oriented towards the final examination. Before long, however, the situation changed, Dirichlet's reputation as an excellent teacher became generally known, and audiences comprised typically between 20 and 40 students, which was quite a large audience at that time.

Although Dirichlet was not on the face of it a brilliant speaker like Jacobi, the great clarity of his thought, his striving for perfection, the self-confidence with which he elaborated on the most complicated matters, and his thoughtful remarks fascinated his students. Whereas mere computations played a major role in the lectures of most of his contemporaries, in Dirichlet's lectures the mathematical argument came to the fore. In this regard Minkowski [**Mi**] speaks "of the other Dirichlet Principle to overcome the problems with a minimum of blind computation and a maximum of penetrating thought", and from that time on he dates "the modern times in the history of mathematics".

[3] Quotation from a family letter of W. Weber of November 21, 1828.

Dirichlet prepared his lectures carefully and spoke without notes. When he could not finish a longer development, he jotted down the last formula on a slip of paper, which he drew out of his pocket at the beginning of the next lecture to continue the argument. A vivid description of his lecturing habits was given by Karl Emil Gruhl (1833–1917), who attended his lectures in Berlin (1853–1855) and who later became a leading official in the Prussian ministry of education (see [**Sc.2**]). An admiring description of Dirichlet's teaching has been passed on to us by Thomas Archer Hirst (1830–1892), who was awarded a doctor's degree in Marburg, Germany, in 1852, and after that studied with Dirichlet and Steiner in Berlin. In Hirst's diary we find the following entry of October 31, 1852 ([**GW**], p. 623): "Dirichlet cannot be surpassed for richness of material and clear insight into it: as a speaker he has no advantages — there is nothing like fluency about him, and yet a clear eye and understanding make it dispensable: without an effort you would not notice his hesitating speech. What is peculiar in him, he never sees his audience — when he does not use the blackboard at which time his back is turned to us, he sits at the high desk facing us, puts his spectacles up on his forehead, leans his head on both hands, and keeps his eyes, when not covered with his hands, mostly shut. He uses no notes, inside his hands he sees an imaginary calculation, and reads it out to us — that we understand it as well as if we too saw it. I like that kind of lecturing." — After Hirst called on Dirichlet and was "met with a very hearty reception", he noted in his diary on October 13, 1852 ([**GW**], p. 622): "He is a rather tall, lanky-looking man, with moustache and beard about to turn grey (perhaps 45 years old), with a somewhat harsh voice and rather deaf: it was early, he was unwashed, and unshaved (what of him required shaving), with his 'Schlafrock', slippers, cup of coffee and cigar ... I thought, as we sat each at an end of the sofa, and the smoke of our cigars carried question and answer to and fro, and intermingled in graceful curves before it rose to the ceiling and mixed with the common atmospheric air, 'If all be well, we will smoke our friendly cigar together many a time yet, good-natured Lejeune Dirichlet'."

The topics of Dirichlet's lectures were mainly chosen from various areas of number theory, foundations of analysis (including infinite series, applications of integral calculus), and mathematical physics. He was the first university teacher in Germany to give lectures on his favourite subject, number theory, and on the application of analytical techniques to number theory; 23 of his lectures were devoted to these topics ([**Bi.1**]; [**Bi.8**], p. 47).

Most importantly, the lectures of Jacobi in Königsberg and Dirichlet in Berlin gave the impetus for a general rise of the level of mathematical instruction in Germany, which ultimately led to the very high standards of university mathematics in Germany in the second half of the nineteenth century and beyond that up to 1933. Jacobi even established a kind of "Königsberg school" of mathematics principally dedicated to the investigation of the theory of elliptic functions. The foundation of the first mathematical seminar in Germany in Königsberg (1834) was an important event in his teaching activities. Dirichlet was less extroverted; from 1834 onwards he conducted a kind of private mathematical seminar in his house which was not even mentioned in the university calendar. The aim of this private seminar was to give his students an opportunity to practice their oral presentation and their skill in solving problems. For a full-length account on the development of the study of mathematics at German universities during the nineteenth century see Lorey [**Lo**].

A large number of mathematicians received formative impressions from Dirichlet by his lectures or by personal contacts. Without striving for a complete list we mention the names of P. Bachmann (1837–1920), the author of numerous books on number theory, G. Bauer (1820–1907), professor in Munich, C.W. Borchardt (1817–1880), Crelle's successor as editor of Crelle's Journal, M. Cantor (1829–1920), a leading German historian of mathematics of his time, E.B. Christoffel (1829–1900), known for his work on differential geometry, R. Dedekind (1831–1916), noted for his truly fundamental work on algebra and algebraic number theory, G. Eisenstein (1823–1852), noted for his profound work on number theory and elliptic functions, A. Enneper (1830–1885), known for his work on the theory of surfaces and elliptic functions, E. Heine (1821–1881), after whom the Heine–Borel Theorem got its name, L. Kronecker (1823–1891), the editor of Dirichlet's collected works, who jointly with Kummer and Weierstraß made Berlin a world centre of mathematics in the second half of the nineteenth century, E.E. Kummer (1810–1893), one of the most important number theorists of the nineteenth century and not only Dirichlet's successor in his chair in Berlin but also the author of the important obituary [**Ku**] on Dirichlet, R. Lipschitz (1832–1903), noted for his work on analysis and number theory, B. Riemann (1826–1866), one of the greatest mathematicians of the 19th century and Dirichlet's successor in Göttingen, E. Schering (1833–1897), editor of the first edition of the first 6 volumes of Gauß' collected works, H. Schröter (1829–1892), professor in Breslau, L. von Seidel (1821–1896), professor in Munich, who introduced the notion of uniform convergence, J. Weingarten (1836–1910), who advanced the theory of surfaces.

Dirichlet's lectures had a lasting effect even beyond the grave, although he did not prepare notes. After his death several of his former students published books based on his lectures: In 1904 G. Arendt (1832–1915) edited Dirichlet's lectures on definite integrals following his 1854 Berlin lectures ([**D.7**]). As early as 1871 G.F. Meyer (1834–1905) had published the 1858 Göttingen lectures on the same topic ([**MG**]), but his account does not follow Dirichlet's lectures as closely as Arendt does. The lectures on "forces inversely proportional to the square of the distance" were published by F. Grube (1835–1893) in 1876 ([**Gr**]). Here one may read how Dirichlet himself explained what Riemann later called "Dirichlet's Principle". And last but not least, there are Dirichlet's lectures on number theory in the masterly edition of R. Dedekind, who over the years enlarged his own additions to a pioneering exposition of the foundations of algebraic number theory based on the concept of ideal.

8. Mathematical Works

In spite of his heavy teaching load, Dirichlet achieved research results of the highest quality during his years in Berlin. When A. von Humboldt asked Gauß in 1845 for a proposal of a candidate for the order *pour le mérite*, Gauß did "not neglect to nominate Professor Dirichlet in Berlin. The same has — as far as I know — not yet published a big work, and also his individual memoirs do not yet comprise a big volume. But they are jewels, and one does not weigh jewels on a grocer's scales"

([**Bi.6**], p. 88)[4]. We quote a few highlights of Dirichlet's *œuvre* showing him at the peak of his creative power.

A. Fourier Series. The question whether or not an "arbitrary" 2π-periodic function on the real line can be expanded into a trigonometric series

$$\frac{a_0}{2} + \sum_{n=1}^{\infty}(a_n \cos nx + b_n \sin nx)$$

was the subject of controversal discussions among the great analysts of the eighteenth century, such as L. Euler, J. d'Alembert, D. Bernoulli, J. Lagrange. Fourier himself did not settle this problem, though he and his predecessors knew that such an expansion exists in many interesting cases. Dirichlet was the first mathematician to prove rigorously for a fairly wide class of functions that such an expansion is possible. His justly famous memoir on this topic is entitled *Sur la convergence des séries trigonométriques qui servent à représenter une fonction arbitraire entre des limites données* (1829) ([**D.1**], pp. 117–132). He points out in this work that some restriction on the behaviour of the function in question is necessary for a positive solution to the problem, since, e.g. the notion of integral *"ne signifie quelque chose"* for the (Dirichlet) function

$$f(x) = \begin{cases} c & \text{for} \quad x \in \mathbb{Q}\,, \\ d & \text{for} \quad x \in \mathbb{R} \setminus \mathbb{Q}\,, \end{cases}$$

whenever $c, d \in \mathbb{R}, c \neq d$ ([**D.1**], p. 132). An extended version of his work appeared in 1837 in German ([**D.1**], pp. 133–160; [**D.4**]). We comment on this German version since it contains various issues of general interest. Before dealing with his main problem, Dirichlet clarifies some points which nowadays belong to any introductory course on real analysis, but which were by far not equally commonplace at that time. This refers first of all to the notion of function. In Euler's *Introductio in analysin infinitorum* the notion of function is circumscribed somewhat tentatively by means of "analytical expressions", but in his book on differential calculus his notion of function is so wide "as to comprise all manners by which one magnitude may be determined by another one". This very wide concept, however, was not generally accepted. But then Fourier in his *Théorie analytique de la chaleur* (1822) advanced the opinion that also any non-connected curve may be represented by a trigonometric series, and he formulated a corresponding general notion of function. Dirichlet follows Fourier in his 1837 memoir: "If to any x there corresponds a single finite y, namely in such a way that, when x continuously runs through the interval from a to b, $y = f(x)$ likewise varies little by little, then y is called a continuous ... function of x. Yet it is not necessary that y in this whole interval depend on x according to the same law; one need not even think of a dependence expressible in terms of mathematical operations" ([**D.1**], p. 135). This definition suffices for Dirichlet since he only considers piecewise continuous functions.

Then Dirichlet defines the integral for a continuous function on $[a, b]$ as the limit of decomposition sums for equidistant decompositions, when the number of intermediate points tends to infinity. Since his paper is written for a manual of physics, he does not formally prove the existence of this limit, but in his lectures [**D.7**] he fully

[4]At that time Dirichlet was not yet awarded the order. He got it in 1855 after Gauß' death, and thus became successor to Gauß also as a recipient of this extraordinary honour.

proves the existence by means of the uniform continuity of a continuous function on a closed interval, which he calls a "fundamental property of continuous functions" (loc. cit., p. 7).

He then tentatively approaches the development into a trigonometric series by means of discretization. This makes the final result plausible, but leaves the crucial limit process unproved. Hence he starts anew in the same way customary today: Given the piecewise continuous[5] 2π-periodic function $f : \mathbb{R} \to \mathbb{R}$, he forms the (Euler-)Fourier coefficients

$$\begin{aligned} a_k &:= \frac{1}{\pi}\int_{-\pi}^{\pi} f(t)\,\cos\,kt\,dt \quad (k \geq 0)\ , \\ b_k &:= \frac{1}{\pi}\int_{-\pi}^{\pi} f(t)\,\sin\,kt\,dt \quad (k \geq 1)\ , \end{aligned}$$

and transforms the partial sum

$$s_n(x) := \frac{a_0}{2} + \sum_{k=1}^{n}(a_k \cos kx + b_k \sin kx)$$

($n \geq 0$) into an integral, nowadays known as *Dirichlet's Integral*,

$$s_n(x) = \frac{1}{2\pi}\int_{-\pi}^{\pi} f(t)\frac{\sin(2n+1)\frac{t-x}{2}}{\sin\frac{t-x}{2}}\,dt\ .$$

The pioneering progress of Dirichlet's work now is to find a precise simple sufficient condition implying

$$\lim_{n\to\infty} s_n(x) = \frac{1}{2}(f(x+0) + f(x-0))\ ,$$

namely, this limit relation holds whenever f is piecewise continuous and piecewise monotone in a neighbourhood of x. A crucial role in Dirichlet's argument is played by a preliminary version of what is now known as the Riemann–Lebesgue Lemma and by a mean-value theorem for integrals.

Using the same method Dirichlet also proves the expansion of an "arbitrary" function depending on two angles into a series of spherical functions ([**D.1**], pp. 283–306). The main trick of this paper is a transformation of the partial sum into an integral of the shape of Dirichlet's Integral.

A characteristic feature of Dirichlet's work is his skilful application of analysis to questions of number theory, which made him the founder of analytic number theory ([**Sh**]). This trait of his work appears for the first time in his paper *Über eine neue Anwendung bestimmter Integrale auf die Summation endlicher oder unendlicher Reihen* (1835) (On a new application of definite integrals to the summation of finite or infinite series, [**D.1**], pp. 237–256; shortened French translation in [**D.1**], pp. 257–270). Applying his result on the limiting behaviour of Dirichlet's Integral for n tending to infinity, he computes the Gaussian Sums in a most lucid way, and he uses the latter result to give an ingenious proof of the quadratic reciprocity theorem. (Recall that Gauß himself published 6 different proofs of his *theorema fundamentale*, the law of quadratic reciprocity (see [**G.2**]).)

[5]finitely many pieces in $[0, 2\pi]$

B. Dirichlet's Theorem on Primes in Arithmetical Progressions. Dirichlet's mastery in the application of analysis to number theory manifests itself most impressively in his proof of the theorem on an infinitude of primes in any arithmetic progression of the form $(a+km)_{k\geq 1}$, where a and m are coprime natural numbers. In order to explain why this theorem is of special interest, Dirichlet gives the following typical example ([**D.1**], p. 309): The law of quadratic reciprocity implies that the congruence $x^2+7 \equiv 0 \,(\bmod\ p)$ is solvable precisely for those primes p different from 2 and 7 which are of the form $7k+1, 7k+2$, or $7k+4$ for some natural number k. But the law of quadratic reciprocity gives no information at all about the existence of primes in any of these arithmetic progressions.

Dirichlet's theorem on primes in arithmetic progressions was first published in German in 1837 (see [**D.1**], pp. 307–312 and pp. 313–342); a French translation was published in *Liouville's Journal*, but not included in Dirichlet's collected papers (see [**D.2**], p. 421). In this work, Dirichlet again utilizes the opportunity to clarify some points of general interest which were not commonplace at that time. Prior to his introduction of the L-series he explains the "essential difference" which "exists between two kinds of infinite series. If one considers instead of each term its absolute value, or, if it is complex, its modulus, two cases may occur. Either one may find a finite magnitude exceeding any finite sum of arbitrarily many of these absolute values or moduli, or this condition is not satisfied by any finite number however large. In the first case, the series always converges and has a unique definite sum irrespective of the order of the terms, no matter if these proceed in one dimension or if they proceed in two or more dimensions forming a so-called double series or multiple series. In the second case, the series may still be convergent, but this property as well as the sum will depend in an essential way on the order of the terms. Whenever convergence occurs for a certain order it may fail for another order, or, if this is not the case, the sum of the series may be quite a different one" ([**D.1**], p. 318).

The crucial new tools enabling Dirichlet to prove his theorem are the L-series which nowadays bear his name. In the original work these series were introduced by means of suitable primitive roots and roots of unity, which are the values of the characters. This makes the representation somewhat lengthy and technical (see e.g. [**Lan**], vol. I, p. 391 ff. or [**N.2**], p. 51 ff.). For the sake of conciseness we use the modern language of characters: By definition, a Dirichlet character $\bmod\ m$ is a homomorphism $\chi : (\mathbb{Z}/m\mathbb{Z})^\times \to S^1$, where $(\mathbb{Z}/m\mathbb{Z})^\times$ denotes the group of prime residue classes $\bmod\, m$ and S^1 the unit circle in $\mathbb{C}$. To any such χ corresponds a map (by abuse of notation likewise denoted by the same letter) $\chi : \mathbb{Z} \to \mathbb{C}$ such that
a) $\chi(n) = 0$ if and only if $(m, n) > 1$,
b) $\chi(kn) = \chi(k)\chi(n)$ for all $k, n \in \mathbb{Z}$,
c) $\chi(n) = \chi(k)$ whenever $k \equiv n \,(\bmod\, m)$,
namely, $\chi(n) := \chi(n + m\mathbb{Z})$ if $(m, n) = 1$.
The set of Dirichlet characters mod$m$ is a multiplicative group isomorphic to $(\mathbb{Z}/m\mathbb{Z})^\times$ with the so-called principal character χ_0 as neutral element. To any such χ Dirichlet associates an L-series

$$L(s, \chi) := \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} \quad (s > 1) \ ,$$

and expands it into an Euler product

$$L(s,\chi)=\prod_p (1-\chi(p)p^{-s})^{-1}\ ,$$

where the product extends over all primes p. He then defines the logarithm

$$\log L(s,\chi)=\sum_p \sum_{k=1}^{\infty}\frac{1}{k}\frac{\chi(p)^k}{p^{ks}}\quad (s>1)$$

and uses it to sift the primes in the progression $(a+km)_{k\geq 1}$ by means of a summation over all $\phi(m)$ Dirichlet characters χ mod m:

$$\begin{aligned}\frac{1}{\phi(m)}\sum_\chi \overline{\chi(a)}\log L(s,\chi) &= \sum_{\substack{k\geq 1,p\\ p^k\equiv a \ (\mathrm{mod}\ m)}}\frac{1}{kp^{ks}}\\ &= \sum_{p\equiv a\ (\mathrm{mod}\ m)}\frac{1}{p^s}+R(s)\ .\end{aligned}\tag{1}$$

Here, $R(s)$ is the contribution of the terms with $k\geq 2$ which converges absolutely for $s>\frac{1}{2}$. For $\chi\neq\chi_0$ the series $L(s,\chi)$ even converges for $s>0$ and is continuous in s. Dirichlet's great discovery now is that

$$L(1,\chi)\neq 0\quad \text{for } \chi\neq\chi_0\ .\tag{2}$$

Combining this with the simple observation that $L(s,\chi_0)\to\infty$ as $s\to 1+0$, formula (1) yields

$$\sum_{p\equiv a \bmod m}\frac{1}{p^s}\longrightarrow\infty\quad \text{for } s\to 1+0$$

which gives the desired result. To be precise, in his 1837 paper Dirichlet proved (2) only for prime numbers m, but he pointed out that in the original draft of his paper he also proved (2) for arbitrary natural numbers m by means of "indirect and rather complicated considerations. Later I convinced myself that the same aim may be achieved by a different method in a much shorter way" ([**D.1**], p. 342). By this he means his class number formula which makes the non-vanishing of $L(1,\chi)$ obvious (see section C).

Dirichlet's theorem on primes in arithmetic progressions holds analogously for $\mathbb{Z}[i]$ instead of $\mathbb{Z}$. This was shown by Dirichlet himself in another paper in 1841 ([**D.1**], pp. 503–508 and pp. 509–532).

C. Dirichlet's Class Number Formula. On September 10, 1838, C.G.J. Jacobi wrote to his brother Moritz Hermann Jacobi (1801–1874), a renowned physicist in St. Petersburg, with unreserved admiration: "Applying Fourier series to number theory, Dirichlet has recently found results touching the utmost of human acumen" ([**Ah.2**], p. 47). This remark goes back to a letter of Dirichlet's to Jacobi on his research on the determination of the class number of binary quadratic forms with fixed determinant. Dirichlet first sketched his results on this topic and on the mean value of certain arithmetic functions in 1838 in an article in Crelle's Journal ([**D.1**], pp. 357–374) and elaborated on the matter in full detail in a very long memoir of 1839–1840, likewise in Crelle's Journal ([**D.1**], pp. 411–496; [**D.3**]).

Following Gauß, Dirichlet considered quadratic forms

$$ax^2 + 2bxy + cy^2$$

with even middle coefficient $2b$. This entails a large number of cases such that the class number formula finally appears in 8 different versions, 4 for positive and 4 for negative determinants. Later on Kronecker found out that the matter can be dealt with much more concisely if one considers from the very beginning forms of the shape

$$f(x, y) := ax^2 + bxy + cy^2 \ . \tag{3}$$

He published only a brief outline of the necessary modifications in the framework of his investigations on elliptic functions ([**Kr**], pp. 371–375); an exposition of book-length was subsequently given by de Seguier ([**Se**]).

For simplicity, we follow Kronecker's approach and consider quadratic forms of the type (3) with integral coefficients a, b, c and discriminant $D = b^2 - 4ac$ assuming that D is not the square of an integer. The crucial question is whether or not an integer n can be represented by the form (3) by attributing suitable integral values to x, y. This question admits no simple answer as long as we consider an individual form f.

The substitution

$$\begin{pmatrix} x \\ y \end{pmatrix} \longmapsto \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \text{ with } \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

transforms f into a so-called *(properly) equivalent* form

$$f'(x, y) = a'x^2 + b'xy + c'y^2$$

which evidently has the same discriminant and represents the same integers. Hence the problem of representation needs to be solved only for a representative system of the *finitely many* equivalence classes of binary forms of fixed discriminant D. Associated with each form f is its group of *automorphs* containing all matrices $\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ transforming f into itself. The really interesting quantity now is the number $R(n, f)$ of representations of n by f which are inequivalent with respect to the natural action of the group of automorphs. Then $R(n, f)$ turns out to be finite, but still there is no simple formula for this quantity.

Define now f to be *primitive* if $(a, b, c) = 1$. Forms equivalent to primitive ones are primitive. Denote by $f_1, \ldots, f_h$ a representative system of primitive binary quadratic forms of discriminant D, where $h = h(D)$ is called the *class number*. For $D < 0$ we tacitly assume that $f_1, \ldots, f_h$ are positive definite. Moreover we assume that D is a *fundamental discriminant*, that is, D is an integer satisfying either

(i) $D \equiv 1 \,(\mathrm{mod}\, 4), D$ square-free, or
(ii) $D \equiv 0 \,(\mathrm{mod}\, 4), \frac{D}{4} \equiv 2$ or $3 \,(\mathrm{mod}\, 4), \frac{D}{4}$ square-free.

Then there is the simple formula

$$\sum_{j=1}^{h} R(n, f_j) = \sum_{m \mid n} \left(\frac{D}{m}\right) \quad (n \neq 0) \ ,$$

where $\left(\frac{D}{\cdot}\right)$ is the so-called *Kronecker symbol*, an extension of the familiar Legendre symbol ([**Z**], p. 38). The law of quadratic reciprocity implies that $n \mapsto \left(\frac{D}{n}\right)$ is a so-called primitive Dirichlet character mod $|D|$. It is known that any primitive real Dirichlet character is one of the characters $\left(\frac{D}{\cdot}\right)$ for some fundamental discriminant D. In terms of generating functions the last sum formula means, supposing that $D < 0$,

$$\sum_{j=1}^{h} \sum_{(x,y)\neq(0,0)} (f_j(x,y))^{-s} = w\zeta(s)L\left(s, \left(\frac{D}{\cdot}\right)\right)$$

with $w = 2, 4$ or 6 as $D < -4, D = -4$ or $D = -3$, respectively. Using geometric considerations, Dirichlet deduces by a limiting process the first of his class number formulae

$$h(D) = \begin{cases} \dfrac{w\sqrt{|D|}}{2\pi} L\left(1, \left(\dfrac{D}{\cdot}\right)\right) & \text{if} \quad D < 0\,, \\ \dfrac{\sqrt{D}}{\log \varepsilon_0} L\left(1, \left(\dfrac{D}{\cdot}\right)\right) & \text{if} \quad D > 0\,. \end{cases} \tag{4}$$

In the second formula, $\varepsilon_0 = \frac{1}{2}(t_0+u_0\sqrt{D})$ denotes the fundamental solution of Pell's equation $t^2 - Du^2 = 4$ (with $t_0, u_0 > 0$ minimal). The case $D > 0$ is decidedly more difficult than the case $D < 0$ because of the more difficult description of the (infinite) group of automorphs in terms of the solutions of Pell's equation. Formula (4) continues to hold even if D is a general discriminant ([**Z**], p. 73 f.). The class number being positive and finite, Dirichlet was able to conclude the non-vanishing of $L(1, \chi)$ (in the crucial case of a real character) mentioned above.

Using Gauß sums Dirichlet was moreover able to compute the values of the L-series in (4) in a simple closed form. This yields

$$h(D) = \begin{cases} -\dfrac{w}{2|D|} \displaystyle\sum_{n=1}^{|D|-1} \left(\frac{D}{n}\right) n & \text{for} \quad D < 0\,, \\ -\dfrac{1}{\log \varepsilon_0} \displaystyle\sum_{n=1}^{D-1} \left(\frac{D}{n}\right) \log \sin \frac{\pi n}{D} & \text{for} \quad D > 0\,, \end{cases}$$

where D again is a fundamental discriminant.

Kronecker's version of the theory of binary quadratic forms has the great advantage of laying the bridge to the theory of quadratic fields: Whenever D is a fundamental discriminant, the classes of binary quadratic forms of discriminant D correspond bijectively to the equivalence classes (in the narrow sense) of ideals in $\mathbb{Q}(\sqrt{D})$. Hence Dirichlet's class number formula may be understood as a formula for the ideal class number of $\mathbb{Q}(\sqrt{D})$, and the gate to the class number formula for arbitrary number fields opens up.

Special cases of Dirichlet's class number formula were already observed by Jacobi in 1832 ([**J.1**], pp. 240–244 and pp. 260–262). Jacobi considered the forms $x^2 + py^2$, where $p \equiv 3 \,(\mathrm{mod}\, 4)$ is a prime number, and computing both sides of the class number formula, he stated the coincidence for $p = 7, \ldots, 103$ and noted that $p = 3$ is an exceptional case. Only after Gauß' death did it become known from his papers that he had known the class number formula already for some time. Gauß' notes are published in [**G.1**], pp. 269–291 with commentaries by Dedekind (ibid., pp. 292–303); see also Bachmann's report [**Ba.3**], pp. 51–53. In a letter to Dirichlet of November 2, 1838, Gauß deeply regretted that unfortunate circumstances had not allowed him to elaborate on his theory of class numbers of quadratic forms which he possessed as early as 1801 ([**Bi.9**], p. 165).

In another great memoir ([**D.1**], pp. 533–618), Dirichlet extends the theory of quadratic forms and his class number formula to the ring of Gaussian integers $\mathbb{Z}[i]$. He draws attention to the fact that in this case the formula for the class number depends on the division of the lemniscate in the same way as it depends on the division of the circle in the case of rational integral forms with positive determinant (i.e., with negative discriminant; see [**D.1**], pp. 538, 613, 621). Moreover, he promised that the details were to appear in the second part of his memoir, which however never came out.

Comparing the class numbers in the complex and the real domains Dirichlet concluded that

$$H(D) = \xi h(D)h(-D)$$

where D is a rational integral non-square determinant (in Dirichlet's notation of quadratic forms), $H(D)$ is the complex class number, and $h(D), h(-D)$ are the real ones. The constant ξ equals 2 whenever Pell's equation $t^2 - Du^2 = -1$ admits a solution in rational integers, and $\xi = 1$ otherwise. For Dirichlet, "this result ... is one of the most beautiful theorems on complex integers and all the more surprising since in the theory of rational integers there seems to be no connection between forms of opposite determinants" ([**D.1**], p. 508 and p. 618). This result of Dirichlet's has been the starting point of vast extensions (see e.g. [**Ba.2**], [**H**], [**He**], No. 8, [**K.4**], [**MC**], [**Si**], [**Wei**]).

D. Dirichlet's Unit Theorem. An algebraic integer is, by definition, a zero of a monic polynomial with integral coefficients. This concept was introduced by Dirichlet in a letter to Liouville ([**D.1**], pp. 619–623), but his notion of what Hilbert later called the ring of algebraic integers in a number field remained somewhat imperfect, since for an algebraic integer ϑ he considered only the set $\mathbb{Z}[\vartheta]$ as the ring of integers of $\mathbb{Q}(\vartheta)$. Notwithstanding this minor imperfection, he succeeded in determining the structure of the unit group of this ring in his poineering memoir *Zur Theorie der complexen Einheiten* (On the theory of complex units, [**D.1**], pp. 639–644). His somewhat sketchy account was later carried out in detail by his student Bachmann in the latter's *Habilitationsschrift* in Breslau ([**Ba.1**]; see also [**Ba.2**]).

In the more familiar modern notation, the unit theorem describes the structure of the group of units as follows: Let K be an algebraic number field with r_1 real and $2r_2$ complex (non-real) embeddings and ring of integers $\mathfrak{o}_K$. Then the group of units of $\mathfrak{o}_K$ is equal to the direct product of the (finite cyclic) group $E(K)$ of roots of unity contained in K and a free abelian group of rank $r := r_1 + r_2 - 1$. This means: There exist r "fundamental units" $\eta_1, \ldots, \eta_r$ and a primitive d-th root of unity ζ ($d = |E(K)|$) such that every unit $\varepsilon \in \mathfrak{o}_K$ is obtained precisely once in the form

$$\varepsilon = \zeta^k \eta_1^{n_1} \cdot \ldots \cdot \eta_r^{n_r}$$

with $0 \le k \le d-1, n_1, \ldots, n_r \in \mathbb{Z}$. This result is one of the basic pillars of algebraic number theory.

In Dirichlet's approach the ring $\mathbb{Z}[\vartheta]$ is of finite index in the ring of all algebraic integers (in the modern sense), and the same holds for the corresponding groups of units. Hence the rank r does not depend on the choice of the generating element ϑ of the field $K = \mathbb{Q}(\vartheta)$. (Note that $\mathbb{Z}[\vartheta]$ depends on that choice.)

An important special case of the unit theorem, namely the case $\vartheta = \sqrt{D}$ ($D > 1$ a square-free integer), was known before. In this case the determination of the units comes down to Pell's equation, and one first encounters the phenomenon that all units are obtained by forming all integral powers of a fundamental unit and multiplying these by ± 1. Dirichlet himself extended this result to the case when ϑ satisfies a cubic equation ([**D.1**], pp. 625–632) before he dealt with the general case.

According to C.G.J. Jacobi the unit theorem is "one of the most important, but one of the thorniest of the science of number theory" ([**J.3**], p. 312, footnote, [**N.1**], p. 123, [**Sm**], p. 99). Kummer remarks that Dirichlet found the idea of proof when listening to the Easter Music in the Sistine Chapel during his Italian journey (1843–1845; see [**D.2**], p. 343).

A special feature of Dirichlet's work is his admirable combination of surprisingly simple observations with penetrating thought which led him to deep results. A striking example of such a simple observation is the so-called *Dirichlet box principle* (also called *drawer principle* or *pigeon-hole principle*), which states that whenever more than n objects are distributed in n boxes, then there will be at least one box containing two objects. Dirichlet gave an amazing application of this most obvious principle in a brief paper ([**D.1**], pp. 633–638), in which he proves the following generalization of a well-known theorem on rational approximation of irrational numbers: *Suppose that the real numbers* $\alpha_1, \ldots, \alpha_m$ *are such that* $1, \alpha_1, \ldots, \alpha_m$ *are linearly independent over* $\mathbb{Q}$. *Then there exist infinitely many integral* $(m+1)$*-tuples* $(x_0, x_1, \ldots, x_m)$ *such that* $(x_1, \ldots, x_m) \neq (0, \ldots, 0)$ *and*

$$|x_0 + x_1\alpha_1 + \ldots + x_m\alpha_m| < (\max_{1 \le j \le m} |x_j|)^{-m} .$$

Dirichlet's proof: Let n be a natural number, and let $x_1, \ldots, x_m$ independently assume all $2n+1$ integral values $-n, -n+1, \ldots, 0, \ldots, n-1, n$. This gives $(2n+1)^m$ fractional parts $\{x_1\alpha_1 + \ldots + x_m\alpha_m\}$ in the half open unit interval $[0, 1[$. Divide $[0, 1[$ into $(2n)^m$ half-open subintervals of equal length $(2n)^{-m}$. Then two of the aforementioned points belong to the same subinterval. Forming the difference of the corresponding $\mathbb{Z}$-linear combinations, one obtains integers $x_0, x_1, \ldots, x_m$, such that $x_1, \ldots, x_m$ are of absolute value at most $2n$ and not all zero and such that

$$|x_0 + x_1\alpha_1 + \ldots + x_m\alpha_m| < (2n)^{-m} .$$

Since n was arbitrary, the assertion follows. As Dirichlet points out, the approximation theorem quoted above is crucial in the proof of the unit theorem because it implies that r independent units can be found. The easier part of the theorem, namely that the free rank of the group of units is at most r, is considered obvious by Dirichlet.

E. Dirichlet's Principle. We pass over Dirichlet's valuable work on definite integrals and on mathematical physics in silence ([**Bu**]), but cannot neglect mentioning the so-called *Dirichlet Principle*, since it played a very important role in the history of analysis (see [**Mo**]). *Dirichlet's Problem* concerns the following problem: Given a (say, bounded) domain $G \subset \mathbb{R}^3$ and a continuous real-valued function f on the (say, smooth) boundary ∂G of G, find a real-valued continuous function u, defined on the closure $\overline{G}$ of G, such that u is twice continuously differentiable on G and satisfies Laplace's equation

$$\Delta u = 0 \quad \text{on } G$$

and such that $u \,|\, \partial G = f$. Dirichlet's Principle gives a deceptively simple method of how to solve this problem: Find a function $v : \overline{G} \to \mathbb{R}$, continuous on $\overline{G}$ and continuously differentiable on G, such that $v \,|\, \partial G = f$ and such that Dirichlet's integral

$$\int_G (v_x^2 + v_y^2 + v_z^2)\, dx\, dy\, dz$$

assumes its minimum value. Then v solves the problem.

Dirichlet's name was attributed to this principle by Riemann in his epoch-making memoir on Abelian functions (1857), although Riemann was well aware of the fact that the method already had been used by Gauß in 1839. Likewise, W. Thomson (Lord Kelvin of Largs, 1824–1907) made use of this principle in 1847 as was also known to Riemann. Nevertheless he named the principle after Dirichlet, "because Professor Dirichlet informed me that he had been using this method in his lectures (since the beginning of the 1840's (if I'm not mistaken))" ([**EU**], p. 278).

Riemann used the two-dimensional version of Dirichlet's Principle in a most liberal way. He applied it not only to plane domains but also to quite arbitrary domains on Riemann surfaces. He did not restrict to sufficiently smooth functions, but admitted singularities, e.g. logarithmic singularities, in order to prove his existence theorems for functions and differentials on Riemann surfaces. As Riemann already pointed out in his doctoral thesis (1851), this method "opens the way to investigate certain functions of a complex variable independently of an [analytic] expression for them", that is, to give existence proofs for certain functions without giving an analytic expression for them ([**EU**], p. 283).

From today's point of view the naïve use of Dirichlet's principle is open to serious doubt, since it is by no means clear that there exists a function v satisfying the boundary condition for which the infimum value of Dirichlet's integral is actually attained. This led to serious criticism of the method in the second half of the nineteenth century discrediting the principle. It must have been a great relief to many mathematicians when D. Hilbert (1862–1943) around the turn of the 20th century proved a precise version of Dirichlet's Principle which was sufficiently general to allow for the usual function-theoretic applications.

There are only a few brief notes on the calculus of probability, the theory of errors and the method of least squares in Dirichlet's collected works. However, a considerable number of unpublished sources on these subjects have survived which have been evaluated in [**F**].

9. Friendship with Jacobi

Dirichlet and C.G.J. Jacobi got to know each other in 1829, soon after Dirichlet's move to Berlin, during a trip to Halle, and from there jointly with W. Weber to Thuringia. At that time Jacobi held a professorship in Königsberg, but he used to visit his family in Potsdam near Berlin, and he and Dirichlet made good use of these occasions to see each other and exchange views on mathematical matters. During their lives they held each other in highest esteem, although their characters were quite different. Jacobi was extroverted, vivid, witty, sometimes quite blunt; Dirichlet was more introvert, reserved, refined, and charming. In the preface to his tables *Canon arithmeticus* of 1839, Jacobi thanks Dirichlet for his help. He might have extended his thanks to the Dirichlet family. To check the half a million numbers, also Dirichlet's wife and mother, who after the death of her husband in 1837 lived in Dirichlet's house, helped with the time-consuming computations (see [**Ah.2**], p. 57).

When Jacobi fell severely ill with *diabetes mellitus*, Dirichlet travelled to Königsberg for 16 days, assisted his friend, and "developed an eagerness never seen at him before", as Jacobi wrote to his brother Moritz Hermann ([**Ah.2**], p. 99). Dirichlet got a history of illness from Jacobi's physician, showed it to the personal physician of King Friedrich Wilhelm IV, who agreed to the treatment, and recommended a stay in the milder climate of Italy during wintertime for further recovery. The matter was immediately brought to the King's attention by the indefatigable A. von Humboldt, and His Majesty on the spot granted a generous support of 2000 talers towards the travel expenses.

Jacobi was happy to have his doctoral student Borchardt, who just had passed his examination, as a companion, and even happier to learn that Dirichlet with his family also would spend the entire winter in Italy to stengthen the nerves of his wife. Steiner, too, had health problems, and also travelled to Italy. They were accompanied by the Swiss teacher L. Schläfli (1814–1895), who was a genius in languages and helped as an interpreter and in return got mathematical instruction from Dirichlet and Steiner, so that he later became a renowned mathematician. Noteworthy events and encounters during the travel are recorded in the letters in [**Ah.2**] and [**H.1**]. A special highlight was the audience of Dirichlet and Jacobi with Pope Gregory XVI on December 28, 1843 (see [**Koe**], p. 317 f.).

In June 1844, Jacobi returned to Germany and got the "transfer to the Academy of Sciences in Berlin with a salary of 3000 talers and the permission, without obligation, to give lectures at the university" ([**P**], p. 27). Dirichlet had to apply twice for a prolongation of his leave because of serious illness. Jacobi proved to be a real friend and took Dirichlet's place at the Military School and at the university and thus helped him to avoid heavy financial losses. In spring 1845 Dirichlet returned to Berlin. His family could follow him only a few months later under somewhat dramatic circumstances with the help of the Hensel family, since in February 1845 Dirichlet's daughter Flora was born in Florence.

In the following years, the contacts between Dirichlet and Jacobi became even closer; they met each other virtually every day. Dirichlet's mathematical rigour was legendary already among his contemporaries. When in 1846 he received a most prestigious call from the University of Heidelberg, Jacobi furnished A. von Humboldt with arguments by means of which the minister should be prompted to improve upon Dirichlet's conditions in order to keep him in Berlin. Jacobi explained (see [**P**], p. 99): "In science, Dirichlet has two features which constitute his speciality. He alone, not myself, not Cauchy, not Gauß knows what a perfectly rigorous mathematical proof is. When Gauß says he has *proved* something, it is highly probable to me, when Cauchy says it, one may bet as much pro as con, when Dirichlet says it, it is *certain*; *I* prefer not at all to go into such subtleties. *Second*, Dirichlet has created a *new branch* of mathematics, the *application of the infinite series, which Fourier introduced into the theory of heat, to the investigation of the properties of the prime numbers...* Dirichlet has preferred to occupy himself mainly with such topics, which offer the greatest difficulties ..." In spite of several increases, Dirichlet was still not yet paid the regular salary of a full professor in 1846; his annual payment was 800 talers plus his income from the Military School. After the call to Heidelberg the sum was increasesd by 700 talers to 1500 talers per year, and Dirichlet stayed in Berlin — with the teaching load at the Military School unchanged.

10. Friendship with Liouville

Joseph Liouville (1809–1882) was one of the leading French mathematicians of his time. He began his studies at the *École Polytechnique* when Dirichlet was about to leave Paris and so they had no opportunity to become acquainted with each other during their student days. In 1833 Liouville began to submit his papers to Crelle. This brought him into contact with mathematics in Germany and made him aware of the insufficient publication facilities in his native country. Hence, in 1835, he decided to create a new French mathematical journal, the *Journal de Mathématiques Pures et Appliquées*, in short, *Liouville's Journal*. At that time, he was only a 26-year-old *répétiteur* (coach). The journal proved to be a lasting success. Liouville directed it single-handedly for almost 40 years — the journal enjoys a high reputation to this day.

In summer 1839 Dirichlet was on vacation in Paris, and he and Liouville were invited for dinner by Cauchy. It was probably on this occasion that they made each other's acquaintance, which soon developed into a devoted friendship. After his return to Berlin, Dirichlet saw to it that Liouville was elected a corresponding member[6] of the Academy of Sciences in Berlin, and he sent a letter to Liouville suggesting that they should enter into a scientific correspondence ([**Lü**], p. 59 ff.). Liouville willingly agreed; part of the correspondence was published later ([**T**]). Moreover, during the following years, Liouville saw to it that French translations of many of Dirichlet's papers were published in his journal. Contrary to Kronecker's initial plans, not all of these translations were printed in [**D.1**], [**D.2**]; the missing items are listed in [**D.2**], pp. 421–422.

The friendship of the two men was deepened and extended to the families during Dirichlet's visits to Liouville's home in Toul in fall of 1853 and in March 1856, when Dirichlet utilized the opportunity to attend a meeting of the French Academy of

[6]He became an external member in 1876.

Sciences in the capacity of a foreign member to which he had been elected in 1854. On the occasion of the second visit, Mme Liouville bought a dress for Mrs Dirichlet, *"la fameuse robe qui fait toujours l'admiration de la société de Gœttingue"*, as Dirichlet wrote in his letter of thanks ([**T**], *Suite*, p. 52).

Mme de Blignières, a daughter of Liouville, remembered an amusing story about the long discussions between Dirichlet and her father ([**T**], p. 47, footnote): Both of them had a lot of say; how was it possible to limit the speaking time fairly? Liouville could not bear lamps, he lighted his room by wax and tallow candles. To measure the time of the speakers, they returned to an old method that probably can be traced back at least to medieval times: They pinned a certain number of pins into one of the candles at even distances. Between two pins the speaker had the privilege not to be interrupted. When the last pin fell, the two geometers went to bed.

11. Vicissitudes of Life

After the deaths of Abraham Mendelssohn Bartholdy in 1835 and his wife Lea in 1842, the Mendelssohn house was first conducted as before by Fanny Hensel, with Sunday music and close contacts among the families of the siblings, with friends and acquaintances. Then came the catastrophic year 1847: Fanny died completely unexpectedly of a stroke, and her brother Felix, deeply shocked by her premature death, died shortly thereafter also of a stroke. Sebastian Hensel, the under-age son of Fanny and Wilhelm Hensel, was adopted by the Dirichlet family. To him we owe interesting first-hand descriptions of the Mendelssohn and Dirichlet families ([**H.1**], [**H.2**]).

Then came the March Revolution of 1848 with its deep political impact. King Friedrich Wilhelm IV proved to be unable to handle the situation, the army was withdrawn, and a civic guard organized the protection of public institutions. Riemann, at that time a student in Berlin, stood guard in front of the Royal Castle of Berlin. Dirichlet with an old rifle guarded the palace of the Prince of Prussia, a brother to the King, who had fled (in fear of the guillotine); he later succeeded the King, when the latter's mental disease worsened, and ultimately became the German Kaiser Wilhelm I in 1871.

After the revolution the reactionary circles took the revolutionaries and other people with a liberal way of thinking severely to task: Jacobi suffered massive pressure, the conservative press published a list of liberal professors: "The red contingent of the staff is constituted by the names ..." (there follow 17 names, including Dirichlet, Jacobi, Virchow; see [**Ah.2**], p. 219). The Dirichlet family not only had a liberal way of thinking, they also acted accordingly. In 1850 Rebecka Dirichlet helped the revolutionary Carl Schurz, who had come incognito, to free the revolutionary G. Kinkel from jail in Spandau ([**Lac**], pp. 244–245). Schurz and Kinkel escaped to England; Schurz later became a leading politician in the USA.

The general feeling at the Military School changed considerably. Immediately after the revolution the school was closed down for some time, causing a considerable loss in income for Dirichlet. When it was reopened, a reactionary spirit had spread among the officers, and Dirichlet no longer felt at ease there.

A highlight in those strained times was the participation of Dirichlet and Jacobi in the celebration of the fiftieth anniversary jubilee of the doctorate of Gauß in Göttingen in 1849. Jacobi gave an interesting account of this event in a letter to his brother ([**Ah.2**], pp. 227–228); for a general account see [**Du**], pp. 275–279. Gauß was in an elated mood at that festivity and he was about to light his pipe with a pipe-light of the original manuscript of his *Disquisitiones arithmeticae*. Dirichlet was horrified, rescued the paper, and treasured it for the rest of his life. After his death the sheet was found among his papers.

The year 1851 again proved to be a catastrophic one: Jacobi died quite unexpectedly of smallpox the very same day, that little Felix, a son of Felix Mendelssohn Bartholdy, was buried. The terrible shock of these events can be felt from Rebecka's letter to Sebastian Hensel ([**H.2**], pp. 133–134). On July 1, 1952, Dirichlet gave a most moving memorial speech to the Academy of Sciences in Berlin in honour of his great colleague and intimate friend Carl Gustav Jacob Jacobi ([**D.5**]).

12. Dirichlet in Göttingen

When Gauß died on February 23, 1855, the University of Göttingen unanimously wanted to win Dirichlet as his successor. It is said that Dirichlet would have stayed in Berlin, if His Majesty would not want him to leave, if his salary would be raised and if he would be exempted from his teaching duties at the Military School ([**Bi.7**], p. 121, footnote 3). Moreover it is said that Dirichlet had declared his willingness to accept the call to Göttingen and that he did not want to revise his decision thereafter. Göttingen acted faster and more efficiently than the slow bureaucracy in Berlin. The course of events is recorded with some regret by Rebecka Dirichlet in a letter of April 4, 1855, to Sebastian Hensel ([**H.2**], p. 187): "Historically recorded, ... the little Weber came from Göttingen as an extraordinarily authorized person to conclude the matter. Paul [Mendelssohn Barthody, Rebecka's brother] and [G.] Magnus [1802–1870, physicist in Berlin] strongly advised that Dirichlet should make use of the call in the manner of professors, since nobody dared to approach the minister before the call was available in black and white; however, Dirichlet did not want this, and I could not persuade him with good conscience to do so."

In a very short time, Rebecka rented a flat in Göttingen, Gotmarstraße 1, part of a large house which still exists, and the Dirichlet family moved with their two younger children, Ernst and Flora, to Göttingen. Rebecka could write to Sebastian Hensel: "Dirichlet is contentissimo" ([**H.2**], p. 189). One year later, the Dirichlet family bought the house in Mühlenstraße 1, which still exists and bears a memorial tablet. The house and the garden (again with a pavillon) are described in the diaries of the Secret Legation Councillor K.A. Varnhagen von Ense (1785–1858), a friend of the Dirichlets', who visited them in Göttingen. Rebecka tried to renew the old glory of the Mendelssohn house with big parties of up to 60–70 persons, plenty of music with the outstanding violinist Joseph Joachim and the renowned pianist Clara Schumann performing — and with Dedekind playing waltzes on the piano for dancing.

Dirichlet rapidly felt very much at home in Göttingen and got into fruitful contact with the younger generation, notably with R. Dedekind and B. Riemann (at that time assistant to W. Weber), who both had achieved their doctor's degree and *Habilitation* under Gauß. They both were deeply grateful to Dirichlet for the stimulance and assistance he gave them. This can be deduced from several of Dedekind's letters to members of his family (e.g. [**Sch**], p. 35): "Most useful for me is my contact with Dirichlet almost every day from whom I really start learning properly; he is always constantly kind to me, tells me frankly which gaps I have to fill in, and immediately gives me instructions and the means to do so." And in another letter (ibid., p. 37) we read the almost prophetic words: "Moreover, I have much contact with my excellent colleague Riemann, who is beyond doubt after or even with Dirichlet the most profound of the living mathematicians and will soon be recognized as such, when his modesty allows him to publish certain things, which, however, temporarily will be understandable only to few." Comparing, e.g. Dedekind's doctoral thesis with his later pioneering deep work one may well appreciate his remark, that Dirichlet "made a new human being" of him ([**Lo**], p. 83). Dedekind attended all of Dirichlet's lectures in Göttingen, although he already was a *Privatdozent*, who at the same time gave the presumably first lectures on Galois theory in the history of mathematics. Clearly, Dedekind was the ideal editor for Dirichlet's lectures on number theory ([**D.6**]).

Riemann already had studied with Dirichlet in Berlin 1847–1849, before he returned to Göttingen to finish his thesis, a crucial part of which was based on Dirichlet's Principle. Already in 1852 Dirichlet had spent some time in Göttingen, and Riemann was happy to have an occasion to look through his thesis with him and to have an extended discussion with him on his *Habilitationsschrift* on trigonometric series in the course of which Riemann got a lot of most valuable hints. When Dirichlet was called to Göttingen, he could provide the small sum of 200 talers payment per year for Riemann which was increased to 300 talers in 1857, when Riemann was advanced to the rank of associate professor.

There can be no doubt that the first years in Göttingen were a happy time for Dirichlet. He was a highly esteemed professor, his teaching load was much less than in Berlin, leaving him more time for research, and he could gather around him a devoted circle of excellent students. Unfortunately, the results of his research of his later years have been almost completely lost. Dirichlet had a fantastic power of concentration and an excellent memory, which allowed him to work at any time and any place without pen and paper. Only when a work was fully carried out in his mind, did he most carefully write it up for publication. Unfortunately, fate did not allow him to write up the last fruits of his thought, about which we have only little knowledge (see [**D.2**], p. 343 f. and p. 420).

When the lectures of the summer semester of the year 1858 had come to an end, Dirichlet made a journey to Montreux (Switzerland) in order to prepare a memorial speech on Gauß, to be held at the Göttingen Society of Sciences, and to write up a work on hydrodynamics. (At Dirichlet's request, the latter work was prepared for publication by Dedekind later; see [**D.2**], pp. 263–301.) At Montreux he suffered a heart attack and returned to Göttingen mortally ill. Thanks to good care he seemed to recover. Then, on December 1, 1858, Rebecka died all of a sudden and completely unexpectedly of a stroke. Everybody suspected that Dirichlet would not for long survive this turn of fate. Sebastian Hensel visited his uncle for the last time on Christmas 1858 and wrote down his feelings later ([**H.2**], p. 311 f.): "Dirichlet's condition was hopeless, he knew precisely how things were going for him, but he faced death calmly, which was edifying to observe. And now the poor Grandmother! Her misery ... to lose also her last surviving child, ... was terrible to observe. It was obvious that Flora, the only child still in the house, could not stay there. I took her to Prussia ..." Dirichlet died on May 5, 1859, one day earlier than his faithful friend Alexander von Humboldt, who died on May 6, 1859, in his 90th year of life. The tomb of Rebecka and Gustav Lejeune Dirichlet in Göttingen still exists and will soon be in good condition again, when the 2006 restorative work is finished. Dirichlet's mother survived her son for 10 more years and died only in her 100th year of age. Wilhelm Weber took over the guardianship of Dirichlet's under-age children ([**Web**], p. 98).

The Academy of Sciences in Berlin honoured Dirichlet by a formal memorial speech delivered by Kummer on July 5, 1860 ([**Ku**]). Moreover, the Academy ordered the edition of Dirichlet's collected works. The first volume was edited by L. Kronecker and appeared in 1889 ([**D.1**]). After Kronecker's death, the editing of the second volume was completed by L. Fuchs and it appeared in 1897 ([**D.2**]).

Conclusion

Henry John Stephen Smith (1826–1883), Dublin-born Savilian Professor of Geometry in the University of Oxford, was known among his contemporaries as the most distinguished scholar of his day at Oxford. In 1858 Smith started to write a report on the theory of numbers beginning with the investigations of P. de Fermat and ending with the then (1865) latest results of Kummer, Kronecker, and Hurwitz. The six parts of Smith's report appeared over the period of 1859 to 1865 and are very instructive to read today ([**Sm**]). When he prepared the first part of his report, Smith got the sad news of Dirichlet's death, and he could not help adding the following footnote to his text ([**Sm**], p. 72) appreciating Dirichlet's great service to number theory: "The death of this eminent geometer in the present year (May 5, 1859) is an irreparable loss to the science of arithmetic. His original investigations have probably contributed more to its advancement than those of any other writer since the time of Gauss, if, at least, we estimate results rather by their importance than by their number. He has also applied himself (in several of his memoirs) to give an elementary character to arithmetical theories which, as they appear in the work of Gauss, are tedious and obscure; and he has done much to *popularize* the theory of numbers among mathematicians — a service which is impossible to appreciate too highly."

Acknowledgement. The author thanks Prof. Dr. S.J. Patterson (Göttingen) for his improvements on the text.

References

[A] Abel, N.H.: Mémorial publié à l'occasion du centenaire de sa naissance. Kristiania: Dybwad, Paris: Gauthier-Villars, London: Williams & Norgate, Leipzig: Teubner, 1902

[Ah.1] Ahrens, W.: Peter Gustav Lejeune-Dirichlet. Math.-naturwiss. Blätter **2**, 36–39 and 51–55 (1905)

[Ah.2] Ahrens, W. (ed.): Briefwechsel zwischen C.G.J. Jacobi und M.H. Jacobi. Leipzig: Teubner, 1907

[Ba.1] Bachmann, P.: De unitatum complexarum theoria. Habilitationsschrift. Breslau, 1864

[Ba.2] Bachmann, P.: Zur Theorie der complexen Zahlen. J. Reine Angew. Math. **67**, 200–204 (1867)

[Ba.3] Bachmann, P.: Über Gauß' zahlentheoretische Arbeiten. Materialien für eine wissenschaftliche Biographie von Gauß, ed. by F. Klein and M. Brendel, Heft 1. Leipzig: Teubner, 1911

[Bi.1] Biermann, K.-R.: Johann Peter Gustav Lejeune Dirichlet. Dokumente für sein Leben und Wirken. (Abh. Dt. Akad. Wiss. Berlin, Kl. Math., Phys. Techn. 1959, No. 2) Berlin: Akademie-Verlag, 1959

[Bi.2] Biermann, K.-R.: Über die Förderung deutscher Mathematiker durch Alexander von Humboldt. In: Alexander von Humboldt. Gedenkschrift zur 100. Wiederkehr seines Todestages. Berlin: Akademie-Verlag, 1959, pp. 83–159

[Bi.3] Biermann, K.-R.: Dirichletiana. Mon.-Ber. Dt. Akad. Wiss. Berlin **2**, 386–389 (1960)

[Bi.4] Biermann, K.-R.: Vorschläge zur Wahl von Mathematikern in die Berliner Akademie. (Abh. Dt. Akad. Wiss. Berlin, Kl. Math., Phys., Techn. 1960, No. 3) Berlin: Akademie-Verlag, 1960

[Bi.5] Biermann, K.-R.: Alexander von Humboldts wissenschaftsorganisatorisches Programm bei der Übersiedlung nach Berlin. Mon.-Ber. Dt. Akad. Wiss. Berlin **10**, 142–147 (1968)

[Bi.6] Biermann, K.-R. (ed.): Briefwechsel zwischen Alexander von Humboldt und Carl Friedrich Gauß. Berlin: Akademie-Verlag, 1977

[Bi.7] Biermann, K.-R. (ed.): Briefwechsel zwischen Alexander von Humboldt und Peter Gustav Lejeune Dirichlet. Berlin: Akademie-Verlag, 1982

[Bi.8] Biermann, K.-R.: Die Mathematik und ihre Dozenten an der Berliner Universität, 1810–1933. Berlin: Akademie-Verlag, 1988

[Bi.9] Biermann, K.-R. (ed.): Carl Friedrich Gauß. Der "Fürst der Mathematiker" in Briefen und Gesprächen. München: C.H. Beck, 1990

[Bu] Butzer, P.: Dirichlet and his role in the founding of mathematical physics. Arch. Int. Hist. Sci. **37**, 49–82 (1987)

[BuJZ] Butzer, P.L., Jansen, M., Zilles, H.: Johann Peter Gustav Lejeune Dirichlet (1805–1859), Genealogie und Werdegang. Dürener Geschichtsblätter, Mitteilungen des Dürener Geschichtsvereins e.V., Nr. **71**, Düren, 1982, pp. 31–56

[D.1] Dirichlet, P.G. Lejeune: Werke, vol. 1. Ed. by L. Kronecker. Berlin: Reimer, 1889

[D.2] Dirichlet, P.G. Lejeune: Werke, vol. 2. Ed. by L. Kronecker, continued by L. Fuchs. Berlin: Reimer, 1897

[D.3] Dirichlet, P.G. Lejeune: Untersuchungen über verschiedene Anwendungen der Infinitesimalanalysis auf die Zahlentheorie. 1839–1840. (Ostwald's Klassiker der exakten Wissenschaften **91**, ed. by R. Haußner.) Leipzig: Engelmann, 1897

[D.4] Dirichlet, P.G. Lejeune: Die Darstellung ganz willkürlicher Funktionen durch Sinus- und Kosinusreihen. 1837. — Seidel, Philipp Ludwig: Note über eine Eigenschaft der Reihen, welche diskontinuierliche Funktionen darstellen. 1847. (Ostwald's Klassiker der exakten Wissenschaften **116**, ed. by H. Liebmann.) Leipzig: Engelmann, 1900

[D.5] Dirichlet, P.G. Lejeune: Gedächtnisrede auf Carl Gustav Jacob Jacobi. Abh. Kgl. Akad. Wiss. Berlin 1852, 1–27; also in J. Reine Angew. Math. **52**, 193–217 (1856); also in [**D.2**], pp. 227–252, and in C.G.J. Jacobi: Gesammelte Werke, vol. 1. (C.W. Borchardt, ed.) Berlin: Reimer, 1881, pp. 1–28. Reprinted in: Reichardt, H. (ed.): Nachrufe auf Berliner Mathematiker des 19. Jahrhunderts. C.G.J. Jacobi, P.G.L. Dirichlet, E.E. Kummer, L. Kronecker, K. Weierstraß. (Teubner-Archiv zur Mathematik **10**.) Leipzig: Teubner, 1988, pp. 7–32

[D.6] Dirichlet, P.G. Lejeune: Vorlesungen über Zahlentheorie von P.G. Lejeune Dirichlet, herausgegeben und mit Zusätzen versehen von R. Dedekind. 4th ed., improved and enlarged. Braunschweig: Vieweg, 1894

[D.7] Dirichlet, P.G. Lejeune: Vorlesungen über die Lehre von den einfachen und mehrfachen bestimmten Integralen, ed. by G. Arendt. Braunschweig: Vieweg, 1904

[Du] Dunnington, G.W.: Carl Friedrich Gauss. Titan of science. Second ed. with additional material by J. Gray and F.-E. Dohse. The Mathematical Association of America, 2004

[Ei] Eisenstein, G.: Mathematische Werke. 2 vols. New York, N.Y.: Chelsea Publ. Comp., 1975

[EU] Elstrodt, J., Ullrich, P.: A real sheet of complex Riemannian function theory: A recently discovered sketch in Riemann's own hand. Hist. Math. **26**, 268–288 (1999)

[Ey] Eytelwein, J.A.: Untersuchungen über die Bewegung des Wassers, wenn auf die Contraction, welche beim Durchgang durch verschiedene Öffnungen statt findet und auf den Widerstand, welcher die Bewegung des Wassers längs den Wänden der Behältnisse verzögert, Rücksicht genommen wird. Abh. Kgl. Preuß. Akad. Wiss., math. Kl., 1814/15, pp. 137–178 and 1818/19, pp. 9–18. French translation by G. Lejeune Dirichlet: Sur le mouvement de l'eau, en ayant égard à la contraction qui a lieu au passage par divers orifices, et à la résistance qui retarde le mouvement le long des parois des vases. Annales des Mines **11**, 417–455 plus six tables, 458–468 (1825)

[F] Fischer, H.: Dirichlet's contributions to mathematical probability theory. Hist. Math. **21**, 39–63 (1994)

[GW] Gardner, J.H., Wilson, R.J.: Thomas Archer Hirst — Mathematician Xtravagant. Amer. Math. Monthly **100**, I. 435–441, II. 531–538, III. 619–625, IV. 723–731, V. 827–834, VI. 907–915 (1993)

[G.1] Gauß, C.F.: Werke. Zweiter Band. Second Printing. Göttingen: Königliche Gesellschaft der Wissenschaften, 1876

[G.2] Gauß, C.F.: Sechs Beweise des Fundamentaltheorems über quadratische Reste. (Ostwald's Klassiker der exakten Wissenschaften **122**, ed. by E. Netto.) Leipzig: Engelmann, 1901

[Gr] Grube, F. (ed.): Vorlesungen über die im umgekehrten Verhältniss des Quadrats der Entfernung wirkenden Kräfte von P.G. Lejeune-Dirichlet. Leipzig: Teubner, 1876, 2nd ed., 1887

[H] Hasse, H.: Über die Klassenzahl abelscher Zahlkörper. Berlin etc.: Springer, 1985

[He] Hecke, E.: Mathematische Werke. 2nd ed. Göttingen: Vandenhoeck & Ruprecht, 1970

[H.1] Hensel, S.: Die Familie Mendelssohn 1729 bis 1847. 2 vols. 14th ed. Berlin: Reimer, 1911

[H.2] Hensel, S.: Ein Lebensbild aus Deutschlands Lehrjahren. Berlin: B. Behr's Verlag, 1903

[J.1] Jacobi, C.G.J.: Gesammelte Werke, vol. 6. (K. Weierstraß, ed.) Berlin: Reimer, 1891

[J.2] Jacobi, C.G.J.: Gesammelte Werke, vol. 7. (K. Weierstraß, ed.) Berlin: Reimer, 1891

[J.3] Jacobi, C.G.J. (ed.): Extraits de lettres de M. Ch. Hermite à M. Jacobi sur différents objets de la théorie des nombres. J. Reine Angew. Math. **40**, 261–315 (1850)

[K.1] Koch, H.: J.P.G. Lejeune Dirichlet zu seinem 175. Geburtstag. Mitt. Math. Ges. DDR, H. **2/4**, 153–164 (1981)

[K.2] Koch, H.: Gustav Peter Lejeune Dirichlet. In: Mathematics in Berlin, ed. by H.G.W. Begehr et al. on behalf of the Berliner Mathematische Gesellschaft. Berlin–Basel–Boston: Birkhäuser, 1998, pp. 33–39

[K.3] Koch, H.: Peter Gustav Lejeune Dirichlet (1805–1859). Zum 200. Geburtstag. Mitt. Dtsch. Math.-Verein. **13**, 144–149 (2005)

[K.4] Koch, H.: Algebraic number theory. Berlin etc.: Springer, 1997 (Originally published as Number Theory II, Vol. **62** of the Encyclopaedia of Mathematical Sciences, Berlin etc.: Springer, 1992)

[Koe] Koenigsberger, L.: Carl Gustav Jacob Jacobi. Festschrift zur Feier der hundertsten Wiederkehr seines Geburtstags. Leipzig: Teubner, 1904

[Kr] Kronecker, L.: Werke, vol. 4. (K. Hensel, ed.) Leipzig and Berlin: Teubner, 1929

[Ku] Kummer, E.E.: Gedächtnisrede auf Gustav Peter Lejeune-Dirichlet. Abh. Kgl. Akad. Wiss. Berlin 1860, 1–36 (1861); also in [**D.2**], pp. 311–344 and in Kummer, E.E.: Collected papers, vol. 2. (A. Weil, ed.) Berlin etc.: Springer, 1975, pp. 721–756. Reprinted in: Reichardt, H. (ed.): Nachrufe auf Berliner Mathematiker des 19. Jahrhunderts. C.G.J. Jacobi, P.G.L. Dirichlet, K. Weierstraß. (Teubner-Archiv zur Mathematik **10**.) Leipzig: Teubner, 1988, pp. 35–71

[Lac] Lackmann, T.: Das Glück der Mendelssohns. Geschichte einer deutschen Familie. Berlin: Aufbau-Verlag, 2005

[Lam] Lampe, E.: Dirichlet als Lehrer der Allgemeinen Kriegsschule. Naturwiss. Rundschau **21**, 482–485 (1906)

[Lan] Landau, E.: Handbuch der Lehre von der Verteilung der Primzahlen. 2 vols. Leipzig: Teubner, 1909. (Reprinted in one volume by Chelsea Publ. Comp., New York, 1953)

[Lo] Lorey, W.: Das Studium der Mathematik an den deutschen Universitäten seit Anfang des 19. Jahrhunderts. Abh. über den math. Unterricht in Deutschland, Bd. 3, H. 9, XII + 428 pp. Leipzig and Berlin: Teubner, 1916

[Lü] Lützen, J.: Joseph Liouville 1809–1882: Master of pure and applied mathematics. Berlin etc.: Springer, 1990

[MC] Meyer, C.: Die Berechnung der Klassenzahl Abelscher Körper über quadratischen Zahlkörpern. Berlin: Akademie-Verlag, 1957

[MG] Meyer, G.F.: Vorlesungen über die Theorie der bestimmten Integrale zwischen reellen Grenzen mit vorzüglicher Berücksichtigung der von P. Gustav Lejeune-Dirichlet im Sommer 1858 gehaltenen Vorträge über bestimmte Integrale. Leipzig: Teubner, 1871

[Mi] Minkowski, H.: Peter Gustav Lejeune Dirichlet und seine Bedeutung für die heutige Mathematik. Jahresber. Dtsch. Math.-Ver. **14**, 149–163 (1905). Also in: Gesammelte Abhandlungen, vol. 2, pp. 447–461. Leipzig: Teubner, 1911; reprint in one volume: New York: Chelsea, 1967

[Mo] Monna, A.F.: Dirichlet's principle. A mathematical comedy of errors and its influence on the development of analysis. Utrecht: Oosthoek, Scheltema & Holkema, 1975

[N.1] Narkiewicz, W.: Elementary and analytic theory of algebraic numbers. Warszawa: PWN – Polish Scientific Publishers, 1974

[N.2] Narkiewicz, W.: The development of prime number theory. Berlin etc.: Springer, 2000

[O.1] Wilhelm Olbers, sein Leben und seine Werke. Vol. 2: Briefwechsel zwischen Obers und Gauß, erste Abteilung. (Ed. by C. Schilling.) Berlin: Springer, 1900

[O.2] Wilhelm Olbers, sein Leben und seine Werke, Vol. 2: Briefwechsel zwischen Olbers und Gauß, zweite Abteilung. (Ed. by C. Schilling and I. Kramer.) Berlin: Springer, 1909

[P] Pieper, H.: Briefwechsel zwischen Alexander von Humboldt und C.G. Jacob Jacobi. Berlin: Akademie-Verlag, 1987

[R] Rowe, D.E.: Gauss, Dirichlet, and the law of biquadratic reciprocity. Math. Intell. **10**, No. 2, 13–25 (1988)

[Sa] Sartorius von Waltershausen, W.: Gauß zum Gedächtnis. Leipzig: Hirzel, 1856, reprinted by Sändig Reprint Verlag, H.R. Wohlwend, Schaan/Liechtenstein, 1981

[Sch] Scharlau, W. (ed.): Richard Dedekind, 1831/1981. Eine Würdigung zu seinem 150. Geburtstag. Braunschweig–Wiesbaden: Vieweg, 1981

[Sc.1] Schubring, G.: Die Promotion von P.G. Lejeune Dirichlet. Biographische Mitteilungen zum Werdegang Dirichlets. NTM, Schriftenr. Gesch. Naturwiss. Tech. Med. **21**, 45–65 (1984)

[Sc.2] Schubring, G.: Die Erinnerungen von Karl Emil Gruhl (1833–1917) an sein Studium der Mathematik und Physik in Berlin (1853–1856). Jahrb. Überblicke Math., Math. Surv. **18**, 143–173 (1985)

[Sc.3] Schubring, G.: The three parts of the Dirichlet Nachlass. Hist. Math. **13**, 52–56 (1986)

[Se] Seguier, J. de: Formes quadratiques et multiplication complexe. Berlin: F.L. Dames, 1894 (339 pp.)

[Sh] Shields, A.: Lejeune Dirichlet and the birth of analytic number theory: 1837–1839. Math. Intell. **11**, 7–11 (1989)

[Si] Siegel, C.L.: Lectures on advanced analytic number theory. Bombay: Tata Institute of Fundamental Research, 1961, reissued 1965

[Sm] Smith, H.J.S.: Report on the theory of numbers. Bronx, New York: Chelsea, 1965. (Also in: Collected papers of Henry John Stephen Smith, vol. 1, 1894. Reprint: Bronx, New York: Chelsea, 1965)

[St] Sturm, R.: Geschichte der mathematischen Professuren im ersten Jahrhundert der Universität Breslau 1811–1911. Jahresber. Dtsch. Math.-Ver. **20**, 314–321 (1911)

[T] Tannery, M.J. (ed.): Correspondance entre Liouville et Dirichlet. Bull. Sci. Math., 2. Ser. **32**, 47–62, 88–95 (1908) and **33**, 47–64 (1908/09)

[Wa] Wangerin, A. (ed.): Über die Anziehung homogener Ellipsoide. Abhandlungen von Laplace (1782), Ivory (1809), Gauß (1813), Chasles (1838) und Dirichlet (1839). (Ostwald's Klassiker der exakten Wissenschaften **19**.) Leipzig and Berlin: Engelmann, 1st ed. 1890, 2nd ed. 1914

[Web] Weber, H.: Wilhelm Weber. Eine Lebensskizze. Breslau: Verlag von E. Trewendt, 1893

[Wei] Weil, A.: Elliptic functions according to Eisenstein and Kronecker. Berlin etc.: Springer, 1976

[Z] Zagier, D.: Zetafunktionen und quadratische Körper. Berlin etc.: Springer, 1981

Mathematisches Institut, Westf. Wilhelms-Universität Münster, Einsteinstr. 62, 48149 Münster, Germany

E-mail address: elstrod@math.uni-muenster.de

Clay Mathematics Proceedings
Volume 7, 2007

An overview of Manin's conjecture for del Pezzo surfaces

T.D. Browning

Abstract. This paper surveys recent progress towards the Manin conjecture for (singular and non-singular) del Pezzo surfaces. To illustrate some of the techniques available, an upper bound of the expected order of magnitude is established for a singular del Pezzo surface of degree four.

1. Introduction

A fundamental theme in mathematics is the study of integer or rational points on algebraic varieties. Let $V \subset \mathbb{P}^n$ be a projective variety that is cut out by a finite system of homogeneous equations defined over $\mathbb{Q}$. Then there are a number of basic questions that can be asked about the set $V(\mathbb{Q}) := V \cap \mathbb{P}^n(\mathbb{Q})$ of rational points on V: when is $V(\mathbb{Q})$ non-empty? how large is $V(\mathbb{Q})$ when it is non-empty? This paper aims to survey the second question, for a large class of varieties V for which one expects $V(\mathbb{Q})$ to be Zariski dense in V.

To make sense of this it is convenient to define the *height* of a projective rational point $x = [x_0, \ldots, x_n] \in \mathbb{P}^n(\mathbb{Q})$ to be $H(x) := \|\mathbf{x}\|$, for any norm $\| \cdot \|$ on $\mathbb{R}^{n+1}$, provided that $\mathbf{x} = (x_0, \ldots, x_n) \in \mathbb{Z}^{n+1}$ and $\gcd(x_0, \ldots, x_n) = 1$. Throughout this work we shall work with the height metrized by the choice of norm $|\mathbf{x}| := \max_{0 \leqslant i \leqslant n} |x_i|$. Given a suitable Zariski open subset $U \subseteq V$, the goal is then to study the quantity

$$N_{U,H}(B) := \#\{x \in U(\mathbb{Q}) : H(x) \leqslant B\}, \tag{1}$$

as $B \to \infty$. It is natural to question whether the asymptotic behaviour of $N_{U,H}(B)$ can be related to the geometry of V, for suitable open subsets $U \subseteq V$. Around 1989 Manin initiated a program to do exactly this for varieties with ample anticanonical divisor [**FMT89**]. Suppose for simplicity that $V \subset \mathbb{P}^n$ is a non-singular complete intersection, with $V = W_1 \cap \cdots \cap W_t$ for hypersurfaces $W_i \subset \mathbb{P}^n$ of degree d_i. Since V is assumed to be Fano, its Picard group is a finitely generated free $\mathbb{Z}$-module, and we denote its rank by ρ_V. In this setting the Manin conjecture takes the following shape [**BM90**, Conjecture C'].

2000 *Mathematics Subject Classification.* Primary 14G05, Secondary 11G35.

Conjecture A. *Suppose that $d_1+\cdots+d_t \leqslant n$. Then there exists a Zariski open subset $U\subseteq V$ and a non-negative constant $c_{V,H}$ such that*

$$N_{U,H}(B)=c_{V,H}B^{n+1-d_1-\cdots-d_t}(\log B)^{\rho_V-1}\big(1+o(1)\big), \tag{2}$$

as $B\rightarrow\infty$.

It should be noted that there exist heuristic arguments supporting the value of the exponents of B and $\log B$ appearing in the conjecture [**SD04**, §8]. The constant $c_{V,H}$ has also received a conjectural interpretation at the hands of Peyre [**Pey95**], and this has been generalised to cover certain other cases by Batyrev and Tschinkel [**BT98b**], and Salberger [**Sal98**]. In fact whenever we refer to the Manin conjecture we shall henceforth mean that the value of the constant $c_{V,H}$ should agree with the prediction of Peyre et al. With this in mind, the Manin conjecture can be extended to cover certain other Fano varieties V which are not necessarily complete intersections, nor non-singular. For the former one simply takes the exponent of B to be the infimum of numbers $a/b\in\mathbb{Q}$ such that $b>0$ and $aH+bK_V$ is linearly equivalent to an effective divisor, where $K_V\in \mathrm{Div}(V)$ is a canonical divisor and $H\in\mathrm{Div}(V)$ is a hyperplane section. For the latter, if V has only rational double points one may apply the conjecture to a minimal desingularisation $\widetilde{V}$ of V, and then use the functoriality of heights. A discussion of these more general versions of the conjecture can be found in the survey of Tschinkel [**Tsc03**]. The purpose of this note is to give an overview of our progress in the case that V is a suitable Fano variety of dimension 2.

Let $d\geqslant 3$. A non-singular surface $S\subset\mathbb{P}^d$ of degree d, with very ample anticanonical divisor $-K_S$, is known as a *del Pezzo surface of degree d*. Their geometry has been expounded by Manin [**Man86**], for example. It is well-known that such surfaces S arise either as the quadratic Veronese embedding of a quadric in $\mathbb{P}^3$, which is a del Pezzo surface of degree 8 in $\mathbb{P}^8$ (isomorphic to $\mathbb{P}^1\times\mathbb{P}^1$), or as the blow-up of $\mathbb{P}^2$ at $9-d$ points in general position, in which case the degree of S satisfies $3\leqslant d\leqslant 9$. Apart from a brief mention in the final section of this paper, we shall say nothing about del Pezzo surfaces of degree 1 or 2 in this work. The arithmetic of such surfaces remains largely elusive.

We proceed under the assumption that $3\leqslant d\leqslant 9$. In terms of the expected asymptotic formula for $N_{U,H}(B)$ for a suitable open subset $U\subseteq S$, the exponent of B is 1, and the exponent of $\log B$ is at most $9-d$, since the geometric Picard group $\mathrm{Pic}(S\otimes_{\mathbb{Q}}\overline{\mathbb{Q}})$ has rank $10-d$. An old result of Segre ensures that the set $S(\mathbb{Q})$ of rational points on S is Zariski dense as soon as it is non-empty. Moreover, S may contain certain so-called *accumulating subvarieties* that can dominate the behaviour of the counting function $N_{S,H}(B)$. These are the possible lines contained in S, whose configuration is intimately related to the configuration of points in the plane that are blown-up to obtain S. Now it is an easy exercise to check that

$$N_{\mathbb{P}^1,H}(B)=\frac{12}{\pi^2}B^2\big(1+o(1)\big),$$

as $B\rightarrow\infty$, so that $N_{V,H}(B)\gg_V B^2$ for any geometrically integral surface $V\subset\mathbb{P}^n$ that contains a line defined over $\mathbb{Q}$. However, if $U\subseteq V$ is defined to be the Zariski open subset formed by deleting all of the lines from V then it follows from combining an estimate of Heath-Brown [**HB02**, Theorem 6] with a simple birational projection argument, that $N_{U,H}(B)=o_V(B^2)$.

Returning to the setting of del Pezzo surfaces $S \subset \mathbb{P}^d$ of degree d, it turns out that there are no accumulating subvarieties when $d = 9$, or when $d = 8$ and S is isomorphic to $\mathbb{P}^1 \times \mathbb{P}^1$, in which case we study $N_{S,H}(B)$. When $3 \leqslant d \leqslant 7$, or when $d = 8$ and S is not isomorphic to $\mathbb{P}^1 \times \mathbb{P}^1$, there are a finite number of accumulating subvarieties, equal to the lines in S. In these cases we study $N_{U,H}(B)$ for the open subset U formed by deleting all of the lines from S. We now proceed to review the progress that has been made towards the Manin conjecture for del Pezzo surfaces of degree $d \geqslant 3$. In doing so we have split our discussion according to the degree of the surface. It will become apparent that the problem of estimating $N_{U,H}(B)$ becomes harder as the degree decreases.

1.1. Del Pezzo surfaces of degree $\geqslant 5$**.** It turns out that the non-singular del Pezzo surfaces S of degree $d \geqslant 6$ are toric, in the sense that they contain the torus $\mathbb{G}_m^2$ as a dense open subset, whose natural action on itself extends to all of S. Thus the Manin conjecture for such surfaces is a special case of the more general work due to Batyrev and Tschinkel [**BT98a**], that establishes this conjecture for all toric varieties. One may compare this result with the work of de la Bretèche [**dlB01**] and Salberger [**Sal98**], who both establish the conjecture for toric varieties defined over $\mathbb{Q}$, and also the work of Peyre [**Pey95**], who handles a number of special cases.

For non-singular del Pezzo surfaces $S \subset \mathbb{P}^5$ of degree 5, the situation is rather less satisfactory. In fact there are very few instances for which the Manin conjecture has been established. The most significant of these is due to de la Bretèche [**dlB02**], who has proved the conjecture when the 10 lines are all defined over $\mathbb{Q}$. In such cases we say that the surface is *split* over $\mathbb{Q}$. Let S_0 be the surface obtained by blowing up $\mathbb{P}^2$ along the four points

$$p_1 = [1,0,0], \quad p_2 = [0,1,0], \quad p_3 = [0,0,1], \quad p_4 = [1,1,1],$$

and let $U_0 \subset S_0$ denote the corresponding open subset formed by deleting the lines from S_0. Then $\mathrm{Pic}(S_0)$ has rank 5, since S_0 is split over $\mathbb{Q}$, and de la Bretèche obtains the following result.

THEOREM 1. *Let $B \geqslant 3$. Then there exists a constant $c_0 > 0$ such that*

$$N_{U_0,H}(B) = c_0 B (\log B)^4 \Big(1 + O\Big(\frac{1}{\log\log B}\Big)\Big).$$

We shall return to the proof of this result below. The other major achievement in the setting of quintic del Pezzo surfaces is a result of de la Bretèche and Fouvry [**dlBF04**]. Here the Manin conjecture is established for the surface obtained by blowing up $\mathbb{P}^2$ along four points in general position, two of which are defined over $\mathbb{Q}$ and two of which are conjugate over $\mathbb{Q}(i)$. In related work, Browning [**Bro03b**] has obtained upper bounds for $N_{U,H}(B)$ that agree with the Manin prediction for several other del Pezzo surfaces of degree 5.

1.2. Del Pezzo surfaces of degree 4**.** A quartic del Pezzo surface $S \subset \mathbb{P}^4$, that is defined over $\mathbb{Q}$, can be recognised as the zero locus of a suitable pair of quadratic forms $Q_1, Q_2 \in \mathbb{Z}[x_0, \dots, x_4]$. Then $S = \mathrm{Proj}(\mathbb{Q}[x_0, \dots, x_4]/(Q_1, Q_2))$ is the complete intersection of the hypersurfaces $Q_1 = 0$ and $Q_2 = 0$ in $\mathbb{P}^4$. When S is non-singular (2) predicts the existence of a constant $c_{S,H} \geqslant 0$ such that

$$N_{U,H}(B) = c_{S,H} B (\log B)^{\rho_S - 1} \big(1 + o(1)\big), \tag{3}$$

as $B \to \infty$, where $\rho_S = \mathrm{rk}\,\mathrm{Pic}(S) \leqslant 6$ and $U \subset S$ is obtained by deleting the 16 lines from S. In this setting the best result available is due to Salberger. In work communicated at the conference *Higher dimensional varieties and rational points* at Budapest in 2001, he establishes the estimate $N_{U,H}(B) = O_{\varepsilon,S}(B^{1+\varepsilon})$ for any $\varepsilon > 0$, provided that the surface contains a conic defined over $\mathbb{Q}$. In fact an examination of Salberger's approach, which is based upon fibering the surface into a family of conics, reveals that one can replace the factor B^ε by $(\log B)^A$ for a large constant A. It would be more interesting to find examples of surfaces S for which the exponent A could be reduced to the expected quantity $\rho_S - 1$.

It emerges that much more can be said if one permits S to contain isolated singularities. For the remainder of this section let $S \subset \mathbb{P}^4$ be a geometrically integral intersection of two quadric hypersurfaces, which has only isolated singularities and is not a cone. Then S contains only rational double points (see Wall [**Wal80**], for example), thereby ensuring that there exists a unique minimal desingularisation $\pi : \widetilde{S} \to S$ of the surface, such that $K_{\widetilde{S}} = \pi^* K_S$. In particular it follows that the asymptotic formula (3) is still expected to hold, with ρ_S now taken to be the rank of the Picard group of $\widetilde{S}$, and $U \subset S$ obtained by deleting all of the lines from S. The classification of such surfaces S is rather classical, and can be found in the work of Hodge and Pedoe [**HP52**, Book IV, §XIII.11], for example. It turns out that up to isomorphism over $\overline{\mathbb{Q}}$, there are 15 possible singularity types for S, each categorised by the *extended Dynkin diagram*. This is the Dynkin diagram that describes the intersection behaviour of the exceptional divisors and the transforms of the lines on the minimal desingularisation $\widetilde{S}$ of S. Of course, if one is interested in a classification over the ground field $\mathbb{Q}$, then many more singularity types can occur (see Lipman [**Lip69**], for example). Over $\overline{\mathbb{Q}}$, Coray and Tsfasman [**CT88**, Proposition 6.1] have calculated the extended Dynkin diagrams for all of the 15 types, and this information allows us to write down a list of surfaces $S = \mathrm{Proj}(\mathbb{Q}[\mathbf{x}]/(Q_1, Q_2))$ that typify each possibility, together with their singularity type and the number of lines that they contain. The author is grateful to Ulrich Derenthal for helping to prepare the following table.

type	$Q_1(\mathbf{x})$	$Q_2(\mathbf{x})$	# lines	singularity
i	$x_0x_1 + x_2x_3$	$x_0x_3 + x_1x_2 + x_2x_4 + x_3x_4$	12	$\mathbf{A}_1$
ii	$x_0x_1 + x_2x_3$	$x_0x_3 + x_1x_2 + x_2x_4 + x_4^2$	9	$2\mathbf{A}_1$
iii	$x_0x_1 + x_2^2$	$x_0x_2 + x_1x_2 + x_3x_4$	8	$2\mathbf{A}_1$
iv	$x_0x_1 + x_2x_3$	$x_2x_3 + x_4(x_0 + x_1 + x_2 - x_3)$	8	$\mathbf{A}_2$
v	$x_0x_1 + x_2^2$	$x_1x_2 + x_2^2 + x_3x_4$	6	$3\mathbf{A}_1$
vi	$x_0x_1 + x_2x_3$	$x_1^2 + x_2^2 + x_3x_4$	6	$\mathbf{A}_1 + \mathbf{A}_2$
vii	$x_0x_1 + x_2x_3$	$x_1x_3 + x_2^2 + x_4^2$	5	$\mathbf{A}_3$
viii	$x_0x_1 + x_2^2$	$(x_0 + x_1)^2 + x_2x_4 + x_3^2$	4	$\mathbf{A}_3$
ix	$x_0x_1 + x_2^2$	$x_2^2 + x_3x_4$	4	$4\mathbf{A}_1$
x	$x_0x_1 + x_2^2$	$x_1x_2 + x_3x_4$	4	$2\mathbf{A}_1 + \mathbf{A}_2$
xi	$x_0x_1 + x_2^2$	$x_0^2 + x_2x_4 + x_3^2$	3	$\mathbf{A}_1 + \mathbf{A}_3$
xii	$x_0x_1 + x_2x_3$	$x_0x_4 + x_1x_3 + x_2^2$	3	$\mathbf{A}_4$
xiii	$x_0x_1 + x_2^2$	$x_0^2 + x_1x_4 + x_3^2$	2	$\mathbf{D}_4$
xiv	$x_0x_1 + x_2^2$	$x_0^2 + x_3x_4$	2	$2\mathbf{A}_1 + \mathbf{A}_3$
xv	$x_0x_1 + x_2^2$	$x_0x_4 + x_1x_2 + x_3^2$	1	$\mathbf{D}_5$

Apart from the surfaces of type vi, vii, viii, xi or xiii, which contain lines defined over $\mathbb{Q}(i)$, each surface in the table is split over $\mathbb{Q}$. Let $\widetilde{S}$ denote the minimal desingularisation of any surface S from the table, and let ρ_S denote the rank of the Picard group of $\widetilde{S}$. Then it is natural to try and establish (3) for such surfaces S. Several of the surfaces are actually special cases of varieties for which the Manin conjecture is already known to hold. Thus we have seen above that it has been established for toric varieties, and it can be checked that the surfaces representing types ix, x, xiv are all equivariant compactifications of $\mathbb{G}_m^2$, and so are toric. Hence (3) holds for these particular surfaces. Similarly it has been shown by Chambert-Loir and Tschinkel [**CLT02**] that the Manin conjecture is true for equivariant compactifications of vector groups. Although identifying such surfaces in the table is not entirely routine, it transpires that the $\mathbf{D}_5$ surface representing type xv is an equivariant compactification of $\mathbb{G}_a^2$. Salberger has raised the question of whether there exist singular del Pezzo surfaces of degree 4 that arise as equivariant compactifications of $\mathbb{G}_a \times \mathbb{G}_m$, but that are not already equivariant compactifications of $\mathbb{G}_a^2$ or $\mathbb{G}_m^2$. This is a natural class of varieties that does not seem to have been studied yet, but for which the existing technology is likely to prove useful.

Let us consider the type xv surface

$$S_1 = \{[x_0, \dots, x_4] \in \mathbb{P}^4 : x_0x_1 + x_2^2 = x_0x_4 + x_1x_2 + x_3^2 = 0\},$$

in more detail. Now we have already seen that (3) holds for S_1. Nonetheless, de la Bretèche and Browning [**dlBBa**] have made an exhaustive study of S_1, partly in an attempt to lay down a template for the treatment of other surfaces in the table. In doing so several new features have been revealed. For $s \in \mathbb{C}$ such that $\Re e(s) > 1$, let

$$Z_{U,H}(s) := \sum_{x \in U(\mathbb{Q})} H(x)^{-s} \tag{4}$$

denote the corresponding height zeta function, where $U = U_1$ denotes the open subset formed by deleting the unique line $x_0 = x_2 = x_3 = 0$ from S_1. The analytic properties of $Z_{U_1,H}(s)$ are intimately related to the asymptotic behaviour of the counting function $N_{U_1,H}(B)$, and it is relatively straightforward to translate between them. For $\sigma \in \mathbb{R}$, let $\mathcal{H}_\sigma$ denote the half-plane $\{s \in \mathbb{C} : \Re e(s) > \sigma\}$. Then with this notation in mind we have the following result [**dlBBa**, Theorem 1].

THEOREM 2. *There exists a constant $\alpha \in \mathbb{R}$ and a function $F(s)$ that is meromorphic on $\mathcal{H}_{9/10}$, with a single pole of order 6 at $s = 1$, such that*

$$Z_{U_1,H}(s) = F(s) + \alpha(s-1)^{-1}$$

for $s \in \mathcal{H}_1$. In particular $Z_{U_1,H}(s)$ has an analytic continuation to $\mathcal{H}_{9/10}$.

It should be highlighted that there exist remarkably precise descriptions of α and $F(s)$ in the theorem. An application of Perron's formula enables one to deduce a corresponding asymptotic formula for $N_{U_1,H}(B)$ that verifies (3), with $\rho_{S_1} = 6$. Actually one is led to the much stronger statement that there exists a polynomial f of degree 5 such that for any $\delta \in (0, 1/12)$ we have

$$N_{U,H}(B) = Bf(\log B) + O(B^{1-\delta}), \tag{5}$$

with $U = U_1$, in which the leading coefficient of f agrees with Peyre's prediction.

No explicit use is made of the fact that S_1 is an equivariant compactification of $\mathbb{G}_a^2$ in the proof of Theorem 2, and this renders the method applicable to other surfaces in the list that are not of this type. For example, in further work de la Bretèche and Browning [**dlBBb**] have also established the Manin conjecture for the $\mathbf{D}_4$ surface

$$S_2 = \{[x_0, \ldots, x_4] \in \mathbb{P}^4 : x_0x_1 + x_2^2 = x_0^2 + x_1x_4 + x_3^2 = 0\},$$

which represents the type `xiii` surface in the table. As indicated above, this surface is not split over $\mathbb{Q}$, and it transpires that $\mathrm{Pic}(\widetilde{S}_2)$ has rank 4. In fact $\widetilde{S}_2$ has singularity type $\mathbf{C}_3$ over $\mathbb{Q}$, in the sense of Lipman [**Lip69**, §24], which becomes a $\mathbf{D}_4$ singularity over $\overline{\mathbb{Q}}$. Building on the techniques developed in the proof of Theorem 2, a result of the same quality is obtained for the corresponding height zeta function $Z_{U_2,H}(s)$, and this leads to an estimate of the shape (5) for any $\delta \in (0, 3/32)$, with $U = U_2$ and $\deg f = 3$.

One of the aims of this survey is to give an overview of the various ideas and techniques that have been used to study the surfaces S_1, S_2 above. We shall illustrate the basic method by giving a simplified analysis of a new example from the table. Let us consider the $3\mathbf{A}_1$ surface

$$S_3 = \{[x_0, \ldots, x_4] \in \mathbb{P}^4 : x_0x_1 + x_2^2 = x_1x_2 + x_2^2 + x_3x_4 = 0\}, \tag{6}$$

which represents the type `v` surface in the table, and is neither toric nor an equivariant compactification of $\mathbb{G}_a^2$. The surface has singularities at the points $[1, 0, 0, 0, 0]$, $[0, 0, 0, 1, 0]$ and $[0, 0, 0, 0, 1]$, and contains precisely 6 lines

$$x_i = x_2 = x_j = 0, \quad x_0 + x_2 = x_1 + x_2 = x_j = 0,$$

where $i \in \{0, 1\}$ and $j \in \{3, 4\}$. Since S_3 is split over $\mathbb{Q}$, one finds that the expected exponent of $\log B$ in (3) is $\rho_{S_3} - 1 = 5$. We shall establish the following result.

Theorem 3. *We have* $N_{U_3,H}(B) = O\big(B(\log B)^5\big)$.

As pointed out to the author by de la Bretèche, it is possible to establish a corresponding lower bound $N_{U_3,H}(B) \gg B(\log B)^5$, using little more than the most basic estimates for integers restricted to lie in fixed congruence classes. In fact, with more work, it ought even to be possible to obtain an asymptotic formula for $N_{U_3,H}(B)$. In the interests of brevity, however, we have chosen to pursue neither of these problems here.

1.3. Del Pezzo surfaces of degree 3. The del Pezzo surfaces $S \subset \mathbb{P}^3$ of degree 3 are readily recognised as the geometrically integral cubic surfaces in $\mathbb{P}^3$, which are not ruled by lines. Given such a surface S defined over $\mathbb{Q}$, we may always find an absolutely irreducible cubic form $C(\mathbf{x}) \in \mathbb{Z}[x_0, x_1, x_2, x_3]$ such that $S = \mathrm{Proj}(\mathbb{Q}[\mathbf{x}]/(C))$. Let us begin by considering the situation for non-singular cubic surfaces. In this setting $U \subset S$ is taken to be the open subset formed by deleting the famous 27 lines from S. Although Peyre and Tschinkel [**PT01a, PT01b**] have provided ample numerical evidence for the validity of the Manin conjecture for diagonal non-singular cubic surfaces, we are unfortunately still rather far away from proving it. The best upper bound available is $N_{U,H}(B) = O_{\varepsilon,S}(B^{4/3+\varepsilon})$, due to Heath-Brown [**HB97**]. This applies when the surface S contains 3 coplanar lines defined over $\mathbb{Q}$, and in particular to the *Fermat cubic surface* $x_0^3 + x_1^3 = x_2^3 + x_3^3$. The problem of proving lower bounds is somewhat easier. Under the assumption that S contains a pair of skew lines defined over $\mathbb{Q}$, Slater and Swinnerton-Dyer

[**SSD98**] have shown that $N_{U,H}(B) \gg_S B(\log B)^{\rho_S - 1}$, as predicted by the Manin conjecture. This does not apply to the Fermat cubic surface, however, since the only skew lines contained in this surface are defined over $\mathbb{Q}(\sqrt{-3})$. It would be interesting to extend the work of Slater and Swinnerton-Dyer to cover such cases.

Much as in the previous section, it turns out that far better estimates are available for singular cubic surfaces. The classification of such surfaces is a well-established subject, and essentially goes back to the work of Cayley [**Cay69**] and Schläfli [**Sch64**] over a century ago. A contemporary classification of singular cubic surfaces, using the terminology of modern classification theory, has since been given by Bruce and Wall [**BW79**]. As in the previous section, the Manin conjecture is already known to hold for several of these surfaces by virtue of the fact that they are equivariant compactifications of $\mathbb{G}_a^2$, or toric. An example of the latter is given by the $3\mathbf{A}_2$ surface

$$S_4 = \{[x_0, x_1, x_2, x_3] \in \mathbb{P}^3 : x_0^3 = x_1 x_2 x_3\}. \tag{7}$$

A number of authors have studied this surface, including de la Bretèche [**dlB98**], Fouvry [**Fou98**], and Heath-Brown and Moroz [**HBM99**]. Of the asymptotic formulae obtained, the most impressive is the first. This consists of an estimate like (5) for any $\delta \in (0, 1/8)$, with $U = U_4 \subset S_4$ and $\deg f = 6$. The next surface to have received serious attention is the *Cayley cubic surface*

$$S_5 = \{[x_0, x_1, x_2, x_3] \in \mathbb{P}^3 : x_0x_1x_2 + x_0x_1x_3 + x_0x_2x_3 + x_1x_2x_3 = 0\}, \tag{8}$$

of singularity type $4\mathbf{A}_1$. This contains 9 lines, all of which are defined over $\mathbb{Q}$, and Heath-Brown [**HB03**] has shown that there exist absolute constants $A_1, A_2 > 0$ such that

$$A_1 B(\log B)^6 \leqslant N_{U_5,H}(B) \leqslant A_2 B(\log B)^6,$$

where $U_5 \subset S_5$ is the usual open subset. An estimate of precisely the same form has also been obtained by Browning [**Bro06**] for the $\mathbf{D}_4$ surface

$$S_6 = \{[x_0, x_1, x_2, x_3] \in \mathbb{P}^3 : x_1x_2x_3 = x_0(x_1 + x_2 + x_3)^2\}.$$

In both cases the corresponding Picard group has rank 7, so that the exponents of B and $\log B$ agree with Manin's prediction.

The final surface to have been studied extensively is the $\mathbf{E}_6$ cubic surface

$$S_7 = \{[x_0, x_1, x_2, x_3] \in \mathbb{P}^3 : x_1x_2^2 + x_2x_0^2 + x_3^3 = 0\}, \tag{9}$$

which contains a unique line $x_2 = x_3 = 0$. Let $U_7 \subset S_7$ denote the open subset formed by deleting the line from S_7, and recall the notation (4) for the height zeta function $Z_{U_7,H}(s)$ and that of the half-plane $\mathcal{H}_\sigma$ introduced before Theorem 2. Then recent work of de la Bretèche, Browning and Derenthal [**dlBBD**] has succeeded in establishing the following result.

THEOREM 4. *There exists a constant $\alpha \in \mathbb{R}$ and a function $F(s)$ that is meromorphic on $\mathcal{H}_{9/10}$, with a single pole of order 7 at $s = 1$, such that*

$$Z_{U_7,H}(s) = F(s) + \alpha(s-1)^{-1}$$

for $s \in \mathcal{H}_1$. In particular $Z_{U_7,H}(s)$ has an analytic continuation to $\mathcal{H}_{9/10}$.

As in Theorem 2, the terms α and $F(s)$ have a very explicit description. An application of Perron's formula now yields an asymptotic formula of the shape (5) for any $\delta \in (0, 1/11)$, with $U = U_7$ and $\deg f = 6$. This too is in complete agreement with the Manin conjecture. It should be remarked that Michael Joyce has independently established the Manin conjecture for S_7 in his doctoral thesis at Brown University, albeit only with a weaker error term of $O(B(\log B)^5)$.

2. Refinements of the Manin conjecture

The purpose of this section is to consider in what way one might hope to refine the conjecture of Manin. We have already seen a number of examples in which asymptotic formulae of the shape (5) hold, and it is very natural to suppose that this is the case for any (possibly singular) del Pezzo surface $S \subset \mathbb{P}^d$ of degree d, where as usual $U \subseteq S$ denotes the open subset formed by deleting any lines from S, and ρ_S denotes the rank of the Picard group of S (possibly of $\widetilde{S}$). Let us record this formally here.

CONJECTURE B. *Let S, U, ρ_S be as above. Then there exists $\delta > 0$, and a polynomial $f \in \mathbb{R}[x]$ of degree $\rho_S - 1$, such that* (5) *holds.*

The leading coefficient of f should of course agree with the prediction of Peyre et al. It would be interesting to gain a conjectural understanding of the lower order coefficients of f, possibly in terms of the geometry of S. At this stage it seems worth drawing attention to the surprising nature of the constants α that appear in Theorems 2 and 4, not least because they contribute to the constant coefficient of f. In both cases we have $\alpha = \frac{12}{\pi^2} + \beta$, where the first term corresponds to an isolated conic in the surface, and the second is purely arithmetic in nature and takes a very complicated shape (see [**dlBBa**, Eq. (5.25)] and [**dlBBD**, Eq. (8.49)]). It arises through the error in approximating certain arithmetic quantities by real-valued continuous functions, and involves the application of results about the equidistribution of squares in fixed residue classes.

One might also ask what one expects to be the true order of magnitude of the error term in (5). This a question that Swinnerton-Dyer has recently addressed [**SD05**, Conjecture 2], inspired by comparisons with the explicit formulae from prime number theory.

CONJECTURE C. *Let S, U, ρ_S be as above. Then there exist positive constants $\theta_1, \theta_2, \theta_3 < 1$ with $\theta_1 < \min\{\theta_2, \theta_3\}$, a polynomial $f \in \mathbb{R}[x]$ of degree $\rho_S - 1$, a constant $\gamma \in \mathbb{R}$, and a sequence of $\gamma_n \in \mathbb{C}$, such for any $\varepsilon > 0$ we have*

$$N_{U,H}(B) = Bf(\log B) + \gamma B^{\theta_3} + \Re e \sum \gamma_n B^{\theta_2 + it_n} + O_\varepsilon(B^{\theta_1+\varepsilon}).$$

Here $t_n \in \mathbb{R}$ form a sequence of positive and monotonically increasing numbers, such that $\sum |\gamma_n|^2$ and $\sum t_n^{-2}$ are convergent.

In fact Swinnerton-Dyer formulates the conjecture for non-singular cubic surfaces, with $\theta_1 < \frac{1}{2} = \theta_2$ and $\gamma = 0$. There is no reason, however, to expect that it doesn't hold more generally, and one might even suppose that the constants θ_2, θ_3 somehow relate to the nature of the surface singularities. In this context there is the recent work of de la Bretèche and Swinnerton-Dyer [**dlBSD**], who have provided significant evidence for this finer conjecture for the singular cubic surface (7). Under the Riemann hypothesis and the assumption that the zeros of the Riemann zeta function are all simple, it is shown that the conjecture holds for S_4, with $(\theta_1, \theta_2, \theta_3) = (\frac{4}{5}, \frac{13}{16}, \frac{9}{11})$ and $\gamma \neq 0$.

3. Available tools

There are a variety of tools that can be brought to bear upon the problem of estimating the counting function (1), for appropriate subsets U of projective algebraic varieties. Most of these are rooted in analytic number theory. When the dimension of the variety is large compared to its degree, the Hardy–Littlewood circle method can often be applied successfully (see Davenport [**Dav05**], for example). When the variety has a suitable "cellular" structure, techniques involving harmonic analysis on adelic groups can be employed (see Tschinkel [**Tsc02**], for example). We shall say nothing about these methods here, save to observe that outside of the surfaces covered by the collective work of Batyrev, Chambert-Loir and Tschinkel [**BT98a, CLT02**], they do not seem capable of establishing the Manin conjecture for all del Pezzo surfaces.

In fact we still have no clear vision of which methods are most appropriate, and it is conceivable that the methods needed to handle the singular del Pezzo surfaces of low degree are quite different from those needed to handle the non-singular surfaces. Given our inability to prove the Manin conjecture for a single non-singular del Pezzo surface of degree 3 or 4, we shall say no more about them here, save to observe that the sharpest results we have are for examples containing conic bundle structures over the ground field. Instead we shall concentrate on the situation for singular del Pezzo surfaces of degree 3 or 4. Disappointing as it may seem, it is hard to imagine that we will see how to prove Manin's conjecture for all del Pezzo surfaces without first attempting to do so for a number of very concrete representative examples. As a cursory analysis of the proofs of Theorems 2–4 shows, the techniques that have been successfully applied so far are decidedly ad-hoc. Nonetheless there are a few salient features that are worthy of amplification, and this will be the focus of the two subsequent sections.

3.1. The universal torsor. Universal torsors were originally introduced by Colliot-Thélène and Sansuc [**CTS76, CTS87**] to aid in the study of the Hasse principle and weak approximation for rational varieties. Since their inception it is now well-recognised that they also have a central rôle to play in proofs of the Manin conjecture for Fano varieties. Let $S \subset \mathbb{P}^d$ be a del Pezzo surface of degree $d \in \{3, 4, 5\}$, and let $\widetilde{S}$ denote the minimal desingularisation of S if it is singular, and $\widetilde{S} = S$ otherwise. Let $E_1, \ldots, E_{10-d} \in \mathrm{Div}(\widetilde{S})$ be generators for the geometric Picard group of $\widetilde{S}$, and let $E_i^\times = E_i \setminus \{\text{zero section}\}$. Working over $\overline{\mathbb{Q}}$, a *universal torsor* above $\widetilde{S}$ is given by the action of $\mathbb{G}_m^{10-d}$ on the map

$$\pi : E_1^\times \times_{\widetilde{S}} \cdots \times_{\widetilde{S}} E_{10-d}^\times \to \widetilde{S}.$$

A proper discussion of universal torsors would take us too far afield at present, and the reader should consult the survey of Peyre [**Pey04**] for further details, or indeed the construction of Hassett and Tschinkel [**HT04**]. The latter outlines an alternative approach to universal torsors via the Cox ring. The guiding principle behind the use of universal torsors is simply that they ought to be arithmetically simpler than the original variety. The universal torsors that we shall encounter all have embeddings as open subsets of affine varieties of higher dimension. Moreover, the general theory ensures that there is a partition of $U(\mathbb{Q})$ — where $U \subset S$ is the usual open subset formed by deleting the lines from S — into a disjoint union of patches, each of which is in bijection with a suitable set of integral points on a universal torsor above $\widetilde{S}$. We shall see shortly how one may often use arguments from elementary number theory to explicitly derive these bijections.

Let us begin by giving a few examples. In the proof of Theorem 1 a passage to the universal torsor is a crucial first step, and was originally carried out by Salberger in his unpublished proof of the bound $N_{U_0,H}(B) = O(B(\log B)^4)$, announced in the *Borel seminar* at Bern in 1993. Recall the Plücker embedding

$$z_{i,j}z_{k,\ell} - z_{i,k}z_{j,\ell} + z_{i,\ell}z_{j,k} = 0,$$

of the Grassmannian $Gr(2,5) \subset \mathbb{P}^9$ of 2-dimensional linear subspaces of $\mathbb{Q}^5$. Here (i,j,k,ℓ) runs through the five vectors formed from elements of the set $\{1,2,3,4,5\}$, with $i<j<k<l$. It turns out that there is a unique universal torsor $\pi : \mathcal{T}_0 \to S_0$ above S_0, and it is a certain open subset of the affine cone over $Gr(2,5)$. To count points of bounded height in $U_0(\mathbb{Q})$ it is then enough to count integral points $(z_{i,j})_{1\leqslant i<j\leqslant 5} \in (\mathbb{Z}\setminus\{0\})^{10}$ on this cone, subject to a number of side conditions. A thorough account of this particular example, and how it extends to arbitrary del Pezzo surfaces of degree 5 can be found in the work of Skorobogatov [**Sko93**]. A second example is calculated by Hassett and Tschinkel [**HT04**] for the $\mathbf{E}_6$ cubic surface (9). There it is shown that there is a unique universal torsor above $\widetilde{S}_7$, given by the equation

$$\tau_\ell\xi_\ell^3\xi_4^2\xi_5 + \tau_2^2\xi_2 + \tau_1^3\xi_1^2\xi_3 = 0, \tag{10}$$

for variables $\tau_1,\tau_2,\tau_\ell,\xi_1,\xi_2,\xi_3,\xi_\ell,\xi_4,\xi_5,\xi_6$. One of the variables does not explicitly appear in (10), and the torsor should be thought of as being embedded in $\mathbb{A}^{10}$. The universal torsors that turn up in the proofs of Theorems 2 and 3 can also be embedded in affine space via a single equation.

We proceed to carry out explicitly the passage to the universal torsor for the $3\mathbf{A}_1$ surface (6). We shall use $\mathbb{N}$ to denote the set of positive integers, and for any $n \geqslant 2$ we let Z^n denote the set of *primitive* vectors in $\mathbb{Z}^n$, by which we mean that the greatest common divisor of the components should be 1. We may clearly assume that S_3 is defined by the forms $Q_1(\mathbf{x}) = x_0x_1 - x_2^2$ and $Q_2(\mathbf{x}) = x_2^2 - x_1x_2 + x_3x_4$. Now if $x \in U_3(\mathbb{Q})$ is represented by the vector $\mathbf{x} \in Z^5$, then $x_0\cdots x_4 \neq 0$ and $H(x) = \max\{|x_0|,|x_1|,|x_3|,|x_4|\}$. Moreover, x_0 and x_1 must share the same sign. On taking x_0,x_1 to both be positive, and noting that $\mathbf{x}$ and $-\mathbf{x}$ represent the same point in $\mathbb{P}^4$, we deduce that

$$N_{U_3,H}(B) = \#\big\{\mathbf{x} \in Z^5 : 0 < x_0, x_1, |x_3|, |x_4| \leqslant B,\ Q_1(\mathbf{x}) = Q_2(\mathbf{x}) = 0\big\}.$$

Let us begin by considering solutions $\mathbf{x} \in Z^5$ to the equation $Q_1(\mathbf{x}) = 0$. There is a bijection between the set of integers x_0,x_1,x_2 such that $x_0,x_1>0$ and $x_0x_1 = x_2^2$, and the set of x_0,x_1,x_2 such that $x_0 = z_0^2z_2, x_1 = z_1^2z_2$ and $x_2 = z_0z_1z_2$, for non-zero integers z_0,z_1,z_2 such that $z_1,z_2>0$ and $\gcd(z_0,z_1)=1$. We now substitute these values into the equation $Q_2(\mathbf{x})=0$, in order to obtain

$$z_0^2z_1^2z_2^2 - z_0z_1^3z_2^2 + x_3x_4 = 0. \tag{11}$$

It follows from the coprimality relation $\gcd(x_0,\ldots,x_4)=1$ that we also have $\gcd(z_2,x_3,x_4)=1$. Now we may conclude from (11) that $z_0z_1^2z_2^2$ divides x_3x_4. Let us write $y_1 = \gcd(z_1,x_3,x_4)$ and $z_1 = y_1y_1', x_3 = y_1y_3', x_4 = y_1y_4'$, with y_1,y_1',y_3',y_4' non-zero integers such that $y_1,y_1'>0$ and $\gcd(y_1',y_3',y_4')=1$. Then $z_0y_1'^2z_2^2$ divides $y_3'y_4'$. We now write $z_0 = y_{03}y_{04}, y_3' = y_{03}y_3$ and $y_4' = y_{04}y_4$, for non-zero integers y_{03},y_{04},y_3,y_4. We therefore conclude that $y_1'^2z_2^2$ divides y_3y_4, whence there exist positive integers $y_{13}, y_{14}, y_{23}, y_{24}$ and non-zero integers y_{33}, y_{34} such that $y_1' = y_{13}y_{14}, z_2 = y_{23}y_{24}, y_3 = y_{13}^2 y_{23}^2 y_{33}$ and $y_4 = y_{14}^2 y_{24}^2 y_{34}$. Substituting these into (11) yields the equation

$$y_{03}y_{04} - y_1 y_{13} y_{14} + y_{33} y_{34} = 0. \tag{12}$$

This equation gives an affine embedding of the unique universal torsor over $\widetilde{S}_3$, though we shall not prove it here. We may combine all of the various coprimality relations above to deduce that

$$\gcd(y_{13}y_{14}y_{23}y_{24}, y_{13}y_{23}y_{33}, y_{14}y_{24}y_{34}) = 1, \tag{13}$$

and

$$\gcd(y_{03}y_{04}, y_{13}y_{14}) = \gcd(y_1, y_{03}y_{04}y_{23}y_{24}) = 1. \tag{14}$$

At this point we may summarize our argument as follows. Let $\mathcal{T}$ denote the set of non-zero integer vectors $\mathbf{y} = (y_1, y_{03}, y_{04}, y_{13}, y_{14}, y_{23}, y_{24}, y_{33}, y_{34})$ such that (12)–(14) all hold, with $y_1, y_{13}, y_{14}, y_{23}, y_{24} > 0$. Then for any $\mathbf{x} \in Z^5$ such that $Q_1(\mathbf{x}) = Q_2(\mathbf{x}) = 0$ and $x_0, x_1, |x_3|, |x_4| > 0$, we have shown that there exists $\mathbf{y} \in \mathcal{T}$ such that

$$\begin{aligned} x_0 &= y_{03}^2 y_{04}^2 y_{23} y_{24}, \\ x_1 &= y_1^2 y_{13}^2 y_{14}^2 y_{23} y_{24}, \\ x_2 &= y_1 y_{03} y_{04} y_{13} y_{14} y_{23} y_{24}, \\ x_3 &= y_1 y_{03} y_{13}^2 y_{23}^2 y_{33}, \\ x_4 &= y_1 y_{04} y_{14}^2 y_{24}^2 y_{34}. \end{aligned}$$

Conversely, it is not hard to check that given any $\mathbf{y} \in \mathcal{T}$ the point $\mathbf{x}$ given above will be a solution of the equations $Q_1(\mathbf{x}) = Q_2(\mathbf{x}) = 0$, with $\mathbf{x} \in Z^5$ and $x_0, x_1, |x_3|, |x_4| > 0$. Let us define the function $\Psi : \mathbb{R}^9 \to \mathbb{R}_{\geqslant 0}$, given by

$$\Psi(\mathbf{y}) = \max \left\{ \begin{array}{ll} |y_{03}^2 y_{04}^2 y_{23} y_{24}|, & |y_1^2 y_{13}^2 y_{14}^2 y_{23} y_{24}|, \\ |y_1 y_{03} y_{13}^2 y_{23}^2 y_{33}|, & |y_1 y_{04} y_{14}^2 y_{24}^2 y_{34}| \end{array} \right\}.$$

Then we have established the following result.

LEMMA 1. *We have* $N_{U_3,H}(B) = \#\{\mathbf{y} \in \mathcal{T} : \Psi(\mathbf{y}) \leqslant B\}$.

In this section we have given several examples of universal torsors, and we have ended by demonstrating how elementary number theory can sometimes be used to calculate their equations with very little trouble. In fact the general machinery of Colliot-Thélène–Sansuc [**CTS76, CTS87**], or that of Hassett–Tschinkel [**HT04**], essentially provides an algorithm for calculating universal torsors over any singular del Pezzo surface of degree 3 or 4. It should be stressed, however, that if this constitutes being given the keys to the city, it does not tell us where in the city the proof is hidden.

3.2. The next step. The purpose of this section is to overview some of the techniques that have been developed for counting integral points on the parametrization that arises out of the passage to the universal torsor, as discussed above. In the proofs of Theorems 1–4 the torsor equations all take the shape

$$A_j + B_j + C_j = 0, \quad (1 \leqslant j \leqslant J),$$

for monomials A_j, B_j, C_j of various degrees in the appropriate variables. By fixing some of the variables at the outset, one is then left with the problem of counting integer solutions to a system of Diophantine equations, subject to certain constraints.

If one is sufficiently clever about which variables to fix first, then one can sometimes be left with a quantity that we know how to estimate — and crucially — for which we can control the overall contribution from the error term when it is summed over the remaining variables.

Let us sketch this phenomenon briefly with the torsor equation (10) that is used in the proof of Theorem 4. It turns out that the way to proceed here is to fix all of the variables apart from $\tau_1, \tau_2, \tau_\ell$. One may then view the equation as a congruence

$$\tau_2^2 \xi_2 \equiv -\tau_1^3 \xi_1^2 \xi_3 \pmod{\xi_\ell^3 \xi_4^2 \xi_5},$$

in order to take care of the summation over τ_ℓ. This allows us to employ very standard facts about the number of integer solutions to polynomial congruences that are restricted to lie in certain regions, and this procedure yields a main term and an error term which the remaining variables need to be summed over. However, while the treatment of the main term is relatively routine, the treatment of the error term presents a much more serious obstacle. We do not have space to discuss it in any detail, but it is here that the unexpected constant α arises in Theorem 4.

The sort of approach discussed above, and more generally the application of lattice methods to count solutions to ternary equations, is a very useful one. It plays a crucial role in the proof of the following result due to Heath-Brown [**HB03**, Lemma 3], which forms the next ingredient in our proof of Theorem 3.

LEMMA 2. *Let $K_1, \dots, K_7 \geqslant 1$ be given, and let $\mathcal{M}$ denote the number of non-zero solutions $m_1, \dots, m_7 \in \mathbb{Z}$ to the equation*

$$m_1 m_2 - m_3 m_4 m_5 + m_6 m_7 = 0,$$

subject to the conditions $K_k < |m_k| \leqslant 2K_k$ for $1 \leqslant k \leqslant 7$, and

$$\gcd(m_1 m_2, m_3 m_4 m_5) = 1. \tag{15}$$

Then we have $\mathcal{M} \ll K_1 K_2 K_3 K_4 K_5$.

For comparison, we note that it is a trivial matter to establish the bound $\mathcal{M} \ll_\varepsilon (K_1 K_2 K_3 K_4 K_5)^{1+\varepsilon}$, using standard estimates for the divisor function. Such a bound would be insufficient for our purposes.

3.3. Completion of the proof of Theorem 3. We are now ready to complete the proof of Theorem 3. We shall begin by estimating the contribution to $N_{U_3,H}(B)$ from the values of $\mathbf{y}$ appearing in Lemma 1 that are constrained to lie in a certain region. Let $Y_1, Y_{i3}, Y_{i4} \geqslant 1$, where throughout this section i denotes a generic index from the set $\{0, 1, 2, 3\}$. Then we write

$$\mathcal{N} = \mathcal{N}(Y_1, Y_{03}, Y_{04}, Y_{13}, Y_{14}, Y_{23}, Y_{24}, Y_{33}, Y_{34})$$

for the total contribution to $N_{U_3,H}(B)$ from $\mathbf{y}$ satisfying

$$Y_1 \leqslant y_1 < 2Y_1, \quad Y_{i3} \leqslant |y_{i3}| < 2Y_{i3}, \quad Y_{i4} \leqslant |y_{i4}| < 2Y_{i4}. \tag{16}$$

Clearly it follows from the inequality $\Psi(\mathbf{y}) \leqslant B$ that $\mathcal{N} = 0$ unless

$$Y_{03}^2 Y_{04}^2 Y_{23} Y_{24} \ll B, \quad Y_1^2 Y_{13}^2 Y_{14}^2 Y_{23} Y_{24} \ll B, \tag{17}$$

and

$$Y_1 Y_{03} Y_{13}^2 Y_{23}^2 Y_{33} \ll B, \quad Y_1 Y_{04} Y_{14}^2 Y_{24}^2 Y_{34} \ll B. \tag{18}$$

In our estimation of $N_{U_3,H}(B)$, we may clearly assume without loss of generality that

$$Y_{03}Y_{13}^2Y_{23}^2Y_{33} \leqslant Y_{04}Y_{14}^2Y_{24}^2Y_{34}. \tag{19}$$

We proceed to show how the equation (12) forces certain constraints upon the choice of dyadic ranges in (16). There are three basic cases that can occur. Suppose first that

$$c_2Y_{03}Y_{04} \leqslant Y_1Y_{13}Y_{14}, \tag{20}$$

for an absolute constant $c_2 > 0$. Then it follows from (12) that

$$Y_{33}Y_{34} \ll Y_1Y_{13}Y_{14} \ll Y_{33}Y_{34}, \tag{21}$$

provided that c_2 is chosen to be sufficiently large. Next, we suppose that

$$c_1Y_{03}Y_{04} \geqslant Y_1Y_{13}Y_{14}, \tag{22}$$

for an absolute constant $c_1 > 0$. Then we may deduce from (12) that

$$Y_{33}Y_{34} \ll Y_{03}Y_{04} \ll Y_{33}Y_{34}, \tag{23}$$

provided that c_1 is chosen to be sufficiently small. Let us henceforth assume that the values of c_1, c_2 are fixed in such a way that (21) holds, if (20) holds, and (23) holds, if (22) holds. Finally we are left with the possibility that

$$c_1Y_{03}Y_{04} \leqslant Y_1Y_{13}Y_{14} \leqslant c_2Y_{03}Y_{04}. \tag{24}$$

We shall need to treat the cases (20), (22) and (24) separately.

We take $\mathbf{m}_{j,k} = (y_{j3}, y_{j4}, y_1, y_{13}, y_{14}, y_{k3}, y_{k4})$ in our application of Lemma 2, for $(j,k) = (0,3)$ and $(3,0)$. In particular the coprimality relation (15) follows from (12)–(14), and we may conclude that

$$\mathcal{N} \ll Y_1Y_{13}Y_{14}Y_{23}Y_{24}\min\{Y_{03}Y_{04}, Y_{33}Y_{34}\}, \tag{25}$$

on summing over all of the available y_{23}, y_{24}. It remains to sum this contribution over the various dyadic intervals Y_1, Y_{i3}, Y_{i4}. Suppose for the moment that we are interested in summing over all possible dyadic intervals $X \leqslant |x| < 2X$, for which $|x| \leqslant \mathcal{X}$. Then there are plainly $O(\log \mathcal{X})$ possible choices for X. In addition to this basic estimate, we shall make frequent use of the estimate $\sum_X X^\delta \ll_\delta \mathcal{X}^\delta$, for any $\delta > 0$.

We begin by assuming that (20) holds, so that (21) also holds. Then we may combine (19) with (21) in order to deduce that

$$Y_{13} \ll \min\left\{\frac{Y_{04}^{1/2}Y_{14}Y_{24}Y_{34}^{1/2}}{Y_{03}^{1/2}Y_{23}Y_{33}^{1/2}}, \frac{Y_{33}Y_{34}}{Y_1Y_{14}}\right\} \ll \frac{Y_{04}^{1/4}Y_{24}^{1/2}Y_{33}^{1/4}Y_{34}^{3/4}}{Y_1^{1/2}Y_{03}^{1/4}Y_{23}^{1/2}}.$$

We may now apply (25) to obtain

$$\begin{aligned}\sum_{\substack{Y_1,Y_{i3},Y_{i4}\\ (20)\text{ holds}}} \mathcal{N} &\ll \sum_{\substack{Y_1,Y_{i3},Y_{i4}\\ (20)\text{ holds}}} Y_1Y_{03}Y_{04}Y_{13}Y_{14}Y_{23}Y_{24}\\ &\ll \sum_{\substack{Y_{03},Y_{04},Y_{33},Y_{34}\\ Y_1,Y_{14},Y_{23},Y_{24}}} Y_1^{1/2}Y_{03}^{3/4}Y_{04}^{5/4}Y_{14}Y_{23}^{1/2}Y_{24}^{3/2}Y_{33}^{1/4}Y_{34}^{3/4}.\end{aligned}$$

But now (18) implies that $Y_{14} \ll B^{1/2}/(Y_1^{1/2}Y_{04}^{1/2}Y_{24}Y_{34}^{1/2})$, and (20) and (21) together imply that $Y_{03} \ll Y_{33}Y_{34}/Y_{04}$. We therefore deduce that

$$\sum_{\substack{Y_1,Y_{i3},Y_{i4}\\ \text{(20) holds}}} \mathcal{N} \ll B^{1/2} \sum_{\substack{Y_{03},Y_{04},Y_{33}\\ Y_1,Y_{23},Y_{24},Y_{34}}} Y_{03}^{3/4}Y_{04}^{3/4}Y_{23}^{1/2}Y_{24}^{1/2}Y_{33}^{1/4}Y_{34}^{1/4}$$
$$\ll B^{1/2} \sum_{\substack{Y_1,Y_{04},Y_{33}\\ Y_{23},Y_{24},Y_{34}}} Y_{23}^{1/2}Y_{24}^{1/2}Y_{33}Y_{34}.$$

Finally it follows from (17) and (21) that $Y_{33} \ll B^{1/2}/(Y_{23}^{1/2}Y_{24}^{1/2}Y_{34})$, whence

$$\sum_{\substack{Y_1,Y_{i3},Y_{i4}\\ \text{(20) holds}}} \mathcal{N} \ll B \sum_{Y_{04},Y_{13},Y_{14},Y_{23},Y_{34}} 1 \ll B(\log B)^5,$$

which is satisfactory for the theorem.

Next we suppose that (22) holds, so that (23) also holds. In this case it follows from (19), together with the inequality $Y_1Y_{13}Y_{14} \ll Y_{03}Y_{04}$, that

$$Y_{13} \ll \min\left\{\frac{Y_{04}^{1/2}Y_{14}Y_{24}Y_{34}^{1/2}}{Y_{03}^{1/2}Y_{23}Y_{33}^{1/2}}, \frac{Y_{03}Y_{04}}{Y_1Y_{14}}\right\} \ll \frac{Y_{03}^{1/4}Y_{04}^{3/4}Y_{24}^{1/2}Y_{34}^{1/4}}{Y_1^{1/2}Y_{23}^{1/2}Y_{33}^{1/4}}.$$

On combining this with the inequality $Y_{14} \ll B^{1/2}/(Y_1^{1/2}Y_{04}^{1/2}Y_{24}Y_{34}^{1/2})$, that follows from (18), we may therefore deduce from (25) that

$$\sum_{\substack{Y_1,Y_{i3},Y_{i4}\\ \text{(22) holds}}} \mathcal{N} \ll \sum_{\substack{Y_1,Y_{i3},Y_{i4}\\ \text{(22) holds}}} Y_1Y_{13}Y_{14}Y_{23}Y_{24}Y_{33}Y_{34}$$
$$\ll \sum_{\substack{Y_1,Y_{03},Y_{04},Y_{33}\\ Y_{14},Y_{23},Y_{24},Y_{34}}} Y_1^{1/2}Y_{03}^{1/4}Y_{04}^{3/4}Y_{14}Y_{23}^{1/2}Y_{24}^{3/2}Y_{33}^{3/4}Y_{34}^{5/4}$$
$$\ll B^{1/2} \sum_{\substack{Y_1,Y_{03},Y_{04}\\ Y_{23},Y_{24},Y_{33},Y_{34}}} Y_{03}^{1/4}Y_{04}^{1/4}Y_{23}^{1/2}Y_{24}^{1/2}Y_{33}^{3/4}Y_{34}^{3/4}.$$

Now it follows from (23) that $Y_{33} \ll Y_{03}Y_{04}/Y_{34}$. We may therefore combine this with the first inequality in (17) to conclude that

$$\sum_{\substack{Y_1,Y_{i3},Y_{i4}\\ \text{(22) holds}}} \mathcal{N} \ll B^{1/2} \sum_{\substack{Y_1,Y_{03},Y_{04}\\ Y_{23},Y_{24},Y_{34}}} Y_{03}Y_{04}Y_{23}^{1/2}Y_{24}^{1/2} \ll B(\log B)^5,$$

which is also satisfactory for the theorem.

Finally we suppose that (24) holds. On combining (19) with the fact that $Y_{33}Y_{34} \ll Y_{03}Y_{04}$, we obtain

$$Y_{33} \ll \min\left\{\frac{Y_{04}Y_{14}^2Y_{24}^2Y_{34}}{Y_{03}Y_{13}^2Y_{23}^2}, \frac{Y_{03}Y_{04}}{Y_{34}}\right\} \ll \frac{Y_{04}Y_{14}Y_{24}}{Y_{13}Y_{23}}.$$

Summing (25) over Y_{33} first, with $\min\{Y_{03}Y_{04}, Y_{33}Y_{34}\} \leqslant Y_{03}^{1/2}Y_{04}^{1/2}Y_{33}^{1/2}Y_{34}^{1/2}$, we therefore obtain

$$\sum_{\substack{Y_1,Y_{i3},Y_{i4}\\ \text{(24) holds}}} \mathcal{N} \ll \sum_{\substack{Y_1,Y_{03},Y_{04},Y_{13}\\ Y_{14},Y_{23},Y_{24},Y_{34}}} Y_1Y_{03}^{1/2}Y_{04}Y_{13}^{1/2}Y_{14}^{3/2}Y_{23}^{1/2}Y_{24}^{3/2}Y_{34}^{1/2}.$$

But then we may sum over Y_{03}, Y_{13} satisfying the inequalities in (17), and then Y_1 satisfying the second inequality in (18), in order to conclude that

$$\sum_{\substack{Y_1, Y_{i3}, Y_{i4} \\ (24) \text{ holds}}} \mathcal{N} \ll B^{1/4} \sum_{\substack{Y_1, Y_{04}, Y_{13} \\ Y_{14}, Y_{23}, Y_{24}, Y_{34}}} Y_1 Y_{04}^{1/2} Y_{13}^{1/2} Y_{14}^{3/2} Y_{23}^{1/4} Y_{24}^{5/4} Y_{34}^{1/2}$$

$$\ll B^{1/2} \sum_{\substack{Y_1, Y_{04}, Y_{14} \\ Y_{23}, Y_{24}, Y_{34}}} Y_1^{1/2} Y_{04}^{1/2} Y_{14} Y_{24} Y_{34}^{1/2} \ll B(\log B)^5.$$

This too is satisfactory for Theorem 3, and thereby completes its proof.

4. Open problems

We close this survey article with a list of five open problems relating to Manin's conjecture for del Pezzo surfaces. In order to encourage activity we have deliberately selected an array of very concrete problems.

(i) *Establish* (3) *for a non-singular del Pezzo surface of degree* 4.
The surface $x_0x_1 - x_2x_3 = x_0^2 + x_1^2 + x_2^2 - x_3^2 - 2x_4^2 = 0$ has Picard group of rank 5.

(ii) *Establish* (3) *for more singular cubic surfaces.*
Can one establish the Manin conjecture for a split singular cubic surface whose universal torsor has more than one equation? The Cayley cubic surface (8) is such a surface.

(iii) *Break the* 4/3*-barrier for a non-singular cubic surface.*
We have yet to prove an upper bound of the shape $N_{U,H}(B) = O_S(B^\theta)$, with $\theta < 4/3$, for a single non-singular cubic surface $S \subset \mathbb{P}^3$. This seems to be hardest when the surface doesn't have a conic bundle structure over $\mathbb{Q}$. The surface $x_0x_1(x_0 + x_1) = x_2x_3(x_2 + x_3)$ admits such a structure; can one break the 4/3-barrier for this example?

(iv) *Establish the lower bound* $N_{U,H}(B) \gg B(\log B)^3$ *for the Fermat cubic.*
The Fermat cubic $x_0^3 + x_1^3 = x_2^3 + x_3^3$ has Picard group of rank 4.

(v) *Better bounds for del Pezzo surfaces of degree* 2.
Non-singular del Pezzo surfaces of degree 2 take the shape

$$t^2 = F(x_0, x_1, x_2),$$

for a non-singular quartic form F. Let $N(F;B)$ denote the number of integers t, x_0, x_1, x_2 such that $t^2 = F(\mathbf{x})$ and $|\mathbf{x}| \leqslant B$. Can one prove that we always have $N(F;B) = O_{\varepsilon,F}(B^{2+\varepsilon})$? Such an estimate would be essentially best possible, as consideration of the form $F_0(\mathbf{x}) = x_0^4 + x_1^4 - x_2^4$ shows. The best result in this direction is due to Broberg [**Bro03a**], who has established the weaker bound $N(F;B) = O_{\varepsilon,F}(B^{9/4+\varepsilon})$. For certain quartic forms, such as $F_1(\mathbf{x}) = x_0^4 + x_1^4 + x_2^4$, the Manin conjecture implies that one ought to be able to replace the exponent $2+\varepsilon$ by $1+\varepsilon$. Can one prove that $N(F_1;B) = O(B^\theta)$ for some $\theta < 2$?

Acknowledgements. The author is extremely grateful to Professors de la Bretèche and Salberger, who have both made several useful comments about an earlier version of this paper. It is also a pleasure to thank the anonymous referee for his careful reading of the manuscript.

References

[BM90] V. V. Batyrev & Y. I. Manin – "Sur le nombre des points rationnels de hauteur borné des variétés algébriques", *Math. Ann.* **286** (1990), no. 1-3, p. 27–43.

[Bro03a] N. Broberg – "Rational points on finite covers of $\mathbb{P}^1$ and $\mathbb{P}^2$", *J. Number Theory* **101** (2003), no. 1, p. 195–207.

[Bro03b] T. D. Browning – "Counting rational points on del Pezzo surfaces of degree five", in *Proceedings of the Session in Analytic Number Theory and Diophantine Equations* (Bonn), Bonner Math. Schriften, vol. 360, Univ. Bonn, 2003, 22 pages.

[Bro06] ———, "The density of rational points on a certain singular cubic surface", *J. Number Theory* **119** (2006), p. 242–283.

[BT98a] V. V. Batyrev & Y. Tschinkel – "Manin's conjecture for toric varieties", *J. Algebraic Geom.* **7** (1998), no. 1, p. 15–53.

[BT98b] ———, "Tamagawa numbers of polarized algebraic varieties", *Astérisque* (1998), no. 251, p. 299–340, Nombre et répartition de points de hauteur bornée (Paris, 1996).

[BW79] J. W. Bruce & C. T. C. Wall – "On the classification of cubic surfaces", *J. London Math. Soc. (2)* **19** (1979), no. 2, p. 245–256.

[Cay69] A. Cayley – "A memoir on cubic surfaces", *Phil. Trans. Roy. Soc.* **159** (1869), p. 231–326.

[CLT02] A. Chambert-Loir & Y. Tschinkel – "On the distribution of points of bounded height on equivariant compactifications of vector groups", *Invent. Math.* **148** (2002), no. 2, p. 421–452.

[CT88] D. F. Coray & M. A. Tsfasman – "Arithmetic on singular Del Pezzo surfaces", *Proc. London Math. Soc. (3)* **57** (1988), no. 1, p. 25–87.

[CTS76] J.-L. Colliot-Thélène & J.-J. Sansuc – "Torseurs sous des groupes de type multiplicatif; applications à l'étude des points rationnels de certaines variétés algébriques", *C. R. Acad. Sci. Paris Sér. A-B* **282** (1976), no. 18, p. Aii, A1113–A1116.

[CTS87] ———, "La descente sur les variétés rationnelles. II", *Duke Math. J.* **54** (1987), no. 2, p. 375–492.

[Dav05] H. Davenport – *Analytic methods for Diophantine equations and Diophantine inequalities*, second ed., Cambridge Mathematical Library, Cambridge University Press, Cambridge, 2005, With a foreword by R. C. Vaughan, D. R. Heath-Brown and D. E. Freeman, Edited and prepared for publication by T. D. Browning.

[dlB98] R. de la Bretèche – "Sur le nombre de points de hauteur bornée d'une certaine surface cubique singulière", *Astérisque* (1998), no. 251, p. 51–77, Nombre et répartition de points de hauteur bornée (Paris, 1996).

[dlB01] ———, "Compter des points d'une variété torique", *J. Number Theory* **87** (2001), no. 2, p. 315–331.

[dlB02] ———, "Nombre de points de hauteur bornée sur les surfaces de del Pezzo de degré 5", *Duke Math. J.* **113** (2002), no. 3, p. 421–464.

[dlBBa] R. de la Bretèche & T. Browning – "On Manin's conjecture for singular del Pezzo surfaces of degree four, I", *Michigan Math. J.*, to appear.

[dlBBb] ———, "On Manin's conjecture for singular del Pezzo surfaces of degree four, II", *Math. Proc. Camb. Phil. Soc.*, to appear.

[dlBBD] R. de la Bretèche, T. D. Browning & U. Derenthal – "On Manin's conjecture for a certain singular cubic surface", *Ann. Sci. École Norm. Sup.*, to appear.

[dlBF04] R. de la Bretèche & É. Fouvry – "L'éclaté du plan projectif en quatre points dont deux conjugués", *J. Reine Angew. Math.* **576** (2004), p. 63–122.

[dlBSD] R. de la Bretèche & P. Swinnerton-Dyer – "Fonction zêta des hauteurs associée à une certaine surface cubique", *submitted*, 2005.

[FMT89] J. Franke, Y. I. Manin & Y. Tschinkel – "Rational points of bounded height on Fano varieties", *Invent. Math.* **95** (1989), no. 2, p. 421–435.

[Fou98] É. Fouvry – "Sur la hauteur des points d'une certaine surface cubique singulière", *Astérisque* (1998), no. 251, p. 31–49, Nombre et répartition de points de hauteur bornée (Paris, 1996).

[HB97] D. R. Heath-Brown – "The density of rational points on cubic surfaces", *Acta Arith.* **79** (1997), no. 1, p. 17–30.

[HB02] ———, "The density of rational points on curves and surfaces", *Ann. of Math. (2)* **155** (2002), no. 2, p. 553–595.

[HB03] ———, "The density of rational points on Cayley's cubic surface", in *Proceedings of the Session in Analytic Number Theory and Diophantine Equations* (Bonn), Bonner Math. Schriften, vol. 360, Univ. Bonn, 2003, 33 pages.

[HBM99] D. R. Heath-Brown & B. Z. Moroz – "The density of rational points on the cubic surface $X_0^3 = X_1X_2X_3$", *Math. Proc. Cambridge Philos. Soc.* **125** (1999), no. 3, p. 385–395.

[HP52] W. V. D. Hodge & D. Pedoe – *Methods of algebraic geometry. Vol. II. Book III: General theory of algebraic varieties in projective space. Book IV: Quadrics and Grassmann varieties*, Cambridge University Press, 1952.

[HT04] B. Hassett & Y. Tschinkel – "Universal torsors and Cox rings", in *Arithmetic of higher-dimensional algebraic varieties (Palo Alto, CA, 2002)*, Progr. Math., vol. 226, Birkhäuser Boston, Boston, MA, 2004, p. 149–173.

[Lip69] J. Lipman – "Rational singularities, with applications to algebraic surfaces and unique factorization", *Inst. Hautes Études Sci. Publ. Math.* (1969), no. 36, p. 195–279.

[Man86] Y. I. Manin – *Cubic forms*, second ed., North-Holland Mathematical Library, vol. 4, North-Holland Publishing Co., Amsterdam, 1986.

[Pey95] E. Peyre – "Hauteurs et mesures de Tamagawa sur les variétés de Fano", *Duke Math. J.* **79** (1995), no. 1, p. 101–218.

[Pey04] ———, "Counting points on varieties using universal torsors", in *Arithmetic of higher-dimensional algebraic varieties (Palo Alto, CA, 2002)*, Progr. Math., vol. 226, Birkhäuser Boston, Boston, MA, 2004, p. 61–81.

[PT01a] E. Peyre & Y. Tschinkel – "Tamagawa numbers of diagonal cubic surfaces, numerical evidence", *Math. Comp.* **70** (2001), no. 233, p. 367–387.

[PT01b] ———, "Tamagawa numbers of diagonal cubic surfaces of higher rank", in *Rational points on algebraic varieties*, Progr. Math., vol. 199, Birkhäuser, Basel, 2001, p. 275–305.

[Sal98] P. Salberger – "Tamagawa measures on universal torsors and points of bounded height on Fano varieties", *Astérisque* (1998), no. 251, p. 91–258, Nombre et répartition de points de hauteur bornée (Paris, 1996).

[Sch64] L. Schläfli – "On the distribution of surfaces of the third order into species", *Phil. Trans. Roy. Soc.* **153** (1864), p. 193–247.

[SD04] P. Swinnerton-Dyer – "Diophantine equations: progress and problems", in *Arithmetic of higher-dimensional algebraic varieties (Palo Alto, CA, 2002)*, Progr. Math., vol. 226, Birkhäuser Boston, Boston, MA, 2004, p. 3–35.

[SD05] ———, "Counting points on cubic surfaces. II", in *Geometric methods in algebra and number theory*, Progr. Math., vol. 235, Birkhäuser Boston, Boston, MA, 2005, p. 303–309.

[Sko93] A. N. Skorobogatov – "On a theorem of Enriques-Swinnerton-Dyer", *Ann. Fac. Sci. Toulouse Math. (6)* **2** (1993), no. 3, p. 429–440.

[SSD98] J. B. Slater & P. Swinnerton-Dyer – "Counting points on cubic surfaces. I", *Astérisque* (1998), no. 251, p. 1–12, Nombre et répartition de points de hauteur bornée (Paris, 1996).

[Tsc02] Y. Tschinkel – "Lectures on height zeta functions of toric varieties", in *Geometry of toric varieties*, Sémin. Congr., vol. 6, Soc. Math. France, Paris, 2002, p. 227–247.

[Tsc03] ———, "Fujita's program and rational points", in *Higher dimensional varieties and rational points (Budapest, 2001)*, Bolyai Soc. Math. Stud., vol. 12, Springer, Berlin, 2003, p. 283–310.

[Wal80] C. T. C. Wall – "The first canonical stratum", *J. London Math. Soc. (2)* **21** (1980), no. 3, p. 419–433.

School of Mathematics, University of Bristol, Bristol BS8 1TW, UK
E-mail address: t.d.browning@bristol.ac.uk

Clay Mathematics Proceedings
Volume 7, 2007

The density of integral solutions for pairs of diagonal cubic equations

Jörg Brüdern and Trevor D. Wooley

Abstract. We investigate the number of integral solutions possessed by a pair of diagonal cubic equations in a large box. Provided that the number of variables in the system is at least thirteen, and in addition the number of variables in any non-trivial linear combination of the underlying forms is at least seven, we obtain a lower bound for the order of magnitude of the number of integral solutions consistent with the product of local densities associated with the system.

1. Introduction

This paper is concerned with the solubility in integers of the equations

$$a_1x_1^3 + a_2x_2^3 + \ldots + a_sx_s^3 = b_1x_1^3 + b_2x_2^3 + \ldots + b_sx_s^3 = 0, \tag{1.1}$$

where $(a_i, b_i) \in \mathbb{Z}^2\setminus\{\mathbf{0}\}$ are fixed coefficients. It is natural to enquire to what extent the Hasse principle holds for such systems of equations. Cook [**C85**], refining earlier work of Davenport and Lewis [**DL66**], has analysed the local solubility problem with great care. He showed that when $s \geq 13$ and p is a prime number with $p \neq 7$, then the system (1.1) necessarily possesses a non-trivial solution in $\mathbb{Q}_p$. Here, by *non-trivial solution*, we mean any solution that differs from the obvious one in which $x_j = 0$ for $1 \leq j \leq s$. No such conclusion can be valid for $s \leq 12$, for there may then be local obstructions for any given set of primes p with $p \equiv 1 \pmod 3$; see [**BW06**] for an example that illuminates this observation. The 7-adic case, moreover, is decidedly different. For $s \leq 15$ there may be 7-adic obstructions to the solubility of the system (1.1), and so it is only when $s \geq 16$ that the existence of non-trivial solutions in $\mathbb{Q}_7$ is assured. This much was known to Davenport and Lewis [**DL66**].

Were the Hasse principle to hold for systems of the shape (1.1), then in view of the above discussion concerning the local solubility problem, the existence of

2000 *Mathematics Subject Classification.* Primary 11D72, Secondary 11L07, 11E76, 11P55.
Key words and phrases. Diophantine equations, exponential sums, Hardy-Littlewood method.
First author supported in part by NSF grant DMS-010440. The authors are grateful to the Max Planck Institut in Bonn for its generous hospitality during the period in which this paper was conceived.

integer solutions to the equations (1.1) would be decided in $\mathbb{Q}_7$ alone whenever $s \geq 13$. Under the more stringent hypothesis $s \geq 14$, this was confirmed by the first author [**B90**], building upon the efforts of Davenport and Lewis [**DL66**], Cook [**C72**], Vaughan [**V77**] and Baker and Brüdern [**BB88**] spanning an interval of more than twenty years. In a recent collaboration [**BW06**] we have been able to add the elusive case $s = 13$, and may therefore enunciate the following conclusion.

THEOREM 1. *Suppose that* $s \geq 13$. *Then for any choice of coefficients* $(a_j, b_j) \in \mathbb{Z}^2 \setminus \{\mathbf{0}\}$ $(1 \leq j \leq s)$, *the simultaneous equations* (1.1) *possess a non-trivial solution in rational integers if and only if they admit a non-trivial solution in* $\mathbb{Q}_7$.

Now let $\mathcal{N}_s(P)$ denote the number of solutions of the system (1.1) in rational integers $x_1, \ldots, x_s$ satisfying the condition $|x_j| \leq P$ $(1 \leq j \leq s)$. When s is large, a naïve application of the philosophy underlying the circle method suggests that $\mathcal{N}_s(P)$ should be of order P^{s-6} in size, but in certain cases this may be false even in the absence of local obstructions. This phenomenon is explained by the failure of the Hasse principle for certain diagonal cubic forms in four variables. When $s \geq 10$ and $b_1, \ldots, b_s \in \mathbb{Z} \setminus \{0\}$, for example, the simultaneous equations

$$5x_1^3 + 9x_2^3 + 10x_3^3 + 12x_4^3 = b_1x_1^3 + b_2x_2^3 + \ldots + b_sx_s^3 = 0 \tag{1.2}$$

have non-trivial (and non-singular) solutions in every p-adic field $\mathbb{Q}_p$ as well as in $\mathbb{R}$, yet all solutions in rational integers must satisfy the condition $x_i = 0$ $(1 \leq i \leq 4)$. The latter must hold, in fact, independently of the number of variables. For such examples, therefore, one has $\mathcal{N}_s(P) = o(P^{s-6})$ when $s \geq 9$, whilst for $s \geq 12$ one may show that $\mathcal{N}_s(P)$ is of order P^{s-7}. For more details, we refer the reader to the discussion surrounding equation (1.2) of [**BW06**]. This example also shows that weak approximation may fail for the system (1.1), even when s is large.

In order to measure the extent to which a system (1.1) may resemble the pathological example (1.2), we introduce the number q_0, which we define by

$$q_0 = \min_{(c,d) \in \mathbb{Z}^2 \setminus \{\mathbf{0}\}} \operatorname{card}\{1 \leq j \leq s : ca_j + db_j \neq 0\}.$$

This important invariant of the system (1.1) has the property that as q_0 becomes larger, the counting function $\mathcal{N}_s(P)$ behaves more tamely. Note that in the example (1.2) discussed above one has $q_0 = 4$ whenever $s \geq 8$.

THEOREM 2. *Suppose that* $s \geq 13$, *and that* $(a_j, b_j) \in \mathbb{Z}^2 \setminus \{\mathbf{0}\}$ $(1 \leq j \leq s)$ *satisfy the condition that the system* (1.1) *admits a non-trivial solution in* $\mathbb{Q}_7$. *Then whenever* $q_0 \geq 7$, *one has* $\mathcal{N}_s(P) \gg P^{s-6}$.

The conclusion of Theorem 2 was obtained in our recent paper [**BW06**] for all cases wherein $q_0 \geq s - 5$. This much suffices to establish Theorem 1; see §8 of [**BW06**] for an account of this deduction. Our main objective in this paper is a detailed discussion of the cases with $7 \leq q_0 \leq s - 6$. We remark that the arguments of this paper as well as those in [**BW06**] extend to establish weak approximation for the system (1.1) when $s \geq 13$ and $q_0 \geq 7$. In the special cases in which $s = 13$ and q_0 is equal to either 5 or 6, a conditional proof of weak approximation is possible by invoking recent work of Swinnerton-Dyer [**SD01**], subject to the as yet unproven finiteness of the Tate-Shafarevich group for elliptic curves over quadratic fields. Indeed, equipped with the latter conclusion, for these particular values of q_0 one may relax the condition on s beyond that addressed by Theorem 2. When $s = 13$

and $q_0 \leq 4$, on the other hand, weak approximation fails in general, as we have already seen in the discussion accompanying the system (1.2).

The critical input into the proof of Theorem 2 is a certain arithmetic variant of Bessel's inequality established in [**BW06**]. We begin in §2 by briefly sketching the principal ideas underlying this innovation. In §3 we prepare the ground for an application of the Hardy-Littlewood method, deriving a lower bound for the major arc contribution in the problem at hand. Some delicate footwork in §4 establishes a mean value estimate that, in all circumstances save for particularly pathological situations, leads in §5 to a viable complementary minor arc estimate sufficient to establish Theorem 2. The latter elusive situations are handled in §6 via an argument motivated by our recent collaboration [**BKW01a**] with Kawada, and thereby we complete the proof of Theorem 2. Finally, in §7, we make some remarks concerning the extent to which our methods are applicable to systems containing fewer than 13 variables.

Throughout, the letter ε will denote a sufficiently small positive number. We use $\ll$ and $\gg$ to denote Vinogradov's well-known notation, implicit constants depending at most on ε, unless otherwise indicated. In an effort to simplify our analysis, we adopt the convention that whenever ε appears in a statement, then we are implicitly asserting that for each $\varepsilon > 0$ the statement holds for sufficiently large values of the main parameter. Note that the "value" of ε may consequently change from statement to statement, and hence also the dependence of implicit constants on ε. Finally, from time to time we make use of vector notation in order to save space. Thus, for example, we may abbreviate $(c_1, \ldots, c_t)$ to $\mathbf{c}$.

2. An arithmetic variant of Bessel's inequality

The major innovation in our earlier paper [**BW06**] is an arithmetic variant of Bessel's inequality that sometimes provides good mean square estimates for Fourier coefficients averaged over sparse sequences. Since this tool plays a crucial role also in our current excursion, we briefly sketch the principal ideas. When P and R are real numbers with $1 \leq R \leq P$, we define the set of smooth numbers $\mathcal{A}(P, R)$ by

$$\mathcal{A}(P, R) = \{n \in \mathbb{N} \cap [1, P] \,:\, p \text{ prime and } p|n \Rightarrow p \leq R\}.$$

The Fourier coefficients that are to be averaged arise in connection with the smooth cubic Weyl sum $h(\alpha) = h(\alpha; P, R)$, defined by

$$h(\alpha; P, R) = \sum_{x \in \mathcal{A}(P,R)} e(\alpha x^3), \tag{2.1}$$

where here and later we write $e(z)$ for $\exp(2\pi i z)$. The sixth moment of this sum has played an important role in many applications in recent years, and that at hand is no exception to the rule. Write $\xi = (\sqrt{2833} - 43)/41$. Then as a consequence of the work of the second author [**W00**], given any positive number ε, there exists a positive number $\eta = \eta(\varepsilon)$ with the property that whenever $1 \leq R \leq P^\eta$, one has

$$\int_0^1 |h(\alpha; P, R)|^6 \, d\alpha \ll P^{3+\xi+\varepsilon}. \tag{2.2}$$

We assume henceforth that whenever R appears in a statement, either implicitly or explicitly, then $1 \leq R \leq P^\eta$ with η a positive number sufficiently small in the context of the upper bound (2.2).

The Fourier coefficients over which we intend to average are now defined by

$$\psi(n)=\int_0^1 |h(\alpha)|^5 e(-n\alpha)\,d\alpha. \tag{2.3}$$

An application of Parseval's identity in combination with conventional circle method technology readily shows that $\sum_n \psi(n)^2$ is of order P^7. Rather than average $\psi(n)$ in mean square over all integers, we instead restrict to the sparse sequence consisting of differences of two cubes, and establish the bound

$$\sum_{1\le x,y\le P} \psi(x^3-y^3)^2 \ll P^{6+\xi+4\varepsilon}. \tag{2.4}$$

Certain contributions to the sum on the left hand side of (2.4) are easily estimated. By Hua's Lemma (see Lemma 2.5 of [**V97**]) and a consideration of the underlying Diophantine equations, one has

$$\int_0^1 |h(\alpha)|^4\,d\alpha \ll P^{2+\varepsilon}.$$

On applying Schwarz's inequality to (2.3), we therefore deduce from (2.2) that the estimate $\psi(n)=O(P^{5/2+\xi/2+\varepsilon})$ holds uniformly in n. We apply this upper bound with $n=0$ in order to show that the terms with $x=y$ contribute at most $O(P^{6+\xi+2\varepsilon})$ to the left hand side of (2.4). The integers x and y with $1\le x,y\le P$ and $|\psi(x^3-y^3)|\le P^{2+\xi/2+2\varepsilon}$ likewise contribute at most $O(P^{6+\xi+4\varepsilon})$ within the summation of (2.4). We estimate the contribution of the remaining Fourier coefficients by dividing into dyadic intervals. When T is a real number with

$$P^{2+\xi/2+2\varepsilon}\le T\le P^{5/2+\xi/2+2\varepsilon}, \tag{2.5}$$

define $\mathcal{Z}(T)$ to be the set of ordered pairs $(x,y)\in\mathbb{N}^2$ with

$$1\le x,y\le P,\quad x\ne y\quad \text{and}\quad T\le|\psi(x^3-y^3)|\le 2T, \tag{2.6}$$

and write $Z(T)$ for $\mathrm{card}(\mathcal{Z}(T))$. Then on incorporating in addition the contributions of those terms already estimated, a familiar dissection argument now demonstrates that there is a number T satisfying (2.5) for which

$$\sum_{1\le x,y\le P} \psi(x^3-y^3)^2 \ll P^{6+\xi+4\varepsilon}+P^{\varepsilon}T^2Z(T). \tag{2.7}$$

An upper bound for $Z(T)$ at this point being all that is required to complete the proof of the estimate (2.4), we set up a mechanism for deriving such an upper bound that has its origins in work of Brüdern, Kawada and Wooley [**BKW01a**] and Wooley [**W02**]. Let $\sigma(n)$ denote the sign of the real number $\psi(n)$ defined in (2.3), with the convention that $\sigma(n)=0$ when $\psi(n)=0$, so that $\psi(n)=\sigma(n)|\psi(n)|$. Then on forming the exponential sum

$$K_T(\alpha)=\sum_{(x,y)\in\mathcal{Z}(T)} \sigma(x^3-y^3)e(\alpha(y^3-x^3)),$$

we find from (2.3) and (2.6) that

$$\int_0^1 |h(\alpha)|^5 K_T(\alpha)\,d\alpha \ge TZ(T).$$

An application of Schwarz's inequality in combination with the upper bound (2.2) therefore permits us to infer that

$$TZ(T) \ll (P^{3+\xi+\varepsilon})^{1/2}\Big(\int_0^1 |h(\alpha)^4 K_T(\alpha)^2| d\alpha\Big)^{1/2}. \tag{2.8}$$

Next, on applying Weyl's differencing lemma (see, for example, Lemma 2.3 of [**V97**]), one finds that for certain non-negative numbers t_l, satisfying $t_l = O(P^\varepsilon)$ for $0 < |l| \le P^3$, one has

$$|h(\alpha)|^4 \ll P^3 + P \sum_{0<|l|\le P^3} t_l e(\alpha l).$$

Consequently, by orthogonality,

$$\begin{aligned}\int_0^1 |h(\alpha)^4 K_T(\alpha)^2|\, d\alpha &\ll P^3 \int_0^1 |K_T(\alpha)|^2 d\alpha + P^{1+\varepsilon} K_T(0)^2 \\ &\ll P^\varepsilon (P^3 Z(T) + PZ(T)^2).\end{aligned}$$

Here we have applied the simple fact that when m is a non-zero integer, the number of solutions of the Diophantine equation $m = x^3 - y^3$ with $1 \le x, y \le P$ is at most $O(P^\varepsilon)$. Since $T \ge P^{2+\xi/2+2\varepsilon}$, the upper bound $Z(T) = O(T^{-2}P^{6+\xi+2\varepsilon})$ now follows from the relation (2.8). On substituting the latter estimate into (2.7), the desired conclusion (2.4) is now immediate.

Note that in the summation on the left hand side of the estimate (2.4), one may restrict the summation over the integers x and y to any subset of $[1, P]^2$ without affecting the right hand side. Thus, on recalling the definition (2.3), we see that we have proved the special case $a = b = c = d = 1$ of the following lemma.

LEMMA 3. *Let a, b, c, d denote non-zero integers. Then for any subset $\mathcal{B}$ of $[1, P] \cap \mathbb{Z}$, one has*

$$\int_0^1\int_0^1 |h(a\alpha)h(b\beta)|^5 \Big|\sum_{x\in\mathcal{B}} e((c\alpha + d\beta)x^3)\Big|^2 d\alpha\, d\beta \ll P^{6+\xi+\varepsilon}.$$

This lemma is a restatement of Theorem 3 of [**BW06**]. It transpires that no great difficulty is encountered when incorporating the coefficients a, b, c, d into the argument described above; see §3 of [**BW06**].

We apply Lemma 3 in the cosmetically more general formulation provided by the following lemma.

LEMMA 4. *Suppose that c_i, d_i $(1 \le i \le 3)$ are integers satisfying the condition*

$$(c_1d_2 - c_2d_1)(c_1d_3 - c_3d_1)(c_2d_3 - c_3d_2) \ne 0.$$

Write $\lambda_j = c_j\alpha + d_j\beta$ $(j = 1, 2, 3)$. Then for any subset $\mathcal{B}$ of $[1, P] \cap \mathbb{Z}$, one has

$$\int_0^1\int_0^1 |h(\lambda_1)h(\lambda_2)|^5 \Big|\sum_{x\in\mathcal{B}} e(\lambda_3 x^3)\Big|^2 d\alpha\, d\beta \ll P^{6+\xi+\varepsilon}.$$

PROOF. The desired conclusion follows immediately from Lemma 3 on making a change of variable. The reader may care to compare the situation here with that occurring in the estimation of the integral J_3 in the proof of Theorem 4 of [**BW06**] (see §4 of the latter). ☐

3. Preparation for the circle method

The next three sections of this paper are devoted to the proof of Theorem 2. In view of the hypotheses of the theorem together with the discussion following its statement, we may suppose henceforth that $s \geq 13$ and $7 \leq q_0 \leq s-6$. With the pairs $(a_j, b_j) \in \mathbb{Z}^2 \setminus \{\mathbf{0}\}$ $(1 \leq j \leq s)$, we associate both the linear forms

$$\Lambda_j = a_j\alpha + b_j\beta \quad (1 \leq j \leq s), \tag{3.1}$$

and the two linear forms $L_1(\boldsymbol{\theta})$ and $L_2(\boldsymbol{\theta})$ defined for $\boldsymbol{\theta} \in \mathbb{R}^s$ by

$$L_1(\boldsymbol{\theta}) = \sum_{j=1}^{s} a_j\theta_j \quad \text{and} \quad L_2(\boldsymbol{\theta}) = \sum_{j=1}^{s} b_j\theta_j. \tag{3.2}$$

We say that two forms Λ_i and Λ_j are *equivalent* when there exists a non-zero rational number λ with $\Lambda_i = \lambda\Lambda_j$. This notion defines an equivalence relation on the set $\{\Lambda_1, \Lambda_2, \ldots, \Lambda_s\}$, and we refer to the number of elements in the equivalence class $[\Lambda_j]$ containing the form Λ_j as its *multiplicity.* Suppose that the s forms Λ_j $(1 \leq j \leq s)$ fall into T equivalence classes, and that the multiplicities of the representatives of these classes are $R_1, \ldots, R_T$. By relabelling variables if necessary, there is no loss in supposing that $R_1 \geq R_2 \geq \ldots \geq R_T \geq 1$. Further, by our hypothesis that $7 \leq q_0 \leq s-6$, it is apparent that for any pair $(c,d) \in \mathbb{Z}^2 \setminus \{\mathbf{0}\}$, the linear form $cL_1(\boldsymbol{\theta}) + dL_2(\boldsymbol{\theta})$ necessarily possesses at least 7 non-zero coefficients, and for some choice $(c,d) \in \mathbb{Z}^2 \setminus \{\mathbf{0}\}$ this linear form has at most $s-6$ non-zero coefficients. Thus we may assume without loss of generality that $6 \leq R_1 \leq s-7$.

We distinguish three cases according to the number of variables and the arrangement of the multiplicities of the forms. We refer to a system (1.1) as being of type I when $T = 2$, as being of type II when $T = 3$ and $R_3 = 1$, and as being of type III in the remaining cases wherein $T \geq 3$ and $s - R_1 - R_2 \geq 2$. The argument required to address the systems of types I and II is entirely different from that required for those of type III, and we defer an account of these former situations to §6 below. Our purpose in the remainder of §3 together with §§4 and 5 is to establish the conclusion of Theorem 2 for type III systems.

Consider then a type III system (1.1) with $s \geq 13$ and $7 \leq q_0 \leq s-6$, and consider a fixed subset $\mathcal{S}$ of $\{1, \ldots, s\}$ with $\mathrm{card}(\mathcal{S}) = 13$. We may suppose that the 13 forms Λ_j $(j \in \mathcal{S})$ fall into t equivalence classes, and that the multiplicities of the representatives of these classes are $r_1, \ldots, r_t$. By relabelling variables if necessary, there is no loss in supposing that $r_1 \geq r_2 \geq \ldots \geq r_t \geq 1$. The condition $R_1 \leq s-7$ ensures that $R_2 + R_3 + \cdots + R_T \geq 7$. Thus, on recalling the additional conditions $s \geq 13$, $T \geq 3$, $R_1 \geq 6$ and $s - R_1 - R_2 \geq 2$, it is apparent that we may make a choice for $\mathcal{S}$ in such a manner that $t \geq 3$, $r_1 = 6$ and $13 - r_1 - r_2 \geq 2$. We may therefore suppose that the profile of multiplicities $(r_1, r_2, \ldots, r_t)$ satisfies $t \geq 3$, $r_1 = 6$, $r_2 \leq 5$ and $r_2 + r_3 + \cdots + r_t = 7$. But then, in view of our earlier condition $r_1 \geq r_2 \geq \ldots \geq r_t \geq 1$, we find that necessarily $r_t \leq 3$. We now relabel variables in the system (1.1), and likewise in (3.1) and (3.2), so that the set $\mathcal{S}$ becomes $\{1, 2, \ldots, 13\}$, and so that Λ_1 becomes a form in the first equivalence class counted by r_1, so that Λ_2 becomes a form in the second equivalence class counted by r_2, and Λ_{13} becomes a form in the tth equivalence class counted by r_t.

We next make some simplifying transformations that ease the analysis of the singular integral, and here we follow the pattern of our earlier work [**BW06**]. First, by taking suitable integral linear combinations of the equations (1.1), we may suppose without loss that

$$b_1 = a_2 = 0 \quad \text{and} \quad b_i = 0 \qquad (8 \le i \le 12). \tag{3.3}$$

Since we may suppose that $a_1 b_2 \neq 0$, the simultaneous equations

$$L_1(\boldsymbol{\theta}) = L_2(\boldsymbol{\theta}) = 0 \tag{3.4}$$

possess a solution $\boldsymbol{\theta}$ with $\theta_j \neq 0$ $(1 \le j \le s)$. Applying the substitution $x_j \to -x_j$ for those indices j with $1 \le j \le s$ for which $\theta_j < 0$, neither the solubility of the system (1.1), nor the corresponding function $\mathcal{N}_s(P)$, are affected, yet the transformed linear system associated with (3.4) has a solution $\boldsymbol{\theta}$ with $\theta_j > 0$ $(1 \le j \le s)$. In addition, the homogeneity of the system (3.4) ensures that a solution of the latter type may be chosen with $\boldsymbol{\theta} \in (0,1)^s$. We now fix this solution $\boldsymbol{\theta}$, and fix also ε to be a sufficiently small positive number, and η to be a positive number sufficiently small in the context of Lemmata 3 and 4 with the property that $\boldsymbol{\theta} \in (\eta, 1)^s$.

At this point we are ready to define the generating functions required in our application of the circle method. In addition to the smooth Weyl sum $h(\alpha)$ defined in (2.1) we require also the classical Weyl sum

$$g(\alpha) = \sum_{\eta P < x \le P} e(\alpha x^3).$$

On defining the generating functions

$$H(\alpha, \beta) = \prod_{j=2}^{12} h(\Lambda_j) \quad \text{and} \quad G(\alpha, \beta) = \prod_{j=13}^{s} g(\Lambda_j), \tag{3.5}$$

we now see from orthogonality that

$$\mathcal{N}_s(P) \ge \int_0^1 \int_0^1 g(\Lambda_1) H(\alpha, \beta) G(\alpha, \beta) \, d\alpha \, d\beta. \tag{3.6}$$

We apply the circle method to obtain a lower bound for the integral on the right hand side of (3.6). In this context, we put $Q = (\log P)^{1/100}$, and when $a, b \in \mathbb{Z}$ and $q \in \mathbb{N}$, we write

$$\mathfrak{N}(q, a, b) = \{(\alpha, \beta) \in [0,1)^2 \,:\, |\alpha - a/q| \le QP^{-3} \text{ and } |\beta - b/q| \le QP^{-3}\}.$$

We then define the major arcs $\mathfrak{N}$ of our Hardy-Littlewood dissection to be the union of the sets $\mathfrak{N}(q, a, b)$ with $0 \le a, b \le q \le Q$ and $(q, a, b) = 1$. The corresponding set $\mathfrak{n}$ of minor arcs are defined by $\mathfrak{n} = [0,1)^2 \setminus \mathfrak{N}$.

It transpires that the contribution of the major arcs within the integral on the right hand side of (3.6) is easily estimated by making use of the work from our previous paper [**BW06**].

LEMMA 5. *Suppose that the system* (1.1) *is of type III with* $s \ge 13$ *and* $7 \le q_0 \le s - 6$, *and possesses a non-trivial* 7*-adic solution. Then, in the setting described in the prequel, one has*

$$\iint_{\mathfrak{N}} g(\Lambda_1) H(\alpha, \beta) G(\alpha, \beta) \, d\alpha \, d\beta \gg P^{s-6}.$$

Proof. Although the formulation of the statements of Lemmata 12 and 13 of [**BW06**] may appear more restrictive than our present circumstances permit, an examination of their proofs will confirm that it is sufficient in fact that the maximum multiplicity of any of $\Lambda_1, \Lambda_2, \dots, \Lambda_{13}$ is at most six amongst the latter forms. Such follows already from the hypotheses of the lemma at hand, and thus the desired conclusion follows in all essentials from the estimate (7.8) of [**BW06**] together with the conclusions of Lemmata 12 and 13 of the latter paper. Note that in [**BW06**] the generating functions employed differ slightly from those herein, in that the exponential sums corresponding to the forms $\Lambda_{13}, \dots, \Lambda_s$ are smooth Weyl sums rather than the present classical Weyl sums. This deviation, however, demands at most cosmetic alterations to the argument of §7 of [**BW06**], and we spare the reader the details. It should be remarked, though, that it is the reference to Lemma 13 of [**BW06**] that calls for the specific construction of the point $\boldsymbol{\theta}$ associated with the equations (3.4). □

4. The auxiliary mean value estimate

The estimate underpinning our earlier work [**BW06**] takes the shape

$$\int_0^1 \int_0^1 |h(\Lambda_1)h(\Lambda_2)\dots h(\Lambda_{12})|\, d\alpha\, d\beta \ll P^{6+\xi+\varepsilon},$$

predicated on the assumption that the maximum multiplicity amongst $\Lambda_1, \dots, \Lambda_{12}$ does not exceed 5. In order to make progress on a viable minor arc treatment in the present situation, we require an analogue of this estimate that permits the replacement of a smooth Weyl sum by a corresponding classical Weyl sum. In preparation for this lemma, we recall an elementary observation from our earlier work, the proof of which is almost self-evident (see Lemma 5 of [**BW06**]).

Lemma 6. *Let k and N be natural numbers, and suppose that $\mathfrak{B} \subseteq \mathbb{C}^k$ is measurable. Let $\omega_i(\mathbf{z})$ $(0 \le i \le N)$ be complex-valued functions of $\mathfrak{B}$. Then whenever the functions $|\omega_0(\mathbf{z})\omega_j(\mathbf{z})^N|$ $(1 \le j \le N)$ are integrable on $\mathfrak{B}$, one has the upper bound*

$$\int_{\mathfrak{B}} |\omega_0(\mathbf{z})\omega_1(\mathbf{z})\dots\omega_N(\mathbf{z})|\, d\mathbf{z} \le N \max_{1\le j\le N} \int_{\mathfrak{B}} |\omega_0(\mathbf{z})\omega_j(\mathbf{z})^N| d\mathbf{z}.$$

It is convenient in what follows to abbreviate, for each index l, the expression $|h(\Lambda_l)|$ simply to h_l, and likewise $|g(\Lambda_l)|$ to g_l and $|G(\alpha,\beta)|$ to G. Furthermore, we write

$$G_0(\alpha,\beta) = \prod_{j=14}^{s} g(\Lambda_j), \tag{4.1}$$

with the implicit convention that $G_0(\alpha,\beta)$ is identically 1 when $s < 14$.

Lemma 7. *Suppose that the system* (1.1) *is of type III with $s \ge 13$ and $7 \le q_0 \le s-6$. Then in the setting described in* §3*, one has*

$$\int_0^1 \int_0^1 |H(\alpha,\beta)G(\alpha,\beta)|\, d\alpha\, d\beta \ll P^{s-7+\xi+\varepsilon}.$$

Proof. We begin by making some analytic observations that greatly simplify the combinatorial details of the argument to come. Write $\mathcal{L} = \{\Lambda_2, \Lambda_3, \dots, \Lambda_{12}\}$, and suppose that the number of equivalence classes in $\mathcal{L}$ is u. By relabelling indices if necessary, we may suppose that $u \ge 3$ and that representatives of these classes are $\widetilde{\Lambda}_i \in \mathcal{L}$ $(1 \le i \le u)$. For each index i we denote by s_i the multiplicity of $\widetilde{\Lambda}_i$ amongst the elements of the set $\mathcal{L}$. Then according to the discussion of the previous section, we may suppose that $\Lambda_1 \in [\widetilde{\Lambda}_1]$, that

$$1 \le s_u \le s_{u-1} \le \ldots \le s_1 = 5 \quad \text{and} \quad s_2 + s_3 + \cdots + s_u = 6, \tag{4.2}$$

and further that if $\Lambda_{13} \in [\widetilde{\Lambda}_i]$ for some index i with $1 \le i \le u$, then in fact

$$\Lambda_{13} \in [\widetilde{\Lambda}_u] \quad \text{and} \quad 1 \le s_u \le 2. \tag{4.3}$$

Next, for a given index i with $2 \le i \le 12$, consider the linear forms Λ_{l_j} $(1 \le j \le s_i)$ equivalent to Λ_i from the set $\mathcal{L}$. Apply Lemma 6 with $N = s_i$, with h_{l_j} in place of ω_j $(1 \le j \le N)$, and with ω_0 replaced by the product of those h_l with $\Lambda_l \notin [\widetilde{\Lambda}_i]$ $(2 \le l \le 12)$, multiplied by $G(\alpha, \beta)$. Then it is apparent that there is no loss of generality in supposing that $\Lambda_{l_j} = \widetilde{\Lambda}_i$ $(1 \le j \le s_i)$. By repeating this argument for successive equivalence classes, moreover, we find that a suitable choice of equivalence class representatives $\widetilde{\Lambda}_l$ $(1 \le l \le u)$ yields the bound

$$\int_0^1 \int_0^1 |H(\alpha,\beta)G(\alpha,\beta)|\, d\alpha\, d\beta \ll \int_0^1 \int_0^1 G\tilde{h}_1^{s_1}\tilde{h}_2^{s_2}\ldots\tilde{h}_u^{s_u}\, d\alpha\, d\beta, \tag{4.4}$$

where we now take the liberty of abbreviating $|h(\widetilde{\Lambda}_l)|$ simply to $\tilde{h}_l$ for each l.

A further simplification is achieved through the use of a device employed in the proof of Lemma 6 of [**BW06**]. We begin by considering the situation in which $\Lambda_{13} \in [\widetilde{\Lambda}_u]$. Let ν be a non-negative integer, and suppose that $s_{u-2} = s_{u-1} + \nu < 5$. Then we may apply Lemma 6 with $N = \nu+2$, with $\tilde{h}_{u-2}$ in place of ω_i $(1 \le i \le \nu+1)$ and $\tilde{h}_{u-1}$ in place of ω_N, and with ω_0 set equal to

$$G\tilde{h}_1^{s_1}\tilde{h}_2^{s_2}\ldots\tilde{h}_{u-3}^{s_{u-3}}\tilde{h}_{u-2}^{s_{u-2}-\nu-1}\tilde{h}_{u-1}^{s_{u-1}-1}\tilde{h}_u^{s_u}.$$

Here, and in what follows, we interpret the vanishing of any exponent as indicating that the associated exponential sum is deleted from the product. In this way we obtain an upper bound of the shape (4.4) in which the exponents s_{u-2} and $s_{u-1} = s_{u-2} - \nu$ are replaced by $s_{u-2} + 1$ and $s_{u-1} - 1$, respectively, or else by $s_{u-2} - \nu - 1$ and $s_{u-1} + \nu + 1$. By relabelling if necessary, we derive an upper bound of the shape (4.4), subject to the constraints (4.2) and (4.3), wherein either the parameter s_{u-1} is reduced, or else the parameter u is reduced. By repeating this process, therefore, we ultimately arrive at a situation in which $u = 3$ and $s_{u-1} = 6 - s_u$, and then the constraints (4.2) and (4.3) imply that necessarily $(s_1, s_2, \ldots, s_u) = (5, 6 - s_3, s_3)$ with $s_3 = 1$ or 2. When $\Lambda_{13} \notin [\widetilde{\Lambda}_u]$ we may proceed likewise, but in the above argument s_{u-1} now plays the rôle of s_{u-2}, and s_u that of s_{u-1}, and with concommitant adjustments to the associated indices throughout. In this second situation we ultimately arrive at a scenario in which $u = 3$ and $s_{u-1} = 5$, and in these circumstances the constraints (4.2) imply that necessarily $(s_1, s_2, \ldots, s_u) = (5, 5, 1)$.

On recalling (4.1) and (4.4), and making use of a trivial inequality for $|G_0(\alpha, \beta)|$, we may conclude thus far that

$$\int_0^1 \int_0^1 |H(\alpha,\beta)G(\alpha,\beta)|\, d\alpha\, d\beta \ll P^{s-13} \int_0^1 \int_0^1 g_{13}\tilde{h}_1^{s_1}\tilde{h}_2^{s_2}\tilde{h}_3^{s_3}\, d\alpha\, d\beta, \tag{4.5}$$

with $(s_1,s_2,s_3)=(5,5,1)$ or $(5,4,2)$. We now write

$$\mathcal{I}_{ij}(\psi)=\int_0^1\int_0^1 \tilde{h}_i^5\tilde{h}_j^5\psi^2\,d\alpha\,d\beta,$$

and we observe that an application of Hölder's inequality yields

$$\int_0^1\int_0^1 g_{13}\tilde{h}_1^{s_1}\tilde{h}_2^{s_2}\tilde{h}_3^{s_3}\,d\alpha\,d\beta\le \mathcal{I}_{12}(g_{13})^{\omega_1}\mathcal{I}_{12}(\tilde{h}_3)^{\omega_2}\mathcal{I}_{13}(\tilde{h}_2)^{\omega_3}, \tag{4.6}$$

where

$$(\omega_1,\omega_2,\omega_3)=\begin{cases}(1/2,1/2,0), & \text{when } s_3=1,\\ (1/2,1/6,1/3), & \text{when } s_3=2.\end{cases}$$

But Lemma 4 is applicable to each of the mean values $\mathcal{I}_{12}(g_{13})$, $\mathcal{I}_{12}(\tilde{h}_3)$ and $\mathcal{I}_{13}(\tilde{h}_2)$, and so we see from (4.6) that

$$\int_0^1\int_0^1 g_{13}\tilde{h}_1^{s_1}\tilde{h}_2^{s_2}\tilde{h}_3^{s_3}\,d\alpha\,d\beta\ll P^{6+\xi+\varepsilon}.$$

The conclusion of Lemma 7 is now immediate on substituting the latter estimate into (4.5). □

5. Minor arcs, with some pruning

Equipped with the mean value estimate provided by Lemma 7, an advance on the minor arc bound complementary to the major arc estimate of Lemma 5 is feasible by the use of appropriate pruning technology. Here, in certain respects, the situation is a little more delicate than was the case in our treatment of the analogous situation in [**BW06**]. The explanation is to be found in the higher multiplicity of coefficient ratios permitted in our present discussion, associated with which is a lower average level of independence amongst the available generating functions.

We begin our account of the minor arcs by defining a set of auxiliary arcs to be employed in the pruning process. Given a parameter X with $1\le X\le P$, we define $\mathfrak{M}(X)$ to be the set of real numbers α with $\alpha\in[0,1)$ for which there exist $a\in\mathbb{Z}$ and $q\in\mathbb{N}$ satisfying $0\le a\le q\le X$, $(a,q)=1$ and $|q\alpha-a|\le XP^{-3}$. We then define sets of major arcs $\mathfrak{M}=\mathfrak{M}(P^{3/4})$ and $\mathfrak{K}=\mathfrak{M}(Q^{1/4})$, and write also $\mathfrak{m}=[0,1)\setminus\mathfrak{M}$ and $\mathfrak{k}=[0,1)\setminus\mathfrak{K}$ for the corresponding sets of minor arcs.

Given a measurable set $\mathfrak{B}\subseteq\mathbb{R}^2$, define the mean-value $\mathcal{J}(\mathfrak{B})$ by

$$\mathcal{J}(\mathfrak{B})=\iint_{\mathfrak{B}}|g(a_1\alpha)G(\alpha,\beta)H(\alpha,\beta)|\,d\alpha\,d\beta. \tag{5.1}$$

Also, put $\mathfrak{E}=\{(\alpha,\beta)\in\mathfrak{n}:\alpha\in\mathfrak{M}\}$. Then on recalling the enhanced version of Weyl's inequality afforded by Lemma 1 of Vaughan [**V86**], one finds from Lemma 7 that

$$\begin{aligned}\mathcal{J}(\mathfrak{n})&\ll\mathcal{J}(\mathfrak{E})+\sup_{\alpha\in\mathfrak{m}}|g(a_1\alpha)|\int_0^1\int_0^1|G(\alpha,\beta)H(\alpha,\beta)|\,d\alpha\,d\beta\\&\ll\mathcal{J}(\mathfrak{E})+P^{s-6-\tau},\end{aligned} \tag{5.2}$$

wherein we have written

$$\tau=(1/4-\xi)/3. \tag{5.3}$$

Our aim now is to show that $\mathcal{J}(\mathfrak{E}) = o(P^{s-6})$, for then it follows from (5.1) and (5.2) in combination with the conclusion of Lemma 5 that

$$\int_0^1\int_0^1 g(\Lambda_1)G(\alpha,\beta)H(\alpha,\beta)\,d\alpha\,d\beta = \mathcal{J}(\mathfrak{n}) + \iint_{\mathfrak{N}} g(\Lambda_1)G(\alpha,\beta)H(\alpha,\beta)\,d\alpha\,d\beta$$
$$\gg P^{s-6} + o(P^{s-6}).$$

The conclusion $\mathcal{N}_s(P) \gg P^{s-6}$ is now immediate, and this completes the proof of Theorem 2 for systems (1.1) of type III.

Before proceeding further, we define

$$H_0(\alpha,\beta) = \prod_{j=2}^{7} h(\Lambda_j) \quad \text{and} \quad H_1(\alpha) = \prod_{j=8}^{12} h(\Lambda_j), \tag{5.4}$$

wherein we have implicitly made use of the discussion of §3 leading to (3.3) that permits us to assume that $\Lambda_j = a_j\alpha$ $(8 \le j \le 12)$. Also, given $\alpha \in \mathfrak{M}$ we put $\mathfrak{E}(\alpha) = \{\beta \in [0,1) : (\alpha,\beta) \in \mathfrak{E}\}$ and write

$$\Theta(\alpha) = \int_{\mathfrak{E}(\alpha)} |G(\alpha,\beta)H_0(\alpha,\beta)|\,d\beta. \tag{5.5}$$

The relation

$$\mathcal{J}(\mathfrak{E}) = \int_{\mathfrak{M}} |g(a_1\alpha)H_1(\alpha)|\Theta(\alpha)\,d\alpha, \tag{5.6}$$

then follows from (5.1), and it is from here that we launch our pruning argument.

Lemma 8. *One has*

$$\sup_{\alpha\in[0,1)} \Theta(\alpha) \ll P^{s-9} \quad \textit{and} \quad \sup_{\alpha\in\mathfrak{K}} \Theta(\alpha) \ll P^{s-9}Q^{-1/72}.$$

Proof. We divide the set $\mathfrak{E}(\alpha)$ into pieces on which major arc and minor arc estimates of various types may be employed so as to estimate the integral defining $\Theta(\alpha)$ in (5.5). Let $\mathfrak{E}_1(\alpha)$ denote the set consisting of those values β in $\mathfrak{E}(\alpha)$ for which $|g(\Lambda_{13})| < P^{3/4+\tau}$, where τ is defined as in (5.3), and put $\mathfrak{E}_2(\alpha) = \mathfrak{E}(\alpha) \setminus \mathfrak{E}_1(\alpha)$. Then on applying a trivial estimate for those exponential sums $g(\Lambda_j)$ with $j \ge 14$, it follows from (3.5) that

$$\sup_{\beta\in\mathfrak{E}_1(\alpha)} |G(\alpha,\beta)| \ll P^{s-49/4+\tau}. \tag{5.7}$$

But the discussion of §3 leading to (3.3) ensures that $b_j \ne 0$ for $2 \le j \le 7$. By making use of the mean value estimate (2.2), one therefore obtains the estimate

$$\int_0^1 |h(\Lambda_j)|^6\,d\beta = \int_0^1 |h(\gamma)|^6\,d\gamma \ll P^{3+\xi+\varepsilon} \qquad (2 \le j \le 7),$$

whence an application of Hölder's inequality leads from (5.4) to the bound

$$\int_0^1 |H_0(\alpha,\beta)|\,d\beta \le \prod_{j=2}^{7}\Big(\int_0^1 |h(\Lambda_j)|^6\,d\beta\Big)^{1/6} \ll P^{3+\xi+\varepsilon}. \tag{5.8}$$

Consequently, by combining (5.7) and (5.8) we obtain

$$\int_{\mathfrak{E}_1(\alpha)} |G(\alpha,\beta)H_0(\alpha,\beta)|\,d\beta \ll P^{s-9+(\xi-1/4)+\tau+\varepsilon} \ll P^{s-9-\tau}.$$

When $\beta \in \mathfrak{E}_2(\alpha)$, on the other hand, one has $|g(\Lambda_{13})| \ge P^{3/4+\tau}$. Applying the enhanced version of Weyl's inequality already cited, we find that the latter can hold only when $\Lambda_{13} \in \mathfrak{M}$ (mod 1). If we now define the set $\mathfrak{F}(\alpha)$ by

$$\mathfrak{F}(\alpha) = \{\beta \in [0,1) : (\alpha,\beta) \in \mathfrak{n} \text{ and } \Lambda_{13} \in \mathfrak{M} \text{ (mod 1)}\},$$

and apply a trivial estimate once again for $g(\Lambda_j)$ $(j \ge 14)$, then we may summarise our deliberations thus far with the estimate

$$\Theta(\alpha) \ll P^{s-9-\tau} + P^{s-13} \int_{\mathfrak{F}(\alpha)} |g(\Lambda_{13}) H_0(\alpha,\beta)| \, d\beta. \tag{5.9}$$

A transparent application of Lemma 6 leads from (5.4) to the upper bound

$$\int_{\mathfrak{F}(\alpha)} |g(\Lambda_{13}) H_0(\alpha,\beta)| d\beta \ll \max_{2 \le j \le 7} \int_{\mathfrak{F}(\alpha)} |g(\Lambda_{13}) h(\Lambda_j)^6| d\beta.$$

The conclusion of the lemma will therefore follow from (5.9) provided that we establish for $2 \le j \le 7$ the two estimates

$$\sup_{\alpha \in [0,1)} \int_{\mathfrak{F}(\alpha)} |g(\Lambda_{13}) h(\Lambda_j)^6| \, d\beta \ll P^4 \tag{5.10}$$

and

$$\sup_{\alpha \in \mathfrak{K}} \int_{\mathfrak{F}(\alpha)} |g(\Lambda_{13}) h(\Lambda_j)^6| \, d\beta \ll P^4 Q^{-1/72}. \tag{5.11}$$

We henceforth suppose that j is an index with $2 \le j \le 7$, and we begin by considering the upper bound (5.10). Given $\alpha \in [0,1)$, we make the change of variable defined by the substitution $b_{13}\gamma = a_{13}\alpha + b_{13}\beta$. Let $\mathfrak{M}_0$ be defined by

$$\mathfrak{M}_0 = \{\gamma \in [0,1) : b_{13}\gamma \in \mathfrak{M} \text{ (mod 1)}\}.$$

Then by the periodicity of the integrand modulo 1, the aforementioned change of variable leads to the upper bound

$$\int_{\mathfrak{F}(\alpha)} |g(\Lambda_{13}) h(\Lambda_j)^6| \, d\beta \le \Big(\sup_{\beta \in \mathfrak{F}(\alpha)} |g(\Lambda_{13})| \Big)^{1/6} \sup_{\lambda \in \mathbb{R}} \mathcal{U}(\lambda), \tag{5.12}$$

in which we write

$$\mathcal{U}(\lambda) = \int_{\mathfrak{M}_0} |g(b_{13}\gamma)|^{5/6} |h(b_j\gamma + \lambda)|^6 \, d\gamma. \tag{5.13}$$

We next examine the first factor on the right hand side of (5.12). Given $\alpha \in \mathfrak{K}$, consider a real number β with $\beta \in \mathfrak{F}(\alpha)$. If it were the case that $\Lambda_{13} \in \mathfrak{K}$ (mod 1), then one would have $\beta = b_{13}^{-1}(\Lambda_{13} - a_{13}\alpha) \in \mathfrak{M}(Q^{3/4})$, whence $(\alpha,\beta) \in \mathfrak{N}$ (see the proof of Lemma 10 in §6 of [**BW06**] for details of a similar argument). But the latter contradicts the hypothesis $\beta \in \mathfrak{F}(\alpha)$, in view of the definition of $\mathfrak{F}(\alpha)$. Thus we conclude that $\Lambda_{13} \in \mathfrak{k}$ (mod 1), and so a standard application of Weyl's inequality (see Lemma 2.4 of [**V97**]) in combination with available major arc estimates (see Theorem 4.1 and Lemma 4.6 of [**V97**]) yields the upper bound

$$\sup_{\beta \in \mathfrak{F}(\alpha)} |g(\Lambda_{13})| \le \sup_{\gamma \in \mathfrak{k}} |g(\gamma)| \ll P Q^{-1/12}. \tag{5.14}$$

Of course, one has also the trivial upper bound

$$\sup_{\beta \in [0,1)} |g(\Lambda_{13})| \le P.$$

We therefore deduce from (5.12) that

$$\int_{\mathfrak{F}(\alpha)} |g(\Lambda_{13})h(\Lambda_j)^6|\,d\beta \ll P^{1/6}U^{-1/72}\sup_{\lambda\in\mathbb{R}} \mathcal{U}(\lambda), \tag{5.15}$$

where $U = Q$ when $\alpha \in \mathfrak{K}$, and otherwise $U = 1$.

Next, on considering the underlying Diophantine equations, it follows from Theorem 2 of Vaughan [**V86**] that for each $\lambda \in \mathbb{R}$, one has the upper bound

$$\int_0^1 |h(b_j\gamma+\lambda)|^8\,d\gamma \ll P^5.$$

Meanwhile, Lemma 9 of [**BW06**] yields the estimate

$$\sup_{\lambda\in\mathbb{R}} \int_{\mathfrak{M}_0} |g(b_{13}\gamma)|^{5/2}|h(b_j\gamma+\lambda)|^2\,d\gamma \ll P^{3/2}.$$

By applying Hölder's inequality to the integral on the right hand side of (5.13), therefore, we obtain

$$\begin{aligned}\mathcal{U}(\lambda) &\le \Big(\int_0^1 |h(b_j\gamma+\lambda)|^8\,d\gamma\Big)^{2/3}\Big(\int_{\mathfrak{M}_0} |g(b_{13}\gamma)|^{5/2}|h(b_j\gamma+\lambda)|^2\,d\gamma\Big)^{1/3}\\ &\ll (P^5)^{2/3}(P^{3/2})^{1/3}.\end{aligned}$$

On substituting the latter estimate into (5.15), we may conclude that

$$\int_{\mathfrak{F}(\alpha)} |g(\Lambda_{13})h(\Lambda_j)^6|\,d\beta \ll P^4U^{-1/72},$$

with U defined as in the sequel to (5.15). The estimates (5.10) and (5.11) that we seek to establish are then immediate, and in view of our earlier discussion this suffices already to complete the proof of the lemma. □

We now employ the bounds supplied by Lemma 8 to prune the integral on the right hand side of (5.6), making use also of an argument similar to that used in the proof of this lemma. Applying these estimates within the aforementioned equation, we obtain the bound

$$\mathcal{J}(\mathfrak{E}) \ll P^{s-9}\mathcal{K}(\mathfrak{k}\cap\mathfrak{M}) + P^{s-9}Q^{-1/72}\mathcal{K}(\mathfrak{K}), \tag{5.16}$$

where we write

$$\mathcal{K}(\mathfrak{B}) = \int_{\mathfrak{B}} |g(a_1\alpha)H_1(\alpha)|\,d\alpha. \tag{5.17}$$

But in view of (5.4), when $\mathfrak{B} \subseteq \mathfrak{M}$, an application of Hölder's inequality to (5.17) yields

$$\mathcal{K}(\mathfrak{B}) \le \prod_{j=8}^{12} \bigg(\Big(\sup_{\alpha\in\mathfrak{B}} |g(a_1\alpha)|\Big)^{1/58}\mathcal{L}_{1,j}^{14/29}\mathcal{L}_{2,j}^{15/29}\bigg)^{1/5}, \tag{5.18}$$

where for $8 \le j \le 12$ we put

$$\mathcal{L}_{1,j} = \int_{\mathfrak{M}} |g(a_1\alpha)|^{57/28}|h(a_j\alpha)|^2\,d\alpha$$

and

$$\mathcal{L}_{2,j} = \int_0^1 |h(a_j\alpha)|^{39/5}\,d\alpha.$$

The integral $\mathcal{L}_{1,j}$ may be estimated by applying Lemma 9 of [**BW06**], and $\mathcal{L}_{2,j}$ via Theorem 2 of Brüdern and Wooley [**BW01**]. Thus we have

$$\mathcal{L}_{1,j} \ll P^{29/28} \quad \text{and} \quad \mathcal{L}_{2,j} \ll P^{24/5} \quad (8 \le j \le 12). \tag{5.19}$$

But as in the argument leading to the estimate (5.14) in the proof of Lemma 8, one has also

$$\sup_{\alpha \in \mathfrak{k}} |g(a_1\alpha)| \ll PQ^{-1/12}. \tag{5.20}$$

Thus, on making use in addition of the trivial estimate $|g(a_1\alpha)| \le P$ valid uniformly in α, and substituting this and the estimates (5.19) and (5.20) into (5.18), we conclude that

$$\mathcal{K}(\mathfrak{k} \cap \mathfrak{M}) \ll P^3 Q^{-1/696} \quad \text{and} \quad \mathcal{K}(\mathfrak{K}) \ll P^3.$$

In this way, we deduce from (5.16) that $\mathcal{J}(\mathfrak{C}) \ll P^{s-6}Q^{-1/696}$. The estimate $\mathcal{J}(\mathfrak{n}) \ll P^{s-6}Q^{-1/696}$ is now confirmed by (5.2), so that by the discussion following that equation, we arrive at the desired lower bound $\mathcal{N}_s(P) \gg P^{s-6}$ for the systems (1.1) of type III under consideration. This completes the proof of Theorem 2 for the latter systems, and so we may turn our attention in the next section to systems of types I and II.

6. An exceptional approach to systems of types I and II

Systems of type II split into two almost separate diagonal cubic equations linked by a single variable. Here we may apply the main ideas from our recent collaboration with Kawada [**BKW01a**] in order to show that this linked cubic variable is almost always simultaneously as often as expected equal both to the first and to the second residual diagonal cubic. A lower bound for $\mathcal{N}_s(P)$ of the desired strength follows with ease. Although systems of type I are accessible in a straightforward fashion to the modern theory of cubic smooth Weyl sums (see, for example, [**V89**] and [**W00**]), we are able to avoid detailed discussion by appealing to the main result underpinning the analysis of type II systems.

In preparation for the statement of the basic estimate of this section, we require some notation. When t is a natural number, and $c_1, \ldots, c_t$ are natural numbers, let $R_t(m; \mathbf{c})$ denote the number of positive integral solutions of the equation

$$c_1x_1^3 + c_2x_2^3 + \cdots + c_tx_t^3 = m. \tag{6.1}$$

In addition, let η be a positive number with $(c_1 + c_2)\eta < 1/4$ sufficiently small in the context of the estimate (2.2), and put $\nu = 16(c_1 + c_2)\eta$. Finally, recall from (5.3) that $\tau = (1/4 - \xi)/3 > 10^{-4}$.

Theorem 9. *Suppose that t is a natural number with $t \ge 6$, and let $c_1, \ldots, c_t$ be natural numbers satisfying $(c_1, \ldots, c_t) = 1$. Then for each natural number d there is a positive number Δ, depending at most on $\mathbf{c}$ and d, with the property that the set $\mathcal{E}_t(P)$, defined by*

$$\mathcal{E}_t(P) = \{n \in \mathbb{N} : \nu P d^{-1/3} < n \le P d^{-1/3} \text{ and } R_t(dn^3; \mathbf{c}) < \Delta P^{t-3}\},$$

has at most $P^{1-\tau}$ elements.

We note that the conclusion of the theorem for $t \ge 7$ is essentially classical, and indeed one may establish that $\text{card}(\mathcal{E}_t(P)) = O(1)$ under the latter hypothesis. It is, however, painless to add these additional cases to the primary case $t = 6$, and this permits economies later in this section. Much improvement is possible in the estimate for $\mathrm{card}(\mathcal{E}_t(P))$ even when $t = 6$ (see Brüdern, Kawada and Wooley [**BKW01a**] for the ideas necessary to save a relatively large power of P). Here we briefly sketch a proof of Theorem 9 that employs a straightforward approach to the problem.

PROOF. Let $\mathfrak{B} \subseteq [0, 1)$ be a measurable set, and consider a natural number m. If we define the Fourier coefficient $\Upsilon_t(m; \mathfrak{B})$ by

$$\Upsilon_t(m;\mathfrak{B}) = \int_{\mathfrak{B}} g(c_1\alpha)g(c_2\alpha)h(c_3\alpha)h(c_4\alpha)\dots h(c_t\alpha)e(-m\alpha)\,d\alpha, \tag{6.2}$$

then it follows from orthogonality that for each $m \in \mathbb{N}$, one has

$$\Upsilon_t(m;[0,1)) \le R_t(m;\mathbf{c}). \tag{6.3}$$

Recall the definition of the sets of major arcs $\mathfrak{M}$ and minor arcs $\mathfrak{m}$ from §5. We observe that the methods of Wooley [**W00**] apply to provide the mean value estimate

$$\int_0^1 |g(c_i\alpha)^2h(c_j\alpha)^4|\,d\alpha \ll P^{3+\xi+\varepsilon} \quad (i = 1, 2 \text{ and } 3 \le j \le t). \tag{6.4}$$

In addition, whenever u is a real number with $u \ge 7.7$, it follows from Theorem 2 of Brüdern and Wooley [**BW01**] that

$$\int_0^1 |h(c_j\alpha)|^u\,d\alpha \ll P^{u-3} \quad (3 \le j \le t). \tag{6.5}$$

Finally, we define the singular series

$$\mathfrak{S}_t(m) = \sum_{q=1}^{\infty} q^{-t} \sum_{\substack{a=1\\(a,q)=1}}^{q} S_1(q,a)S_2(q,a)\dots S_t(q,a)e(-ma/q),$$

where we write

$$S_i(q,a) = \sum_{r=1}^{q} e(c_iar^3/q) \quad (1 \le i \le t).$$

Then in view of (6.5), the presence of two classical Weyl sums within the integral on the right hand side of (6.2) permits the use of the argument applied by Vaughan in §5 of [**V89**] so as to establish that when τ is a positive number sufficiently small in terms of η, one has

$$\Upsilon_t(m;\mathfrak{M}) = \mathcal{C}_t(\eta;m)\mathfrak{S}_t(m)m^{t/3-1} + O(P^{t-3}(\log P)^{-\tau}),$$

where $\mathcal{C}_t(\eta; m)$ is a non-negative number related to the singular integral. When $\nu^3P^3 < m \le P^3$, it follows from Lemma 8.5 of [**W91**] (see also Lemma 5.4 of [**V89**]) that $\mathcal{C}_t(\eta; m) \gg 1$, in which the implicit constant depends at most on t, $\mathbf{c}$ and η. The methods of Chapter 4 of [**V97**] (see, in particular, Theorem 4.5) show that $\mathfrak{S}_t(m) \gg 1$ uniformly in m, with an implicit constant depending at most on t and $\mathbf{c}$. Here it may be worth remarking that a homogenised version of the representation problem (6.1) defines a diagonal cubic equation in $t+1 \ge 7$ variables. Non-singular p-adic solutions of the latter equation are guaranteed by the work of Lewis [**L57**], and the coprimality of the coefficients $c_1, c_2, \dots, c_t$ ensures that a p-adic solution of the homogenised equation may be found in which the homogenising variable is equal to 1. Thus the existence of non-singular p-adic solutions for the equation (6.1) is assured, and it is this observation that permits us to conclude that $\mathfrak{S}_t(m) \gg 1$.

Our discussion thus far permits us to conclude that when Δ is a positive number sufficiently small in terms of t, $\mathbf{c}$ and η, then for each $m \in (\nu^3 P^3, P^3]$ one has $\Upsilon_t(m; \mathfrak{M}) > 2\Delta P^{t-3}$. But $\Upsilon_t(m; [0,1)) = \Upsilon_t(m; \mathfrak{M}) + \Upsilon_t(m; \mathfrak{m})$, and so it follows from (6.2) and (6.3) that for each $n \in \mathcal{E}_t(P)$, one has

$$|\Upsilon_t(dn^3; \mathfrak{m})| > \Delta P^{t-3}. \tag{6.6}$$

When $n \in \mathcal{E}_t(P)$, we now define σ_n via the relation $|\Upsilon_t(dn^3; \mathfrak{m})| = \sigma_n \Upsilon_t(dn^3; \mathfrak{m})$, and then put

$$K_t(\alpha) = \sum_{n \in \mathcal{E}_t(P)} \sigma_n e(-dn^3 \alpha).$$

Here, in the event that $\Upsilon_t(dn^3; \mathfrak{m}) = 0$, we put $\sigma_n = 0$. Consequently, on abbreviating $\operatorname{card}(\mathcal{E}_t(P))$ to E_t, we find that by summing the relation (6.6) over $n \in \mathcal{E}_t(P)$, one obtains

$$E_t \Delta P^{t-3} < \int_{\mathfrak{m}} g(c_1\alpha) g(c_2\alpha) h(c_3\alpha) h(c_4\alpha) \dots h(c_t\alpha) K_t(\alpha)\, d\alpha. \tag{6.7}$$

An application of Lemma 6 within (6.7) reveals that

$$E_t \Delta P^{t-3} \ll \max_{i=1,2} \max_{3 \le j \le t} \int_{\mathfrak{m}} |g(c_i\alpha)^2 h(c_j\alpha)^{t-2} K_t(\alpha)|\, d\alpha.$$

On making a trivial estimate for $h(c_j\alpha)$ in case $t > 6$, we find by applying Schwarz's inequality that there are indices $i \in \{1,2\}$ and $j \in \{3,4,\dots,t\}$ for which

$$E_t \Delta P^{t-3} \ll \Big(\sup_{\alpha \in \mathfrak{m}} |g(c_i\alpha)| \Big) P^{t-6} \mathcal{T}_1^{1/2} \mathcal{T}_2^{1/2},$$

where we write

$$\mathcal{T}_1 = \int_0^1 |g(c_i\alpha)^2 h(c_j\alpha)^4|\, d\alpha \quad \text{and} \quad \mathcal{T}_2 = \int_0^1 |h(c_j\alpha)^4 K_t(\alpha)^2|\, d\alpha.$$

The first of the latter integrals can plainly be estimated via (6.4), and a consideration of the underlying Diophantine equation reveals that the second may be estimated in similar fashion. Thus, on making use of the enhanced version of Weyl's inequality (Lemma 1 of [**V86**]) by now familiar to the reader, we arrive at the estimate

$$E_t \Delta P^{t-3} \ll (P^{3/4+\varepsilon})(P^{t-6})(P^{3+\xi+\varepsilon}) \ll P^{t-2-2\tau+2\varepsilon}.$$

The upper bound $E_t \le P^{1-\tau}$ now follows whenever P is sufficiently large in terms of t, $\mathbf{c}$, η, Δ and τ. This completes the proof of the theorem. □

We may now complete the proof of Theorem 2 for systems of type II. From the discussion in §3, we may suppose that $s \ge 13$, that $7 \le q_0 \le s-6$, and that amongst the forms Λ_i $(1 \le i \le s)$ there are precisely 3 equivalence classes, one of which has multiplicity 1. By taking suitable linear combinations of the equations (1.1), and by relabelling the variables if necessary, it thus suffices to consider the pair of equations

$$\begin{aligned} a_1x_1^3 + \dots + a_rx_r^3 \qquad\qquad\qquad\qquad &= d_1x_s^3, \\ b_{r+1}x_{r+1}^3 + \dots + b_{s-1}x_{s-1}^3 &= d_2x_s^3, \end{aligned} \tag{6.8}$$

where we have written $d_1 = -a_s$ and $d_2 = -b_s$, both of which we may suppose to be non-zero. We may apply the substitution $x_j \to -x_j$ whenever necessary so as to ensure that all of the coefficients in the system (6.8) are positive. Next write A and B for the greatest common divisors of $a_1, \dots, a_r$ and $b_{r+1}, \dots, b_{s-1}$ respectively. On replacing x_s by ABy, with a new variable y, we may cancel a factor A from the coefficients of the first equation, and likewise B from the second. There is consequently no loss in assuming that $A = B = 1$ for the system (6.8).

In view of the discussion of §3, the hypotheses $s \geq 13$ and $7 \leq q_0 \leq s - 6$ permit us to assume that in the system (6.8), one has $r \geq 6$ and $s - r \geq 7$. Let Δ be a positive number sufficiently small in terms of a_i $(1 \leq i \leq r)$, b_j $(r+1 \leq j \leq s-1)$, and d_1, d_2. Also, put $d = \min\{d_1, d_2\}$, $D = \max\{d_1, d_2\}$, and recall that $\nu = 16(c_1+c_2)\eta$. Note here that by taking η sufficiently small in terms of $\mathbf{d}$, we may suppose without loss that $\nu d^{-1/3} < \frac{1}{2}D^{-1/3}$. Then as a consequence of Theorem 9, for all but at most $P^{1-\tau}$ of the integers x_s with $\nu P d^{-1/3} < x_s \leq P D^{-1/3}$ one has $R_r(d_1 x_s^3; \mathbf{a}) \geq \Delta P^{r-3}$, and likewise for all but at most $P^{1-\tau}$ of the same integers x_s one has $R_{s-r-1}(d_2 x_s^3; \mathbf{b}) \geq \Delta P^{s-r-4}$. Thus we see that

$$\begin{aligned}\mathcal{N}_s(P) &\geq \sum_{1 \leq x_s \leq P} R_r(d_1 x_s^3; \mathbf{a}) R_{s-r-1}(d_2 x_s^3; \mathbf{b}) \\ &\gg (P - 2P^{1-\tau})(P^{r-3})(P^{s-r-4}).\end{aligned}$$

The bound $\mathcal{N}_s(P) \gg P^{s-6}$ that we sought in order to confirm Theorem 2 for type II systems is now apparent.

The only remaining situations to consider concern type I systems with $s \geq 13$ and $7 \leq q_0 \leq s - 6$. Here the simultaneous equations take the shape

$$\begin{aligned} a_1 x_1^3 + \dots + a_{r-1} x_{r-1}^3 &= d_1 x_r^3, \\ b_{r+1} x_{r+1}^3 + \dots + b_{s-1} x_{s-1}^3 &= d_2 x_s^3, \end{aligned} \tag{6.9}$$

with $r \geq 7$ and $s - r \geq 7$. As in the discussion of type II systems, one may make changes of variable so as to ensure that $(a_1, \dots, a_{r-1}) = 1$ and $(b_{r+1}, \dots, b_{s-1}) = 1$, and in addition that all of the coefficients in the system (6.9) are positive. But as a direct consequence of Theorem 9, in a manner similar to that described in the previous paragraph, one obtains

$$\begin{aligned}\mathcal{N}_s(P) &\geq \sum_{1 \leq x_r \leq P} \sum_{1 \leq x_s \leq P} R_{r-1}(d_1 x_r^3; \mathbf{a}) R_{s-r-1}(d_2 x_s^3; \mathbf{b}) \\ &\gg (P - P^{1-\tau})^2 (P^{r-4})(P^{s-r-4}) \gg P^{s-6}.\end{aligned}$$

This confirms the lower bound $\mathcal{N}_s(P) \gg P^{s-6}$ for type I systems, and thus the proof of Theorem 2 is complete in all cases.

7. Asymptotic lower bounds for systems of smaller dimension

Although our methods are certainly not applicable to general systems of the shape (1.1) containing 12 or fewer variables, we are nonetheless able to generalise the approach described in the previous section so as to handle systems containing at most 3 distinct coefficient ratios. We sketch below the ideas required to establish such conclusions, leaving the reader to verify the details as time permits. It is appropriate in future investigations of pairs of cubic equations, therefore, to restrict attention to systems containing four or more coefficient ratios.

THEOREM 10. *Suppose that* $s \geq 11$, *and that* $(a_j, b_j) \in \mathbb{Z}^2 \setminus \{\mathbf{0}\}$ $(1 \leq j \leq s)$ *satisfy the condition that the system* (1.1) *admits a non-trivial solution in* $\mathbb{Q}_p$ *for* *every prime number p. Suppose in addition that the number of equivalence classes amongst the forms $\Lambda_j = a_j\alpha + b_j\beta$ $(1 \le j \le s)$ is at most 3. Then whenever $q_0 \ge 7$, one has $\mathcal{N}_s(P) \gg P^{s-6}$.*

We note that the hypothesis $q_0 \ge 7$ by itself ensures that there must be at least 3 equivalence classes amongst the forms Λ_j $(1 \le j \le s)$ when $8 \le s \le 12$, and at least 4 equivalence classes when $8 \le s \le 10$. The discussion in the introduction, moreover, explains why it is that the hypothesis $q_0 \ge 7$ must be imposed, at least until such time as the current state of knowledge concerning the density of rational solutions to (single) diagonal cubic equations in six or fewer variables dramatically improves. The class of simultaneous diagonal cubic equations addressed by Theorem 10 is therefore as broad as it is possible to address given the restriction that there be at most three distinct equivalence classes amongst the forms Λ_j $(1 \le j \le s)$. In addition, we note that although, when $s \le 12$, one may have p-adic obstructions to the solubility of the system (1.1) for any prime number p with $p \equiv 1 \pmod 3$, for each fixed system with $s \ge 4$ and $q_0 \ge 3$ such an obstruction must come from at worst a finite set of primes determined by the coefficients $\mathbf{a}, \mathbf{b}$.

We now sketch the proof of Theorem 10. When $s \ge 13$, of course, the desired conclusion follows already from that of Theorem 2. We suppose henceforth, therefore, that s is equal to either 11 or 12. Next, in view of the discussion of §3, we may take suitable linear combinations of the equations and relabel variables so as to transform the system (1.1) to the shape

$$\sum_{i=1}^{l} \lambda_i x_i^3 = \sum_{j=1}^{m} \mu_j y_j^3 = \sum_{k=1}^{n} \nu_k z_k^3, \tag{7.1}$$

with $\lambda_i, \mu_j, \nu_k \in \mathbb{Z} \setminus \{0\}$ $(1 \le i \le l,\ 1 \le j \le m,\ 1 \le k \le n)$, wherein

$$l \ge m \ge n, \quad l+m+n = s, \quad l+n \ge 7 \quad \text{and} \quad m+n \ge 7. \tag{7.2}$$

By applying the substitution $x_i \to -x_i$, $y_j \to -y_j$ and $z_k \to -z_k$ wherever necessary, moreover, it is apparent that we may assume without loss that all of the coefficients in the system (7.1) are positive. In this way we conclude that

$$\mathcal{N}_s(P) \ge \sum_{1 \le N \le P^3} R_l(N;\boldsymbol{\lambda}) R_m(N;\boldsymbol{\mu}) R_n(N;\boldsymbol{\nu}). \tag{7.3}$$

Finally, we note that the only possible triples (l, m, n) permitted by the constraints (7.2) are $(5, 5, 2)$, $(5, 4, 3)$ and $(4, 4, 4)$ when $s = 12$, and $(4, 4, 3)$ when $s = 11$. We consider these four triples (l, m, n) in turn. Throughout, we write τ for a sufficiently small positive number.

We consider first the triple of multiplicities $(5, 5, 2)$. Let $(\nu_1, \nu_2) \in \mathbb{N}^2$, and denote by $\mathfrak{X}$ the multiset of integers $\{\nu_1 z_1^3 + \nu_2 z_2^3 : z_1, z_2 \in \mathcal{A}(P, P^\eta)\}$. Consider a 5-tuple $\boldsymbol{\xi}$ of natural numbers, and denote by $\mathfrak{X}(P;\boldsymbol{\xi})$ the multiset of integers $N \in \mathfrak{X} \cap [\frac{1}{2}P^3, P^3]$ for which the equation $\xi_1 u_1^3 + \cdots + \xi_5 u_5^3 = N$ possesses a p-adic solution $\mathbf{u}$ for each prime p. It follows from the hypotheses of the statement of the theorem that the multiset $\mathfrak{X}(P;\boldsymbol{\lambda};\boldsymbol{\mu}) = \mathfrak{X}(P;\boldsymbol{\lambda}) \cap \mathfrak{X}(P;\boldsymbol{\mu})$ is non-empty. Indeed, by considering a suitable arithmetic progression determined only by $\boldsymbol{\lambda}$, $\boldsymbol{\mu}$ and $\boldsymbol{\nu}$, a simple counting argument establishes that $\mathrm{card}(\mathfrak{X}(P;\boldsymbol{\lambda};\boldsymbol{\mu})) \gg P^2$. Then by the methods of [**BKW01a**] (see also the discussion following the statement of Theorem 1.2 of [**BKW01b**]), one has the lower bound $R_5(N;\boldsymbol{\lambda}) \gg P^2$ for each $N \in \mathfrak{X}(P;\boldsymbol{\lambda};\boldsymbol{\mu})$ with at most $O(P^{2-\tau})$ possible exceptions. Similarly, one has $R_5(N;\boldsymbol{\mu}) \gg P^2$ for each $N \in \mathfrak{X}(P;\boldsymbol{\lambda};\boldsymbol{\mu})$ with at most $O(P^{2-\tau})$ possible exceptions. Thus we see that for systems with coefficient ratio multiplicity profile $(5,5,2)$, one has the lower bound

$$\begin{aligned} \mathcal{N}_{12}(P) &\geq \sum_{N\in\mathfrak{X}(P;\boldsymbol{\lambda};\boldsymbol{\mu})} R_5(N;\boldsymbol{\lambda})R_5(N;\boldsymbol{\mu}) \\ &\gg (P^2-2P^{2-\tau})(P^2)^2 \gg P^6. \end{aligned} \tag{7.4}$$

Consider next the triple of multiplicities $(5,4,3)$. Let $(\nu_1,\nu_2,\nu_3)\in\mathbb{N}^3$, and take $\tau>0$ as before. We now denote by $\mathfrak{Y}$ the multiset of integers

$$\{\nu_1 z_1^3+\nu_2 z_2^3+\nu_3 z_3^3 \,:\, z_1,z_2,z_3\in\mathcal{A}(P,P^\eta)\}.$$

Consider a v-tuple $\boldsymbol{\xi}$ of natural numbers with $v\geq 4$, and denote by $\mathfrak{Y}_v(P;\boldsymbol{\xi})$ the multiset of integers $N\in\mathfrak{Y}\cap[\frac{1}{2}P^3,P^3]$ for which the equation $\xi_1u_1^3+\cdots+\xi_vu_v^3=N$ possesses a p-adic solution $\mathbf{u}$ for each prime p. The hypotheses of the statement of the theorem ensure that the multiset $\mathfrak{Y}(P;\boldsymbol{\lambda};\boldsymbol{\mu})=\mathfrak{Y}_5(P;\boldsymbol{\lambda})\cap\mathfrak{Y}_4(P;\boldsymbol{\mu})$ is non-empty. Indeed, again by considering a suitable arithmetic progression determined only by $\boldsymbol{\lambda}$, $\boldsymbol{\mu}$ and $\boldsymbol{\nu}$, one may show that $\mathrm{card}(\mathfrak{Y}(P;\boldsymbol{\lambda};\boldsymbol{\mu}))\gg P^3$. When $s\geq 4$, the methods of [**BKW01a**] may on this occasion be applied to establish the lower bound $R_5(N;\boldsymbol{\lambda})\gg P^2$ for each $N\in\mathfrak{Y}(P;\boldsymbol{\lambda};\boldsymbol{\mu})$, with at most $O(P^{3-\tau})$ possible exceptions. Likewise, one obtains the lower bound $R_4(N;\boldsymbol{\mu})\gg P$ for each $N\in\mathfrak{Y}(P;\boldsymbol{\lambda};\boldsymbol{\mu})$, with at most $O(P^{3-\tau})$ possible exceptions. Thus we find that for systems with coefficient ratio multiplicity profile $(5,4,3)$, one has the lower bound

$$\begin{aligned} \mathcal{N}_{12}(P) &\geq \sum_{N\in\mathfrak{Y}(P;\boldsymbol{\lambda};\boldsymbol{\mu})} R_5(N;\boldsymbol{\lambda})R_4(N;\boldsymbol{\mu}) \\ &\gg (P^3-2P^{3-\tau})(P^2)(P) \gg P^6. \end{aligned} \tag{7.5}$$

The triple of multiplicities $(4,4,3)$ may plainly be analysed in essentially the same manner, so that

$$\begin{aligned} \mathcal{N}_{11}(P) &\geq \sum_{N\in\mathfrak{Y}(P;\boldsymbol{\lambda};\boldsymbol{\mu})} R_4(N;\boldsymbol{\lambda})R_4(N;\boldsymbol{\mu}) \\ &\gg (P^3-2P^{3-\tau})(P)^2 \gg P^5. \end{aligned} \tag{7.6}$$

An inspection of the cases listed in the aftermath of equation (7.3) reveals that it is only the multiplicity triple $(4,4,4)$ that remains to be tackled. But here conventional exceptional set technology in combination with available estimates for cubic Weyl sums may be applied. Consider a 4-tuple $\boldsymbol{\xi}$ of natural numbers, and denote by $\mathfrak{Z}(P;\boldsymbol{\xi})$ the set of integers $N\in[\frac{1}{2}P^3,P^3]$ for which the equation $\xi_1u_1^3+\cdots+\xi_4u_4^3=N$ possesses a p-adic solution $\mathbf{u}$ for each prime p. It follows from the hypotheses of the statement of the theorem that the set

$$\mathfrak{Z}(P;\boldsymbol{\lambda};\boldsymbol{\mu};\boldsymbol{\nu})=\mathfrak{Z}(P;\boldsymbol{\lambda})\cap\mathfrak{Z}(P;\boldsymbol{\mu})\cap\mathfrak{Z}(P;\boldsymbol{\nu})$$

is non-empty. But the estimates of Vaughan [**V86**] permit one to prove that the lower bound $R_4(N;\boldsymbol{\lambda})\gg P$ holds for each $N\in\mathfrak{Z}(P;\boldsymbol{\lambda};\boldsymbol{\mu};\boldsymbol{\nu})$ with at most $O(P^3(\log P)^{-\tau})$ possible exceptions, and likewise when $R_4(N;\boldsymbol{\lambda})$ is replaced by $R_4(N;\boldsymbol{\mu})$ or $R_4(N;\boldsymbol{\nu})$. Thus, for systems with coefficient ratio multiplicity profile

(4, 4, 4), one arrives at the lower bound

$$\begin{aligned}\mathcal{N}_{12}(P) &\geq \sum_{N\in\mathfrak{Z}(\boldsymbol{\lambda};\boldsymbol{\mu};\boldsymbol{\nu})} R_4(N;\boldsymbol{\lambda})R_4(N;\boldsymbol{\mu})R_4(N;\boldsymbol{\nu}) \\ &\gg (P^3 - 3P^3(\log P)^{-\tau})(P)^3 \gg P^6. \end{aligned} \tag{7.7}$$

On collecting together (7.4), (7.5), (7.6) and (7.7), the proof of the theorem is complete.

References

[BB88] R. C. Baker & J. Brüdern – "On pairs of additive cubic equations", *J. Reine Angew. Math.* **391** (1988), p. 157–180.

[B90] J. Brüdern – "On pairs of diagonal cubic forms", *Proc. London Math. Soc. (3)* **61** (1990), no. 2, p. 273–343.

[BKW01a] J. Brüdern, K. Kawada & T. D. Wooley – "Additive representation in thin sequences, I: Waring's problem for cubes", *Ann. Sci. École Norm. Sup. (4)* **34** (2001), no. 4, p. 471–501.

[BKW01b] ———, "Additive representation in thin sequences, III: asymptotic formulae", *Acta Arith.* **100** (2001), no. 3, p. 267–289.

[BW01] J. Brüdern & T. D. Wooley – "On Waring's problem for cubes and smooth Weyl sums", *Proc. London Math. Soc. (3)* **82** (2001), no. 1, p. 89–109.

[BW06] ———, "The Hasse principle for pairs of diagonal cubic forms", *Ann. of Math.*, to appear.

[C72] R. J. Cook – "Pairs of additive equations", *Michigan Math. J.* **19** (1972), p. 325–331.

[C85] ———, "Pairs of additive congruences: cubic congruences", *Mathematika* **32** (1985), no. 2, p. 286–300 (1986).

[DL66] H. Davenport & D. J. Lewis – "Cubic equations of additive type", *Philos. Trans. Roy. Soc. London Ser. A* **261** (1966), p. 97–136.

[L57] D. J. Lewis – "Cubic congruences", *Michigan Math. J.* **4** (1957), p. 85–95.

[SD01] P. Swinnerton-Dyer – "The solubility of diagonal cubic surfaces", *Ann. Sci. École Norm. Sup. (4)* **34** (2001), no. 6, p. 891–912.

[V77] R. C. Vaughan – "On pairs of additive cubic equations", *Proc. London Math. Soc. (3)* **34** (1977), no. 2, p. 354–364.

[V86] ———, "On Waring's problem for cubes", *J. Reine Angew. Math.* **365** (1986), p. 122–170.

[V89] ———, "A new iterative method in Waring's problem", *Acta Math.* **162** (1989), no. 1-2, p. 1–71.

[V97] ———, *The Hardy-Littlewood method*, second ed., Cambridge Tracts in Mathematics, vol. 125, Cambridge University Press, Cambridge, 1997.

[W91] T. D. Wooley – "On simultaneous additive equations. II", *J. Reine Angew. Math.* **419** (1991), p. 141–198.

[W00] ———, "Sums of three cubes", *Mathematika* **47** (2000), no. 1-2, p. 53–61 (2002).

[W02] ———, "Slim exceptional sets for sums of cubes", *Canad. J. Math.* **54** (2002), no. 2, p. 417–448.

Institut für Algebra und Zahlentheorie, Pfaffenwaldring 57, Universität Stuttgart, D-70511 Stuttgart, Germany

E-mail address: bruedern@mathematik.uni-stuttgart.de

Department of Mathematics, University of Michigan, 2074 East Hall, 530 Church Street, Ann Arbor, MI 48109-1043, U.S.A.

E-mail address: wooley@umich.edu

Clay Mathematics Proceedings
Volume 7, 2007

Second moments of GL_2 automorphic L-functions

Adrian Diaconu and Dorian Goldfeld

Abstract. The main objective of this paper is to explore a variant of the Rankin-Selberg method introduced by Anton Good about twenty years ago in the context of second integral moments of L-functions attached to modular forms on $SL_2(\mathbb{Z})$. By combining Good's idea with some novel techniques, we shall establish the meromorphic continuation and sharp polynomial growth estimates for certain functions of two complex variables (double Dirichlet series) naturally attached to second integral moments.

1. Introduction

In 1801, in the Disquisitiones Arithmeticae [**Gau01**], Gauss introduced the class number $h(d)$ as the number of inequivalent binary quadratic forms of discriminant d. Gauss conjectured that the average value of $h(d)$ is $\frac{2\pi}{7\zeta(3)}\sqrt{|d|}$ for negative discriminants d. This conjecture was first proved by I. M. Vinogradov [**Vin18**] in 1918. Remarkably, Gauss also made a similar conjecture for the average value of $h(d)\log(\epsilon_d)$, where d ranges over positive discriminants and ϵ_d is the fundamental unit of the real quadratic field $\mathbb{Q}(\sqrt{d})$. Of course, Gauss did not know what a fundamental unit of a real quadratic field was, but he gave the definition that $\epsilon_d = \frac{t+u\sqrt{d}}{2}$, where t, u are the smallest positive integral solutions to Pell's equation $t^2 - du^2 = 4$. For example, he conjectured that

$$d \equiv 0 \pmod 4 \to \sum_{d\le x} h(d)\log(\epsilon_d) \;\sim\; \frac{4\pi^2}{21\zeta(3)}x^{\frac{3}{2}},$$

while

$$d \equiv 1 \pmod 4 \to \sum_{d\le x} h(d)\log(\epsilon_d) \;\sim\; \frac{\pi^2}{18\zeta(3)}x^{\frac{3}{2}}.$$

These latter conjectures were first proved by C. L. Siegel [**Sie44**] in 1944.

In 1831, Dirichlet introduced his famous L–functions

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s},$$

2000 *Mathematics Subject Classification.* Primary 11F66.

where χ is a character (mod q) and $\Re(s) > 1$. The study of moments

$$\sum_q L(s, \chi_q)^m,$$

say, where χ_q is the real character associated to a quadratic field $\mathbb{Q}(\sqrt{q})$, was not achieved until modern times. In the special case when $s = 1$ and $m = 1$, the value of the first moment reduces to the aforementioned conjecture of Gauss because of the Dirichlet class number formula (see [**Dav00**], pp. 43-53) which relates the special value of the L–function $L(1, \chi_q)$ with the class number and fundamental unit of the quadratic field $\mathbb{Q}(\sqrt{q})$.

Let

$$L(s) = \sum_{n=1}^{\infty} a(n) n^{-s}$$

be the L–function associated to a modular form for the modular group. The main focus of this paper is to obtain meromorphic continuation and growth estimates in the complex variable w of the Dirichlet series

$$\int_1^{\infty} \left|L\left(\tfrac{1}{2} + it\right)\right|^k t^{-w} dt.$$

We shall show, by a new method, that it is possible to obtain meromorphic continuation and rather strong growth estimates of the above Dirichlet series for the case $k = 2$. It is then possible, by standard methods, to obtain asymptotics, as $T \to \infty$, for the second integral moment

$$\int_0^T |L(\tfrac{1}{2} + it)|^2 \, dt.$$

In the special case that the modular form is an Eisenstein series this yields asymptotics for the fourth moment of the Riemann zeta-function.

Moment problems associated to the Riemann zeta-function $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$ were intensively studied in the beginning of the last century. In 1918, Hardy and Littlewood [**HL18**] obtained the second moment

$$\int_0^T \left|\zeta\left(\tfrac{1}{2} + it\right)\right|^2 \, dt \;\sim\; T \log T,$$

and in 1926, Ingham [**Ing26**], obtained the fourth moment

$$\int_0^T \left|\zeta\left(\tfrac{1}{2} + it\right)\right|^4 \, dt \;\sim\; \frac{1}{2\pi^2} \cdot T (\log T)^4.$$

Heath-Brown (1979) [**HB81**] obtained the fourth moment with error term of the form

$$\int_0^T \left|\zeta\left(\tfrac{1}{2} + it\right)\right|^4 \, dt \;=\; \frac{1}{2\pi^2} \cdot T \cdot P_4(\log T) \;+\; \mathcal{O}\left(T^{\frac{7}{8}+\epsilon}\right),$$

where $P_4(x)$ is a certain polynomial of degree four.

Let $f(z) = \sum_{n=1}^{\infty} a(n) e^{2\pi i n z}$ be a cusp form of weight κ for the modular group with associated L–function $L_f(s) = \sum_{n=1}^{\infty} a(n) n^{-s}$. Anton Good [**Goo82**] made a significant breakthrough in 1982 when he proved that

$$\int_0^T \left|L_f\left(\tfrac{\kappa}{2}+it\right)\right|^2 dt \;=\; 2aT(\log(T)+b)+\mathcal{O}\left((T\log T)^{\frac{2}{3}}\right)$$

for certain constants a, b. It seems likely that Good's method can apply to Eisenstein series.

In 1989, Zavorotny [**Zav89**], improved Heath-Brown's 1979 error term to

$$\int_0^T \left|\zeta\left(\tfrac{1}{2}+it\right)\right|^4 \, dt \;=\; \frac{1}{2\pi^2}\cdot T\cdot P_4(\log T) \;+\; \mathcal{O}\left(T^{\frac{2}{3}+\epsilon}\right).$$

Shortly afterwards, Motohashi [**Mot92**], [**Mot93**] slightly improved the above error term to

$$\mathcal{O}\left(T^{\frac{2}{3}}(\log T)^B\right)$$

for some constant $B > 0$. Motohashi introduced the double Dirichlet series [**Mot95**], [**Mot97**]

$$\int_1^\infty \zeta(s+it)^2\zeta(s-it)^2 t^{-w}\, dt$$

into the picture and gave a spectral interpretation to the moment problem.

Unfortunately, an old paper of Anton Good [**Goo86**], going back to 1985, which had much earlier outlined an alternative approach to the second moment problem for $GL(2)$ automorphic forms using Poincaré series has been largely forgotten. Using Good's approach, it is possible to recover the aforementioned results of Zavorotny and Motohashi. It is also possible to generalize this method to more general situations; for instance see [**DG**], where the case of $GL(2)$ automorphic forms over an imaginary quadratic field is considered. Our aim here is to explore Good's method and show that it is, in fact, an exceptionally powerful tool for the study of moment problems.

Second moments of $GL(2)$ Maass forms were investigated in [**Jut97**], [**Jut05**]. Higher moments of L–functions associated to automorphic forms seem out of reach at present. Even the conjectured values of such moments were not obtained until fairly recently (see [**CF00**], [**CG01**], [**CFK$^+$**], [**CG84**], [**DGH03**], [**KS99**], [**KS00**]).

Let $\mathcal{H}$ denote the upper half-plane. A complex valued function f defined on $\mathcal{H}$ is called an automorphic form for $\Gamma = SL_2(\mathbb{Z})$, if it satisfies the following properties:

(1) We have

$$f\left(\frac{az+b}{cz+d}\right) \;=\; (cz+d)^\kappa f(z) \qquad \text{for } \begin{pmatrix} a & b\\ c & d\end{pmatrix}\in\Gamma;$$

(2) $f(iy) = \mathcal{O}(y^\alpha)$ for some α, as $y\to\infty$;

(3) κ is either an even positive integer and f is holomorphic, or $\kappa = 0$, in which case, f is an eigenfunction of the non-euclidean Laplacian $\Delta = -y^2\left(\frac{\partial^2}{\partial x^2}+\frac{\partial^2}{\partial y^2}\right)$ $(z = x+iy\in\mathcal{H})$ with eigenvalue λ. In the first case, we call f a modular form of weight κ, and in the second, we call f a Maass form with eigenvalue λ.

In addition, if f satisfies

$$\int_0^1 f(x+iy)\, dx \;=\; 0,$$

then it is called a cusp form.

Let f and g be two cusp forms for Γ of the same weight κ (for Maass forms we take $\kappa = 0$) with Fourier expansions

$$f(z) = \sum_{m\neq 0} a_m \, |m|^{\frac{\kappa-1}{2}} \, W(mz), \;\; g(z) = \sum_{n\neq 0} b_n \, |n|^{\frac{\kappa-1}{2}} \, W(nz) \;\; (z = x+iy, \; y > 0).$$

Here, if f, for example, is a modular form, $W(z) = e^{2\pi i z}$, and the sum is restricted to $m \geq 1$, while if f is a Maass form with eigenvalue $\lambda_1 = \frac{1}{4} + r_1^2$,

$$W(z) = W_{\frac{1}{2}+ir_1}(z) = y^{\frac{1}{2}} K_{ir_1}(2\pi y) e^{2\pi i x} \qquad (z = x+iy, \; y > 0),$$

where $K_\nu(y)$ is the K–Bessel function. Throughout, we shall assume that both f and g are eigenfunctions of the Hecke operators, normalized so that the first Fourier coefficients $a_1 = b_1 = 1$. Furthermore, if f and g are Maass cusp forms, we shall assume them to be even.

Associated to f and g, we have the L–functions:

$$L_f(s) = \sum_{m=1}^{\infty} a_m m^{-s}; \qquad L_g(s) = \sum_{n=1}^{\infty} b_n n^{-s}.$$

In [**Goo86**], Anton Good found a natural method to obtain the meromorphic continuation of multiple Dirichlet series of type

$$\int_1^\infty L_f(s_1+it) L_g(s_2-it) \, t^{-w} \, dt, \tag{1.1}$$

where $L_f(s)$ and $L_g(s)$ are the L–functions associated to automorphic forms f and g on $GL(2,\mathbb{Q})$. For fixed g and fixed $s_1, s_2, w \in \mathbb{C}$, the integral (1.1) may be interpreted as the image of a linear map from the Hilbert space of cusp forms to $\mathbb{C}$ given by

$$f \;\longrightarrow\; \int_1^\infty L_f(s_1+it) L_g(s_2-it) \, t^{-w} \, dt.$$

The Riesz representation theorem guarantees that this linear map has a kernel. Good computes this kernel explicitly. For example when $s_1 = s_2 = \frac{1}{2}$, he shows that there exists a Poincaré series P_w and a certain function K such that

$$\langle f, \; \bar{P}_w g \rangle = \int_{-\infty}^{\infty} L_f(\tfrac{1}{2}+it) \overline{L_g(\tfrac{1}{2}+it)} \; K(t,w) \, dt,$$

where $\langle \;, \; \rangle$ denotes the Petersson inner product on the Hilbert space of cusp forms. Remarkably, it is possible to choose P_w so that

$$K(t,w) \sim |t|^{-w}, \qquad (\text{as } |t| \to \infty).$$

Good's approach has been worked out for congruence subgroups in [**Zha**].

There are, however, two serious obstacles in Good's method.

- *Although $K(t,w) \sim |t|^{-w}$ as $|t| \to \infty$ and w fixed, it has a quite different behavior when $t \ll |\Im(w)|$. In this case it grows exponentially in $|t|$.*
- *The function $\langle f, \; \bar{P}_w g \rangle$ has infinitely many poles in w, occurring at the eigenvalues of the Laplacian. So there is a problem to obtain polynomial growth in w by the use of convexity estimates such as the Phragmén-Lindelöf theorem.*

In this paper, we introduce novel techniques for surmounting the above two obstacles. The key idea is to use instead another function K_β, instead of K, so that (1.1) satisfies a functional equation $w \to 1 - w$. This allows one to obtain growth estimates for (1.1) in the regions $\Re(w) > 1$ and $-\epsilon < \Re(w) < 0$. In order to apply the Phragmén-Lindelöf theorem, one constructs an auxiliary function with the same poles as (1.1) and which has good growth properties. After subtracting this auxiliary function from (1.1), one may apply the Phragmen-Lindelöf theorem. It appears that the above methods constitute a new technique which may be applied in much greater generality. We will address these considerations in subsequent papers.

For $\Re(w)$ sufficiently large, consider the function $Z(w)$ defined by the absolutely convergent integral

$$Z(w) = \int_1^\infty L_f(\tfrac{1}{2} + it) L_g(\tfrac{1}{2} - it) t^{-w}\, dt. \tag{1.2}$$

The main object of this paper is to prove the following.

THEOREM 1.3. *Suppose f and g are two cusp forms of weight $\kappa \geq 12$ for $SL(2, \mathbb{Z})$. The function $Z(w)$, originally defined by* (1.2) *for $\Re(w)$ sufficiently large, has a meromorphic continuation to the half-plane $\Re(w) > -1$, with at most simple poles at*

$$w = 0,\ \frac{1}{2} + i\mu,\ -\frac{1}{2} + i\mu,\ \frac{\rho}{2},$$

where $\frac{1}{4} + \mu^2$ is an eigenvalue of Δ and $\zeta(\rho) = 0$; when $f = g$, it has a pole of order two at $w = 1$. Furthermore, for fixed $\epsilon > 0$, and $\epsilon < \delta < 1 - \epsilon$, we have the growth estimate

$$Z(\delta + i\eta) \ll_\epsilon (1 + |\eta|)^{2 - \frac{3\delta}{4}}, \tag{1.4}$$

provided $|w|, |w-1|, |w \pm \frac{1}{2} - \mu|, \left|w - \frac{\rho}{2}\right| > \epsilon$ with $w = \delta + i\eta$, and for all μ, ρ, as above.

Note that in the special case when $f(z) = g(z)$ is the usual $SL_2(\mathbb{Z})$ Eisenstein series at $s = \frac{1}{2}$ (suitably renormalized), a stronger result is already known (see [**IJM00**] and [**Ivi02**]) for $\Re(\delta) > \frac{1}{2}$. It is remarked in [**IJM00**] that their methods can be extended to holomorphic cusp forms, but that obtaining such results for Maass forms is problematic.

2. Poincaré series

To obtain Theorem 1.3, we shall need two Poincaré series, the second one being first considered by A. Good in [**Goo86**]. The first Poincaré series $P(z; v, w)$ is defined by

$$P(z; v, w) = \sum_{\gamma \in \Gamma / Z} (\Im(\gamma z))^v \left(\frac{\Im(\gamma z)}{|\gamma z|} \right)^w \qquad (Z = \{\pm I\}). \tag{2.1}$$

This series converges absolutely for $\Re(v)$ and $\Re(w)$ sufficiently large. Writing

$$P(z; v, w) = \frac{1}{2} \sum_{\gamma \in SL_2(\mathbb{Z})} y^{v+w} |z|^{-w} \Big| [\gamma] = \sum_{\gamma \in \Gamma_\infty \backslash \Gamma} y^{v+w} \cdot \sum_{m=-\infty}^{\infty} |z + m|^{-w} \Big| [\gamma],$$

and using the well-known Fourier expansion of the above inner sum, one can immediately write

$$
\begin{aligned}
(2.2)\qquad P(z;v,w) &= \sqrt{\pi}\,\frac{\Gamma\left(\frac{w-1}{2}\right)}{\Gamma\left(\frac{w}{2}\right)}\,E(z,v+1)\\
&+ 2\,\pi^{\frac{w}{2}}\Gamma\Big(\frac{w}{2}\Big)^{-1}\sum_{\substack{k=-\infty\\ k\neq 0}}^{\infty}|k|^{\frac{w-1}{2}}P_k\Big(z;v+\frac{w}{2},\frac{w-1}{2}\Big),
\end{aligned}
$$

where $\Gamma(s)$ is the usual Gamma function, $E(z,s)$ is the classical non-holomorphic Eisenstein series for $SL_2(\mathbb{Z})$, and $P_k(z;v,s)$ is the classical Poincaré series defined by

$$
(2.3)\qquad P_k(z;v,s) = |k|^{-\frac{1}{2}}\sum_{\gamma\in\Gamma_\infty\backslash\Gamma}(\Im(\gamma z))^v\,W_{\frac{1}{2}+s}(k\cdot\gamma z).
$$

It is not hard to show that $P_k(z;v,s)\in L^2\big(\Gamma\backslash\mathcal{H}\big)$, for $|\Re(s)|+\frac{3}{4}>\Re(v)>|\Re(s)|+\frac{1}{2}$ (see [**Zha**]).

To define the second Poincaré series $P_\beta(z,w)$, let $\beta(z,w)$ be defined for $z\in\mathcal{H}$ and $\Re(w)>0$ by

$$
(2.4)\qquad \beta(z,w) = \begin{cases} \frac{1}{i}\int\limits_{-\log z}^{-\log\bar{z}}\left[\frac{2ye^\xi}{(ze^\xi-1)(\bar{z}e^\xi-1)}\right]^{1-w}d\xi & \text{if } \Re(z) = x\geq 0 \text{ and } \Re(w)>0\,,\\[2ex] \beta(-\bar{z},w) & \text{if } x<0,\end{cases}
$$

where the logarithm takes its principal values, and the integration is along a vertical line segment. It can be easily checked that $\beta(z,w)$ satisfies the following two properties:

$$
(2.5)\qquad \beta(\alpha z,w) = \beta(z,w)\qquad (\alpha>0),
$$

and for z off the imaginary axis,

$$
(2.6)\qquad \Delta\beta = w(1-w)\beta.
$$

If we write $z=re^{i\theta}$ with $r>0$ and $0<\theta<\frac{\pi}{2}$, then by (2.4) and (2.5), we have

$$
\begin{aligned}
\beta(z,w) &= \beta\big(e^{i\theta},w\big) = \frac{1}{i}\int\limits_{-i\theta}^{i\theta}\left[\frac{2\,e^\xi\sin\theta}{(e^{\xi+i\theta}-1)(e^{\xi-i\theta}-1)}\right]^{1-w}d\xi\\
(2.7)\qquad &= \int\limits_{-\theta}^{\theta}\left[\frac{2\,e^{it}\sin\theta}{(e^{i(t+\theta)}-1)(e^{i(t-\theta)}-1)}\right]^{1-w}dt\\
&= \int\limits_{-\theta}^{\theta}\left(\frac{\sin\theta}{\cos t-\cos\theta}\right)^{1-w}dt\\
&= \sqrt{2\pi\sin\theta}\;\Gamma(w)\,P_{-\frac{1}{2}}^{\frac{1}{2}-w}(\cos\theta),
\end{aligned}
$$

where $P_\nu^\mu(z)$ is the spherical function of the first kind. This function is a solution of the differential equation

$$(1-z^2)\,\frac{d^2u}{dz^2} - 2z\,\frac{du}{dz} + \left[\nu(\nu+1) - \frac{\mu^2}{1-z^2}\right] u \;=\; 0 \qquad (\mu,\,\nu \in \mathbb{C}). \tag{2.8}$$

There is another linearly independent solution of (2.8) denoted by $Q_\nu^\mu(z)$ and called the spherical function of the second kind. We shall need these functions for real values of $z = x$ and $-1 \le x \le 1$. For these values, one can take as linearly independent solutions the functions defined by

$$P_\nu^\mu(x) \;=\; \frac{1}{\Gamma(1-\mu)}\left(\frac{1+x}{1-x}\right)^{\frac{\mu}{2}} F\left(-\nu, \nu+1; 1-\mu; \frac{1-x}{2}\right); \tag{2.9}$$

$$Q_\nu^\mu(x) \;=\; \frac{\pi}{2\sin\mu\pi}\left[P_\nu^\mu(x)\cos\mu\pi - \frac{\Gamma(\nu+\mu+1)}{\Gamma(\nu-\mu+1)}P_\nu^{-\mu}(x)\right]. \tag{2.10}$$

Here

$$F(\alpha,\beta;\gamma;z) \;=\; \frac{\Gamma(\gamma)}{\Gamma(\alpha)\Gamma(\beta)}\cdot\sum_{n=0}^{\infty}\frac{1}{n!}\,\frac{\Gamma(\alpha+n)\Gamma(\beta+n)}{\Gamma(\gamma+n)}\,z^n$$

is the Gauss hypergeometric function. We shall need an additional formula (see [**GR94**], page 1023, 8.737-2) relating the spherical functions, namely

$$P_\nu^\mu(-x) \;=\; P_\nu^\mu(x)\cos[(\mu+\nu)\pi] - \frac{2}{\pi}\,Q_\nu^\mu(x)\sin[(\mu+\nu)\pi]. \tag{2.11}$$

Now, we define the second Poincaré series $P_\beta(z,w)$ by

$$P_\beta(z,w) \;=\; \sum_{\gamma\in\Gamma/Z}\beta(\gamma z, w) \qquad (Z \;=\; \{\pm I\}). \tag{2.12}$$

It can be observed that the series in the right hand side converges absolutely for $\Re(w) > 1$.

3. Multiple Dirichlet series

Fix two cusp forms f, g of weight κ for $\Gamma = SL(2,\mathbb{Z})$ as in Section 1. Here f, g are holomorphic for $\kappa \ge 12$ and are Maass forms if $\kappa = 0$. Define

$$F(z) = y^\kappa\overline{f(z)}g(z).$$

For complex variables s_1, s_2, w, we are interested in studying the multiple Dirichlet series of type

$$\int_1^\infty L_f\,(s_1+it)\,L_g\,(s_2-it)\,t^{-w}\,dt.$$

As was first discovered by Good [**Goo86**], such series can be constructed by considering inner products of F with Poincaré series of the type that we have introduced in Section 2. Good shows that such inner products lead to multiple Dirichlet series of the form

$$\int_0^\infty L_f\,(s_1+it)\,L_g\,(s_2-it)\,K(s_1,s_2,t,w)\,dt,$$

with a suitable kernel function $K(s_1, s_2, t, w)$. One of the main difficulties of the theory is to obtain kernel functions K with good asymptotic behavior. The following kernel functions arise naturally in our approach.

First, if f, g are holomorphic cusp forms of weight κ, then we define:

$$K(s;v,w) \;=\; 2^{1-w-2v-2\kappa}\,\pi^{-v-\kappa}\,\frac{\Gamma(w+v+\kappa-1)\,\Gamma(s)\,\Gamma(v+\kappa-s)}{\Gamma\big(\frac{w}{2}+s\big)\,\Gamma\big(\frac{w}{2}+v+\kappa-s\big)}; \tag{3.1}$$

$$\begin{aligned} &K_\beta(t,w) \;=\\ &\quad 2^{1-\kappa}\,\pi^{-\kappa-1}\left|\Gamma\Big(\frac{\kappa}{2}+it\Big)\right|^2 \int_0^{\frac{\pi}{2}} \beta\big(e^{i\theta},w\big)\sin^{\kappa-2}(\theta)\,\cosh[t(2\theta-\pi)]\,d\theta. \end{aligned} \tag{3.2}$$

Also, for $0<\theta<2\pi$, let $\widetilde{W}_{\frac{1}{2}+\nu}\left(e^{i\theta},s\right)$ denote the Mellin transform of $W_{\frac{1}{2}+\nu}\left(ue^{i\theta}\right)$. Then, if f and g are both Maass cusp forms, we define $K(s;v,w)$ and $K_\beta(t,w)$ with $t\ge 0$, by

$$\begin{aligned} &K(s;v,w) \;=\\ &\sum_{\epsilon_1,\,\epsilon_2=\pm1}\int_0^{\pi} \widetilde{W}_{\frac12+ir_1}\left(\epsilon_1 e^{i\theta},\,s\right)\;\overline{\widetilde{W}_{\frac12+ir_2}\left(\epsilon_2\,e^{i\theta},\,\bar v-\bar s\right)}\,\sin^{v+w-2}(\theta)\,d\theta; \end{aligned} \tag{3.3}$$

$$\begin{aligned} &K_\beta(t,w) \;=\\ &\sum_{\epsilon_1,\,\epsilon_2=\pm1}\int_0^{\pi} \beta\big(e^{i\theta},w\big)\sin^{-2}(\theta)\,\widetilde{W}_{\frac12+ir_1}\left(\epsilon_1 e^{i\theta},\,it\right)\overline{\widetilde{W}_{\frac12+ir_2}\left(\epsilon_2\,e^{i\theta},\,it\right)}\,d\theta. \end{aligned} \tag{3.4}$$

We have the following.

Proposition 3.5. *Fix two cusp forms f, g of weight κ for $SL(2,\mathbb{Z})$ with associated L-functions $L_f(s), L_g(s)$. For $\Re(v)$ and $\Re(w)$ sufficiently large, we have*

$$\begin{aligned} &\langle P(*;\,v,w),\,F\rangle =\\ &\quad\int_{-\infty}^{\infty} L_f\left(\sigma-\frac{\kappa}{2}+\frac12+it\right)L_g\left(v+\frac{\kappa}{2}+\frac12-\sigma-it\right)K(\sigma+it;v,w)\,dt, \end{aligned}$$

and

$$\langle P_\beta(*;\,w),\,F\rangle = \int_0^{\infty} L_f(\tfrac12+it)L_g(\tfrac12-it)K_\beta(t,w)\,dt,$$

where $K(s;v,w)$, $K_\beta(t,w)$ are given by (3.1) *and* (3.2)*, if f and g are holomorphic, and by* (3.3) *and* (3.4)*, if f and g are both Maass cusp forms.*

Proof. We evaluate

$$I(v,w) \;=\; \langle P(*;v,w),F\rangle \;=\; \int\!\!\int_{\Gamma\backslash\mathcal{H}} P(z;v,w)f(z)\overline{g(z)}\,y^{\kappa}\,\frac{dx\,dy}{y^2}$$

by the unfolding technique. We have

$$I(v,w) = \\ = \int_0^\infty \int_{-\infty}^\infty f(z)\overline{g(z)}\,|z|^{-w} y^{v+w+\kappa-2}\, dx\, dy = \\ = \int_0^\pi \int_0^\infty f\left(re^{i\theta}\right)\overline{g\left(re^{i\theta}\right)}\, r^{v+\kappa-1} \sin^{v+w+\kappa-2}(\theta)\, dr\, d\theta = \\ = \sum_{m,\,n\neq 0} \frac{a_m b_n}{|mn|^{\frac{1-\kappa}{2}}} \int_0^\pi\int_0^\infty W_{\frac12+ir_1}\left(mre^{i\theta}\right)\overline{W_{\frac12+ir_2}\left(nre^{i\theta}\right)}\, r^{v+\kappa-1}\sin^{v+w+\kappa-2}(\theta)\, dr\, d\theta.$$

By Mellin transform theory, we may express

$$W_{\frac12+ir_1}\left(mre^{i\theta}\right) = \frac{1}{2\pi i}\int_{(\sigma)}\int_0^\infty W_{\frac12+ir_1}\left(mue^{i\theta}\right) u^s\, \frac{du}{u}\, r^{-s}\, ds.$$

Making the substitution $u \mapsto \frac{u}{|m|}$, we have

$$W_{\frac12+ir_1}\left(re^{i\theta}\right) = \frac{1}{2\pi i}\int_{(\sigma)}\int_0^\infty W_{\frac12+ir_1}\left(\frac{m}{|m|}\,ue^{i\theta}\right)\frac{u^s}{|m|^s}\,\frac{du}{u}\, r^{-s}\, ds.$$

Plugging this in the last expression of $\langle P(\cdot; v,w), F\rangle$, we obtain

$$I(v,w) = \frac{1}{2\pi i}\int_{(\sigma)}\sum_{m,\,n\neq 0}\frac{a_m b_n}{|m|^{s+\frac{1-\kappa}{2}}|n|^{\frac{1-\kappa}{2}}}\int_0^\pi\int_0^\infty W_{\frac12+ir_1}\left(\frac{m}{|m|}\,ue^{i\theta}\right)u^s\,\frac{du}{u} \\ \cdot\int_0^\infty \overline{W_{\frac12+ir_2}\left(nre^{i\theta}\right)}\, r^{v-s+\kappa}\,\frac{dr}{r}\cdot\sin^{v+w+\kappa-2}(\theta)\, d\theta\, ds.$$

Recall that if f and g are Maass forms, then both are even. The proposition immediately follows by making the substitution $r \mapsto \frac{r}{|n|}$.

The second formula in Proposition 3.5 can be proved by a similar argument. □

4. The kernels $K(t,w)$ and $K_\beta(t,w)$

In this section, we shall study the behavior in the variable t of the kernels

$$K(t,w) := K\Big(\frac{\kappa}{2}+it;0,w\Big) \\ = 2^{1-w-2\kappa}\,\pi^{-\kappa}\,\frac{\Gamma(w+\kappa-1)\,\Gamma\left(\frac{\kappa}{2}+it\right)\,\Gamma(\frac{\kappa}{2}-it)}{\Gamma\big(\frac{w}{2}+\frac{\kappa}{2}+it\big)\,\Gamma\big(\frac{w}{2}+\frac{\kappa}{2}-it\big)} \tag{4.1}$$

and $K_\beta(t,w)$ given by (3.2). This will play an important role in the sequel. We begin by proving the following.

PROPOSITION 4.2. *For $t \gg 0$, the kernels $K(t,w)$ and $K_\beta(t,w)$ are meromorphic functions of the variable w. Furthermore, for $-1 < \Re(w) < 2$, $|\Im(w)| \to \infty$, we have the asymptotic formulae*

$$K(t,w) = \mathcal{A}(w)\,t^{-w}\cdot\left(1 + \mathcal{O}_\kappa\left(\frac{|\Im(w)|^4}{t^2}\right)\right), \tag{4.3}$$

$$\begin{aligned} K_\beta(t,w) &= \\ &= 2^{1-\kappa}\,\pi^{-\kappa-1}|\Gamma(\tfrac{\kappa}{2}+it)|^2\int\limits_0^{\frac{\pi}{2}}\beta\big(e^{i\theta},w\big)\sin^{\kappa-2}(\theta)\,\cosh[t(2\theta-\pi)]\,d\theta \qquad (4.4)\\ &= \mathcal{B}(w)\,t^{-w}\left(1+\mathcal{O}_\kappa\left(\frac{|\Im(w)|^3}{t^2}\right)\right), \end{aligned}$$

where

$$\mathcal{A}(w)=\frac{\Gamma(w+\kappa-1)}{2^{2\kappa+w-1}\,\pi^\kappa}\quad \textit{and}\quad \mathcal{B}(w)=\frac{2\pi^{w-\frac12}\Gamma(w)\Gamma(w+\kappa-1)}{\Gamma(w+\frac12)(4\pi)^{\kappa+w-1}}.$$

PROOF. Let s and a be complex numbers with $|a|$ large and $|a|<|s|^{\frac12}$. Using the well-known asymptotic representation for large values of $|s|$:

$$\Gamma(s)=\sqrt{2\pi}\cdot s^{s-\frac12}\,e^{-s}\left(1+\frac{1}{12\,s}+\frac{1}{288\,s^2}-\frac{139}{51840\,s^3}\;+\;\mathcal{O}\left(|s|^{-4}\right)\right),$$

which is valid provided $-\pi<\arg(s)<\pi$, we have

$$\begin{aligned} \frac{\Gamma(s)}{\Gamma(s+a)} &= s^{-a}\left(1+\frac{a}{s}\right)^{-s-a+\frac12}\\ &\quad e^a\cdot\left(1-\frac{1}{12\,(s+a)}\;+\;\mathcal{O}\left(|s|^{-2}\right)\right)\left(1+\frac{1}{12\,s}\;+\;\mathcal{O}\left(|s|^{-2}\right)\right). \end{aligned}$$

Since $|s|>|a|^2$, it easily follows that

$$(\tfrac12-s-a)\log\left(1+\frac{a}{s}\right)+a\;=\;\frac{a\,(1-a)}{2\,s}\;+\;\frac{a^3}{6\,s^2}\;+\;\mathcal{O}\left(|a|^2|s|^{-2}\right).$$

Consequently,

$$\begin{aligned} \tfrac{\Gamma(s)}{\Gamma(s+a)} \;=\; s^{-a}e^{\frac{a\,(1-a)}{2\,s}+\frac{a^3}{6\,s^2}+\mathcal{O}\left(|a|^2|s|^{-2}\right)}\cdot\left(1-\tfrac{1}{12\,(s+a)}\;+\;\mathcal{O}\left(|s|^{-2}\right)\right)\\ \cdot\left(1+\tfrac{1}{12\,s}\;+\;\mathcal{O}\left(|s|^{-2}\right)\right). \end{aligned}$$

Now, we have by the Taylor expansion that

$$e^{\frac{a\,(1-a)}{2\,s}+\frac{a^3}{6\,s^2}}=1+\frac{a(1-a)}{2s}+\mathcal{O}\left(\frac{|a|^4}{|s|^2}\right).$$

It follows that

$$\frac{\Gamma(s)}{\Gamma(s+a)}\;=\;s^{-a}\left(1+\frac{a(1-a)}{2s}+\mathcal{O}\left(\frac{|a|^4}{|s^2|}\right)\right). \qquad (4.5)$$

Now

$$K(t,w)=2^{1-w-2\kappa}\,\pi^{-\kappa}\,\Gamma(w+\kappa-1)\,\frac{\Gamma\left(\frac{\kappa}{2}+it\right)\,\Gamma(\frac{\kappa}{2}-it)}{\Gamma\left(\frac{w}{2}+\frac{\kappa}{2}+it\right)\Gamma\left(\frac{w}{2}+\frac{\kappa}{2}-it\right)}.$$

We may apply (4.5) (with $s=\frac{\kappa}{2}\pm it,\ a=\frac{w}{2}$) to obtain (for $t\to\infty$)

$$\begin{aligned} K(t,w) &= \tfrac{\Gamma(w+\kappa-1)}{2^{2\kappa+w-1}\,\pi^\kappa}\,\left|\tfrac{\kappa}{2}+it\right|^{-w}\cdot\left(1\;+\;\mathcal{O}\left(\tfrac{|w|^4}{\kappa^2+t^2}\right)\right)\\ &= \tfrac{\Gamma(w+\kappa-1)}{2^{2\kappa+w-1}\,\pi^\kappa}\,t^{-w}\cdot\left(1\;+\;\mathcal{O}\left(\tfrac{|w|^4}{t^2}\right)\right). \end{aligned}$$

This proves the asymptotic formula (4.3). □

We now continue on to the proof of (4.4). Recall that

$$K_\beta(t,w) \;=\; \frac{4|\Gamma(\frac{\kappa}{2}+it)|^2}{(2\pi)^{\kappa+1}}\int_0^{\frac{\pi}{2}} \beta\big(e^{i\theta},w\big)\sin^{\kappa-2}(\theta)\,\cosh[t(2\theta-\pi)]\,d\theta.$$

We shall split the θ–integral into two parts. Accordingly, we write

$$K_\beta(t,w) \;=$$
$$= \frac{4|\Gamma(\frac{\kappa}{2}+it)|^2}{(2\pi)^{\kappa+1}}\left(\int_0^{|\Im(w)|^{-\frac12}} + \int_{|\Im(w)|^{-\frac12}}^{\frac{\pi}{2}}\right)\beta\big(e^{i\theta},w\big)\sin^{\kappa-2}(\theta)\,\cosh[t(2\theta-\pi)]\,d\theta.$$

First of all, we may assume $t \gg |\Im(w)|^{\frac32+\epsilon}$. Otherwise, the asymptotic formula (4.4) is not valid.

$$\begin{aligned}
&\int_{|\Im(w)|^{-\frac12}}^{\frac{\pi}{2}} \beta\big(e^{i\theta},w\big)\sin^{\kappa-2}(\theta)\,\cosh[t(2\theta-\pi)]\,d\theta\\
&\qquad\ll\quad e^{\pi t}e^{-\frac{2t}{\sqrt{|\Im(w)|}}}\cdot \max_{|\Im(w)|^{-\frac12}\le\theta\le\frac{\pi}{2}} \big|\,\beta\big(e^{i\theta},w\big)\big|\\
&\qquad\ll\quad e^{\pi t}e^{-|\Im(w)|^{1+\epsilon}},
\end{aligned}$$

since $t \gg |\Im(w)|^{\frac32+\epsilon}$ and $\beta\left(e^{i\theta},w\right)$ is bounded. It follows that

$$\begin{aligned}
K_\beta(t,w) \quad&=\quad \frac{4|\Gamma(\frac{\kappa}{2}+it)|^2}{(2\pi)^{\kappa+1}}\int_0^{|\Im(w)|^{-\frac12}} \beta\big(e^{i\theta},w\big)\sin^{\kappa-2}(\theta)\,\cosh[t(2\theta-\pi)]\,d\theta\\
&\qquad\qquad + \quad \mathcal{O}\left(e^{-|\Im(w)|^{1+\epsilon}}\right)\\
&=\quad \frac{2|\Gamma(\frac{\kappa}{2}+it)|^2\cdot e^{\pi t}}{(2\pi)^{\kappa+1}}\int_0^{|\Im(w)|^{-\frac12}} \beta\big(e^{i\theta},w\big)\sin^{\kappa-2}(\theta)\,e^{-2\theta t}\,d\theta\\
&\qquad\qquad +\mathcal{O}\left(e^{-|\Im(w)|^{1+\epsilon}}\right).
\end{aligned}$$

Now, for $\theta \ll |\Im(w)|^{-\frac12}$, we have

$$\begin{aligned}
&\beta\left(e^{i\theta},w\right)\\
&= \int_{-\theta}^{\theta}\left(\tfrac{\sin\theta}{\cos u-\cos\theta}\right)^{1-w}\,du\\
&= 2(\sin\theta)^{1-w}\cdot\theta\int_0^1 \big(\cos(\theta u)-\cos(\theta)\big)^{w-1}\,du\\
&= 2(\sin\theta)^{1-w}\cdot\theta\int_0^1 \left(\theta^2\,\tfrac{(1-u^2)}{2!}-\theta^4\,\tfrac{(1-u^4)}{4!}+\theta^6\,\tfrac{(1-u^6)}{6!}\;-\;\cdots\right)^{w-1}\,du\\
&= \sqrt{\pi}\;2^{1-w}(\sin\theta)^{1-w}\cdot\theta^{2w-1}\left[\tfrac{\Gamma(w)}{\Gamma\left(\frac12+w\right)}\;+\;\tfrac{\theta^2(w-1)}{6}\left(-\tfrac{2\Gamma(w)}{\Gamma\left(\frac12+w\right)}+\tfrac{\Gamma(1+w)}{\Gamma\left(\frac32+w\right)}\right)\;+\cdots\right]\\
&= \sqrt{\pi}\;2^{1-w}(\sin\theta)^{1-w}\cdot\theta^{2w-1}\left[\tfrac{\Gamma(w)}{\Gamma\left(\frac12+w\right)}\left(1+\theta^2h_2(w)+\theta^4h_4(w)+\theta^6h_6(w)\;+\cdots\right)\right],
\end{aligned}$$

where

$$h_2(w) = \frac{1-w^2}{6+12w}, \qquad h_4(w) = \frac{(w-1)(-21-5w+9w^2+5w^3)}{360(3+8w+4w^2)},$$

$$h_6(w) = \frac{(1-w)(3+w)(465-314w-80w^2+14w^3+35w^4)}{45360(1+2w)(3+2w)(5+2w)}, \qquad \cdots$$

and where $h_{2\ell}(w) = \mathcal{O}\left(|\Im(w)|^\ell\right)$ for $\ell = 1,2,3,\ldots$, and

$$\frac{\Gamma(w)}{\Gamma\left(\frac{1}{2}+w\right)}\left(1+\theta^2 h_2(w)+\theta^4 h_4(w)+\theta^6 h_6(w) \;+\; \cdots\right)$$

converges absolutely for all $w \in \mathbb{C}$ and any fixed θ.

We may now substitute this expression for $\beta\left(e^{i\theta}, w\right)$ into the above integral for $K_\beta(t,w)$. We then obtain

$$K_\beta(t,w) =$$

$$= \frac{|\Gamma\left(\frac{\kappa}{2}+it\right)|^2\cdot e^{\pi t}\,\Gamma(w)}{2^{\kappa+w-1}\pi^{\frac{1}{2}+\kappa}\,\Gamma\left(\frac{1}{2}+w\right)} \int\limits_0^{|\Im(w)|^{-\frac{1}{2}}} (\sin\theta)^{\kappa-w-1}\theta^{2w-1}\, e^{-2\theta t}\left(1+\theta^2 h_2(w)+\;\cdots\right) d\theta \\ + \;\mathcal{O}\left(e^{-|\Im(w)|^{1+\epsilon}}\right)$$

$$= \frac{|\Gamma\left(\frac{\kappa}{2}+it\right)|^2\cdot e^{\pi t}\,\Gamma(w)}{2^{\kappa+w-1}\pi^{\frac{1}{2}+\kappa}\,\Gamma\left(\frac{1}{2}+w\right)} \int\limits_0^{|\Im(w)|^{-\frac{1}{2}}} \theta^{\kappa+w-2}\, e^{-2\theta t}\left(1+\theta^2 \tilde{h}_2(w)+\theta^4\tilde{h}_4(w)+\;\cdots\right) d\theta \\ +\mathcal{O}\left(e^{-|\Im(w)|^{1+\epsilon}}\right)$$

$$= \frac{|\Gamma\left(\frac{\kappa}{2}+it\right)|^2\cdot e^{\pi t}\,\Gamma(w)}{2^{\kappa+w-1}\pi^{\frac{1}{2}+\kappa}\,\Gamma\left(\frac{1}{2}+w\right)} \int\limits_0^{\infty} \theta^{\kappa+w-2}\, e^{-2\theta t}\left(1+\theta^2 \tilde{h}_2(w)+\theta^4\tilde{h}_4(w)+\;\cdots\right) d\theta \\ + \;\mathcal{O}\left(e^{-|\Im(w)|^{1+\epsilon}}\right)$$

$$= \frac{|\Gamma\left(\frac{\kappa}{2}+it\right)|^2\cdot e^{\pi t}\,\Gamma(w)\Gamma(\kappa+w-1)}{t^{\kappa+w-1}\cdot 4^{\kappa+w-1}\pi^{\frac{1}{2}+\kappa}\,\Gamma\left(\frac{1}{2}+w\right)}\left(1\;+\;\mathcal{O}\left(\frac{|\Im(w)|^3}{t^2}\right)\right),$$

where, in the above, $\tilde{h}_{2\ell}(w) = \mathcal{O}\left(|\Im(w)|^\ell\right)$ for $\ell = 1,2,\ldots$.

If we now apply the identity

$$\begin{aligned}\left|\Gamma\left(\tfrac{\kappa}{2}+it\right)\right|^2 \;&=\; t\cdot|1+it|^2|2+it|^2|3+it|^2\cdots\left|\tfrac{\kappa}{2}-1+it\right|^2\frac{\pi}{\sinh \pi t}\\ &=\; 2\pi t^{\kappa-1}e^{-\pi t}\left(1\;+\;\mathcal{O}_\kappa\left(t^{-2}\right)\right)\end{aligned}$$

in the above expression, we obtain the second part of Proposition 4.2. □

For t smaller than $|\Im(w)|^{2+\epsilon}$, we have the following

PROPOSITION 4.6. *Fix $\epsilon > 0$, $\kappa \geq 12$. For $-1 < \Re(w) < 2$ and $0 \leq t \ll |\Im(w)|^{2+\epsilon}$, with $\Im(w) \to \infty$, we have*

$$\left|\sin\left(\frac{\pi w}{2}\right)K_\beta(t,1-w) - \cos\left(\frac{\pi w}{2}\right)K_\beta(t,w)\right| \;\ll_\kappa\; t^{\frac{1}{2}}|\Im(w)|^{\kappa-\frac{3}{2}}.$$

PROOF. Let $g(w,\theta)$ denote the function defined by

$$g(w,\theta) \;=\; \Gamma(w)\,P_{-\frac{1}{2}}^{\frac{1}{2}-w}(\cos\theta).$$

We observe that

$$\sin\left(\frac{\pi w}{2}\right) g(1-w,\theta) \quad - \quad \cos\left(\tfrac{\pi w}{2}\right) g(w,\theta) \;= \;= \;-\; \frac{\cos \pi w}{2\cos\left(\frac{\pi w}{2}\right)} \left[g(w,\theta)+g(w,\pi-\theta)\right]. \tag{4.7}$$

To see this, apply (2.10) and (2.11) with $\nu = -\frac{1}{2}$ and $\mu = \frac{1}{2} - w$. We have:

$$g(1-w,\theta) \;=\; g(w,\theta)\sin\pi w - \frac{2}{\pi}\,\Gamma(w)\,Q_{-\frac{1}{2}}^{\frac{1}{2}-w}(\cos\theta)\cos\pi w;$$

$$g(w,\pi-\theta) \;=\; g(w,\theta)\cos\pi w + \frac{2}{\pi}\,\Gamma(w)\,Q_{-\frac{1}{2}}^{\frac{1}{2}-w}(\cos\theta)\sin\pi w.$$

Multiplying the first by $\sin\pi w$, the second by $\cos\pi w$, and then adding the resulting identities, we obtain

$$g(1-w,\theta)\sin\pi w + g(w,\pi-\theta)\cos\pi w \;=\; g(w,\theta),$$

from which (4.7) immediately follows by adding $g(w,\theta)\cos\pi w$ on both sides.

Now, if f and g are holomorphic, it follows from (2.7), (3.3), and (4.7) that

$$\begin{aligned}
&\sin\left(\tfrac{\pi w}{2}\right) K_\beta(t,1-w) - \cos\left(\tfrac{\pi w}{2}\right) K_\beta(t,w)\\
&= \quad -2^{\frac{1}{2}-\kappa}\,\pi^{-\kappa-\frac{1}{2}}\left|\Gamma\left(\frac{\kappa}{2}+it\right)\right|^2 \frac{\cos\pi w}{\cos\left(\frac{\pi w}{2}\right)} \int\limits_0^{\frac{\pi}{2}} \left[g(w,\theta)+g(w,\pi-\theta)\right]\\
&\qquad\qquad \sin^{\kappa-\frac{3}{2}}(\theta)\,\cosh[t(2\theta-\pi)]\,d\theta\\
&= \quad -2^{\frac{1}{2}-\kappa}\,\pi^{-\kappa-\frac{1}{2}}\left|\Gamma\left(\frac{\kappa}{2}+it\right)\right|^2 \frac{\Gamma(w)\cos\pi w}{\cos\left(\frac{\pi w}{2}\right)} \int\limits_0^{\pi} P_{-\frac{1}{2}}^{\frac{1}{2}-w}(\cos\theta)\\
&\qquad\qquad \sin^{\kappa-\frac{3}{2}}(\theta)\,\cosh[t(2\theta-\pi)]\,d\theta.
\end{aligned} \tag{4.8}$$

By (2.9), we have

$$P_{-\frac{1}{2}}^{\frac{1}{2}-w}(\cos\theta) \;=\; \frac{1}{\Gamma(w+\frac{1}{2})}\,\cot^{\frac{1}{2}-w}\left(\frac{\theta}{2}\right) F\left(\frac{1}{2},\frac{1}{2};w+\frac{1}{2};\sin^2\left(\frac{\theta}{2}\right)\right).$$

Invoking the well-known transformation formula

$$F(\alpha,\beta;\gamma;z) \;=\; (1-z)^{-\alpha}F\left(\alpha,\gamma-\beta;\gamma;\frac{z}{z-1}\right),$$

we can further write

$$P_{-\frac{1}{2}}^{\frac{1}{2}-w}(\cos\theta) \;=\; \frac{\cos^{-w-\frac{1}{2}}\left(\frac{\theta}{2}\right)\sin^{w-\frac{1}{2}}\left(\frac{\theta}{2}\right)}{\Gamma(w+\frac{1}{2})}\,F\left(\frac{1}{2},w;w+\frac{1}{2};-\tan^2\left(\frac{\theta}{2}\right)\right).$$

Now, represent the hypergeometric function on the right hand side by its inverse Mellin transform obtaining:

$$\begin{aligned}
P_{-\frac{1}{2}}^{\frac{1}{2}-w}(\cos\theta) \quad &= \quad \frac{1}{\Gamma(\frac{1}{2})\Gamma(w)}\cos^{-w-\frac{1}{2}}\left(\frac{\theta}{2}\right)\sin^{w-\frac{1}{2}}\left(\frac{\theta}{2}\right)\\
&\quad\cdot\ \frac{1}{2\pi i}\int\limits_{-i\infty}^{i\infty} \frac{\Gamma(\frac{1}{2}+z)\Gamma(w+z)\Gamma(-z)}{\Gamma(z+w+\frac{1}{2})}\,\tan^{2z}\left(\frac{\theta}{2}\right)dz.
\end{aligned} \tag{4.9}$$

Here, the path of integration is chosen such that the poles of $\Gamma(\frac{1}{2}+z)$ and $\Gamma(w+z)$ lie to the left of the path, and the poles of the function $\Gamma(-z)$ lie to the right of it.

It follows that

$$\sin\left(\frac{\pi w}{2}\right) K_\beta(t,1-w) - \cos\left(\frac{\pi w}{2}\right) K_\beta(t,w)$$
$$= \quad -2^{\frac{1}{2}-\kappa}\,\pi^{-\kappa-\frac{1}{2}}\left|\Gamma\Big(\frac{\kappa}{2}+it\Big)\right|^2 \frac{\Gamma(w)\cos(\pi w)}{\cos\left(\frac{\pi w}{2}\right)} \int\limits_0^\pi \frac{\cos^{-w-\frac{1}{2}}\left(\frac{\theta}{2}\right)\sin^{w-\frac{1}{2}}\left(\frac{\theta}{2}\right)}{\Gamma(\frac{1}{2})\Gamma(w)}$$
$$\cdot\left(\frac{1}{2\pi i}\int\limits_{-i\infty}^{i\infty} \frac{\Gamma(\frac{1}{2}+z)\Gamma(w+z)\Gamma(-z)}{\Gamma(z+w+\frac{1}{2})}\tan^{2z}\left(\frac{\theta}{2}\right)dz\right)\cdot\sin^{\kappa-\frac{3}{2}}(\theta)\,\cosh[t(2\theta-\pi)]\,d\theta.$$

In the above, we apply the identity $\sin(\theta) = 2\sin\left(\frac{\theta}{2}\right)\cos\left(\frac{\theta}{2}\right)$; after exchanging integrals and simplifying, we obtain

$$\sin\left(\frac{\pi w}{2}\right) K_\beta(t,1-w) - \cos\left(\frac{\pi w}{2}\right) K_\beta(t,w) = \frac{|\Gamma(\frac{\kappa}{2}+it)|^2}{2\pi^{\kappa+1}}\frac{\cos(\pi w)}{\cos\left(\frac{\pi w}{2}\right)}$$
$$\cdot\frac{1}{2\pi i}\int\limits_{-i\infty}^{i\infty}\frac{\Gamma(\frac{1}{2}+z)\Gamma(w+z)\Gamma(-z)}{\Gamma(z+w+\frac{1}{2})} \tag{4.10}$$
$$\cdot\int\limits_0^\pi \cos^{\kappa-w-2z-2}\left(\frac{\theta}{2}\right)\sin^{2z+w+\kappa-2}\left(\frac{\theta}{2}\right)\cosh[t(2\theta-\pi)]\,d\theta\,dz.$$

Note that $\sin\left(\frac{\pi w}{2}\right) K_\beta(t,1-w) - \cos\left(\frac{\pi w}{2}\right) K_\beta(t,w)$ satisfies a functional equation $w \mapsto 1-w$. We may, therefore, assume, without loss of generality, that $\Im(w) > 0$. Fix $\epsilon > 0$. We break the z–integral in (4.10) into three parts according as

$$-\infty < \Im(z) < -\left(\tfrac{1}{2}+\epsilon\right)\Im(w), \qquad -\left(\tfrac{1}{2}+\epsilon\right)\Im(w) \le \Im(z) \le \left(\tfrac{1}{2}+\epsilon\right)\Im(w),$$

$$\left(\tfrac{1}{2}+\epsilon\right)\Im(w) < \Im(z) < \infty.$$

Under the assumptions that $\Im(w) \to \infty$ and $0 \le t \ll \Im(w)^{2+\epsilon}$, it follows easily from Stirling's estimate for the Gamma function that

$$\int\limits_{-i\infty}^{-i\left(\frac{1}{2}+\epsilon\right)\Im(w)} \left|\frac{\Gamma(\frac{1}{2}+z)\Gamma(w+z)\Gamma(-z)}{\Gamma(z+w+\frac{1}{2})}\right| dz \;=\; \mathcal{O}\left(e^{-\left(\frac{\pi}{2}+\epsilon\right)\Im(w)}\right),$$

$$\int\limits_{i\left(\frac{1}{2}+\epsilon\right)\Im(w)}^{i\infty} \left|\frac{\Gamma(\frac{1}{2}+z)\Gamma(w+z)\Gamma(-z)}{\Gamma(z+w+\frac{1}{2})}\right| dz \;=\; \mathcal{O}\left(e^{-\left(\frac{\pi}{2}+\epsilon\right)\Im(w)}\right),$$

and, therefore,

$$\sin\left(\frac{\pi w}{2}\right) K_\beta(t, 1-w) - \cos\left(\frac{\pi w}{2}\right) K_\beta(t, w)$$

$$(4.11)\qquad = -\frac{\left|\Gamma\left(\frac{\kappa}{2}+it\right)\right|^2}{2\pi^{\kappa+1}} \frac{\cos \pi w}{\cos\left(\frac{\pi w}{2}\right)} \cdot \frac{1}{2\pi i} \int\limits_{-i\left(\frac{1}{2}+\epsilon\right)\Im(w)}^{i\left(\frac{1}{2}+\epsilon\right)\Im(w)} \frac{\Gamma(\frac{1}{2}+z)\Gamma(w+z)\Gamma(-z)}{\Gamma(z+w+\frac{1}{2})}$$
$$\cdot \int\limits_0^\pi \cos^{\kappa-w-2z-2}\left(\frac{\theta}{2}\right) \sin^{2z+w+\kappa-2}\left(\frac{\theta}{2}\right) \cosh[t(2\theta-\pi)]\, d\theta\, dz$$
$$+ \mathcal{O}\left(e^{-\epsilon\Im(w)}\right).$$

Next, we evaluate the θ–integral on the right hand side of (4.11):

$$\int\limits_0^\pi \cos^{\kappa-w-2z-2}\left(\frac{\theta}{2}\right) \sin^{2z+w+\kappa-2}\left(\frac{\theta}{2}\right) \cosh[t(2\theta-\pi)]\, d\theta$$
$$= \frac{e^{-\pi t}}{2} \int\limits_0^\pi \cos^{\kappa-w-2z-2}\left(\frac{\theta}{2}\right) \sin^{2z+w+\kappa-2}\left(\frac{\theta}{2}\right) e^{2t\theta}\, d\theta$$
$$(4.12)\qquad f + \frac{e^{\pi t}}{2} \int\limits_0^\pi \cos^{\kappa-w-2z-2}\left(\frac{\theta}{2}\right) \sin^{2z+w+\kappa-2}\left(\frac{\theta}{2}\right) e^{-2t\theta}\, d\theta$$
$$= e^{-\pi t} \int\limits_0^{\pi/2} \cos^{\kappa-w-2z-2}(\theta) \sin^{2z+w+\kappa-2}(\theta)\, e^{4t\theta}\, d\theta$$
$$+ e^{\pi t} \int\limits_0^{\pi/2} \cos^{\kappa-w-2z-2}(\theta) \sin^{2z+w+\kappa-2}(\theta)\, e^{-4t\theta}\, d\theta,$$

where for the last equality we made the substitution

$$\theta \mapsto 2\theta.$$

Using the formula (see [**GR94**], page 511, 3.892-3),

$$\int_0^{\pi/2} e^{2i\beta x} \sin^{2\mu} x \cos^{2\nu} x\, dx =$$
$$= 2^{-2\mu-2\nu-1}\Big(e^{\pi i(\beta-\nu-\frac{1}{2})} \frac{\Gamma(\beta-\nu-\mu)\Gamma(2\nu+1)}{\Gamma(\beta-\mu+\nu+1)} F(-2\mu, \beta-\mu-\nu; 1+\beta-\mu+\nu; -1)$$
$$+ e^{\pi i(\mu+\frac{1}{2})} \frac{\Gamma(\beta-\nu-\mu)\Gamma(2\mu+1)}{\Gamma(\beta-\nu+\mu+1)} F(-2\nu, \beta-\mu-\nu; 1+\beta+\mu-\nu; -1)\Big),$$

which is valid for $\Re(\mu)$, $\Re(\nu) > -\frac{1}{2}$, one can write the first integral in (4.12) as

$$2^{3-2\kappa} \sum_{\epsilon=\pm 1} e^{-\epsilon\pi t} \cdot \Big(e^{\pi i \frac{(1-\kappa+w+2z-4it\epsilon)}{2}} \frac{\Gamma(2-\kappa-2it\epsilon)\Gamma(-1+\kappa-w-2z)}{\Gamma(1-2it\epsilon-w-2z)}$$
$$\cdot F(2-\kappa-w-2z, 2-\kappa-2it\epsilon; 1-w-2z-2it\epsilon; -1)$$
$$+ e^{\pi i \frac{(-1+\kappa+w+2z)}{2}} \frac{\Gamma(2-\kappa-2it\epsilon)\Gamma(-1+\kappa+w+2z)}{\Gamma(1-2it\epsilon+w+2z)}$$
$$\cdot F(2-\kappa+w+2z, 2-\kappa-2it\epsilon; 1+w+2z-2it\epsilon; -1)) \Big).$$

If we replace the θ–integral on the right hand side of (4.11) by the above expression, it follows that

$$\sin\left(\frac{\pi w}{2}\right) K_\beta(t, 1-w) - \cos\left(\frac{\pi w}{2}\right) K_\beta(t, w)$$
$$= -\frac{|\Gamma(\frac{\kappa}{2}+it)|^2}{2^{2\kappa-2}\pi^{\kappa+1}} \frac{\cos \pi w}{\cos\left(\frac{\pi w}{2}\right)} \cdot \sum_{\epsilon=\pm 1} e^{-\epsilon\pi t} \Gamma(2-\kappa-2it\epsilon)$$
$$\cdot \frac{1}{2\pi i} \int\limits_{-i\left(\frac{1}{2}+\epsilon\right)\Im(w)}^{i\left(\frac{1}{2}+\epsilon\right)\Im(w)} \frac{\Gamma(\frac{1}{2}+z)\Gamma(w+z)\Gamma(-z)}{\Gamma(z+w+\frac{1}{2})}$$
$$\cdot \Bigg(e^{\pi i \frac{(1-\kappa+w+2z-4it\epsilon)}{2}} \frac{\Gamma(-1+\kappa-w-2z)}{\Gamma(1-2it\epsilon-w-2z)} \tag{4.13}$$
$$\cdot F(2-\kappa-w-2z, 2-\kappa-2it\epsilon; 1-w-2z-2it\epsilon; -1)$$
$$+ e^{\pi i \frac{(-1+\kappa+w+2z)}{2}} \frac{\Gamma(-1+\kappa+w+2z)}{\Gamma(1-2it\epsilon+w+2z)}$$
$$\cdot F(2-\kappa+w+2z, 2-\kappa-2it\epsilon; 1+w+2z-2it\epsilon; -1)) \Bigg) dz$$
$$+ \mathcal{O}\left(e^{-\epsilon\Im(w)}\right).$$

To complete the proof of Proposition 4.6., we require the following Lemma.

Lemma 4.14. *Fix $\kappa \geq 12$. Let $-1 < \Re(w) < 2$, $0 \leq t \ll |\Im(w)|^{2+\epsilon}$, $\Re(z) = -\epsilon'$ with ϵ, ϵ' small positive numbers, and $|\Im(z)| < 2|\Im(w)|$. Then, we have the following estimates:*

$$F(2-\kappa-w-2z, 2-\kappa-2it\epsilon; 1-w-2z-2it\epsilon; -1) \ll \sqrt{\min\{1, 2t, |\Im(w+2z)|\}},$$

$$F(2-\kappa+w+2z, 2-\kappa-2it\epsilon; 1+w+2z-2it\epsilon; -1) \ll \sqrt{\min\{1, 2t, |\Im(w+2z)|\}}.$$

Proof. We shall make use of the following well-known identity of Kummer:

$$F(a, b, c; -1) = 2^{c-a-b} F(c-a, c-b, c; -1).$$

It follows that

$$\begin{aligned} &F(2-\kappa-w-2z, 2-\kappa-2it\epsilon, 1-w-2z-2it\epsilon; -1) \\ &\qquad = 2^{2\kappa-3} F(\kappa-1-2it\epsilon, \kappa-1-w-2z, 1-w-2z-2it\epsilon; -1) \end{aligned} \tag{4.15}$$

and

$$\begin{aligned} &F(2-\kappa+w+2z, 2-\kappa-2it\epsilon; 1+w+2z-2it\epsilon; -1) \\ &\qquad = 2^{2\kappa-3} F(\kappa-1-2it\epsilon, \kappa-1+w+2z, 1+w+2z-2it\epsilon, -1). \end{aligned} \tag{4.16}$$

Now, we represent the hypergeometric function on the right hand side of (4.15) as

$$F(a,b,c;-1) \;=\; \frac{\Gamma(c)}{\Gamma(a)\Gamma(b)}\cdot\frac{1}{2\pi i}\int\limits_{\delta-i\infty}^{\delta+i\infty}\frac{\Gamma(a+\xi)\Gamma(b+\xi)\Gamma(-\xi)}{\Gamma(c+\xi)}\,d\xi, \tag{4.17}$$

with

$$\begin{aligned} a &= \kappa-1-2it\epsilon \\ b &= \kappa-1-w-2z \\ c &= 1-w-2z-2it\epsilon. \end{aligned}$$

This integral representation is valid, if, for instance, $-1<\delta<0$. We may also shift the line of integration to $0<\delta<1$ which crosses a simple pole with residue 1. Clearly, the main contribution comes from small values of the imaginary part of ξ.

If, for example, we use Stirling's formula

$$\Gamma(s)=\sqrt{2\pi}\cdot|t|^{\sigma-\frac12}\;e^{-\frac12\pi|t|+i\left(t\log|t|-t+\frac{\pi}{2}\cdot\frac{t}{|t|}\left(\sigma-\frac12\right)\right)}\cdot\Big(1+\mathcal{O}\left(|t|^{-1}\right)\Big),$$

where $s=\sigma+it,\ 0\le\sigma\le1,\ |t|\gg0$, we have

$$\begin{aligned}\left|\frac{\Gamma(a+\xi)\Gamma(b+\xi)\Gamma(c)\Gamma(-\xi)}{\Gamma(a)\Gamma(b)\Gamma(c+\xi)}\right| &\ll e^{\frac{\pi}{2}\left(-|W-\xi|+|2t+W-\xi|-|\xi|-|\xi-2t|\right)} \\ &\cdot\frac{t^{\frac32-\kappa}\,W^{\frac32-\kappa}\,|W-\xi|^{-\frac32+\kappa+\delta}\,|\xi-2t|^{-\frac32+\kappa+\delta}\sqrt{2t+W}}{|\xi|^{\frac12+\delta}\,|2t+W-\xi|^{\frac12+\delta}},\end{aligned} \tag{4.18}$$

where $W=\Im(w+2z)\ge0$. This bound is valid provided

$$\min\Big(|W-\xi|,|2t+W-\xi|,|\xi|,|\xi-2t|\Big)$$

is sufficiently large. If this minimum is close to zero, we can eliminate this term and obtain a similar expression. There are 4 cases to consider.

Case 1: $|\xi|\le W,\ |\xi|\le2t$. In this case, the exponential term in (4.18) becomes $e^0=1$ and we obtain

$$\left|\frac{\Gamma(a+\xi)\Gamma(b+\xi)\Gamma(c)\Gamma(-\xi)}{\Gamma(a)\Gamma(b)\Gamma(c+\xi)}\right|\ll|\xi|^{-\frac12}.$$

Case 2: $|\xi|\le W,\ |\xi|>2t$. In this case the exponential term in (4.18) becomes

$$+e^{\frac{\pi}{2}\left(-W+\xi+2t+W-\xi-|\xi|-|\xi|+2t\right)}$$

which has exponential decay in $(|\xi|-t)$.

Case 3: $|\xi|>W,\ |\xi|\le2t$. Here, the exponential term in (4) takes the form

$$e^{\frac{\pi}{2}\left(-|\xi|+W+2t+W-\xi-|\xi|-2t+\xi\right)}$$

which has exponential decay in $(|\xi|-W)$.

Case 4: $|\xi|>W,\ |\xi|>2t$. In this last case, we get

$$e^{\frac{\pi}{2}\left(-|\xi|-W+2t+W+|\xi|-2|\xi|-2t\right)}$$

if ξ is negative. Note that this has exponential decay in $|\xi|$. If ξ is positive, we get

$$e^{\frac{\pi}{2}\left(-|\xi|+W+|2t+W-\xi|-2|\xi|+2t\right)}.$$

This last expression has exponential decay in $(2|\xi| - W - 2t)$ if $2t + W - \xi > 0$. Otherwise it has exponential decay in $|\xi|$.

It is clear that the major contribution to the integral (4.17) for the hypergeometric function will come from case 1. This gives immediately the first estimate in Lemma 4.14. The second estimate in Lemma 4.14 can be established by a similar method. □

We remark that for $t = 0$, one can easily obtain the estimate in Proposition 4.6 by directly using the formula (see [**GR94**], page 819, 7.166),

$$\int_0^\pi P_\nu^{-\mu}(\cos\theta)\sin^{\alpha-1}(\theta)\,d\theta \;=\; 2^{-\mu}\pi\frac{\Gamma(\frac{\alpha+\mu}{2})\Gamma(\frac{\alpha-\mu}{2})}{\Gamma(\frac{1+\alpha+\nu}{2})\Gamma(\frac{\alpha-\nu}{2})\Gamma(\frac{\mu+\nu+2}{2})\Gamma(\frac{\mu-\nu+1}{2})},$$

which is valid for $\Re(\alpha \pm \mu) > 0$, and then by applying Stirling's formula. It follows from this that

$$\sin\left(\frac{\pi w}{2}\right) K_\beta(0, 1-w) - \cos\left(\frac{\pi w}{2}\right) K_\beta(0, w) \ll |\Im(w)|^{\kappa-2}.$$

Finally, we return to the estimation of $\sin\left(\frac{\pi w}{2}\right) K_\beta(0, 1-w) - \cos\left(\frac{\pi w}{2}\right) K_\beta(0, w)$ using (4.13) and Lemma 4.14. If we apply Stirling's asymptotic expansion for the Gamma function, as we did before, it follows (after noting that $t, \Im(w) > 0$) that

$$\left|\sin\left(\frac{\pi w}{2}\right) K_\beta(0, 1-w) - \cos\left(\frac{\pi w}{2}\right) K_\beta(0, w)\right|$$

$$\ll \; t^{\frac12} \int\limits_{-i\left(\frac12+\epsilon\right)\Im(w)}^{i\left(\frac12+\epsilon\right)\Im(w)} \frac{|\Im(w+2z)|^{\kappa-\frac32}}{\Im(w)^{\frac12}(1+|\Im(z)|)^{\frac12}|\Im(w+2z+2\epsilon t)|^{\frac12}}\,\sqrt{\min\{1, 2t, |\Im(w+2z)|\}}\,dz$$

$$\ll \; t^{\frac12}\Im(w)^{\kappa-\frac32}.$$

This completes the proof of Proposition 4.6. □

5. The analytic continuation of $I(v, w)$

To obtain the analytic continuation of

$$I(v, w) \;=\; \langle P(*; v, w), F\rangle \;=\; \int\int_{\Gamma\backslash\mathcal{H}} P(z; v, w) f(z)\overline{g(z)}\, y^\kappa \,\frac{dx\,dy}{y^2},$$

we will compute the inner product $\langle P(*; v, w), F\rangle$ using Selberg's spectral theory. First, let us fix u_0, u_1, $u_2, \ldots$ an orthonormal basis of Maass cusp forms which are simultaneous eigenfunctions of all the Hecke operators T_n, $n = 1, 2, \ldots$ and T_{-1}, where

$$(T_{-1}\,u)(z) \;=\; u(-\bar z).$$

We shall assume that u_0 is the constant function, and the eigenvalue of u_j, for $j = 1, 2, \ldots$, will be denoted by $\lambda_j = \frac14 + \mu_j^2$. Since the Poincaré series $P_k(z; v, s)$ $(k \in Z,\ k \neq 0)$ is square integrable, for $|\Re(s)| + \frac34 > \Re(v) > |\Re(s)| + \frac12$, we can spectrally decompose it as

$$
\begin{aligned}
P_k(z;v,s) \;&=\; \sum_{j=1}^{\infty} \langle P_k(*;v,s), u_j\rangle\, u_j(z) \\
&+\; \frac{1}{4\pi}\int_{-\infty}^{\infty} \langle P_k(*;v,s), E(*,\tfrac12+i\mu)\rangle E(z,\tfrac12+i\mu)\, d\mu.
\end{aligned} \tag{5.1}
$$

Here we used the simple fact that $\langle P_k(*;v,s), u_0\rangle \;=\; 0$.

We shall need to write (5.1) explicitly. In order to do so, let u be a Maass cusp form in our basis with eigenvalue $\lambda = \frac14 + \mu^2$. Writing

$$
u(z) \;=\; \rho(1) \sum_{\nu\neq 0} c_\nu\, |\nu|^{-\frac12}\, W_{\frac12+i\mu}(\nu z),
$$

then by (2.3) and an unfolding process, we have

$$
\begin{aligned}
\langle P_k(*;v,s), u\rangle \;&=\; |k|^{-\frac12} \int_0^\infty\int_0^1 y^v\, W_{\frac12+s}(kz)\, \overline{u(z)}\, \frac{dx\,dy}{y^2} \\
&=\; \overline{\rho(1)} \sum_{\nu\neq 0} \frac{c_\nu}{\sqrt{|k\nu|}} \int_0^\infty\int_0^1 y^{v-1}\, W_{\frac12+s}(kz)\, W_{\frac12+i\mu}(-\nu z)\, \frac{dx\,dy}{y} \\
&=\; \overline{\rho(1)}\, c_k \int_0^\infty y^v\, K_s(2\pi|k|y)\, K_{i\mu}(2\pi|k|y)\, \frac{dy}{y} \\
&=\; \pi^{-v}\, \frac{\overline{\rho(1)}}{8}\, \frac{c_k}{|k|^v}\, \frac{\Gamma\big(\frac{-s+v-i\mu}{2}\big)\Gamma\big(\frac{s+v-i\mu}{2}\big)\Gamma\big(\frac{-s+v+i\mu}{2}\big)\Gamma\big(\frac{s+v+i\mu}{2}\big)}{\Gamma(v)}.
\end{aligned}
$$

Let $\mathcal{G}(s;v,w)$ denote the function defined by

$$
\mathcal{G}(s;v,w) \;=\; \pi^{-v-\frac{w}{2}}\, \frac{\Gamma\big(\frac{-s+v+1}{2}\big)\Gamma\big(\frac{s+v}{2}\big)\Gamma\big(\frac{-s+v+w}{2}\big)\Gamma\big(\frac{s+v+w-1}{2}\big)}{\Gamma\big(v+\frac{w}{2}\big)}. \tag{5.2}
$$

Then, replacing v by $v+\frac{w}{2}$ and s by $\frac{w-1}{2}$, we obtain

$$
\Big\langle P_k\Big(*;v+\frac{w}{2},\frac{w-1}{2}\Big), u\Big\rangle \;=\; \frac{\overline{\rho(1)}}{8}\, \frac{c_k}{|k|^{v+\frac{w}{2}}}\, \mathcal{G}(\tfrac12+i\mu;v,w). \tag{5.3}
$$

Next, we compute the inner product between $P_k\Big(z;v+\frac{w}{2},\frac{w-1}{2}\Big)$ and the Eisenstein series $E(z,\bar{s})$. This is well-known to be the Mellin transform of the constant term of $P_k\Big(z;v+\frac{w}{2},\frac{w-1}{2}\Big)$. More precisely, if we write

$$
P_k\Big(z;v+\frac{w}{2},\frac{w-1}{2}\Big) \;=\; y^{v+\frac{w}{2}+\frac12} K_{\frac{w-1}{2}}(2\pi|k|y)e(kx) + \sum_{n=-\infty}^{\infty} a_n\Big(y;v+\frac{w}{2},\frac{w-1}{2}\Big)e(nx),
$$

where we denoted $e^{2\pi i x}$ by $e(x)$, then for $\Re(s)>1$,

$$
\Big\langle P_k\Big(\cdot;v+\frac{w}{2},\frac{w-1}{2}\Big),\, E(\cdot,\bar{s})\Big\rangle \;=\; \int_0^\infty a_0\Big(y;v+\frac{w}{2},\frac{w-1}{2}\Big) y^{s-2}\, dy.
$$

Now, by a standard computation, we have

$$a_0\Big(y; v+\frac{w}{2}, \frac{w-1}{2}\Big) = \sum_{c=1}^{\infty} \sum_{\substack{r=1 \\ (r,\,c)=1}}^{c} e\left(\frac{kr}{c}\right) \int_{-\infty}^{\infty} \left(\frac{y}{c^2x^2+c^2y^2}\right)^{v+\frac{w+1}{2}} \cdot K_{\frac{w-1}{2}}\left(\frac{2\pi|k|y}{c^2x^2+c^2y^2}\right) e\left(\frac{-kx}{c^2x^2+c^2y^2}\right) dx.$$

Making the substitution $x \mapsto \frac{x}{c^2}$ and $y \mapsto \frac{y}{c^2}$, we obtain

$$\Big\langle P_k\Big(*; v+\frac{w}{2}, \frac{w-1}{2}\Big), E(*, \bar{s})\Big\rangle = \sum_{c=1}^{\infty} \tau_c(k)\, c^{-2s} \cdot \int_0^{\infty}\int_{-\infty}^{\infty} \frac{y^{s+v+\frac{w-3}{2}}}{(x^2+y^2)^{v+\frac{w+1}{2}}} \cdot K_{\frac{w-1}{2}}\left(\frac{2\pi|k|y}{x^2+y^2}\right) \cdot e\left(\frac{-kx}{x^2+y^2}\right) dx\, dy.$$

Here, $\tau_c(k)$ is the Ramanujan sum given by

$$\tau_c(k) = \sum_{\substack{r=1 \\ (r,c)=1}}^{c} e\left(\frac{kr}{c}\right).$$

Recalling that

$$\sum_{c=1}^{\infty} \tau_c(k)\, c^{-2s} = \frac{\sigma_{1-2s}(|k|)}{\zeta(2s)},$$

where for a positive integer n, $\sigma_s(n) = \sum_{d|n} d^s$, it follows after making the substitution $x \mapsto |k|x$, $y \mapsto |k|y$ that

$$\Big\langle P_k\Big(*; v+\frac{w}{2}, \frac{w-1}{2}\Big), E(\cdot, \bar{s})\Big\rangle = |k|^{s-v-\frac{w}{2}-\frac{1}{2}} \cdot \frac{\sigma_{1-2s}(|k|)}{\zeta(2s)} \int_0^{\infty}\int_{-\infty}^{\infty} \frac{y^{s+v+\frac{w-3}{2}}}{(x^2+y^2)^{v+\frac{w+1}{2}}} \cdot K_{\frac{w-1}{2}}\left(\frac{2\pi y}{x^2+y^2}\right) e\left(-\frac{k}{|k|}\,\frac{x}{x^2+y^2}\right) dx\, dy. \tag{5.4}$$

The double integral on the right hand side can be computed in closed form by making the substitution $z \mapsto -\frac{1}{z}$. For $\Re(s) > 0$ and for $\Re(v-s) > -1$, we successively have:

$$\int_0^\infty\int_{-\infty}^\infty \frac{y^{s+v+\frac{w-3}{2}}}{(x^2+y^2)^{v+\frac{w+1}{2}}}\cdot K_{\frac{w-1}{2}}\left(\frac{2\pi y}{x^2+y^2}\right) e\left(-\frac{k}{|k|}\,\frac{x}{x^2+y^2}\right) dx\,dy \tag{5.5}$$
$$= \int_0^\infty\int_{-\infty}^\infty y^{s+v+\frac{w-3}{2}}\,(x^2+y^2)^{-s}\cdot K_{\frac{w-1}{2}}(2\pi y)\, e\left(\frac{k}{|k|}\,x\right) dx\,dy$$
$$= \int_0^\infty y^{s+v+\frac{w-3}{2}}\, K_{\frac{w-1}{2}}(2\pi y)\cdot \int_{-\infty}^\infty (x^2+y^2)^{-s}\, e\left(\frac{k}{|k|}\,x\right) dx\,dy$$
$$= \frac{2^{-v-\frac{w}{2}+1}\,\pi^{s-v-\frac{w}{2}}}{\Gamma(s)}\int_0^\infty y^{v+\frac{w}{2}-1}\, K_{\frac{w-1}{2}}(y)\, K_{s-\frac12}(y)\; dy$$
$$= \frac{\mathcal{G}(s;v,w)}{4\,\pi^{-s}\,\Gamma(s)}.$$

Combining (5.4) and (5.5), we obtain

$$\left\langle P_k\Big(*;v+\frac{w}{2},\frac{w-1}{2}\Big),\, E(\cdot,\bar{s})\right\rangle = |k|^{s-v-\frac{w}{2}-\frac12}\cdot\frac{\sigma_{1-2s}(|k|)}{4\,\pi^{-s}\,\Gamma(s)\,\zeta(2s)}\;\mathcal{G}(s;v,w) \tag{5.6}$$

Using (5.1), (5.3) and (5.6), one can decompose $P_k\big(\cdot;v+\frac{w}{2},\frac{w-1}{2}\big)$ as

(5.7)

$$P_k\Big(z;v+\frac{w}{2},\frac{w-1}{2}\Big)$$
$$= \sum_{j=1}^\infty \frac{\overline{\rho_j(1)}}{8}\,\frac{c_k^{(j)}}{|k|^{v+\frac{w}{2}}}\,\mathcal{G}(\tfrac12+i\mu_j;v,w)\,u_j(z)$$
$$+\ \frac{1}{16\pi}\int_{-\infty}^\infty \frac{1}{\pi^{-\frac12+i\mu}\,\Gamma(\frac12-i\mu)\,\zeta(1-2i\mu)}\,\frac{\sigma_{2i\mu}(|k|)}{|k|^{v+\frac{w}{2}+i\mu}}\;\mathcal{G}(\tfrac12-i\mu;v,w)E(z,\tfrac12+i\mu)\;d\mu.$$

Now from (2.2) and (5.7), we deduce that

$$\pi^{-\frac{w}{2}}\Gamma\Big(\frac{w}{2}\Big)\,P(z;v,w)\ =\ \pi^{\frac{1-w}{2}}\,\Gamma\left(\frac{w-1}{2}\right)\,E(z,v+1) \tag{5.8}$$
$$+\ \frac12\sum_{u_j-\text{even}}\overline{\rho_j(1)}\,L_{u_j}(v+\tfrac12)\,\mathcal{G}(\tfrac12+i\mu_j;v,w)\;u_j(z)$$
$$+\ \frac{1}{4\pi}\int_{-\infty}^\infty \frac{\zeta(v+\frac12+i\mu)\,\zeta(v+\frac12-i\mu)}{\pi^{-\frac12+i\mu}\,\Gamma(\frac12-i\mu)\,\zeta(1-2i\mu)}\;\mathcal{G}(\tfrac12-i\mu;v,w)E(z,\tfrac12+i\mu)\;d\mu.$$

The series corresponding to the discrete spectrum converges absolutely for $(v,w)\in C^2$, apart from the poles of $\mathcal{G}(\frac12+i\mu_j;v,w)$. To handle the continuous part of the spectrum, we write the above integral as

$$\frac{1}{4\pi i}\int_{(\frac12)}\frac{\zeta(v+s)\zeta(v+1-s)}{\pi^{s-1}\Gamma(1-s)\zeta(2-2s)}\,\mathcal{G}(1-s;v,w)E(z,s)\;ds.$$

As a function of v and w, this integral can be meromorphically continued by shifting the line $\Re(s) = \frac{1}{2}$. For instance, to obtain continuation to a region containing $v = 0$, take v with $\Re(v) = \frac{1}{2} + \epsilon$, $\epsilon > 0$ sufficiently small, and take $\Re(w)$ large. By shifting the line of integration $\Re(s) = \frac{1}{2}$ to $\Re(s) = \frac{1}{2} - 2\epsilon$, we are allowed to take $\frac{1}{2} - \epsilon \le \Re(v) \le \frac{1}{2} + \epsilon$. We now assume $\Re(v) = \frac{1}{2} - \epsilon$, and shift back the line of integration to $\Re(s) = \frac{1}{2}$. It is not hard to see that in this process we encounter simple poles at $s = 1 - v$ and $s = v$ with residues

$$\pi^{\frac{1-w}{2}} \frac{\Gamma\big(\frac{w}{2}\big)\Gamma\big(\frac{2v+w-1}{2}\big)}{\Gamma\big(v+\frac{w}{2}\big)} E(z, 1-v),$$

and

$$\begin{aligned}&\pi^{\frac{3}{2}-2v-\frac{w}{2}} \frac{\Gamma(v)\Gamma\big(\frac{2v+w-1}{2}\big)\Gamma\big(\frac{w}{2}\big)}{\Gamma(1-v)\Gamma\big(v+\frac{w}{2}\big)} \frac{\zeta(2v)}{\zeta(2-2v)} E(z, v)\\ &= \pi^{\frac{1-w}{2}} \frac{\Gamma\big(\frac{2v+w-1}{2}\big)\Gamma\big(\frac{w}{2}\big)}{\Gamma\big(v+\frac{w}{2}\big)} E(z, 1-v),\end{aligned}$$

respectively, where for the last identity we applied the functional equation of the Eisenstein series $E(z, v)$. In this way, we obtained the meromorphic continuation of the above integral to a region containing $v = 0$. Continuing this procedure, one can prove the meromorphic continuation of the Poincaré series $P(z; v, w)$ to $\mathbb{C}^2$.

Using Parseval's formula, we obtain

$$\begin{aligned}(5.9)\quad \pi^{-\frac{w}{2}}\Gamma\Big(\frac{w}{2}\Big) I(v,w) \;&=\; \pi^{\frac{1-w}{2}}\,\Gamma\left(\frac{w-1}{2}\right) \langle E(\cdot, v+1), F\rangle\\ &+ \frac{1}{2}\sum_{u_j-\text{even}} \overline{\rho_j(1)}\, L_{u_j}(v+\tfrac{1}{2})\,\mathcal{G}(\tfrac{1}{2}+i\mu_j; v, w)\,\langle u_j, F\rangle\\ &+ \frac{1}{4\pi}\int_{-\infty}^{\infty} \frac{\zeta(v+\frac{1}{2}+i\mu)\,\zeta(v+\frac{1}{2}-i\mu)}{\pi^{-\frac{1}{2}+i\mu}\,\Gamma(\frac{1}{2}-i\mu)\,\zeta(1-2i\mu)}\;\mathcal{G}(\tfrac{1}{2}-i\mu; v, w)\,\langle E(\cdot, \tfrac{1}{2}+i\mu), F\rangle\, d\mu,\end{aligned}$$

which gives the meromorphic continuation of $I(v, w)$. We record this fact in the following

PROPOSITION 5.10. *The function $I(v,w)$, originally defined for $\Re(v)$ and $\Re(w)$ sufficiently large, has a meromorphic continuation to $\mathbb{C}^2$.*

We conclude this section by remarking that from (5.9), one can also obtain information about the polar divisor of the function $I(v, w)$. When $v = 0$, this issue is further discussed in the next section.

6. Proof of Theorem 1.3

To prove the first part of Theorem 1.3, assume for the moment that $f = g$. By Proposition 5.10, we know that the function $I(v, w)$ admits a meromorphic continuation to $\mathbb{C}^2$. Furthermore, if we specialize $v = 0$, the function $I(0, w)$ has its first pole at $w = 1$. Using the asymptotic formula (4), one can write

$$(6.1)\qquad I(0,w) \;=\; \int_{-\infty}^{\infty} \left|L_f(\tfrac{1}{2}+it)\right|^2 K(t,w)\; dt \;=\; 2\int_{0}^{\infty} \left|L_f(\tfrac{1}{2}+it)\right|^2 K(t,w)\; dt,$$

for at least $\Re(w)$ sufficiently large. Here the kernel $K(t,w)$ is given by (4.1). As the first pole of $I(0,w)$ occurs at $w=1$, it follows from (4.3) and Landau's Lemma that

$$Z(w) \;=\; \int_1^\infty \left|L_f(\tfrac12+it)\right|^2 t^{-w}\; dt$$

converges absolutely for $\Re(w)>1$. If $f\neq g$, the same is true for the integral defining $Z(w)$ by Cauchy's inequality. The meromorphic continuation of $Z(w)$ to the region $\Re(w)>-1$ follows now from (4.3). This proves the first part of the theorem.

To obtain the polynomial growth in $|\Im(w)|$, for $\Re(w)>0$, we invoke the functional equation (see [**Goo86**])

$$\begin{aligned}\cos\left(\frac{\pi w}{2}\right) I_\beta(w) - \sin\left(\frac{\pi w}{2}\right) I_\beta(1-w) \\ = \frac{2\pi\,\zeta(w)\,\zeta(1-w)}{(2w-1)\,\pi^{-w}\,\Gamma(w)\,\zeta(2w)}\langle E(\cdot,1-w),F\rangle.\end{aligned} \tag{6.2}$$

It is well-known that $\langle E(\cdot,1-w),F\rangle$ is (essentially) the Rankin-Selberg convolution of f and g. Precisely, we have:

$$\langle E(\cdot,1-w),F\rangle \;=\; (4\pi)^{w-\kappa}\Gamma(\kappa-w)\,L(1-w,f\times g). \tag{6.3}$$

It can be observed that the expression on the right hand side of (6.2) has polynomial growth in $|\Im(w)|$, away from the poles for $-1<\Re(w)<2$.

On the other hand, from the asymptotic formula (4), the integral

$$I_\beta(w) \;:=\; \int_0^\infty L_f(\tfrac12+it)L_g(\tfrac12-it)K_\beta(t,w)\; dt$$

is absolutely convergent for $\Re(w)>1$. We break $I_\beta(w)$ into two integrals:

$$\begin{aligned} I_\beta(w) \;&=\; \int_0^\infty L_f(\tfrac12+it)L_g(\tfrac12-it)K_\beta(t,w)\; dt \\ &= \int_0^{T_w} + \int_{T_w}^\infty \;:=\; I_\beta^{(1)}(w)+I_\beta^{(2)}(w),\end{aligned} \tag{6.4}$$

where $T_w \ll |\Im(w)|^{2+\epsilon}$ (for small fixed $\epsilon>0$), and T_w will be chosen optimally later.

Now, take w such that $-\epsilon<\Re(w)<-\frac{\epsilon}{2}$, and write the functional equation (6.2) as

$$\begin{aligned}\cos\left(\frac{\pi w}{2}\right) I_\beta^{(2)}(w) \;&=\; \left(\sin\left(\frac{\pi w}{2}\right) I_\beta^{(1)}(1-w) \;-\; \cos\left(\frac{\pi w}{2}\right) I_\beta^{(1)}(w)\right) \\ &+ \sin\left(\frac{\pi w}{2}\right) I_\beta^{(2)}(1-w) \\ &+ \frac{2\pi\,\zeta(w)\,\zeta(1-w)}{(2w-1)\,\pi^{-w}\,\Gamma(w)\,\zeta(2w)}\;\langle E(\cdot,1-w),F\rangle.\end{aligned} \tag{6.5}$$

Next, by Proposition 4.2,

$$\begin{aligned}\frac{I_\beta^{(2)}(w)}{\mathcal{B}(w)} &= \int_{T_w}^{\infty} L_f(\tfrac12+it)L_g(\tfrac12-it)\,t^{-w}\left(1+\mathcal{O}\left(\frac{|\Im(w)|^3}{t^2}\right)\right)\,dt\\ &= Z(w)-\int_1^{T_w} L_f(\tfrac12+it)L_g(\tfrac12-it)\,t^{-w}\,dt \;+\;\mathcal{O}\left(\frac{|\Im(w)|^3}{T_w^{1-\epsilon}}\right)\\ &= Z(w)+\mathcal{O}\left(T_w^{1+\epsilon}\;+\;\frac{|\Im(w)|^3}{T_w^{1-\epsilon}}\right).\end{aligned}$$

It follows that

$$Z(w)=\frac{I_\beta^{(2)}(w)}{\mathcal{B}(w)}\;+\;\mathcal{O}\left(T_w^{1+\epsilon}\;+\;\frac{|\Im(w)|^3}{T_w^{1-\epsilon}}\right). \tag{6.6}$$

We may estimate $\frac{I_\beta^{(2)}(w)}{\mathcal{B}(w)}$ using (6.5). Consequently,

$$\begin{aligned}&\frac{I_\beta^{(2)}(w)}{\mathcal{B}(w)} \\ &= \frac{1}{\mathcal{B}(w)}\Bigg[\left(\tan\left(\frac{\pi w}{2}\right)I_\beta^{(1)}(1-w)\;-\;I_\beta^{(1)}(w)\right)+\tan\left(\frac{\pi w}{2}\right)I_\beta^{(2)}(1-w)\\ &\qquad+\frac{2\pi\,\zeta(w)\,\zeta(1-w)}{\cos\left(\frac{\pi w}{2}\right)(2w-1)\,\pi^{-w}\,\Gamma(w)\,\zeta(2w)}\;\langle E(\cdot,1-w),F\rangle\Bigg].\end{aligned} \tag{6.7}$$

We estimate each term on the right hand side of (6.7) using Proposition 4.2 and Proposition 4.6. First of all

$$\begin{aligned}&\frac{\tan\left(\frac{\pi w}{2}\right)I_\beta^{(1)}(1-w)\;-\;I_\beta^{(1)}(w)}{\mathcal{B}(w)}\\ &\qquad= \frac{\sin\left(\frac{\pi w}{2}\right)I_\beta^{(1)}(1-w)\;-\;\cos\left(\frac{\pi w}{2}\right)I_\beta^{(1)}(w)}{\cos\left(\frac{\pi w}{2}\right)\mathcal{B}(w)}\\ &\qquad= \int_0^{T_w} L_f(\tfrac12+it)L_g(\tfrac12-it)\cdot\frac{t^{\frac12}|\Im(w)|^{\kappa-\frac32}}{|\Im(w)|^{\kappa-2-\epsilon}}\,dt\\ &\qquad\ll T_w^{\frac32+\epsilon}|\Im(w)|^{\frac12+\epsilon}.\end{aligned} \tag{6.8}$$

Next, using Stirling's formula to bound the Gamma function,

$$\begin{aligned}(6.9)\qquad &\frac{\tan\left(\frac{\pi w}{2}\right) I_\beta^{(2)}(1-w)}{\mathcal{B}(w)} \\ &= \int_{T_w}^{\infty} L_f(\cdot)L_g(\cdot)\frac{\mathcal{B}(1-w)}{\mathcal{B}(w)} t^{-1-\frac{\epsilon}{2}}\left(1+\mathcal{O}\left(\frac{|\Im(w)|^3}{t^2}\right)\right)\,dt \\ &= \mathcal{O}\left(\frac{\mathcal{B}(1-w)}{\mathcal{B}(w)}\cdot\left(1+\frac{|\Im(w)|^3}{T_w^2}\right)\right) \\ &\ll \left|\frac{\Gamma(1-w)\Gamma(1-w+\kappa-1)\Gamma\left(\frac{1}{2}+w\right)}{\Gamma(w)\Gamma(w+\kappa-1)\Gamma\left(\frac{3}{2}-w\right)}\right|\cdot\left(1+\frac{|\Im(w)|^3}{T_w^2}\right) \\ &\ll |\Im(w)|^{1+2\epsilon}+\frac{|\Im(w)|^{4+2\epsilon}}{T_w^2}.\end{aligned}$$

Using the functional equation of the Riemann zeta-function (6.3), and Stirling's asymptotic formula, we have

$$(6.10)\qquad \left|\frac{2\pi\,\zeta(w)\,\zeta(1-w)}{\mathcal{B}(w)\cos\left(\frac{\pi w}{2}\right)(2w-1)\,\pi^{-w}\,\Gamma(w)\,\zeta(2w)}\,\langle E(\cdot,1-w),F\rangle\right| \ll_\epsilon |\Im(w)|^{1+\epsilon}.$$

Now, we can optimize T_w by letting

$$T_w^{\frac{3}{2}+\epsilon}|\Im(w)|^{\frac{1}{2}+\epsilon} = \frac{|\Im(w)|^3}{T_w^{1-\epsilon}} \implies T_w = |\Im(w)|.$$

Thus, we get

$$Z(w) = \mathcal{O}\left(|\Im(w)|^{2+2\epsilon}\right).$$

One cannot immediately apply the Phragmén-Lindelöf principle as the above function may have simple poles at $w=\frac{1}{2}\pm i\mu_j$, $j\ge 1$. To surmount this difficulty, let

$$(6.11)\quad \mathcal{G}_0(s,w) = \frac{\Gamma\left(w-\frac{1}{2}\right)}{\Gamma\left(\frac{w}{2}\right)}\left[\Gamma\left(\frac{1-s}{2}\right)\Gamma\left(\frac{w-s}{2}\right)+\Gamma\left(\frac{s}{2}\right)\Gamma\left(\frac{w+s-1}{2}\right)\right],$$

and define $\mathcal{J}(w) = \mathcal{J}_{\rm discr}(w) + \mathcal{J}_{\rm cont}(w)$, where

$$(6.12)\qquad \mathcal{J}_{\rm discr}(w) = \frac{1}{2}\sum_{u_j-\text{even}} \overline{\rho_j(1)}\,L_{u_j}\left(\tfrac{1}{2}\right)\mathcal{G}_0\left(\tfrac{1}{2}+i\mu_j,w\right)\langle u_j,F\rangle$$

and

$$\begin{aligned}(6.13)\qquad &\mathcal{J}_{\rm cont}(w) \\ &= \frac{1}{4\pi}\int_{-\infty}^{\infty}\frac{\zeta(\frac{1}{2}+i\mu)\,\zeta(\frac{1}{2}-i\mu)}{\pi^{-\frac{1}{2}+i\mu}\,\Gamma(\frac{1}{2}-i\mu)\,\zeta(1-2i\mu)}\,\mathcal{G}_0\left(\tfrac{1}{2}-i\mu,w\right)\langle E(\cdot,\tfrac{1}{2}+i\mu),F\rangle\,d\mu.\end{aligned}$$

In (6.13), the contour of integration must be slightly modified when $\Re(w)=\frac{1}{2}$ to avoid passage through the point $s=w$.

From the upper bounds of Hoffstein-Lockhart [**HL94**] and Sarnak [**Sar94**], we have that

$$\left|\overline{\rho_j(1)}\,\langle u_j,F\rangle\right| \ll_\epsilon |\mu_j|^{N+\epsilon},$$

for a suitable N. It follows immediately that the series defining $\mathcal{J}_{\mathrm{discr}}(w)$ converges absolutely everywhere in C, except for points where $\mathcal{G}_0(\frac{1}{2}+i\mu_j,w)$, $j\geq 1$, have poles. The meromorphic continuation of $\mathcal{J}_{\mathrm{cont}}(w)$ follows easily by shifting the line of integration to the left. The key point for introducing the auxiliary function $\mathcal{J}(w)$ is that

$$I(0,w)\,-\,\mathcal{J}(w)\qquad(\Re(w)>-\epsilon)$$

(may) have poles only at $w=0$, $\frac{1}{2}$, 1, and moreover,

$$\cos\left(\frac{\pi w}{2}\right)\mathcal{J}(w)$$

has polynomial growth in $|\Im(w)|$, away from the poles, for $-\epsilon<\Re(w)<2$. To obtain a good polynomial bound in $|\Im(w)|$ for this function, it can be observed using Stirling's formula that the main contribution to $\mathcal{J}_{\mathrm{discr}}(w)$ comes from terms corresponding to $|\mu_j|$ close to $|\Im(w)|$. Applying Cauchy's inequality, we have that

$$\left|\frac{\mathcal{J}_{\mathrm{discr}}(w)}{2A(w)}\right|\ll\frac{1}{|A(w)|}\cdot\Bigg(\sum_{\substack{u_j\\|\mu_j|<2|\Im(w)|}}|\rho_j(1)\,\langle u_j,F\rangle|^2\Bigg)^{\frac{1}{2}}\cdot\Bigg(\sum_{\substack{u_j\\|\mu_j|<2|\Im(w)|}}L_{u_j}^2(\tfrac{1}{2})\,|\mathcal{G}_0(\tfrac{1}{2}+i\mu_j,w)|^2\Bigg)^{\frac{1}{2}}.$$

Using Stirling's asymptotic formula, we have the estimates

$$\frac{1}{|A(w)|}\ll|\Im(w)|^{-\Re(w)-\kappa+\frac{3}{2}}\,e^{\frac{\pi}{2}|\Im(w)|}$$

$$|\mathcal{G}_0(\tfrac{1}{2}+i\mu_j,w)|\ll_\epsilon|\Im(w)|^{\frac{\Re(w)}{2}-\frac{3}{4}+\epsilon}e^{-\frac{\pi}{2}|\Im(w)|}\qquad(\Re(w)<1+\epsilon).$$

Also, the Hoffstein-Lockhart estimate [**HL94**] gives

$$|\rho_j(1)|^2\ll_\epsilon|\Im(w)|^\epsilon e^{\pi|\mu_j|},$$

for $\mu_j\ll|\Im(w)|$. It follows that

$$\left|\frac{\mathcal{J}_{\mathrm{discr}}(w)}{2A(w)}\right|\ll|\Im(w)|^{-\frac{\Re(w)}{2}-\kappa+\frac{3}{4}+2\epsilon}\cdot\Bigg(\sum_{\substack{u_j\\|\mu_j|<2|\Im(w)|}}e^{\pi|\mu_j|}\cdot|\langle u_j,F\rangle|^2\Bigg)^{\frac{1}{2}}\cdot\Bigg(\sum_{\substack{u_j\\|\mu_j|<2|\Im(w)|}}L_{u_j}^2(\tfrac{1}{2})\Bigg)^{\frac{1}{2}}.$$

A very sharp bound for the first sum on the right hand side was recently obtained by Bernstein and Reznikov (see [**BR99**]). It gives an upper bound on the order of $|\Im(w)|^{\kappa+\epsilon}$. Finally, Kuznetsov's bound (see [**Mot97**]) gives an estimate on the order of $|\Im(w)|^{1+\epsilon}$ for the second sum. We obtain the final estimate

$$\left|\frac{\mathcal{J}_{\mathrm{discr}}(w)}{2A(w)}\right|\ll_\epsilon|\Im(w)|^{-\frac{\Re(w)}{2}+\frac{7}{4}+4\epsilon}\qquad(\Re(w)<1+\epsilon).\tag{6.14}$$

It is not hard to see that the same estimate holds for $\frac{\mathcal{J}_{\mathrm{cont}}(w)}{2A(w)}$. To see this, we apply in (6.3) the convexity bound for the Rankin-Selberg L–function together with Stirling's formula. It follows that

$$|\langle E(\cdot, \tfrac{1}{2}+i\mu), F\rangle| \ll_\epsilon |\mu|^{\kappa+\epsilon}\, e^{-\frac{\pi}{2}|\mu|}.$$

Then,

$$\left|\frac{\mathcal{J}_{\rm cont}(w)}{2A(w)}\right| \ll_\epsilon |\Im(w)|^{-\frac{\Re(w)}{2}+\frac{3}{4}+2\epsilon} \int\limits_{-2|\Im(w)|}^{2|\Im(w)|} \frac{|\zeta(\frac{1}{2}+i\mu)|^2}{|\zeta(1-2i\mu)|}\, d\mu \qquad (\Re(w) < 1+\epsilon).$$

By the well-known bounds

$$|\zeta(1+it)|^{-1} \ll 1, \qquad \int\limits_0^T |\zeta(\tfrac{1}{2}+it)|^2\, dt \ll_\epsilon T^{1+\epsilon},$$

we obtain

$$\left|\frac{\mathcal{J}_{\rm cont}(w)}{2A(w)}\right| \ll_\epsilon |\Im(w)|^{-\frac{\Re(w)}{2}+\frac{7}{4}+3\epsilon} \qquad (\Re(w) < 1+\epsilon). \tag{6.15}$$

It can be easily seen that the function

$$Z(w) - \frac{\mathcal{J}(w)}{2A(w)} \qquad (\Re(w) > -\epsilon)$$

(may) have poles only at $w = 0,\ \frac{1}{2},\ 1$. We can now apply the Phragmén-Lindelöf principle, and Theorem 1.3 follows. □

Finally, we remark that the choice of the function $\mathcal{G}_0(s,w)$ defined by (6.11) is not necessarily the optimal one. We were rather concerned with making the method as transparent as possible, and in fact, the exponent $2-2\delta$ instead of $2-\frac{3}{4}\delta$ should be obtainable.

While a previous version of this manuscript has circulated, A. Ivić kindly pointed out to us that from the results obtained by Motohashi [**Mot94**] one can easily obtain the exponent (mentioned above) $2-2\delta$, but only in the range $\frac{1}{2} < \delta \leq 1$.

Acknowledgments

The authors would like to extend their warmest thanks to Paul Garrett, Aleksandar Ivić, and the referee for their critical comments and suggestions.

References

[BR99] J. Bernstein & A. Reznikov – "Analytic continuation of representations and estimates of automorphic forms", *Ann. of Math. (2)* **150** (1999), no. 1, p. 329–352.

[CF00] J. B. Conrey & D. W. Farmer – "Mean values of L-functions and symmetry", *Internat. Math. Res. Notices* (2000), no. 17, p. 883–908.

[CFK+] J. B. Conrey, D. W. Farmer, J. P. Keating, M. O. Rubenstein & N. C. Snaith – "Moments of zeta and L-functions".

[CG84] J. B. Conrey & A. Ghosh – "On mean values of the zeta-function", *Mathematika* **31** (1984), no. 1, p. 159–161.

[CG01] J. B. Conrey & S. M. Gonek – "High moments of the Riemann zeta-function", *Duke Math. J.* **107** (2001), no. 3, p. 577–604.

[Dav00] H. Davenport – *Multiplicative number theory*, third ed., Graduate Texts in Mathematics, vol. 74, Springer-Verlag, New York, 2000, Revised and with a preface by Hugh L. Montgomery.

[DG] A. Diaconu & D. Goldfeld – "Second moments of quadratic Hecke L–series and multiple Dirichlet series I", in *Multiple Dirichlet Series, Automorphic Forms and Analytic Number Theory, Proceedings of the Workshop on Multiple Dirichlet Series, July 11-14, 2005,* Proceedings of Symposia in Pure Mathematics, AMS, (to appear).

[DGH03] A. Diaconu, D. Goldfeld & J. Hoffstein – "Multiple Dirichlet series and moments of zeta and L-functions", *Compositio Math.* **139** (2003), no. 3, p. 297–360.

[Gau01] C. F. Gauss – "Disquisitiones Arithmeticae", 1801.

[Goo82] A. Good – "The square mean of Dirichlet series associated with cusp forms", *Mathematika* **29** (1982), no. 2, p. 278–295 (1983).

[Goo86] A. Good – "The convolution method for Dirichlet series", in *The Selberg trace formula and related topics (Brunswick, Maine, 1984)*, Contemp. Math., vol. 53, Amer. Math. Soc., Providence, RI, 1986, p. 207–214.

[GR94] I. S. Gradshteyn & I. M. Ryzhik – *Table of integrals, series, and products*, fifth ed., Academic Press Inc., Boston, MA, 1994.

[HB81] D. R. Heath-Brown – "An asymptotic series for the mean value of Dirichlet L-functions", *Comment. Math. Helv.* **56** (1981), no. 1, p. 148–161.

[HL18] G. H. Hardy & J. E. Littlewood – "Contributions to the theory of the Riemann zeta-function and the theory of the distributions of primes", *Acta Mathematica* **41** (1918), p. 119–196.

[HL94] J. Hoffstein & P. Lockhart – "Coefficients of Maass forms and the Siegel zero", *Ann. of Math. (2)* **140** (1994), no. 1, p. 161–181, With an appendix by Dorian Goldfeld, Hoffstein and Daniel Lieman.

[IJM00] A. Ivić, M. Jutila & Y. Motohashi – "The Mellin transform of powers of the zeta-function", *Acta Arith.* **95** (2000), no. 4, p. 305–342.

[Ing26] A. E. Ingham – "Mean-value theorems in the theory of the Riemann zeta-function", *Proceedings of the London Mathematical Society* **27** (1926), p. 273–300.

[Ivi02] A. Ivić – "On the estimation of $\mathcal{Z}_2(s)$", in *Analytic and probabilistic methods in number theory (Palanga, 2001)*, TEV, Vilnius, 2002, p. 83–98.

[Jut97] M. Jutila – "Mean values of Dirichlet series via Laplace transforms", in *Analytic number theory (Kyoto, 1996)*, London Math. Soc. Lecture Note Ser., vol. 247, Cambridge Univ. Press, Cambridge, 1997, p. 169–207.

[Jut05] ______, "The Mellin transform of the fourth power of Riemann's zeta-function", in *Number theory*, Ramanujan Math. Soc. Lect. Notes Ser., vol. 1, Ramanujan Math. Soc., Mysore, 2005, p. 15–29.

[KS99] N. M. Katz & P. Sarnak – *Random matrices, Frobenius eigenvalues, and monodromy*, American Mathematical Society Colloquium Publications, vol. 45, American Mathematical Society, Providence, RI, 1999.

[KS00] J. P. Keating & N. C. Snaith – "Random matrix theory and $\zeta(1/2 + it)$", *Comm. Math. Phys.* **214** (2000), no. 1, p. 57–89.

[Mot92] Y. Motohashi – "Spectral mean values of Maass waveform L-functions", *J. Number Theory* **42** (1992), no. 3, p. 258–284.

[Mot93] ______, "An explicit formula for the fourth power mean of the Riemann zeta-function", *Acta Math.* **170** (1993), no. 2, p. 181–220.

[Mot94] ______, "The mean square of Hecke L-series attached to holomorphic cusp-forms", *Kokyuroku RIMS Kyoto University* (1994), no. 886, p. 214–227, Analytic number theory (Japanese) (Kyoto, 1993).

[Mot95] ______, "A relation between the Riemann zeta-function and the hyperbolic Laplacian", *Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4)* **22** (1995), no. 2, p. 299–313.

[Mot97] ______, *Spectral theory of the Riemann zeta-function*, Cambridge Tracts in Mathematics, vol. 127, Cambridge University Press, Cambridge, 1997.

[Sar94] P. Sarnak – "Integrals of products of eigenfunctions", *Internat. Math. Res. Notices* (1994), no. 6, p. 251 ff., approx. 10 pp. (electronic).

[Sie44] C. L. Siegel – "The average measure of quadratic forms with given determinant and signature", *Ann. of Math. (2)* **45** (1944), p. 667–685.

[Vin18] I. M. Vinogradov – "On the mean value of the number of classes of proper primitive forms of negative discriminant", *Soobchshneyia Khar'kovskogo mathematicheskogo obshestva (Transactions of the Kharkov Math. Soc.)* **16** (1918), p. 10–38.

[Zav89] N. I. ZAVOROTNY – "Automorphic functions and number theory, part I, II (Russian)", *Akad. Nauk SSSR, Dal'nevostochn. Otdel., Vladivostok* **254** (1989), p. 69–124a.
[Zha] W. ZHANG – "Integral mean values of modular L–functions", preprint.

SCHOOL OF MATHEMATICS, UNIVERSITY OF MINNESOTA, MINNEAPOLIS, MN 55455
E-mail address: cad@math.umn.edu

COLUMBIA UNIVERSITY, DEPARTMENT OF MATHEMATICS, NEW YORK, NY 10027
E-mail address: goldfeld@math.columbia.edu

Clay Mathematics Proceedings
Volume 7, 2007

CM points and weight $3/2$ modular forms

Jens Funke

Abstract. We survey the results of [**Fun02**] and of our joint work with Bruinier [**BF06**] on using the theta correspondence for the dual pair $\mathrm{SL}(2)\times\mathrm{O}(1,2)$ to realize generating series of values of modular functions on a modular curve as (non)-holomorphic modular forms of weight $3/2$.

1. Introduction

The theta correspondence has been an important tool in the theory of automorphic forms with manifold applications to arithmetic questions.

In this paper, we consider a specific theta lift for an isotropic quadratic space V over $\mathbb{Q}$ of signature $(1,2)$. The theta kernel we employ associated to the lift has been constructed by Kudla-Millson (e.g., [**KM86, KM90**]) in much greater generality for $\mathrm{O}(p,q)$ ($\mathrm{U}(p,q)$) to realize generating series of cohomological intersection numbers of certain, 'special' cycles in locally symmetric spaces of orthogonal (unitary) type as holomorphic Siegel (Hermitian) modular forms. In our case for $\mathrm{O}(1,2)$, the underlying locally symmetric space M is a modular curve, and the special cycles, parametrized by positive integers N, are the classical CM points $Z(N)$; i.e., quadratic irrationalities of discriminant $-N$ in the upper half plane.

We survey the results of [**Fun02**] and of our joint work with Bruinier [**BF06**] on using this particular theta kernel to define lifts of various kinds of functions F on the underlying modular curve M. The theta lift is given by

$$I(\tau,F)=\int_M F(z)\theta(\tau,z), \tag{1.1}$$

where $\tau\in\mathbb{H}$, the upper half plane, $z\in M$, and $\theta(\tau,z)$ is the theta kernel in question. Then $I(\tau,F)$ is a (in general non-holomorphic) modular form of weight $3/2$ for a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. One key feature of the theta kernel is its very rapid decay on M, which distinguishes it from other theta kernels which are usually moderately increasing. Consequently, we can lift some rather nonstandard, even exponentially increasing, functions F.

2000 *Mathematics Subject Classification.* Primary 11F37, Secondary 11F11, 11F27.
Partially supported by NSF grant DMS-0305448.

Note that Kudla and Millson, who focus entirely on the (co)homological aspects of their general lift, study in this situation only the lift of the constant function 1 in the compact case of a Shimura curve, when V is anisotropic.

One feature of our work is that it provides a uniform approach to several topics and (in part previously known) results, which so far all have been approached by (entirely) different methods. We discuss the following cases in some detail:

(i) The lift of the constant function 1. Then $I(\tau, 1)$ realizes the generating series of the (geometric) degree of the 0-cycles $Z(N)$ as the holomorphic part of a non-holomorphic modular form. As a special case, we recover Zagier's well known Eisenstein series $\mathcal{F}(\tau, s)$ of weight $3/2$ at $s = 1/2$ (in our normalization) whose Fourier coefficients of positive index are given by the Kronecker-Hurwitz class numbers $H(N)$ [**Zag75, HZ76**].

(ii) The lift of a modular function f of weight 0 on M. In that case, we obtain a generalization with a completely different proof of Zagier's influential result [**Zag02**] on the generating series of the traces of the singular moduli, that is, the sum of values of the classical j-invariant over the CM points of a given discriminant. Moreover, our method provides a generalization to modular curves of arbitrary genus.

(iii) The lift of the logarithm of the Petersson metric $\log \|\Delta\|$ of the discriminant function Δ. This was suggested to us by U. Kühn. In that case, the lift $I(\tau, \|\log \Delta\|)$ turns out to be the *derivative* of Zagier's Eisenstein series $\mathcal{F}'(\tau, s)$ at $s = 1/2$. Furthermore, one can interpret the Fourier coefficients as the *arithmetic* degree of the ($\mathbb{Z}$ extension of the) CM cycles. This provides a different approach for the result of (Kudla, Rapoport and) Yang [**Yan04**] in this case, part of Kudla's general program on realizing generating series in arithmetic geometry as modular forms, in particular as derivatives of Eisenstein series. Their result in the modular curve case grew out of their extensive and deep work on the analogous but more involved case for Shimura curves [**KRY04, KRY06**].

(iv) The lift of a weight 0 Maass cusp form f on M. For this input, our lift is equivalent to a theta lift introduced by Maass [**Maa59**], which was studied and applied by Duke [**Duk88**] (to obtain equidistribution results for the CM points and certain geodesics in M) and Katok and Sarnak [**KS93**] (to obtain nonnegativity of the L-function of f at the center of the criticial strip).

The paper is mostly expository; for convenience of the reader and for future use, we briefly discuss the construction of the theta kernel and also give general formulas for the Fourier coefficients.

However, we also discuss a few new aspects. Namely:

(v) For any meromorphic modular form f, we give an explicit formula for the positive Fourier coefficients of the lift $I(\tau, \log \|f\|)$ of the logarithm of the Petersson metric of f in the case when the divisor of f is *not* (necessarily) disjoint to one of the 0-cycles $Z(N)$. In particular, for the j-invariant, we realize the logarithm of the *norm* of the singular moduli as the Fourier coefficients of a non-holomorphic modular form of weight $3/2$. Recall that the norms of the singular moduli were studied by Gross-Zagier [**GZ85**].

In this context and also in view of (iii) it will be interesting to consider the lift for the logarithm of the Petersson metric of a Borcherds product [**Bor98**]. We will come back to this point in the near future.

(vi) Bringmann, Ono, and Rouse [**BOR05**] consider the intersection of a modular curve with a Hirzebruch-Zagier curve T_N in a Hilbert modular curve. Based on our work, they realize the generating series of the traces of the singular moduli on these intersections as a weakly holomorphic modular form of weight 2. They proceed to find some beautiful formulas involving Hilbert class polynomials.

In the last section of this paper, we show how one can obtain such generating series in the context of the Kudla-Millson machinery and generalize this aspect of [**BOR05**] to the intersection of a modular curve with certain special divisors inside locally symmetric spaces associated to $\mathrm{O}(n,2)$.

Some comments on the usage of this particular kernel function for the lift are in order. The lift I is designed to produce *holomorphic* generating series, while often theta series and integrals associated to indefinite quadratic forms give rise to non-holomorphic modular forms. Furthermore, the lift focuses a priori only on the positive coefficients which correspond to the CM points, while the negative coefficients (which correspond to certain geodesics in M) often vanish. For these geodesics, in the Kudla-Millson theory [**KM86, KM90**], there is another lift for signature $(2,1)$ with weight 2 forms as input, which produces generating series of periods over the geodesics, see also [**FM02**]. This lift is closely related to Shintani's theta lift [**Shi75**].

Finally note that J. Bruinier [**Bru06**] wrote up a survey on some aspects of our work as well. I also thank him and U. Kühn for comments on the present paper. We also thank the Centre de Recerca Matemàtica in Bellaterra/Spain for its hospitality during fall 2005.

2. Basic notions

2.1. CM points. Let V be a rational vector space of dimension 3 with a non-degenerate symmetric bilinear form $(\ ,\ )$ of signature $(1,2)$. We assume that V is given by

$$V = \{X \in M_2(\mathbb{Q}); \mathrm{tr}(X) = 0\} \tag{2.1}$$

with $(X,Y) = \mathrm{tr}(XY)$ and associated quadratic form $q(X) = \frac{1}{2}(X,X) = \det(X)$. We let $\underline{G} = \mathrm{Spin}\, V \simeq \mathrm{SL}_2$, which acts on V by $g.X := gXg^{-1}$. We set $G = \underline{G}(\mathbb{R})$ and let $D = G/K$ be the associated symmetric space, where $K = \mathrm{SO}(2)$ is the standard maximal compact subgroup of G. We have $D \simeq \mathbb{H} = \{z \in \mathbb{C};\ \Im(z) > 0\}$. Let $L \subset V(\mathbb{Q})$ be an integral lattice of full rank and let Γ be a congruence subgroup of G which takes L to itself. We write $M = \Gamma\backslash D$ for the attached locally symmetric space, which is a modular curve. Throughout the paper let p be a prime or $p = 1$. For simplicity, we assume that the lattice L is given by

$$L = \left\{ [a,b,c] := \begin{pmatrix} b & -2c \\ 2ap & -b \end{pmatrix} :\ a,b,c \in \mathbb{Z} \right\}. \tag{2.2}$$

(For arbitrary even lattices, see [**BF06**]). Then we can take $\Gamma = \Gamma_0^*(p)$, the extension of the Hecke subgroup $\Gamma_0(p)$ by the Fricke involution W_p. Note that then M has only one cusp.

We identify D with the space of lines in $V(\mathbb{R})$ on which the form $(\ ,\ )$ is positive:

$$D \simeq \{z \subset V(\mathbb{R});\ \dim z = 1 \text{ and } (\ ,\ )|_z > 0\}. \tag{2.3}$$

We pick as base point of D the line z_0 spanned by $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. For $z \in \mathbb{H}$, we choose $g_z \in G/K$ such that $g_z i = z$; the action is the usual linear fractional transformation on $\mathbb{H}$. Then $z \longmapsto g_z z_0$ gives rise to a G-equivariant isomorphism $\mathbb{H} \simeq D$. The positive line associated to $z = x + iy \in \mathbb{H}$ is generated by $X(z) := g_z.\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. We let $(\ ,\ )_z$ be the minimal majorant of $(\ ,\ )$ associated to $z \in D$. One easily sees that $(X, X)_z = (X, X(z))^2 - (X, X)$.

The classical CM points are now given as follows. For $X = [a, b, c] \in V$ such that $q(X) = 4acp - b^2 = N > 0$, we put

$$D_X = \operatorname{span}(X) \in D. \tag{2.4}$$

It is easy to see that D_X is explicitly given by the point $\frac{-b+i\sqrt{N}}{2ap}$ in the upper half plane. The stabilizer Γ_X of X in Γ is finite. We then denote by $Z(X)$ the image of D_X in M, counted with multiplicity $\frac{1}{|\overline{\Gamma}_X|}$. Here $\overline{\Gamma}_X$ denotes the image of Γ_X in $\mathrm{PGL}_2(\mathbb{Z})$. Furthermore, Γ acts on $L_N = \{X \in L;\ q(X) = N\}$ with finitely many orbits. The CM points of discriminant $-N$ are given by

$$Z(N) = \sum_{X \in \Gamma \backslash L_N} Z(X). \tag{2.5}$$

We can interpret this in terms of positive definite binary quadratic forms as well. For $N > 0$ a positive integer, we let $\mathcal{Q}_{N,p}$ be the set of positive definite binary quadratic forms of the form $apX^2 + bXY + cY^2$ of discriminant $-N = b^2 - 4acp$ with $a, b, c, \in \mathbb{Z}$. Then $\Gamma = \Gamma_0^*(p)$ acts on $\mathcal{Q}_{N,p}$ in the usual way, and the obvious map from $\mathcal{Q}_{N,p}$ to L_N is $\Gamma_0^*(p)$-equivariant, and L_N is in bijection with $\mathcal{Q}_{N,p} \coprod -\mathcal{Q}_{N,p}$. (The vector $X = [a, b, c] \in L_N$ with $a < 0$ corresponds to a negative definite form).

For a Γ-invariant function F on $D \simeq \mathbb{H}$, we define its trace by

$$\mathbf{t}_F(N) = \sum_{z \in Z(N)} F(z) = \sum_{X \in \Gamma \backslash L_N} \frac{1}{|\overline{\Gamma}_X|} F(D_X). \tag{2.6}$$

2.2. The Theta lift. Kudla and Millson [**KM86**] have explicitly constructed a Schwartz function $\varphi_{KM} = \varphi$ on $V(\mathbb{R})$ valued in $\Omega^{1,1}(D)$, the differential $(1,1)$-forms on D. It is given by

$$\varphi(X, z) = \left((X, X(z))^2 - \frac{1}{2\pi} \right) e^{-\pi (X,X)_z}\, \omega, \tag{2.7}$$

where $\omega = \frac{dx \wedge dy}{y^2} = \frac{i}{2} \frac{dz \wedge d\bar{z}}{y^2}$. We have $\varphi(g.X, gz) = \varphi(X, z)$ for $g \in G$. We define

$$\varphi^0(X, z) = e^{\pi(X,X)} \varphi(X, z) = \left((X, X(z))^2 - \frac{1}{2\pi} \right) e^{-2\pi R(X,z)}\, \omega, \tag{2.8}$$

with $R(X, z) = \frac{1}{2}(X, X)_z - \frac{1}{2}(X, X)$. Note tha $R(X, z) = 0$ if and only if $z = D_X$, i.e., if X lies in the line generated by $X(z)$.

For $\tau = u + iv \in \mathbb{H}$, we put $g'_\tau = \left(\begin{smallmatrix} 1 & u \\ 0 & 1 \end{smallmatrix}\right) \left(\begin{smallmatrix} v^{1/2} & 0 \\ 0 & v^{-1/2} \end{smallmatrix}\right)$, and we define

$$\varphi(X, \tau, z) = \varphi^0(\sqrt{v} X, z) e^{2\pi i q(X) \tau}. \tag{2.9}$$

Then, see [**KM90, Fun02**], the theta kernel

$$\theta(\tau, z) := \sum_{X \in L} \varphi(X, \tau, z) \tag{2.10}$$

defines a *non-holomorphic* modular form of weight 3/2 with values in $\Omega^{1,1}(M)$, for the congruence subgroup $\Gamma_0(4p)$. By [**Fun02, BF06**] we have

$$\theta(\tau, z) = O(e^{-Cy^2}) \qquad \text{as} \qquad y \to \infty, \tag{2.11}$$

uniformly in x, for some constant $C > 0$.

In this paper, we discuss for certain Γ-invariant functions F with possible logarithmic singularities inside D, the theta integral

$$I(\tau, F) := \int_M F(z)\theta(\tau, z). \tag{2.12}$$

Note that by (2.11), $I(\tau, F)$ typically converges even for exponentially increasing F. It is clear that $I(\tau, F)$ defines a (in general non-holomorphic) modular form on the upper half plane of weight 3/2. The Fourier expansion is given by

$$I(\tau, F) = \sum_{N=-\infty}^{\infty} a_N(v) q^N \tag{2.13}$$

with

$$a_N(v) = \int_M \sum_{X \in L_N} F(z)\varphi^0(\sqrt{v}X, z). \tag{2.14}$$

For the computation of the Fourier expansion of $I(\tau, f)$, Kudla's construction of a Green function ξ^0 associated to φ^0 is crucial, see [**Kud97**]. We let

$$\xi^0(X, z) = -Ei(-2\pi R(X, z)) = \int_1^\infty e^{-2\pi R(X,z)t} \frac{dt}{t}, \tag{2.15}$$

where $Ei(w)$ denotes the exponential integral, see [**Ste84**]. For $q(X) > 0$, the function $\xi^0(X, z)$ has logarithmic growth at the point D_X, while it is smooth on D if $q(X) \leq 0$.

We let ∂, $\bar{\partial}$ and d be the usual differentials on D and set $d^c = \frac{1}{4\pi i}(\partial - \bar{\partial})$.

THEOREM 2.1 (Kudla [**Kud97**], Proposition 11.1). *Let X be a nonzero vector in V. Set $D_X = \emptyset$ if $q(X) \leq 0$. Then, outside D_X, we have*

$$dd^c \xi^0(X, z) = \varphi^0(X, z). \tag{2.16}$$

In particular, $\varphi^0(X, z)$ is exact for $q(X) \leq 0$. Furthermore, if $q(X) > 0$ or if $q(X) < 0$ and $q(X) \notin -(\mathbb{Q}^\times)^2$ (so that $\overline{\Gamma}_X$ is infinite cyclic), we have for a smooth function F on $\Gamma_X \backslash D$ that

$$\int_{\Gamma_X \backslash D} F(z)\varphi^0(X, z) = \delta_{D_X}(F) + \int_{\Gamma_X \backslash D} (dd^c F(z))\, \xi^0(X, z). \tag{2.17}$$

Here δ_{D_X} denotes the delta distribution concentrated at D_X. By Propositions 2.2 and 4.1 of [**BF06**] *and their proofs, (2.17) does not only hold for compactly support functions F on $\Gamma_X \backslash D$, but also for functions of "linear-exponential" growth on $\Gamma_X \backslash D$.*

In Proposition 4.11, we will give an extension of Theorem 2.1 to F having logarithmic singularities inside D.

By the usual unfolding argument, see [**BF06**], section 4, we have

LEMMA 2.2. *Let $N > 0$ or $N < 0$ such that $N \notin -(\mathbb{Q}^\times)^2$. Then*

$$a_N(v) = \sum_{X \in \Gamma \backslash L_N} \int_{\Gamma_X \backslash D} F(z) \varphi^0(\sqrt{v}X, z).$$

If F is smooth on X, then by Theorem 2.17 we obtain

$$a_N(v) = \mathbf{t}_F(N) + \sum_{X \in \Gamma \backslash L_N} \frac{1}{|\overline{\Gamma}_X|} \int_D (dd^c F(z)) \cdot \xi^0(\sqrt{v}X, z), \qquad (N > 0)$$

$$a_N(v) = \sum_{X \in \Gamma \backslash L_N} \int_{\Gamma_X \backslash D} (dd^c F(z)) \cdot \xi^0(\sqrt{v}X, z) \qquad (N < 0, \quad N \notin -(\mathbb{Q}^\times)^2)$$

For $N = -m^2$, unfolding is (typically) not valid, since in that case $\overline{\Gamma}_X$ is trivial. In the proof of Theorem 7.8 in [**BF06**] we outline

LEMMA 2.3. *Let $N = -m^2$. Then*

$$\begin{aligned} a_N(v) = \sum_{X \in \Gamma \backslash L_N} \frac{1}{2\pi i} \int_M d & \left(F(z) \sum_{\gamma \in \Gamma} \partial \xi^0(\sqrt{v}X, \gamma z) \right) \\ & + \frac{1}{2\pi i} \int_M d \left(\bar{\partial} F(z) \sum_{\gamma \in \Gamma} \xi^0(\sqrt{v}X, \gamma z) \right) \\ & - \frac{1}{2\pi i} \int_M (\partial \bar{\partial} F(z)) \sum_{\gamma \in \Gamma} \xi^0(\sqrt{v}X, \gamma z). \end{aligned}$$

Note that with our choice of the particular lattice L in (2.2), we actually have $\#\Gamma \backslash L_{-m^2} = m$, and as representatives we can take $\{ \left(\begin{smallmatrix} m & 2k \\ & -m \end{smallmatrix} \right) ; k = 0, \dots, m-1 \}$.

Finally, we have

$$a_0(v) = \int_M F(z) \sum_{X \in L_0} \varphi^0(\sqrt{v}X, z). \tag{2.18}$$

We split this integral into two pieces a_0' for $X = 0$ and $a''(v) = a_0(v) - a_0'$ for $X \neq 0$. However, unless F is at most mildly increasing, the two individual integrals will not converge and have to be regularized in a certain manner following [**Bor98, BF06**]. For $a_0''(v)$, we have only one Γ-equivalence class of isotropic lines in L, since Γ has only one cusp. We denote by $\ell_0 = \mathbb{Q}X_0$ the isotropic line spanned by the primitive vector in L, $X_0 = \left(\begin{smallmatrix} 0 & 2 \\ 0 & 0 \end{smallmatrix} \right)$. Note that the pointwise stabilizer of ℓ_0 is Γ_∞, the usual parabolic subgroup of Γ. We obtain

LEMMA 2.4.

$$a_0' = -\frac{1}{2\pi} \int_M^{reg} F(z) \omega, \tag{2.19}$$

(2.20)
$$a_0''(v) = \frac{1}{2\pi i}\int_M^{reg} d\left(F(z)\sum_{\gamma\in\Gamma_\infty\backslash\Gamma}\sum_{n=-\infty}^{\infty}{}' \partial\xi^0(\sqrt{v}nX_0,\gamma z)\right)$$
$$+\frac{1}{2\pi i}\int_M^{reg} d\left(\bar\partial F(z)\sum_{\gamma\in\Gamma_\infty\backslash\Gamma}\sum_{n=-\infty}^{\infty}{}' \xi^0(\sqrt{v}nX_0,\gamma z)\right)$$
$$-\frac{1}{2\pi i}\int_M^{reg} (\partial\bar\partial F(z))\sum_{\gamma\in\Gamma_\infty\backslash\Gamma}\sum_{n=-\infty}^{\infty}{}' \xi^0(\sqrt{v}nX_0,\gamma z).$$

Here $\sum'$ *indicates that the sum only extends over* $n \neq 0$.

3. The lift of modular functions

3.1. The lift of the constant function. The modular trace of the constant function $F = 1$ is already very interesting. In that case, the modular trace of index N is the (geometric) degree of the 0-cycle $Z(N)$:

(3.1)
$$\mathbf{t}_1(N) = \deg Z(N) = \sum_{X\in\Gamma\backslash L_N} \frac{1}{|\overline{\Gamma}_X|}.$$

For $p = 1$, this is twice the famous *Kronecker-Hurwitz* class number $H(N)$ of positive definite binary integral (not necessarily primitive) quadratic forms of discriminant $-N$. From that perspective, we can consider $\deg Z(N)$ for a general lattice L as a generalized class number. On the other hand, $\deg Z(N)$ is essentially the number of length N vectors in the lattice L modulo Γ. So we can think about $\deg Z(N)$ also as the direct analogue of the classical representation numbers by quadratic forms in the positive definite case.

THEOREM 3.1 ([**Fun02**]). *Recall that we write* $\tau = u + iv \in \mathbb{H}$. *Then*

$$I(\tau,1) = \mathrm{vol}(X) + \sum_{N=1}^{\infty} \deg Z(N)q^N + \frac{1}{8\pi\sqrt{v}}\sum_{n=-\infty}^{\infty}\beta(4\pi v n^2)q^{-n^2}.$$

Here $\mathrm{vol}(X) = -\frac{1}{2\pi}\int_X \omega \in \mathbb{Q}$ *is the (normalized) volume of the modular curve* M. *Furthermore,* $\beta(s) = \int_1^\infty e^{-st}t^{-3/2}dt$.

In particular, for $p = 1$, we recover Zagier's well known Eisenstein series $\mathcal{F}(\tau)$ of weight 3/2, see [**Zag75, HZ76**]. Namely, we have

THEOREM 3.2. *Let* $p = 1$, *so that* $\deg Z(N) = 2H(N)$. *Then*

$$\frac{1}{2}I(\tau,1) = \mathcal{F}(\tau) = -\frac{1}{12} + \sum_{N=1}^{\infty} H(N)q^N + \frac{1}{16\pi\sqrt{v}}\sum_{n=-\infty}^{\infty}\beta(4\pi n^2 v)q^{-n^2}$$

REMARK 3.3. We can view Theorem 3.1 on one hand as the generalization of Zagier's Eisenstein series. On the other hand, we can consider Theorem 3.2 as a special case of the Siegel-Weil formula, realizing the theta integral as an Eisenstein series. Note however that here Theorem 3.2 arises by explicit computation and comparison of the Fourier expansions on both sides. For a more intrinsic proof, see Section 3.3 below.

Remark 3.4. Lemma 2.2 immediately takes care of a large class of coefficients. However, the calculation of the Fourier coefficients of index $-m^2$ is quite delicate and represents the main technical difficulty for Theorem 3.1, since the usual unfolding argument is not allowed. We have two ways of computing the integral. In [**Fun02**], we employ a method somewhat similar to Zagier's method in [**Zag81**], namely we appropriately regularize the integral in order to unfold. In [**BF06**], we use Lemma 2.3, i.e., explicitly the fact that for negative index, the Schwartz function $\varphi_{KM}(x)$ (with $(x,x)<0$) is *exact* and apply Stokes' Theorem.

Remark 3.5. In joint work with O. Imamoglu [**FI**], we are currently considering the analogue of the present situation to general hyperbolic space $(1,q)$. We study a similar theta integral for constant and other input. In particular, we realize the generating series of certain 0-cycles inside hyperbolic manifolds as Eisenstein series of weight $(q+1)/2$.

3.2. The lift of modular functions and weak Maass forms. In [**BF04**], we introduced the space of weak Maass forms. For weight 0, it consists of those Γ-invariant and harmonic functions f on $D \simeq \mathbb{H}$ which satisfy $f(z)=O(e^{Cy})$ as $z\to\infty$ for some constant C. We denote this space by $H_0(\Gamma)$. A form $f\in H_0(\Gamma)$ can be written as $f=f^+ + f^-$, where the Fourier expansions of f^+ and f^- are of the form

$$(3.2)\quad f^+(z)=\sum_{n\in\mathbb{Z}} b^+(n)e(nz) \qquad \text{and} \qquad f^-(z)=b^-(0)v+\sum_{n\in\mathbb{Z}-\{0\}} b^-(n)e(n\bar{z}),$$

where $b^+(n)=0$ for $n\ll 0$ and $b^-(n)=0$ for $n\gg 0$. We let $H_0^+(\Gamma)$ be the subspace of those f that satisfy $b^-(n)=0$ for $n\geq 0$. It consists for those $f\in H_0(\Gamma)$ such that f^- is exponentially decreasing at the cusps. We define a $\mathbb{C}$-antilinear map by $(\xi_0 f)(z)=y^{-2}\overline{L_0 f(z)}=R_0\overline{f(z)}$. Here L_0 and R_0 are the weight 0 Maass lowering and raising operators. Then the significance of $H_0^+(\Gamma)$ lies in the fact, see [**BF04**], Section 3, that ξ_0 maps $H_0^+(\Gamma)$ onto $S_2(\Gamma)$, the space of weight 2 cusp forms for Γ. Furthermore, we let $M_0^!(\Gamma)$ be the space of modular functions for Γ (or weakly holomorphic modular forms for Γ of weight 0). Note that $\ker\xi = M_0^!(\Gamma)$. We therefore have a short exact sequence

$$(3.3)\qquad 0 \longrightarrow M_0^!(\Gamma) \longrightarrow H_0^+(\Gamma) \xrightarrow{\ \xi_0\ } S_2(\Gamma) \longrightarrow 0\,.$$

Theorem 3.6 ([**BF06**], Theorem 1.1). *For $f\in H_0^+(\Gamma)$, assume that the constant coefficient $b^+(0)$ vanishes. Then*

$$I(\tau,f)=\sum_{N>0}\mathbf{t}_f(N)q^N+\sum_{n\geq 0}\big(\sigma_1(n)+p\sigma_1(\tfrac{n}{p})\big)b^+(-n)-\sum_{m>0}\sum_{n>0} mb^+(-mn)q^{-m^2}$$

is a weakly holomorphic modular form (i.e., meromorphic with the poles concentrated inside the cusps) of weight $3/2$ for the group $\Gamma_0(4p)$. If $a(0)$ does not vanish, then <u>in addition</u> non-holomorphic terms as in Theorem 3.1 occur, namely

$$\frac{1}{8\pi\sqrt{v}}b^+(0)\sum_{n=-\infty}^{\infty}\beta(4\pi v n^2)q^{-n^2}.$$

For $p=1$, we let $J(z):=j(z)-744$ be the normalized Hauptmodul for $\mathrm{SL}_2(\mathbb{Z})$. Here $j(z)$ is the famous j-invariant. The values of j at the CM points are of classical interest and are known as *singular moduli*. For example, they are algebraic integers.

In fact, the values at the CM points of discriminant D generate the Hilbert class field of the imaginary quadratic field $\mathbb{Q}(\sqrt{D})$. Hence its modular trace (which can also be considered as a suitable Galois trace) is of particular interest. Zagier [**Zag02**] realized the generating series of the traces of the singular moduli as a weakly holomorpic modular form of weight 3/2. For $p = 1$, Theorem 3.6 recovers this influential result of Zagier [**Zag02**].

Theorem 3.7 (Zagier [**Zag02**]). *We have that*

$$-q^{-1} + 2 + \sum_{N=1}^{\infty} \mathbf{t}_J(N) q^N$$

is a weakly holomorphic modular form of weight $3/2$ *for* $\Gamma_0(4)$.

Remark 3.8. The proof of Theorem 3.6 follows Lemmas 2.2, 2.3, and 2.4. The formulas given there simplify greatly since the input f is harmonic (or even holomorphic) and $\overline{\partial} f$ is rapidly decreasing (or even vanishes). Again, the coefficients of index $-m^2$ are quite delicate. Furthermore, $a_0''(v)$ vanishes unless b_0^+ is nonzero, while we use a method of Borcherds [**Bor98**] to explicitly compute the average value a_0' of f. (Actually, for a_0', Remark 4.9 in [**BF06**] only covers the holomorphic case, but the same argument as in the proof of Theorem 7.8 in [**BF06**] shows that the calculation is also valid for H_0^+).

Remark 3.9. Note that Zagier's approach to the above result is quite different. To obtain Theorem 3.7, he explicitly constructs a weakly holomorphic modular form of weight 3/2, which turns to be the generating series of the traces of the singular moduli. His proof heavily depends on the fact that the Riemann surface in question, $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$, has genus 0. In fact, Zagier's proof extends to other genus 0 Riemann surfaces, see [**Kim04, Kim**].

Our approach addresses several questions and issues which arise from Zagier's work:

- We show that the condition 'genus 0' is irrelevant in this context; the result holds for (suitable) modular curves of any genus.
- A geometric interpretation of the constant coefficient is given as the regularized average value of f over M, see Lemma 2.4. It can be explicitly computed, see Remark 3.8 above.
- A geometric interpretation of the coefficient(s) of negative index is given in terms of the behavior of f at the cusp, see Definition 4.4 and Theorem 4.5 in [**BF06**].
- We settle the question when the generating series of modular traces for a weakly holomorphic form $f \in M_0^!(\Gamma)$ is part of a weakly holomorphic form of weight 3/2 (as it is the case for $J(z)$) or when it is part of a *non*holomorphic form (as it is the case for the constant function $1 \in M_0^!(\Gamma)$). This behavior is governed by the (non)vanishing of the constant coefficient of f.

Remark 3.10. Theorem 3.6 has inspired several papers of K. Ono and his collaborators, see [**BO05, BO, BOR05**]. In Section 5, we generalize some aspects of [**BOR05**].

REMARK 3.11. As this point we are not aware of any particular application of the above formula in the case when f is a weak Maass form and not weakly holomorphic. However, it is important to see that the result does not (directly) depend on the underlying complex structure of D. This suggests possible generalizations to locally symmetric spaces for other orthogonal groups when they might or might not be an underlying complex structure, most notably for hyperbolic space associated to signature $(1, q)$, see [**FI**]. The issue is to find appropriate analogues of the space of weak Maass forms in these situations.

In any case, the space of weak Maass forms has already displayed its significance, for example in the work of Bruinier [**Bru02**], Bruinier-Funke [**BF04**], and Bringmann-Ono [**BO06**].

3.3. The lift of the weight 0 Eisenstein Series. For $z \in \mathbb{H}$ and $s \in \mathbb{C}$, we let

$$\mathcal{E}_0(z,s) = \frac{1}{2}\zeta^*(2s+1) \sum_{\gamma \in \Gamma_\infty \backslash \mathrm{SL}_2(\mathbb{Z})} (\Im(\gamma z))^{s+\frac{1}{2}}$$

be the Eisenstein series of weight 0 for $\mathrm{SL}_2(\mathbb{Z})$. Here Γ_∞ is the standard stabilizer of the cusp $i\infty$ and $\zeta^*(s) = \pi^{-s/2}\Gamma(\frac{s}{2})\zeta(s)$ is the completed Riemann Zeta function. Recall that with the above normalization, $\mathcal{E}_0(z,s)$ converges for $\Re(s) > 1/2$ and has a meromorphic continuation to $\mathbb{C}$ with a simple pole at $s = 1/2$ with residue $1/2$.

THEOREM 3.12 ([**BF06**], Theorem 7.1). *Let $p = 1$. Then*

$$I(\tau, \mathcal{E}_0(z,s)) = \zeta^*(s + \frac{1}{2})\mathcal{F}(\tau, s).$$

Here we use the normalization of Zagier's Eisenstein series as given in [**Yan04**], *in particular $\mathcal{F}(\tau) = \mathcal{F}(\tau, \frac{1}{2})$.*

We prove this result by switching to a mixed model of the Weil representation and using not more than the definition of the two Eisenstein series involved. In particular, we do not have to compute the Fourier expansion of the Eisenstein series. One can also consider Theorem 3.12 and its proof as a special case of the extension of the Siegel-Weil formula by Kudla and Rallis [**KR94**] to the divergent range. Note however, that our case is actually not covered in [**KR94**], since for simplicity they only consider the integral weight case to avoid dealing with metaplectic coverings.

Taking residues at $s = 1/2$ on both sides of Theorem 3.12 one obtains again

THEOREM 3.13.

$$I(\tau, 1) = \tfrac{1}{2}\mathcal{F}(\tau, \tfrac{1}{2}),$$

as asserted by the Siegel-Weil formula.

From our point of view, one can consider Theorem 3.2/3.13 as some kind of *geometric* Siegel-Weil formula (Kudla): The geometric degrees of the 0-cycles $Z(N)$ in (regular) (co)homology form the Fourier coefficients of the special value of an Eisenstein series. For the analogous (compact) case of a Shimura curve, see [**KRY04**].

3.4. Other inputs.

3.4.1. *Maass cusp forms.* We can also consider $I(\tau, f)$ for $f \in L^2_{cusp}(\Gamma\backslash D)$, the space of cuspidal square integrable functions on $\Gamma\backslash D = M$. In that case, the lift is closely related to another theta lift I_M first introduced by Maass [**Maa59**] and later reconsidered by Duke [**Duk88**] and Katok and Sarnak [**KS93**]. The Maass lift uses a similar theta kernel associated to a quadratic space of signature $(2, 1)$ and maps rapidly decreasing functions on M to forms of weight $1/2$. In fact, in [**Maa59, KS93**] only Maass forms are considered, that is, eigenfunctions of the hyperbolic Laplacian Δ.

To describe the relationship between I and I_M, we need the operator ξ_k which maps forms of weight k to forms of "dual" weight $2 - k$. It is given by

$$\xi_k(f)(\tau) = v^{k-2}\overline{L_k f(\tau)} = R_{-k} v^k \overline{f(\tau)}, \tag{3.4}$$

where L_k and R_{-k} are the usual Maass lowering and raising operators. In [**BF06**], we establish an explicit relationship between the two kernel functions and obtain

THEOREM 3.14 ([**BF06**]). *For $f \in L^2_{cusp}(\Gamma\backslash D)$, we have*

$$\xi_{1/2} I_M(\tau, f) = -\pi I(\tau, f).$$

If f is an eigenfunction of Δ with eigenvalue λ, then we also have

$$\xi_{3/2} I(\tau, f) = -\frac{\lambda}{4\pi} I_M(\tau, f).$$

REMARK 3.15. The theorem shows that the two lifts are essentially equivalent on Maass forms. However, the theta kernel for I_M is moderately increasing. Hence one cannot define the Maass lift on H_0^+, at least not without regularization. On the other hand, since $I(\tau, f)$ is holomorphic for $f \in H_0^+$, we have $\xi_{3/2} I(\tau, f) = 0$ (which would be the case $\lambda = 0$).

REMARK 3.16. Duke [**Duk88**] uses the Maass lift to establish an equidistribution result for the CM points and also certain geodesics in M (which in our context correspond to the negative coefficients). Katok and Sarnak [**KS93**] use the fact that the periods over these geodesics correspond to the values of L-functions at the center of the critical strip to extend the nonnegativity of those values to Maass Hecke eigenforms. It seems that for these applications one could have also used our lift I.

3.4.2. *Petersson metric of (weakly) holomorphic modular forms.* Similarly, one could study the lift for the Petersson metric of a (weakly) holomorphic modular form f of weight k for Γ. For such an f, we define its Petersson metric by $\|f(z)\| = |f(z)y^{k/2}|$. Then by Lemma 2.2 the holomorphic part of the positive Fourier coefficients of $I(\tau, \|f\|)$ is given by the $\mathbf{t}_{\|f\|}(N)$. It would be very interestig to find an application for this modular trace.

It should also be interesting to consider the lift of the Petersson metric for a *meromorphic* modular form f or, in weight 0, of a meromorphic modular function itself. Of course, in these cases, the integral is typcially divergent and needs to be normalized. To find an appropriate normalization would be interesting in its own right.

3.4.3. *Other Weights.* Zagier [**Zag02**] also discusses a few special cases of traces for a (weakly holomorphic) modular form f of negative weight $-2k$ (for small k) by considering the modular trace of $R_{-2} \circ R_{-4} \circ \cdots \circ R_{-2k} f$, where R_ℓ denotes the raising operator for weight ℓ. For k even, Zagier obtains a correspondence in which forms of weight $-2k$ correspond to forms of positive weight $3/2+k$. Zagier's student Fricke [**Fri**] following our work [**BF06**] introduces theta kernels similar to ours to realize Zagier's correspondence via theta liftings. It would be interesting to see whether his approach can be understood in terms of the extension of the Kudla-Millson theory to cycles with coefficients by Funke and Millson [**FM**]. For k odd, Zagier's correspondence takes a different form, namely forms of weight $-2k$ correspond to forms of negative weight $1/2-k$. For this correspondence, one needs to use a different approach, constructing other theta kernels.

4. The lift of $\log \|f\|$

In this section, we study the lift for the logarithm of the Petersson metric of a meromorphic modular form f of weight k for Γ. We normalize the Petersson metric such that it is given by

$$\|f(z)\| = e^{-kC/2} |f(z)(4\pi y)^{k/2}|,$$

with $C = \frac{1}{2}(\gamma + \log 4\pi)$. Here γ is Euler's constant.

The motivation to consider such input comes from the fact that the positive Fourier coefficients of the lift will involve the trace $\mathbf{t}_{\log \|f\|}(N)$. It is well known that such a trace plays a significant role in arithmetic geometry as we will also see below.

4.1. The lift of $\log\|\Delta\|$. We first consider the discriminant function

$$\Delta(z) = e^{2\pi i z} \prod_{n=1}^{\infty} \left(1 - e^{2\pi i n z}\right)^{24}.$$

Via the Kronecker limit formula

$$-\frac{1}{12} \log |\Delta(z) y^6| = \lim_{s \to \frac{1}{2}} \left(\mathcal{E}_0(z,s) - \zeta^*(2s-1) \right) \tag{4.1}$$

we can use Theorem 3.12 to compute the lift $I(\tau, \|\Delta\|)$. Namely, we take the constant term of the Laurent expansion at $s = 1/2$ on both sides of Theorem 3.12 and obtain

THEOREM 4.1. *We have*

$$-\frac{1}{12} I\left(\tau, \log \|\Delta(z)\|\right) = \mathcal{F}'(\tau, \frac{1}{2}).$$

On the other hand, we can give an interpretation in arithmetic geometry in the context of the program of Kudla, Rapoport and Yang, see e.g. [**KRY06**]. We give a very brief sketch. For more details, see [**Yan04, KRY04, BF06**]. We let $\mathcal{M}$ be the Deligne-Rapoport compactification of the moduli stack over $\mathbb{Z}$ of elliptic curves, so $\mathcal{M}(\mathbb{C})$ is the orbifold $SL_2(\mathbb{Z})\backslash\mathbb{H} \cup \infty$. We let $\widehat{CH}^1_{\mathbb{R}}(\mathcal{M})$ be the extended arithmetic Chow group of $\mathcal{M}$ with real coefficients and let $\langle\, , \rangle$ be the extended Gillet-Soulé intersection pairing, see [**Sou92, Bos99, BKK, Küh01**]. The normalized metrized Hodge bundle $\widehat{\omega}$ on $\mathcal{M}$ defines an element

$$\widehat{c}_1(\widehat{\omega}) = \tfrac{1}{12}(\infty, -\log \|\Delta(z)\|^2) \in \widehat{CH}^1_{\mathbb{R}}(\mathcal{M}). \tag{4.2}$$

For $N \in \mathbb{Z}$ and $v > 0$, Kudla, Rapoport and Yang construct elements $\widehat{\mathcal{Z}}(N,v) = (\mathcal{Z}(N), \Xi(N,v)) \in \widehat{CH}^1_{\mathbb{R}}(\mathcal{M})$. Here for $N > 0$ the complex points of $\mathcal{Z}(N)$ are the CM points $Z(N)$ and $\xi(N,v) = \sum_{X \in L_N} \xi^0(\sqrt{v}X)$ is a Green's function for $Z(N)$. In [**BF06**] we indicate

THEOREM 4.2 ([**BF06**]).

$$-\frac{1}{12} I\left(\tau, \log\left(\|\Delta(z)\|\right)\right) = 4 \sum_{N \in \mathbb{Z}} \langle \widehat{\mathcal{Z}}(N,v), \widehat{\omega} \rangle q^N.$$

We therefore recover

THEOREM 4.3 ((Kudla-Rapoport-Yang) [**Yan04**]). *For the generating series of the arithmetic degrees $\langle \widehat{\mathcal{Z}}(N,v), \widehat{\omega} \rangle$, we have*

$$\sum_{N \in \mathbb{Z}} \langle \widehat{\mathcal{Z}}(N,v), \widehat{\omega} \rangle q^N = \frac{1}{4} \mathcal{F}'(\tau, \frac{1}{2}).$$

REMARK 4.4. One can view our treatment of the above result as some kind of arithmetic Siegel-Weil formula in the given situation, realizing the "arithmetic theta series" (Kudla) of the arithmetic degrees of the cycles $\mathcal{Z}(N)$ on the left hand side of Theorem 4.3 as an honest theta integral (and as the derivative of an Eisenstein series).

Our proof is different than the one given in [**Yan04**]. We use two different ways of 'interpreting' the theta lift, the Kronecker limit formula, and unwind the basic definitions and formulas of the Gillet-Soulé intersection pairing. The proof given in [**Yan04**] is based on the explicit computation of both sides, which is not needed with our method. The approach and techniques in [**Yan04**] are the same as the ones Kudla, Rapoport, and Yang [**KRY04**] employ in the analogous situation for 0-cycles in Shimura curves. In that case again, the generating series of the arithmetic degrees of the analogous cycles is the *derivative* of a certain Eisenstein series.

It needs to be stressed that the present case is considerably easier than the Shimura curve case. For example, in our situation the finite primes play no role, since the CM points do not intersect the cusp over $\mathbb{Z}$. Moreover, our approach is not applicable in the Shimura curve case, since there are no Eisenstein series (and no Kronecker limit formula). See also Remark 4.10 below.

Finally note that by Lemma 2.2 we see that the main (holomorphic) part of the positive Fourier coefficients of the lift is given by $\mathbf{t}_{\log \|\Delta(z) y^6\|}(N)$, which is equal to the Faltings height of the cycle $\mathcal{Z}(N)$. For details, we refer again the reader to [**Yan04**].

4.2. The lift for general f. In this section, we consider $I(\tau, \log \|f\|)$ for a general meromorphic modular form f. Note that while $\log \|f\|$ is of course integrable, we cannot evaluate $\log \|f\|$ at the divisor of f. So if the divisor of f is not disjoint from (one) of the 0-cycles $Z(N)$, we need to expect complications when computing the Fourier expansion of $I(\tau, \log \|f\|)$.

We let t be the order of f at the point $D_X = z_0$, i.e., t is the smallest integer such that

$$\lim_{z \to z_0} (z - z_0)^{-t} f(z) =: f^{(t)}(z_0) \notin \{0, \infty\}.$$

Note that the value $f^{(t)}(z_0)$ does depend on z_0 itself and not just on the Γ-equivalence class of z_0. If f has order t at z_0 we put

$$||f^{(t)}(z_0)|| = e^{-C(t+k/2)}|f^{(t)}(z_0)(4\pi y_0)^{t+k/2}|$$

LEMMA 4.5. *The value $||f^{(t)}(z_0)||$ depends only on the Γ-equivalence class of z_0, i.e.,*

$$||f^{(t)}(\gamma z_0)|| = ||f^{(t)}(z_0)||$$

for $\gamma \in \Gamma$.

PROOF. It's enough to do the case $t \geq 0$. For $t < 0$, consider $1/f$. We successively apply the raising operator $R_\ell = 2i\frac{\partial}{\partial \tau} + \ell y^{-1}$ to f and obtain

$$\left(-\frac{1}{2}i\right)^t R_{k+t-2} \circ \cdots \circ R_k f(z) = f^{(t)}(z) + \text{lower derivatives of } f. \tag{4.3}$$

But $|R_{k+t-2} \cdots R_k e^{-C(t+k/2)} f(z)(4\pi)y^{t+k/2}|$ has weight 0 and its value at z_0 is equal to $||f^{(t)}(z_0)||$ since the lower derivatives of f vanish at z_0. □

THEOREM 4.6. *Let f be a meromorphic modular form of weight k. Then for $N > 0$, the N-th Fourier coefficient of $I(\tau, \log \|f\|)$ is given by*

$$a_N(v) = \sum_{z \in Z(N)} \tfrac{1}{|\Gamma_z|} \left(\log ||f^{(ord(f,z))}(z)|| - \tfrac{ord(f,z)}{2} \log((4\pi)^2 N v) + \tfrac{k}{16\pi i} J(4\pi N v) \right),$$

where

$$J(t) = \int_0^\infty e^{-tw}[(w+1)^{\frac{1}{2}} - 1]w^{-1} dw.$$

We give the proof of Theorem 4.6 in the next section.

REMARK 4.7. We will leave the computation of the other Fourier coefficients for another time. Note however, that the coefficient for $N < 0$ such that $N \notin -(\mathbb{Q})^2$ can be found in [**KRY04**], section 12.

REMARK 4.8. The constant coefficient a_0' of the lift is given by

$$\int_M^{reg} \log ||f(z)|| \frac{dx\, dy}{y^2}, \tag{4.4}$$

see Lemma 2.4. An explicit formula can be obtained by means of Rohrlich's modular Jensen's formula [**Roh84**], which holds for f holomorphic on D and not vanishing at the cusp. For an extension of this formula in the context of arithmetic intersection numbers, see e.g. Kühn [**Küh01**]. See also Remark 4.10 below.

EXAMPLE 4.9. In the case of the classical j-invariant the modular trace of the logarithm of the j-invariant is the logarithm of the *norm* of the singular moduli, i.e.,

$$\mathbf{t}_{\log|j|}(N) = \log|\prod_{z \in Z(N)} j(z)|. \tag{4.5}$$

Recall that the norms of the singular moduli were studied by Gross-Zagier [**GZ85**]. On the other hand, we have $j(\rho) = 0$ for $\rho = \frac{1+i\sqrt{3}}{2}$ and $\frac{1}{3}\rho \in Z(3N^2)$. Hence for these indices the trace is not defined. Note that the third derivative $j'''(\rho)$ is the first non-vanishing derivative of j at ρ. Thus

(4.6)
$$I(\tau, \log|j|) = \sum_{D>0} \mathbf{t'}_{\log|j|}(D) q^D + \sum_{N=1}^{\infty} \Big(\log \|j^{(3)}(\rho)\| - \tfrac{1}{2}\log(48\pi^2 N^2 v) \Big) q^{3N^2} + \dots$$

Here $\mathbf{t'}_{\log|j|}(D)$ denotes the usual trace for $D \neq 3N^2$, while for $D = 3N^2$ one excludes the term corresponding to ρ.

Finally note that Gross-Zagier [**GZ85**] in their analytic approach to the singular moduli (sections 5-7) also make essential use of the *derivative* of an Eisenstein series (of weight 1 for the Hilbert modular group).

Remark 4.10. It is a very interesting problem to consider the special case when f is a Borcherds product, that is, when

$$\log ||f(z)|| = \Phi(z, g), \tag{4.7}$$

where $\Phi(z, g)$ is a theta lift of a (weakly) holomorphic modular form of weight 1/2 via a certain regularized theta integral, see [**Bor98, Bru02**]. The calculation of the constant coefficient a'_0 of the lift $I(\tau, \Phi(z, g))$ boils down (for general signature $(n, 2)$) to work of Kudla [**Kud03**] and Bruinier and Kühn [**BK03**] on integrals of Borcherds forms. (The present case of a modular curve is excluded to avoid some technical difficulties). Roughly speaking, one obtains a linear combination of Fourier coefficients of the *derivative* of a certain Eisenstein series.

From that perspective, it is reasonable to expect that for the Petersson metric of Borcherds products, the full lift $I(\tau, \Phi(z, g))$ will involve the derivative of certain Eisenstein series, in particular in view of Kudla's approach in [**Kud03**] via the Siegel-Weil formula. Note that the discriminant function Δ can be realized as a Borcherds product. Therefore, one can reasonably expect a new proof for Theorem 4.1. Furthermore, this method a priori is also available for the Shimura curve case (as opposed to the Kronecker limit formula), and one can hope to have a new approach to some aspects (say, at least for the Archimedean prime) of the work of Kudla, Rapoport, and Yang [**KRY04, KRY06**] on arithmetic generating series in the Shimura curve case.

We will come back to these issues in the near future.

4.3. Proof of Theorem 4.6. For the proof of the theorem, we will show how Theorem 2.1 extends to functions which have a logarithmic singularity at the CM point D_X. This will then give the formula for the positive coefficients.

Proposition 4.11. *Let $q(X) = N > 0$ and let f be a meromorphic modular form of weight k with order t at $D_X = z_0$. Then*

$$\begin{aligned}\int_D \log||f(z)||\varphi^0(X, z) &= ||f^{(t)}(z_0)|| - \frac{t}{2}\log((4\pi)^2 N) + \int_D dd^c \log||f(z)|| \cdot \xi^0(X, z) \\ &= ||f^{(t)}(z_0)|| - \frac{t}{2}\log((4\pi)^2 N) + \frac{k}{16\pi i}\int_D \xi^0(X, z)\frac{dxdy}{y^2}.\end{aligned}$$

Note that by [**KRY04**], section 12 we have

$$\int_D \xi^0(X, z)\frac{dxdy}{y^2} = J(4\pi N).$$

Proof of Proposition 4.11. The proof consists of a careful analysis and extension of the proof of Theorem 2.1 given in [**Kud97**]. We will need

Lemma 4.12. *Let*

$$\tilde{\xi}^0(X,z) = \xi^0(X,z) + \log|z - z_0|^2.$$

Then $\tilde{\xi}^0(X,z)$ *extends to a smooth function on* D *and*

$$\tilde{\xi}^0(X,z_0) = -\gamma - \log(4\pi N/y_0^2).$$

In particular, writing $z - z_0 = re^{i\theta}$, *we have*

$$\frac{\partial}{\partial r}\tilde{\xi}^0(X,z) = O(1)$$

in a neighborhood of z_0.

Proof of Lemma 4.12. This is basically Lemma 11.2 in [**Kud97**]. We have

$$R(X,z) = 2N\left[\frac{r^2}{2y_0(y_0 + r\cos\theta)}\right]\left[\frac{r^2}{2y_0(y_0 + r\cos\theta)} + 2\right]. \tag{4.8}$$

Since

$$Ei(z) = \gamma + \log(-z) + \int_0^z \frac{e^t - 1}{t}dt,$$

we have

$$\tilde{\xi}^0(X,z) = -\gamma - \log\left(\left[\frac{4\pi N}{2y_0(y_0 + r\cos\theta)}\right]\left[\frac{r^2}{2y_0(y_0 + r\cos\theta)} + 2\right]\right) - \int_0^{-2\pi R(X,z)} \frac{e^t - 1}{t}dt. \tag{4.9}$$

The claims follow. □

For the proof of the proposition, we first note that (2.17) in Theorem 2.1 still holds for $F = \log\|f\|$ when the divisor of f is disjoint to D_X. We now consider $\int_D dd^c \log||f(z)|| \cdot \xi^0(X,z)$. Since $\log||(z-z_0)^{-t}f(z)||$ is smooth at $z = z_0$, we see

$$\begin{aligned}\int_D dd^c \log||f(z)|| \cdot \xi^0(X,z) &= \int_D dd^c \log||(z-z_0)^{-t}f(z)|| \cdot \xi^0(X,z)\\ &= -\log||f^{(t)}(z_0)|| - tC + t\log(4\pi y_0)\\ &\quad + \int_D \log||(z-z_0)^{-t}f(z)|| \cdot \varphi^0(X,z).\end{aligned} \tag{4.10}$$

So for the proposition it suffices to proof

$$\int_D \log|z - z_0|^{-t} \cdot \varphi^0(X,z) = \frac{t}{2}\left(\gamma + \log(4\pi N/y_0^2)\right). \tag{4.11}$$

For this, we let U_ε be an ε-neighborhood of z_0. We see

(4.12)

$$\begin{aligned}\int_{D-U_\varepsilon} dd^c \log|z-z_0|^t \cdot \xi^0(X,z) &= \int_{D-U_\varepsilon} \log|z-z_0|^t \cdot dd^c\xi^0(X,z)\\ &\quad + \int_{\partial\{D-U_\varepsilon\}} \left(\xi^0 d^c \log|z-z_0|^t - \log|z-z_0|^t d^c\xi^0\right).\end{aligned}$$

Of course $dd^c \log|z-z_0|^t = 0$ (outside z_0), so the integral on the left hand side vanishes. For the first term on the right hand side, we note $dd^c\xi^0 = \varphi^0$, and using the rapid decay of $\xi^0(X)$, we obtain

$$\int_D \log|z-z_0|^t \varphi^0(X,z) = \lim_{\varepsilon\to 0}\int_{\partial U_\varepsilon} \left(\xi^0 d^c \log|z-z_0|^t - \log|z-z_0|^t d^c\xi^0\right). \tag{4.13}$$

For the right hand side of 4.13, we write $z-z_0 = re^{i\theta}$. Using $d^c = \frac{r}{4\pi}\frac{\partial}{\partial r}d\theta - \frac{1}{4\pi r}\frac{\partial}{\partial\theta}dr$, we see $d^c\log|z-z_0| = \frac{1}{4\pi}d\theta$. Via Lemma 4.12, we now obtain

$$\begin{aligned}
&\int_{\partial U_\varepsilon} \left(\xi^0 d^c \log|z-z_0|^t - \log|z-z_0|^t d^c\xi^0\right) \\
&= \int_0^{2\pi} \left[(-\log\varepsilon^2 + \tilde{\xi}^0)\frac{t}{4\pi}d\theta - t\log\varepsilon(-\frac{1}{2\pi}d\theta + O(\varepsilon)d\theta)\right] \\
&= \int_0^{2\pi} \left[\tilde{\xi}^0\frac{t}{4\pi}d\theta - t\log\varepsilon O(\varepsilon)d\theta\right] \\
&\to \frac{t}{2}\tilde{\xi}^0(X,z_0) = -\frac{t}{2}\left(\gamma + \log(4N\pi/y_0^2)\right) \qquad \text{as } \varepsilon\to 0.
\end{aligned}$$

The proposition follows. □

5. Higher dimensional analogues

We change the setting from the previous sections and let V now be a rational quadratic space of signature $(n,2)$. We let $G = \mathrm{SO}_0(V(\mathbb{R}))$ be the connected component of the identity of $\mathrm{O}(V(\mathbb{R}))$. We let D be the associated symmetric space, which we realize as the space of negative two-planes in $V(\mathbb{R})$:

$$D = \{z \subset V(\mathbb{R});\ \dim z = 2 \text{ and } (\ ,\ )|_z < 0\}. \tag{5.1}$$

We let L be an even lattice in V and Γ a congruence subgroup inside G stabilizing L. We assume for simplicity that Γ is neat and that Γ acts on the discriminant group $L^\#/L$ trivially. We set $M = \Gamma\backslash D$. It is well known that D has a complex structure and M is a (in general) quasi-projective variety.

A vector $x \in V$ such that $(x,x) > 0$ defines a divisor D_x by

$$D_x = \{z \in D;\ z \perp x\}. \tag{5.2}$$

The stabilizer Γ_x acts on D_x, and we define the special divisor $Z(x) = \Gamma_x\backslash D_x \hookrightarrow M$. For $N \in \mathbb{Z}$, we set $L_N = \{x \in L;\ q(x) := \frac{1}{2}(x,x) = N\}$ and for $N > 0$, we define the composite cycle $Z(N)$ by

$$Z(N) = \sum_{x\in\Gamma\backslash L_N} Z(x). \tag{5.3}$$

For $n = 1$, these are the CM points inside a modular (or Shimura) curve discussed before, while for $n = 2$, these are (for $\mathbb{Q}$-rank 1) the famous Hirzebruch-Zagier divisors inside a Hilbert modular surface, see [**HZ76**] or [**vdG88**]. On the other hand, we let $U \subset V$ be a rational positive definite subspace of dimension $n-1$. We then set

$$D_U = \{z \in D;\ z \perp U\}. \tag{5.4}$$

This is an embedded upper half plane $\mathbb{H}$ inside D. We let Γ_U be the stabilizer of U inside Γ and set $Z(U) = \Gamma_U \backslash D_U$ which defines a modular or Shimura curve. We denote by ι_U the embedding of $Z(U)$ into M (which we frequently omit). Therefore

$$D_U \cap D_x = \begin{cases} D_{U,x} & \text{if } x \notin U \\ D_U & \text{if } x \in U. \end{cases} \tag{5.5}$$

Here $D_{U,x}$ is the point (negative two plane in $V(\mathbb{R})$) in D, which is orthogonal to both U and x. We denote its image in M by $Z(U,x)$. Consequently $Z(U)$ and $Z(x)$ intersect transversally in $Z(U,x)$ if and only if $\gamma x \notin U$ for all $\gamma \in \Gamma$ while $Z(U) = Z(x)$ if and only if $\gamma x \in U$ for one $\gamma \in \Gamma$. This defines a (set theoretic) intersection

$$(Z(U) \cap Z(N))_M \tag{5.6}$$

in (the interior of) M consisting of 0- and 1-dimensional components. For $n = 2$, the Hilbert modular surface case, this follows Hirzebruch and Zagier ([**HZ76**]). For f a function on the curve $Z(U)$, we let $(Z(U) \cap Z(N))_M [f]$ be the evaluation of f on $(Z(U) \cap Z(N))_M$. Here on the 1-dimensional components we mean by this the (regularized) average value of f over the curve, see (2.19). Now write

$$L = \sum_{i=1}^{r} (L_U + \lambda_i) \ \perp \ (L_{U^\perp} + \mu_i) \tag{5.7}$$

with $\lambda_i \in L_U^\#$ and $\mu_i \in L_{U^\perp}^\#$ such that $\lambda_1 = \mu_1 = 0$.

Lemma 5.1. *Let $r(N_1, L_U + \lambda_i) = \#\{x \in L_U + \lambda_i : q(x) = N_1\}$ be the representation number of the positive definite (coset of the) lattice L_U, and let $Z(N_2, L_{U^\perp} + \mu_i) = \sum_{\substack{x \in \Gamma_U \backslash (L_{U^\perp} + \mu_i) \\ q(x) = N_2}} Z(x)$ be the CM cycle inside the curve $Z(U)$. Let f be a function on the curve $Z(U)$. Then*

$$\begin{aligned}(Z(U) \cap Z(N))_M [f] = & \sum_{\substack{N_1 \geq 0, N_2 > 0 \\ N_1 + N_2 = N}} \sum_{i=1}^{r} r(N_1, L_U + \lambda_i) Z(N_2, L_{U^\perp} + \mu_i)[f] \\ & - \frac{1}{2\pi} r(N, L_U) \int_{Z(U)}^{reg} f(z)\omega.\end{aligned}$$

Proof. A vector $x \in L_U \cap L_N$ gives rise to a 1-dimensional intersection, and conversely a 1-dimensional intersection arises from a vector $x \in L_N$ which can be taken after translating by a suitable $\gamma \in \Gamma$ to be in L_U. Thus the 1-dimensional component is equal to $Z(U)$ occurring with multiplicity $r(N, L_U)$. Note that only the component $\lambda_1 = \mu_1 = 0$ occurs. This gives the second term. For the 0-dimensional components, we first take an $x = x_1 + x_2 \in L_N$ with $x_1 \in L_U + \lambda_i$ and $x_2 \in L_{U^\perp} + \mu_i$ such that $q(x_1) = N_1$ and $q(x_2) = N_2$. This gives rise to the transversal intersection point $Z(U,x)$ if x cannot be Γ-translated into U. Note that this point lies in the CM cycle $Z(N_2, L_{U^\perp} + \mu_i)$ inside $Z(U)$. In fact, in this way, we see by changing x_2 by $y_2 \in L_{U^\perp} + \mu_i$ of the same length N_2 that the whole cycle $Z(N_2, L_{U^\perp} + \mu_i)$ lies in the transversal part of $Z(U) \cap Z(N)$. (Here we need that Γ_U acts trivially on the cosets). Moreover, its multiplicity is the representation number $r(N_1, L_U + \lambda_i)$. (Here we need that Γ_U acts trivially on U since Γ is neat). This gives the first term. ∎

We now let $\varphi_V \in [\mathcal{S}(V(\mathbb{R})) \otimes \Omega^{1,1}(D)]^G$ be the Kudla-Millson Schwartz form for V. Then the associated theta function $\theta(\tau, \varphi_V)$ for the lattice L is a modular form of weight $(n+2)/2$ with values in the differential forms of Hodge type $(1,1)$ of M. Moreover, for $N > 0$, the N-th Fourier coefficient is a Poincaré dual form for the special divisor $Z(N)$. It is therefore natural to consider the integral

$$I_V(\tau, Z(U), f) := \int_{Z(U)} f(z)\theta_V(\tau, z, L) \tag{5.8}$$

and to expect that this involves the evaluation of f at $(Z(N) \cap Z(U))_M$. (Note however that the intersection of the two relative cycles $Z(U)$ and $Z(N)$ is not cohomological).

PROPOSITION 5.2. *We have*

$$I_V(\tau, Z(U), f) = \sum_{i=1}^{r} \vartheta(\tau, L_U + \lambda_i) I_{U^\perp}(\tau, L_{U^\perp} + \mu_i, f).$$

Here $\vartheta(\tau, L_U + \lambda_i) = \sum_{x \in L_U + \lambda_i} e^{2\pi i q(x)\tau}$ *is the standard theta function of the positive definite lattice* L_U*, and* $I_{U^\perp}(\tau, L_{U^\perp} + \mu_i, f)$ *is the lift of* f *considered in the main body of the paper for the space* $U^\perp$ *of signature* $(1,2)$ *(and the coset* μ_i *of the lattice* $L_{U^\perp}$*).*

PROOF. Under the pullback $i_U^* : \Omega^{1,1}(D) \longrightarrow \Omega^{1,1}(D_U)$, we have, see [**KM86**], $i_U^* \varphi_V = \varphi_U^+ \otimes \varphi_{U^\perp}$, where φ_U^+ is the usual (positive definite) Gaussian on U. Then

(5.9)

$$\theta_{\varphi_V}(\tau, z, L) = \sum_{x \in L} \varphi_V(X, \tau, z) = \sum_{i=1}^{r} \sum_{x \in L_U + \lambda_i} \varphi_U^+(x, \tau) \sum_{y \in L_{U^\perp} + \mu_i} \varphi_{U^\perp}(y, \tau, z),$$

which implies the assertion. □

Making the Fourier expansion $I_V(\tau, Z(U), f)$ explicit, and using Lemma 5.1 and Theorem 3.6 (in its form for cosets of a general lattice, [**BF06**]), we obtain

THEOREM 5.3. *Let* $f \in M_0^!(Z(U))$ *be a modular function on* $Z(U)$ *such that the constant Fourier coefficient of* f *at all the cusps of* $Z(U)$ *vanishes. Then* $\theta_{\varphi_V}(\tau, L)$ *is a weakly holomorphic modular form of weight* $(n+2)/2$ *whose Fourier expansion involves the generating series*

$$\sum_{N>0} \left((Z(U) \cap Z(N))_M \, [f] \right) q^N$$

of the evaluation of f *along* $(Z(U) \cap Z(N))_M$.

REMARK 5.4. This generalizes a result of Bringmann, Ono, and Rouse (Theorem 1.1 of [**BOR05**]), where they consider some special cases of Theorem 5.3 for $n = 2$ in the case of Hilbert modular surfaces, where the cycles $Z(N)$ and $Z(U)$ are the famous Hirzebruch-Zagier curves [**HZ76**]. Note that [**BOR05**] uses our Theorem 3.6 as a starting point.

References

[BF04] J. H. Bruinier & J. Funke – "On two geometric theta lifts", *Duke Math. J.* **125** (2004), no. 1, p. 45–90.

[BF06] ———, "CM traces of modular functions", *J. Reine Angew. Math.* **594** (2006), p. 1–33.

[BK03] J. H. Bruinier & U. Kühn – "Integrals of automorphic Green's functions associated to Heegner divisors", *Int. Math. Res. Not.* (2003), no. 31, p. 1687–1729.

[BKK] J. Burgos, J. Kramer & U. Kühn – "Cohomological Arithmetic Chow groups", to appear in J. Inst. Math. Jussieu.

[BO] K. Bringmann & K. Ono – "Arithmetic properties of coefficients of half-integral weight Maass-Poincare series", preprint.

[BO05] ———, "Identities for traces of singular moduli", *Acta Arith.* **119** (2005), no. 4, p. 317–327.

[BO06] ———, "The $f(q)$ mock theta function conjecture and partition ranks", *Inventiones Math.* **165** (2006), p. 243–266.

[Bor98] R. E. Borcherds – "Automorphic forms with singularities on Grassmannians", *Invent. Math.* **132** (1998), no. 3, p. 491–562.

[BOR05] K. Bringmann, K. Ono & J. Rouse – "Traces of singular moduli on Hilbert modular surfaces", *Int. Math. Res. Not.* (2005), no. 47, p. 2891–2912.

[Bos99] J.-B. Bost – "Potential theory and Lefschetz theorems for arithmetic surfaces", *Ann. Sci. École Norm. Sup. (4)* **32** (1999), no. 2, p. 241–312.

[Bru02] J. H. Bruinier – *Borcherds products on O(2, l) and Chern classes of Heegner divisors*, Lecture Notes in Mathematics, vol. 1780, Springer-Verlag, Berlin, 2002.

[Bru06] ———, "Traces of CM-values of modular functions and related topics", in *Proceedings of the Conference on "Automorphic Forms and Automorphic L-Functions"*, vol. 1468, RIMS Kokyuroku, Kyoto, 2006.

[Duk88] W. Duke – "Hyperbolic distribution problems and half-integral weight Maass forms", *Invent. Math.* **92** (1988), no. 1, p. 73–90.

[FI] J. Funke & O. Imamoglu – in preparation.

[FM] J. Funke & J. Millson – "Cycles with local coefficients for orthogonal groups and vector-valued Siegel modular forms", to appear in American J. Math., (2006).

[FM02] ———, "Cycles in hyperbolic manifolds of non-compact type and Fourier coefficients of Siegel modular forms", *Manuscripta Math.* **107** (2002), no. 4, p. 409–444.

[Fri] K.-H. Fricke – "Gleichverteilung gesclossener Geodätischer im Fundamentalbereich der Modulgruppe", Ph.D. Thesis (in preparation), Bonn.

[Fun02] J. Funke – "Heegner divisors and nonholomorphic modular forms", *Compositio Math.* **133** (2002), no. 3, p. 289–321.

[GZ85] B. H. Gross & D. B. Zagier – "On singular moduli", *J. Reine Angew. Math.* **355** (1985), p. 191–220.

[HZ76] F. Hirzebruch & D. Zagier – "Intersection numbers of curves on Hilbert modular surfaces and modular forms of Nebentypus", *Invent. Math.* **36** (1976), p. 57–113.

[Kim] C. H. Kim – "Traces of singular moduli and Borcherds products", preprint.

[Kim04] ———, "Borcherds products associated with certain Thompson series", *Compos. Math.* **140** (2004), no. 3, p. 541–551.

[KM86] S. S. Kudla & J. J. Millson – "The theta correspondence and harmonic forms. I", *Math. Ann.* **274** (1986), no. 3, p. 353–378.

[KM90] ———, "Intersection numbers of cycles on locally symmetric spaces and Fourier coefficients of holomorphic modular forms in several complex variables", *Inst. Hautes Études Sci. Publ. Math.* (1990), no. 71, p. 121–172.

[KR94] S. S. Kudla & S. Rallis – "A regularized Siegel-Weil formula: the first term identity", *Ann. of Math. (2)* **140** (1994), no. 1, p. 1–80.

[KRY04] S. S. Kudla, M. Rapoport & T. Yang – "Derivatives of Eisenstein series and Faltings heights", *Compos. Math.* **140** (2004), no. 4, p. 887–951.

[KRY06] ———, *Modular forms and special cycles on Shimura curves*, Annals of Mathematics Studies, vol. 161, Princeton University Press, Princeton, NJ, 2006.

[KS93] S. Katok & P. Sarnak – "Heegner points, cycles and Maass forms", *Israel J. Math.* **84** (1993), no. 1-2, p. 193–227.

[Kud97] S. S. KUDLA – "Central derivatives of Eisenstein series and height pairings", *Ann. of Math. (2)* **146** (1997), no. 3, p. 545–646.
[Kud03] ———, "Integrals of Borcherds forms", *Compositio Math.* **137** (2003), no. 3, p. 293–349.
[Küh01] U. KÜHN – "Generalized arithmetic intersection numbers", *J. Reine Angew. Math.* **534** (2001), p. 209–236.
[Maa59] H. MAASS – "Über die räumliche Verteilung der Punkte in Gittern mit indefiniter Metrik", *Math. Ann.* **138** (1959), p. 287–315.
[Roh84] D. E. ROHRLICH – "A modular version of Jensen's formula", *Math. Proc. Cambridge Philos. Soc.* **95** (1984), no. 1, p. 15–20.
[Shi75] T. SHINTANI – "On the construction of holomorphic cusp forms of half integral weight", *Nagoya Math. J.* **58** (1975), p. 83–126.
[Sou92] C. SOULÉ – *Lectures on Arakelov geometry*, Cambridge Studies in Advanced Mathematics, vol. 33, Cambridge University Press, Cambridge, 1992, With the collaboration of D. Abramovich, J.-F. Burnol and J. Kramer.
[Ste84] I. A. STEGUN (ed.) – *Pocketbook of mathematical functions*, Verlag Harri Deutsch, Thun, 1984, Abridged edition of *Handbook of mathematical functions* edited by Milton Abramowitz and Irene A. Stegun, Material selected by Michael Danos and Johann Rafelski.
[vdG88] G. VAN DER GEER – *Hilbert modular surfaces*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), vol. 16, Springer-Verlag, Berlin, 1988.
[Yan04] T. YANG – "Faltings heights and the derivative of Zagier's Eisenstein series", in *Heegner points and Rankin L-series*, Math. Sci. Res. Inst. Publ., vol. 49, Cambridge Univ. Press, Cambridge, 2004, p. 271–284.
[Zag75] D. ZAGIER – "Nombres de classes et formes modulaires de poids 3/2", *C. R. Acad. Sci. Paris Sér. A-B* **281** (1975), no. 21, p. Ai, A883–A886.
[Zag81] ———, "The Rankin-Selberg method for automorphic functions which are not of rapid decay", *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* **28** (1981), no. 3, p. 415–437 (1982).
[Zag02] ———, "Traces of singular moduli", in *Motives, polylogarithms and Hodge theory, Part I (Irvine, CA, 1998)*, Int. Press Lect. Ser., vol. 3, Int. Press, Somerville, MA, 2002, p. 211–244.

DEPARTMENT OF MATHEMATICAL SCIENCES, NEW MEXICO STATE UNIVERSITY, P.O. BOX 30001, 3MB, LAS CRUCES, NM 88003, USA
E-mail address: jfunke@nmsu.edu

Clay Mathematics Proceedings
Volume 7, 2007

The path to recent progress on small gaps between primes

D. A. Goldston, J. Pintz, and C. Y. Yıldırım

Abstract. We present the development of ideas which led to our recent findings about the existence of small gaps between primes.

1. Introduction

In the articles *Primes in Tuples I & II* ([**GPYa**], [**GPYb**]) we have presented the proofs of some assertions about the existence of small gaps between prime numbers which go beyond the hitherto established results. Our method depends on tuple approximations. However, the approximations and the way of applying the approximations has changed over time, and some comments in this paper may provide insight as to the development of our work.

First, here is a short narration of our results. Let

$$\theta(n) := \begin{cases} \log n & \text{if } n \text{ is prime,} \\ 0 & \text{otherwise,} \end{cases} \tag{1}$$

and

$$\Theta(N;q,a) := \sum_{\substack{n\le N \\ n\equiv a \ (\bmod\ q)}} \theta(n). \tag{2}$$

In this paper N will always be a large integer, p will denote a prime number, and p_n will denote the n-th prime. The prime number theorem says that

$$\lim_{x\to\infty} \frac{|\{p:\ p\le x\}|}{\frac{x}{\log x}} = 1, \tag{3}$$

and this can also be expressed as

$$\sum_{n\le x} \theta(n) \sim x \qquad \text{as } x\to\infty. \tag{4}$$

2000 *Mathematics Subject Classification.* Primary 11N05.

The first author was supported by NSF grant DMS-0300563, the NSF Focused Research Group grant 0244660, and the American Institute of Mathematics; the second author by OTKA grants No. T38396, T43623, T49693 and the Balaton program; the third author by TÜBİTAK .

It follows trivially from the prime number theorem that

$$\liminf_{n\to\infty} \frac{p_{n+1}-p_n}{\log p_n} \le 1. \tag{5}$$

By combining former methods with a construction of certain (rather sparsely distributed) intervals which contain more primes than the expected number by a factor of e^γ, Maier [**Mai88**] had reached the best known result in this direction that

$$\liminf_{n\to\infty} \frac{p_{n+1}-p_n}{\log p_n} \le 0.24846\ldots\ . \tag{6}$$

It is natural to expect that modulo q the primes would be almost equally distributed among the reduced residue classes. The deepest knowledge on primes which plays a role in our method concerns a measure of the distribution of primes in reduced residue classes referred to as the level of distribution of primes in arithmetic progressions. We say that the primes have *level of distribution* α if

$$\sum_{q\le Q} \max_{\substack{a \\ (a,q)=1}} \left|\Theta(N;q,a) - \frac{N}{\phi(q)}\right| \ll \frac{N}{(\log N)^A} \tag{7}$$

holds for any $A>0$ and any arbitrarily small fixed $\epsilon>0$ with

$$Q = N^{\alpha-\epsilon}. \tag{8}$$

The *Bombieri-Vinogradov theorem* provides the level $\frac{1}{2}$, while the *Elliott-Halberstam conjecture* asserts that the primes have level of distribution 1.

The Bombieri-Vinogradov theorem allows taking $Q = N^{\frac{1}{2}}(\log N)^{-B(A)}$ in (7), by virtue of which we have proved unconditionally in [**GPYa**] that for any fixed $r \ge 1$,

$$\liminf_{n\to\infty} \frac{p_{n+r}-p_n}{\log p_n} \le (\sqrt{r}-1)^2\ ; \tag{9}$$

in particular,

$$\liminf_{n\to\infty} \frac{p_{n+1}-p_n}{\log p_n} = 0. \tag{10}$$

In fact, assuming that the level of distribution of primes is α, we obtain more generally than (9) that, for $r \ge 2$,

$$\liminf_{n\to\infty} \frac{p_{n+r}-p_n}{\log p_n} \le (\sqrt{r}-\sqrt{2\alpha})^2. \tag{11}$$

Furthermore, assuming that $\alpha > \frac{1}{2}$, there exists an explicitly calculable constant $C(\alpha)$ such that for $k \ge C(\alpha)$ any sequence of k-tuples

$$\{(n+h_1, n+h_2, \ldots, n+h_k)\}_{n=1}^{\infty}, \tag{12}$$

with the set of distinct integers $\mathcal{H} = \{h_1, h_2, \ldots, h_k\}$ *admissible* in the sense that $\prod_{i=1}^{k}(n+h_i)$ has no fixed prime factor for every n, contains at least two primes infinitely often. For instance if $\alpha \ge 0.971$, then this holds for $k \ge 6$, giving

$$\liminf_{n\to\infty}(p_{n+1}-p_n) \le 16, \tag{13}$$

in view of the shortest admissible 6-tuple $(n, n+4, n+6, n+10, n+12, n+16)$.

By incorporating Maier's method into ours in [**GPY06**] we improved (9) to

$$\liminf_{n\to\infty} \frac{p_{n+r} - p_n}{\log p_n} \le e^{-\gamma}(\sqrt{r} - 1)^2, \tag{14}$$

along with an extension for primes in arithmetic progressions where the modulus can tend slowly to infinity as a function of p_n.

In [**GPYb**] the result (10) was considerably improved to

$$\liminf_{n\to\infty} \frac{p_{n+1} - p_n}{(\log p_n)^{\frac{1}{2}}(\log\log p_n)^2} < \infty. \tag{15}$$

In fact, the methods of [**GPYb**] lead to a much more general result: When $\mathcal{A} \subseteq \mathbb{N}$ is a sequence satisfying $\mathcal{A}(N) := |\{n; n \le N, n \in \mathcal{A}\}| > C(\log N)^{1/2}(\log\log N)^2$ for all sufficiently large N, infinitely many of the differences of two elements of $\mathcal{A}$ can be expressed as the difference of two primes.

2. Former approximations by truncated divisor sums

The von Mangoldt function

$$\Lambda(n) := \begin{cases} \log p & \text{if} \quad n = p^m,\ m \in \mathbb{Z}^+, \\ 0 & \text{otherwise,} \end{cases} \tag{16}$$

can be expressed as

$$\Lambda(n) = \sum_{d|n} \mu(d) \log(\frac{R}{d}) \qquad \text{for } n > 1. \tag{17}$$

Since the proper prime powers contribute negligibly, the prime number theorem (4) can be rewritten as

$$\psi(x) := \sum_{n\le x} \Lambda(n) \sim x \qquad \text{as } x \to \infty. \tag{18}$$

It is natural to expect that the truncated sum

$$\Lambda_R(n) := \sum_{\substack{d|n \\ d\le R}} \mu(d) \log(\frac{R}{d}) \qquad \text{for } n \ge 1. \tag{19}$$

mimics the behaviour of $\Lambda(n)$ on some averages.

The beginning of our line of research is Goldston's [**G92**] alternative rendering of the proof of Bombieri and Davenport's theorem on small gaps between primes. Goldston replaced the application of the circle method in the original proof by the use of the truncated divisor sum (19). The use of functions like $\Lambda_R(n)$ goes back to Selberg's work [**Sel42**] on the zeros of the Riemann zeta-function $\zeta(s)$. The most beneficial feature of the truncated divisor sums is that they can be used in place of $\Lambda(n)$ on some occasions when it is not known how to work with $\Lambda(n)$ itself. The principal such situation arises in counting the primes in tuples. Let

$$\mathcal{H} = \{h_1, h_2, \ldots, h_k\} \text{ with } 1 \le h_1, \ldots, h_k \le h \text{ distinct integers} \tag{20}$$

(the restriction of h_i to positive integers is inessential; the whole set $\mathcal{H}$ can be shifted by a fixed integer with no effect on our procedure), and for a prime p denote by $\nu_p(\mathcal{H})$ the number of distinct residue classes modulo p occupied by the elements of $\mathcal{H}$. The singular series associated with the k-tuple $\mathcal{H}$ is defined as

$$\mathfrak{S}(\mathcal{H}) := \prod_p (1 - \frac{1}{p})^{-k}(1 - \frac{\nu_p(\mathcal{H})}{p}). \tag{21}$$

Since $\nu_p(\mathcal{H}) = k$ for $p > h$, the product is convergent. The admissibility of $\mathcal{H}$ is equivalent to $\mathfrak{S}(\mathcal{H}) \neq 0$, and to $\nu_p(\mathcal{H}) \neq p$ for all primes. Hardy and Littlewood [**HL23**] conjectured that

$$\sum_{n\leq N} \Lambda(n;\mathcal{H}) := \sum_{n\leq N} \Lambda(n+h_1)\cdots\Lambda(n+h_k) = N(\mathfrak{S}(\mathcal{H})+o(1)), \quad \text{as } N \to \infty. \tag{22}$$

The prime number theorem is the $k = 1$ case, and for $k \geq 2$ the conjecture remains unproved. (This conjecture is trivially true if $\mathcal{H}$ is inadmissible).

A simplified version of Goldston's argument in [**G92**] was given in [**GY03**] as follows. To obtain information on small gaps between primes, let

$$\psi(n,h) := \psi(n+h)-\psi(n) = \sum_{n<m\leq n+h} \Lambda(m), \quad \psi_R(n,h) := \sum_{n<m\leq n+h} \Lambda_R(m), \tag{23}$$

and consider the inequality

$$\sum_{N<n\leq 2N} (\psi(n,h) - \psi_R(n,h))^2 \geq 0. \tag{24}$$

The strength of this inequality depends on how well $\Lambda_R(n)$ approximates $\Lambda(n)$. On multiplying out the terms and using from [**G92**] the formulas

(25)
$$\sum_{n\leq N} \Lambda_R(n)\Lambda_R(n+k) \sim \mathfrak{S}(\{0,k\})N, \quad \sum_{n\leq N} \Lambda(n)\Lambda_R(n+k) \sim \mathfrak{S}(\{0,k\})N \quad (k \neq 0)$$

(26)
$$\sum_{n\leq N} \Lambda_R(n)^2 \sim N\log R, \quad \sum_{n\leq N} \Lambda(n)\Lambda_R(n) \sim N\log R,$$

valid for $|k| \leq R \leq N^{\frac{1}{2}}(\log N)^{-A}$, gives, taking $h = \lambda \log N$ with $\lambda \ll 1$,

(27)
$$\sum_{N<n\leq 2N} (\psi(n+h) - \psi(n))^2 \geq (hN\log R + Nh^2)(1-o(1)) \geq (\frac{\lambda}{2} + \lambda^2 - \epsilon)N(\log N)^2$$

(in obtaining this one needs the two-tuple case of Gallagher's singular series average given in (46) below, which can be traced back to Hardy and Littlewood's and Bombieri and Davenport's work). If the interval $(n, n+h]$ never contains more than one prime, then the left-hand side of (27) is at most

$$\log N \sum_{N<n\leq 2N} (\psi(n+h) - \psi(n)) \sim \lambda N(\log N)^2, \tag{28}$$

which contradicts (27) if $\lambda > \frac{1}{2}$, and thus one obtains

$$\liminf_{n\to\infty} \frac{p_{n+1} - p_n}{\log p_n} \leq \frac{1}{2}. \tag{29}$$

Later on Goldston et al. in [**FG96**], [**FG99**], [**G95**], [**GY98**], [**GY01**], [**GYa**] applied this lower-bound method to various problems concerning the distribution of primes and in [**GGÖS00**] to the pair correlation of zeros of the Riemann zeta-function. In most of these works the more delicate divisor sum

$$\lambda_R(n) := \sum_{r\le R} \frac{\mu^2(r)}{\phi(r)} \sum_{d|(r,n)} d\mu(d) \tag{30}$$

was employed especially because it led to better conditional results which depend on the Generalized Riemann Hypothesis.

The left-hand side of (27) is the second moment for primes in short intervals. Gallagher [**Gal76**] showed that the Hardy-Littlewood conjecture (22) implies that the moments for primes in intervals of length $h \sim \lambda \log N$ are the moments of a Poisson distribution with mean λ. In particular, it is expected that

$$\sum_{n\le N} (\psi(n+h) - \psi(n))^2 \sim (\lambda + \lambda^2) N (\log N)^2 \tag{31}$$

which in view of (28) implies (10) but is probably very hard to prove. It is known from the work of Goldston and Montgomery [**GM87**] that assuming the Riemann Hypothesis, an extension of (31) for $1 \le h \le N^{1-\epsilon}$ is equivalent to a form of the pair correlation conjecture for the zeros of the Riemann zeta-function. We thus see that the factor $\frac{1}{2}$ in (27) is what is lost from the truncation level R, and an obvious strategy is to try to improve on the range of R where (25)-(26) are valid. In fact, the asymptotics in (26) are known to hold for $R \le N$ (the first relation in (26) is a special case of a result of Graham [**Gra78**]). It is easy to see that the second relation in (25) will hold with $R = N^{\alpha-\epsilon}$, where α is the level of distribution of primes in arithmetic progressions. For the first relation in (25) however, one can prove the the formula is valid for $R = N^{1/2+\eta}$ for a small $\eta > 0$, but unless one also assumes a somewhat unnatural level of distribution conjecture for Λ_R, one can go no further. Thus increasing the range of R in (25) is not currently possible.

However, there is another possible approach motivated by Gallagher's work [**Gal76**]. In 1999 the first and third authors discovered how to calculate some of the higher moments of the short divisor sums (19) and (30). At first this was achieved through straightforward summation and only the triple correlations of $\Lambda_R(n)$ were worked out in [**GY03**]. In applying these formulas, the idea of finding approximate moments with some expressions corresponding to (24) was eventually replaced with

$$\sum_{N<n\le 2N} (\psi(n,h) - \rho \log N)(\psi_R(n,h) - C)^2 \tag{32}$$

which if positive for some $\rho > 1$ implies that for some n we have $\psi(n,h) \ge 2\log N$. Here C is available to optimize the argument. Thus the problem was switched from trying to find a good fit for $\psi(n,h)$ with a short divisor sum approximation to the easier problem of trying to maximize a given quadratic form, or more generally a mollification problem. With just third correlations this resulted in (29), thus giving no improvement over Bombieri and Davenport's result. Nevertheless the new method was not totally fruitless since it gave

$$\liminf_{n\to\infty} \frac{p_{n+r} - p_n}{\log p_n} \le r - \frac{\sqrt{r}}{2}, \tag{33}$$

whereas the argument leading to (29) gives $r-\frac{1}{2}$. Independently of us, Sivak [**Siv05**] incorporated Maier's method into [**GY03**] and improved upon (33) by the factor $e^{-\gamma}$ (cf. (6) and (14)).

Following [**GY03**], with considerable help from other mathematicians, in [**GYc**] the k-level correlations of $\Lambda_R(n)$ were calculated. This leap was achieved through replacing straightforward summation with complex integration upon the use of Perron type formulae. Thus it became feasible to approximate $\Lambda(n,\mathcal{H})$ which was defined in (22) by

$$\Lambda_R(n;\mathcal{H}) := \Lambda_R(n+h_1)\Lambda_R(n+h_2)\cdots\Lambda_R(n+h_k). \tag{34}$$

Writing

$$\Lambda_R(n;\mathbf{H}) := (\log R)^{k-|\mathcal{H}|}\Lambda_R(n;\mathcal{H}), \quad \psi_R^{(k)}(n,h) := \sum_{1\le h_1,\ldots,h_k\le h} \Lambda_R(n;\mathbf{H}), \tag{35}$$

where the distinct components of the k-dimensional vector $\mathbf{H}$ are the elements of the set $\mathcal{H}$, $\psi_R^{(j)}(n,h)$ provided the approximation to $\psi(n,h)^j$, and the expression

$$\sum_{N<n\le 2N} (\psi(n,h)-\rho\log N)(\sum_{j=0}^{k} a_j\psi_R^{(j)}(n,h)(\log R)^{k-j})^2 \tag{36}$$

could be evaluated. Here the a_j are constants available to optimize the argument. The optimization turned out to be a rather complicated problem which will not be discussed here, but the solution was recently completed in [**GYb**] with the result that for any fixed $\lambda > (\sqrt{r}-\sqrt{\frac{\alpha}{2}})^2$ and N sufficiently large,

$$\sum_{\substack{n\le N\\ p_{n+r}-p_n\le\lambda\log p_n}} 1 \gg_r \sum_{\substack{p\le N\\ p:\,\text{prime}}} 1. \tag{37}$$

In particular, unconditionally, for any fixed $\eta > 0$ and for all sufficiently large $N > N_0(\eta)$, a positive proportion of gaps $p_{n+1}-p_n$ with $p_n \le N$ are smaller than $(\frac{1}{4}+\eta)\log N$. This is numerically a little short of Maier's result (6), but (6) was shown to hold for a sparse sequence of gaps. The work [**GYb**] also turned out to be instrumental in Green and Tao's [**GT**] proof that the primes contain arbitrarily long arithmetic progressions.

The efforts made in 2003 using divisor sums which are more complicated than $\Lambda_R(n)$ and $\lambda_R(n)$ gave rise to more difficult calculations and didn't meet with success. During this work Granville and Soundararajan provided us with the idea that the method should be applied directly to individual tuples rather than sums over tuples which constitute approximations of moments. They replaced the earlier expressions with

$$\sum_{N<n\le 2N} (\sum_{h_i\in\mathcal{H}} \Lambda(n+h_i) - r\log 3N)(\tilde{\Lambda}_R(n;\mathcal{H}))^2, \tag{38}$$

where $\tilde{\Lambda}_R(n;\mathcal{H})$ is a short divisor sum which should be large when $\mathcal{H}$ is a prime tuple. This is the type of expression which is used in the proof of the result described in connection with (12)–(13) above. However, for obtaining the results (9)–(11). we need arguments based on using (32) and (36).

3. Detecting prime tuples

We call the tuple (12) a *prime tuple* when all of its components are prime numbers. Obviously this is equivalent to requiring that

$$P_{\mathcal{H}}(n) := (n+h_1)(n+h_2)\cdots(n+h_k) \tag{39}$$

is a product of k primes. As the generalized von Mangoldt function

$$\Lambda_k(n) := \sum_{d|n} \mu(d)(\log \frac{n}{d})^k \tag{40}$$

vanishes when n has more than k distinct prime factors, we may use

$$\frac{1}{k!} \sum_{\substack{d|P_{\mathcal{H}}(n) \\ d\le R}} \mu(d)(\log \frac{R}{d})^k \tag{41}$$

for approximating prime tuples. (Here $1/k!$ is just a normalization factor. That (41) will be also counting some tuples by including proper prime power factors doesn't pose a threat since in our applications their contribution is negligible). But this idea by itself brings restricted progress: now the right-hand side of (6) can be replaced with $1 - \frac{\sqrt{3}}{2}$.

The efficiency of the argument is greatly increased if instead of trying to include tuples composed only of primes, one looks for tuples with primes in many components. So in [**GPYa**] we employ

$$\Lambda_R(n;\mathcal{H},\ell) := \frac{1}{(k+\ell)!} \sum_{\substack{d|P_{\mathcal{H}}(n) \\ d\le R}} \mu(d)(\log \frac{R}{d})^{k+\ell}, \tag{42}$$

where $|\mathcal{H}| = k$ and $0 \le \ell \le k$, and consider those $P_{\mathcal{H}}(n)$ which have at most $k+\ell$ distinct prime factors. In our applications the optimal order of magnitude of the integer ℓ turns out to be about $\sqrt{k}$. To implement this new approximation in the skeleton of the argument, the quantities

$$\sum_{n\le N} \Lambda_R(n;\mathcal{H}_1,\ell_1)\Lambda_R(n;\mathcal{H}_2,\ell_2), \tag{43}$$

and

$$\sum_{n\le N} \Lambda_R(n;\mathcal{H}_1,\ell_1)\Lambda_R(n;\mathcal{H}_2,\ell_2)\theta(n+h_0), \tag{44}$$

are calculated as R, $N \to \infty$. The latter has three cases according as $h_0 \notin \mathcal{H}_1 \cup \mathcal{H}_2$, or $h_0 \in \mathcal{H}_1 \setminus \mathcal{H}_2$, or $h_0 \in \mathcal{H}_1 \cap \mathcal{H}_2$. Here $M = |\mathcal{H}_1| + |\mathcal{H}_2| + \ell_1 + \ell_2$ is taken as a fixed integer which may be arbitrarily large. The calculation of (43) is valid with R as large as $N^{\frac{1}{2}-\epsilon}$ and $h \le R^C$ for any constant $C > 0$. The calculation of (44) can be carried out for R as large as $N^{\frac{\alpha}{2}-\epsilon}$ and $h \le R$. It should be noted that in [**GYb**] in the same context the usage of (34), which has k truncations, restricted the range of the divisors greatly, for then $R \le N^{\frac{1}{4k}-\epsilon}$ was needed. Moreover the calculations were more complicated compared to the present situation of dealing with only one truncation.

Requiring the positivity of the quantity

$$\sum_{n=N+1}^{2N}\Big(\sum_{1\le h_0\le h}\theta(n+h_0)-r\log 3N\Big)\Big(\sum_{\substack{\mathcal{H}\subset\{1,2,\ldots,h\}\\|\mathcal{H}|=k}}\Lambda_R(n;\mathcal{H},\ell)\Big)^2,\qquad (h=\lambda\log 3N), \tag{45}$$

which can be calculated easily from asymptotic formulas for (43) and (44), and Gallagher's [**Gal76**] result that with the notation of (20) for fixed k

$$\sum_{\mathcal{H}}\mathfrak{S}(\mathcal{H})\sim h^k \qquad \text{as} \quad h\to\infty, \tag{46}$$

yields the results (9)–(11). For the proof of the result mentioned in connection with (12), the positivity of (38) with $r=1$ and $\Lambda_R(n;\mathcal{H},\ell)$ for an $\mathcal{H}$ satisfying (20) in place of $\tilde{\Lambda}_R(n;\mathcal{H})$ is used. For (13), the positivity of an optimal linear combination of the quantities for (12) is pursued.

The proof of (15) in [**GPYb**] also depends on the positivity of (45) for $r=1$ and $h=\frac{C\log N}{k}$ modified with the extra restriction

$$\Big(P_{\mathcal{H}}(n),\prod_{p\le\sqrt{\log N}}p\Big)=1 \tag{47}$$

on the tuples to be summed over, but involves some essential differences from the procedure described above. Now the size of k is taken as large as $c\frac{\sqrt{\log N}}{(\log\log N)^2}$ (where c is a sufficiently small explicitly calculable absolute constant). This necessitates a much more refined treatment of the error terms arising in the argument, and in due course the restriction (47) is brought in to avoid the complications arising from the possibly irregular behaviour of $\nu_p(\mathcal{H})$ for small p. In the new argument a modified version of the Bombieri-Vinogradov theorem is needed. Roughly speaking, in the version developed for this purpose, compared to (7) the range of the moduli q is curtailed a little bit in return for a little stronger upper-bound. Moreover, instead of Gallagher's result (46) which was for fixed k (though the result may hold for k growing as some function of h, we do not know exactly how large this function can be in addition to dealing with the problem of non-uniformity in k), the weaker property that $\sum_{\mathcal{H}}\mathfrak{S}(\mathcal{H})/h^k$ is non-decreasing (apart from a factor of $1+o(1)$) as a function of k is proved and employed. The whole argument is designed to give the more general result which was mentioned after (15).

4. Small gaps between almost primes

In the context of our work, by *almost prime* we mean an E_2*-number*, i.e. a natural number which is a product of two distinct primes. We have been able to apply our methods to finding small gaps between almost primes in collaboration with S. W. Graham. For this purpose a Bombieri-Vinogradov type theorem for $\Lambda*\Lambda$ is needed, and the work of Motohashi [**Mot76**] on obtaining such a result for the Dirichlet convolution of two sequences is readily applicable (see also [**Bom87**]). In [**GGPYa**] alternative proofs of some results of [**GPYa**] such as (10) and (13) are given couched in the formalism of the Selberg sieve. Denoting by q_n the n-th E_2-number, in [**GGPYa**] and [**GGPYb**] it is shown that there is a constant C such that for any positive integer r,

$$\liminf_{n\to\infty}(q_{n+r}-q_n)\le Cre^r; \tag{48}$$

in particular

$$\liminf_{n\to\infty}(q_{n+1} - q_n) \leq 6. \tag{49}$$

Furthermore in [**GGPYc**] proofs of a strong form of the Erdös–Mirsky conjecture and related assertions have been obtained.

5. Further remarks on the origin of our method

In 1950 Selberg was working on applications of his sieve method to the twin prime and Goldbach problems and invented a weighted sieve method that gave results which were later superseded by other methods and thereafter largely neglected. Much later in 1991 Selberg published the details of this work in Volume II of his Collected Works [**Sel91**], describing it as "by now of historical interest only". In 1997 Heath-Brown [**HB97**] generalized Selberg's argument from the twin prime problem to the problem of almost prime tuples. Heath-Brown let

$$\Pi = \prod_{i=1}^{k}(a_i n + b_i) \tag{50}$$

with certain natural conditions on the integers a_i and b_i. Then the argument of Selberg (for the case $k = 2$) and Heath-Brown for the general case is to choose $\rho > 0$ and the numbers λ_d of the Selberg sieve so that, with τ the divisor function,

$$Q = \sum_{n\leq x}\{1 - \rho\sum_{i=1}^{k}\tau(a_i n + b_i)\}(\sum_{d|\Pi}\lambda_d)^2 > 0. \tag{51}$$

From this it follows that there is at least one value of n for which

$$\sum_{i=1}^{k}\tau(a_i n + b_i) < \frac{1}{\rho}. \tag{52}$$

Selberg found in the case $k = 2$ that $\rho = \frac{1}{14}$ is acceptable, which shows that one of n and $n + 2$ has at most two, while the other has at most three prime factors for infinitely many n. Remarkably, this is exactly the same type of tuple argument of Granville and Soundararajan which we have used, and the similarity doesn't end here. Multiplying out, we have $Q = Q_1 - \rho Q_2$ where

$$Q_1 = \sum_{n\leq x}(\sum_{d|\Pi}\lambda_d)^2 > 0, \qquad Q_2 = \sum_{i=1}^{k}\sum_{n\leq x}\tau(a_i n + b_i)\}(\sum_{d|\Pi}\lambda_d)^2 > 0. \tag{53}$$

The goal is now to pick λ_d optimally. As usual, the λ_d are first made 0 for $d > R$. At this point it appears difficult to find the exact solution to this problem. Further discussion of this may be found in [**Sel91**] and [**HB97**]. Heath-Brown, desiring to keep Q_2 small, made the choice

$$\lambda_d = \mu(d)(\frac{\log(R/d)}{\log R})^{k+1}, \tag{54}$$

and with this choice we see

$$Q_1 = \frac{((k+1)!)^2}{(\log R)^{2k+2}}\sum_{n\leq x}(\Lambda_R(n;\mathcal{H},1))^2. \tag{55}$$

Hence Heath-Brown used the approximation for a k-tuple with at most $k + 1$ distinct prime factors. This observation was the starting point for our work with the approximation $\Lambda_R(n;\mathcal{H},\ell)$. The evaluation of Q_2 with its τ weights is much harder to evaluate than Q_1 and requires Kloosterman sum estimates. The weight Λ in Q_2 in place of τ requires essentially the same analysis as Q_1 if we use the Bombieri-Vinogradov theorem. Apparently these arguments were never viewed as directly applicable to primes themselves, and this connection was missed until now.

References

[Bom87] E. Bombieri – "Le grand crible dans la théorie analytique des nombres", *Astérisque* (1987), no. 18, p. 103.

[BD66] E. Bombieri & H. Davenport – "Small differences between prime numbers", *Proc. Roy. Soc.* Ser. A, **293** (1966), p. 1–18.

[FG96] J. B. Friedlander & D. A. Goldston – "Variance of distribution of primes in residue classes", *Quart. J. Math. Oxford Ser. (2)* **47** (1996), no. 187, p. 313–336.

[FG99] ———, "Note on a variance in the distribution of primes", in *Number theory in progress, Vol. 2 (Zakopane-Kościelisko, 1997)*, de Gruyter, Berlin, 1999, p. 841–848.

[Gal76] P. X. Gallagher – "On the distribution of primes in short intervals", *Mathematika* **23** (1976), no. 1, p. 4–9.

[G92] D. A. Goldston – "On Bombieri and Davenport's theorem concerning small gaps between primes", *Mathematika* **39** (1992), no. 1, p. 10–17.

[G95] ———, "A lower bound for the second moment of primes in short intervals", *Exposition. Math.* **13** (1995), no. 4, p. 366–376.

[GGÖS00] D. A. Goldston, S. M. Gonek, A. E. Özlük & C. Snyder – "On the pair correlation of zeros of the Riemann zeta-function", *Proc. London Math. Soc. (3)* **80** (2000), no. 1, p. 31–49.

[GGPYa] D. A. Goldston, S. Graham, J. Pintz & C. Y. Yildirim – "Small gaps between primes or almost primes", (2005), preprint 2005-14 of *http://aimath.org/preprints.html*.

[GGPYb] ———, "Small gaps between products of two primes", (2006), preprint 2006-60 of *http://aimath.org/preprints.html*.

[GGPYc] ———, "Small gaps between almost primes, the parity problem, and some conjectures of Erdös on consecutive integers", preprint (2005).

[GM87] D. A. Goldston & H. L. Montgomery – "Pair correlation of zeros and primes in short intervals", in *Analytic number theory and Diophantine problems (Stillwater, OK, 1984)*, Progr. Math., vol. 70, Birkhäuser Boston, Boston, MA, 1987, p. 183–203.

[GPYa] D. A. Goldston, J. Pintz & C. Y. Yildirim – "Primes in tuples I", (2005), preprint 2005-19 of *http://aimath.org/preprints.html*, to appear in *Ann. of Math.*

[GPYb] ———, "Primes in tuples II", preprint (2005).

[GPY06] ———, "Primes in tuples III: On the difference $p_{n+\nu}-p_n$", *Funct. Approx. Comment. Math.* **XXXV** (2006), p. 79–89.

[GY98] D. A. Goldston & C. Y. Yildirim – "Primes in short segments of arithmetic progressions", *Canad. J. Math.* **50** (1998), no. 3, p. 563–580.

[GY01] ———, "On the second moment for primes in an arithmetic progression", *Acta Arith.* **100** (2001), no. 1, p. 85–104.

[GY03] ———, "Higher correlations of divisor sums related to primes. I. Triple correlations", *Integers* **3** (2003), p. A5, 66 pp. (electronic).

[GYa] ———, "Higher correlations of divisor sums related to primes II: Variations in the error term in the prime number theorem", (2003), preprint 2004-29 of *http://aimath.org/preprints.html*.

[GYb] ———, "Higher correlations of divisor sums related to primes III: Small gaps between primes", (2004), preprint 2005-12 of *http://aimath.org/preprints.html*.

[GYc] ———, "Higher correlations of divisor sums related to primes IV: k-correlations", (2002), preprint 2002-11 of *http://aimath.org/preprints.html*.

[Gra78] S. Graham – "An asymptotic estimate related to Selberg's sieve", *J. Number Theory* **10** (1978), no. 1, p. 83–94.

[GT] B. Green & T. Tao – "The primes contain arbitrarily long arithmetic progressions", (2004), preprint at *arXiv:math.NT/0404188*.

[HL23] G. H. Hardy & J. E. Littlewood – "Some problems of 'Partitio Numerorum': III. On the the expression of a number as a sum of primes", *Acta Math.* **44** (1923), p. 1–70.

[HB97] D. R. Heath-Brown – "Almost-prime k-tuples", *Mathematika* **44** (1997), no. 2, p. 245–266.

[Mai88] H. Maier – "Small differences between prime numbers", *Michigan Math. J.* **35** (1988), no. 3, p. 323–344.

[Mot76] Y. Motohashi – "An induction principle for the generalization of Bombieri's prime number theorem", *Proc. Japan Acad.* **52** (1976), no. 6, p. 273–275.

[Sel42] A. Selberg – "On the zeros of Riemann's zeta-function", *Skr. Norske Vid. Akad. Oslo I.* **1942** (1942), no. 10, p. 59.

[Sel91] ———, *Lectures on sieves, in Collected papers. Vol. II*, Springer-Verlag, Berlin, 1991.

[Siv05] J. Sivak – "Méthodes de crible appliquées aux sommes de Kloosterman et aux petits écarts entre nombres premiers", Thesis, Paris Sud (Paris XI), 2005.

Department of Mathematics, San Jose State University, San Jose, CA 95192, USA
E-mail address: goldston@math.sjsu.edu

Rényi Mathematical Institute of the Hungarian Academy of Sciences, H-1364 Budapest, P.O.B. 127, Hungary
E-mail address: pintz@renyi.hu

Department of Mathematics, Boğaziçi University, Bebek, Istanbul 34342, Turkey & Feza Gürsey Enstitüsü, Cengelköy, Istanbul, P.K. 6, 81220, Turkey
E-mail address: yalciny@boun.edu.tr

Clay Mathematics Proceedings
Volume 7, 2007

Negative values of truncations to $L(1, \chi)$

Andrew Granville and K. Soundararajan

Abstract. For fixed large x we give upper and lower bounds for the minimum of $\sum_{n\le x} \chi(n)/n$ as we minimize over all real-valued Dirichlet characters χ. This follows as a consequence of bounds for $\sum_{n\le x} f(n)/n$ but now minimizing over all completely multiplicative, real-valued functions f for which $-1 \le f(n) \le 1$ for all integers $n \ge 1$. Expanding our set to all multiplicative, real-valued multiplicative functions of absolute value ≤ 1, the minimum equals $-0.4553\cdots + o(1)$, and in this case we can classify the set of optimal functions.

1. Introduction

Dirichlet's celebrated class number formula established that $L(1, \chi)$ is positive for primitive, quadratic Dirichlet characters χ. One might attempt to prove this positivity by trying to establish that the partial sums $\sum_{n\le x} \chi(n)/n$ are all non-negative. However, such truncated sums can get negative, a feature which we will explore in this note.

By quadratic reciprocity we may find an arithmetic progression $\pmod{4\prod_{p\le x} p}$ such that any prime q lying in this progression satisfies $\left(\frac{p}{q}\right) = -1$ for each $p \le x$. Such primes q exist by Dirichlet's theorem on primes in arithmetic progressions, and for such q we have $\sum_{n\le x} \left(\frac{n}{q}\right)/n = \sum_{n\le x} \lambda(n)/n$ where $\lambda(n) = (-1)^{\Omega(n)}$ is the Liouville function. Turán [6] suggested that $\sum_{n\le x} \lambda(n)/n$ may be always positive, noting that this would imply the truth of the Riemann Hypothesis (and previously Pólya had conjectured that the related $\sum_{n\le x} \lambda(n)$ is non-positive for all $x \ge 2$, which also implies the Riemann Hypothesis). In [**Has58**] Haselgrove showed that both the Turán and Pólya conjectures are false (in fact $x = 72,185,376,951,205$ is the smallest integer x for which $\sum_{n\le x} \lambda(n)/n < 0$, as was recently determined in [**BFM**]). We therefore know that truncations to $L(1, \chi)$ may get negative.

Let $\mathcal{F}$ denote the set of all completely multiplicative functions $f(\cdot)$ with $-1 \le f(n) \le 1$ for all positive integers n, let $\mathcal{F}_1$ be those for which each $f(n) = \pm 1$, and $\mathcal{F}_0$ be those for which each $f(n) = 0$ or ± 1. Given any x and any $f \in \mathcal{F}_0$ we may find a primitive quadratic character χ with $\chi(n) = f(n)$ for all $n \le x$ (again, by using

2000 *Mathematics Subject Classification.* Primary 11M20.

Le premier auteur est partiellement soutenu par une bourse du Conseil de recherches en sciences naturelles et en génie du Canada. The second author is partially supported by the National Science Foundation and the American Institute of Mathematics (AIM).

quadratic reciprocity and Dirichlet's theorem on primes in arithmetic progressions) so that, for any $x \geq 1$,

$$\min_{\substack{\chi \text{ a quadratic} \\ \text{character}}} \sum_{n\leq x} \frac{\chi(n)}{n} = \delta_0(x) := \min_{f\in\mathcal{F}_0} \sum_{n\leq x} \frac{f(n)}{n}.$$

Moreover, since $\mathcal{F}_1 \subset \mathcal{F}_0 \subset \mathcal{F}$ we have that

$$\delta(x) := \min_{f\in\mathcal{F}} \sum_{n\leq x} \frac{f(n)}{n} \quad \leq \delta_0(x) \leq \quad \delta_1(x) := \min_{f\in\mathcal{F}_1} \sum_{n\leq x} \frac{f(n)}{n}.$$

We expect that $\delta(x) \sim \delta_1(x)$ and even, perhaps, that $\delta(x) = \delta_1(x)$ for sufficiently large x.

Trivially $\delta(x) \geq -\sum_{n\leq x} 1/n = -(\log x + \gamma + O(1/x))$. Less trivially $\delta(x) \geq -1$, as may be shown by considering the non-negative multiplicative function $g(n) = \sum_{d|n} f(d)$ and noting that

$$0 \leq \sum_{n\leq x} g(n) = \sum_{d\leq x} f(d)\Big[\frac{x}{d}\Big] \leq \sum_{d\leq x} \Big(x\frac{f(d)}{d} + 1\Big).$$

We will show that $\delta(x) \leq \delta_1(x) < 0$ for all large values of x, and that $\delta(x) \to 0$ as $x \to \infty$.

Theorem 1. *For all large x and all $f \in \mathcal{F}$ we have*

$$\sum_{n\leq x} \frac{f(n)}{n} \geq -\frac{1}{(\log\log x)^{\frac{3}{5}}}.$$

Further, there exists a constant $c > 0$ such that for all large x there exists a function $f(= f_x) \in \mathcal{F}_1$ such that

$$\sum_{n\leq x} \frac{f(n)}{n} \leq -\frac{c}{\log x}.$$

In other words, for all large x,

$$-\frac{1}{(\log\log x)^{\frac{3}{5}}} \leq \delta(x) \leq \delta_0(x) \leq \delta_1(x) \leq -\frac{c}{\log x}.$$

Note that Theorem 1 implies that there exists some absolute constant $c_0 > 0$ such that $\sum_{n\leq x} f(n)/n \geq -c_0$ for all x and all $f \in \mathcal{F}$, and that equality occurs only for bounded x. It would be interesting to determine c_0 and all x and f attaining this value, which is a feasible goal developing the methods of this article.

It would be interesting to determine more precisely the asymptotic nature of $\delta(x), \delta_0(x)$ and $\delta_1(x)$, and to understand the nature of the optimal functions.

Instead of completely multiplicative functions we may consider the larger class $\mathcal{F}^*$ of multiplicative functions, and analogously define

$$\delta^*(x) := \min_{f\in\mathcal{F}^*} \sum_{n\leq x} \frac{f(n)}{n} \; .$$

Theorem 2. *We have*

$$\delta^*(x) = \Big(1 - 2\log(1+\sqrt{e}) + 4\int_1^{\sqrt{e}} \frac{\log t}{t+1}dt\Big)\log 2 + o(1) = -0.4553\ldots + o(1).$$

If $f^* \in \mathcal{F}^*$ and x is large then

$$\sum_{n\le x} \frac{f^*(n)}{n} \ge -\frac{1}{(\log\log x)^{\frac{3}{5}}},$$

unless

$$\sum_{k=1}^{\infty} \frac{1+f^*(2^k)}{2^k} \ll (\log x)^{-\frac{1}{20}}.$$

Finally

$$\sum_{n\le x} \frac{f^*(n)}{n} = \delta^*(x) + o(1)$$

if and only if

$$\Big(\sum_{k=1}^{\infty} \frac{1+f^*(2^k)}{2^k}\Big)\log x + \sum_{3\le p\le x^{1/(1+\sqrt{e})}} \sum_{k=1}^{\infty} \frac{1-f^*(p^k)}{p^k} + \sum_{x^{1/(1+\sqrt{e})}\le p\le x} \frac{1+f^*(p)}{p} = o(1).$$

2. Constructing negative values

Recall Haselgrove's result [**Has58**]: there exists an integer N such that

$$\sum_{n\le N} \frac{\lambda(n)}{n} = -\delta$$

with $\delta > 0$, where $\lambda \in \mathcal{F}_1$ with $\lambda(p) = -1$ for all primes p. Let $x > N^2$ be large and consider the function $f = f_x \in \mathcal{F}_1$ defined by $f(p) = 1$ if $x/(N+1) < p \le x/N$ and $f(p) = -1$ for all other p. If $n \le x$ then we see that $f(n) = \lambda(n)$ unless $n = p\ell$ for a (unique) prime $p \in (x/(N+1), x/N]$ in which case $f(n) = \lambda(\ell) = \lambda(n) + 2\lambda(\ell)$. Thus

$$\begin{aligned}\sum_{n\le x} \frac{f(n)}{n} &= \sum_{n\le x} \frac{\lambda(n)}{n} + 2\sum_{x/(N+1)<p\le x/N} \frac{1}{p} \sum_{\ell\le x/p} \frac{\lambda(\ell)}{\ell} \\ &= \sum_{n\le x} \frac{\lambda(n)}{n} - 2\delta \sum_{x/(N+1)<p\le x/N} \frac{1}{p}.\end{aligned} \tag{2.1}$$

A standard argument, as in the proof of the prime number theorem, shows that

$$\sum_{n\le x} \frac{\lambda(n)}{n} = \frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty} \frac{\zeta(2s+2)}{\zeta(s+1)} \frac{x^s}{s} ds \ll \exp(-c\sqrt{\log x}),$$

for some $c > 0$. Further, the prime number theorem readily gives that

$$\sum_{x/(N+1)<p\le x/N} \frac{1}{p} \sim \log\Big(\frac{\log(x/N)}{\log(x/(N+1))}\Big) \asymp \frac{1}{N\log x}.$$

Inserting these estimates in (2.1) we obtain that $\delta(x) \le -c/\log x$ for large x (here $c \asymp \delta/N$), as claimed in Theorem 1.

Remark 2.1. In [**BFM**] it is shown that one can take $\delta = 2.0757641\cdots 10^{-9}$ for $N = 72204113780255$ and therefore we may take $c \approx 2.87\cdot 10^{-23}$.

3. The lower bound for $\delta(x)$

PROPOSITION 3.1. *Let f be a completely multiplicative function with $-1 \le f(n) \le 1$ for all n, and set $g(n) = \sum_{d|n} f(d)$ so that g is a non-negative multiplicative function. Then*

$$\sum_{n\le x} \frac{f(n)}{n} = \frac{1}{x}\sum_{n\le x} g(n) + (1-\gamma)\frac{1}{x}\sum_{n\le x} f(n) + O\Big(\frac{1}{(\log x)^{\frac{1}{5}}}\Big).$$

PROOF. Define $F(t) = \frac{1}{t}\sum_{n\le t} f(n)$. We will make use of the fact that $F(t)$ varies slowly with t. From [**GS03**, Corollary 3],we find that if $1 \le w \le x/10$ then

$$\Big||F(x)| - |F(x/w)|\Big| \ll \Big(\frac{\log 2w}{\log x}\Big)^{1-\frac{2}{\pi}} \log\Big(\frac{\log x}{\log 2w}\Big) + \frac{\log\log x}{(\log x)^{2-\sqrt{3}}}. \tag{3.1}$$

We may easily deduce that

$$\Big|F(x) - F(x/w)\Big| \ll \Big(\frac{\log 2w}{\log x}\Big)^{1-\frac{2}{\pi}} \log\Big(\frac{\log x}{\log 2w}\Big) + \frac{\log\log x}{(\log x)^{2-\sqrt{3}}} \ll \Big(\frac{\log 2w}{\log x}\Big)^{\frac{1}{4}}. \tag{3.2}$$

Indeed, if $F(x)$ and $F(x/w)$ are of the same sign then (3.2) follows at once from (3.1). If $F(x)$ and $F(x/w)$ are of opposite signs then we may find $1 \le v \le w$ with $|\sum_{n\le x/v} f(n)| \le 1$ and then using (3.1) first with $F(x)$ and $F(x/v)$, and second with $F(x/v)$ and $F(x/w)$ we obtain (3.2).

We now turn to the proof of the Proposition. We start with

$$\sum_{n\le x} g(n) = \sum_{d\le x} f(d)\Big[\frac{x}{d}\Big] = x\sum_{d\le x}\frac{f(d)}{d} - \sum_{d\le x} f(d)\Big\{\frac{x}{d}\Big\}. \tag{3.3}$$

Now

$$\begin{aligned}\sum_{d\le x} f(d)\Big\{\frac{x}{d}\Big\} &= \sum_{j\le x}\ \sum_{x/(j+1)<d\le x/j} f(d)\Big(\frac{x}{d} - j\Big)\\ &= \sum_{j\le \log x}\int_{x/(j+1)}^{x/j} \frac{x}{t^2} \sum_{x/(j+1)<d\le t} f(d)dt + O\Big(\frac{x}{\log x}\Big).\end{aligned}$$

From (3.2) we see that if $j \le \log x$, and $x/(j+1) < t \le x/j$ then

$$\sum_{x/(j+1)<d\le t} f(d) = \Big(t - \frac{x}{(j+1)}\Big)\frac{1}{x}\sum_{n\le x} f(n) + O\Big(\frac{x\log(j+1)}{j(\log x)^{\frac{1}{4}}}\Big).$$

Using this above we conclude that

$$\sum_{d\le x} f(d)\Big\{\frac{x}{d}\Big\} = \Big(\sum_{n\le x} f(n)\Big)\sum_{j\le\log x}\Big(\log\Big(\frac{j+1}{j}\Big) - \frac{1}{j+1}\Big) + O\Big(\frac{x(\log\log x)^2}{(\log x)^{\frac{1}{4}}}\Big). \tag{3.4}$$

Since $\sum_{j\le J}(\log(1+1/j) - 1/(j+1)) = \log(J+1) - \sum_{j\le J+1} 1/j + 1 = 1 - \gamma + O(1/J)$, when we insert (3.4) into (3.3) we obtain the Proposition. $\square$

Set $u = \sum_{p\le x}(1-f(p))/p$. By Theorem 2 of A. Hildebrand [**Hil87**] (with f there being our function g, $K=2$, $K_2=1.1$, and $z=2$) we obtain that

$$\frac{1}{x}\sum_{n\le x} g(n) \gg \prod_{p\le x}\Big(1-\frac{1}{p}\Big)\Big(1+\frac{g(p)}{p}+\frac{g(p^2)}{p^2}+\dots\Big)\sigma_-\Big(\exp\Big(\sum_{p\le x}\frac{\max(0,1-g(p))}{p}\Big)\Big) + O(\exp(-(\log x)^\beta)),$$

where β is some positive constant and $\sigma_-(\xi)=\xi\rho(\xi)$ with ρ being the Dickman function[1]. Since $\max(0,1-g(p))\le(1-f(p))/2$ we deduce that

$$\begin{aligned}\frac{1}{x}\sum_{n\le x} g(n) &\gg (e^{-u}\log x)(e^{u/2}\rho(e^{u/2})) + O(\exp(-(\log x)^\beta)) \\ &\gg e^{-ue^{u/2}}(\log x) + O(\exp(-(\log x)^\beta)),\end{aligned} \tag{3.5}$$

since $\rho(\xi)=\xi^{-\xi+o(\xi)}$.

On the other hand, a special case of the main result in [**HT91**] implies that

$$\frac{1}{x}\Big|\sum_{n\le x} f(n)\Big| \ll e^{-\kappa u}, \tag{3.6}$$

where $\kappa = 0.32867\ldots$. Combining Proposition 3.1 with (3.5) and (3.6) we immediately get that $\delta(x)\ge -c/(\log\log x)^\xi$ for any $\xi<2\kappa$. This completes the proof of Theorem 1.

Remark 3.2. The bound (3.5) is attained only in certain very special cases, that is, when there are very few primes $p > x^{e^{-u}}$ for which $f(p)=1+o(1)$. In this case one can get a far stronger bound than (3.6). Since the first part of Theorem 1 depends on an interaction between these two bounds, this suggests that one might be able to improve Theorem 1 significantly by determining how (3.5) and (3.6) depend upon one another.

4. Proof of Theorem 2

Given $f^*\in\mathcal{F}^*$ we associate a completely multiplicative function $f\in\mathcal{F}$ by setting $f(p)=f^*(p)$. We write $f^*(n)=\sum_{d|n}h(d)f(n/d)$ where h is the multiplicative function given by $h(p^k)=f^*(p^k)-f(p)f^*(p^{k-1})$ for $k\ge1$. Now,

$$\begin{aligned}\sum_{n\le x}\frac{f^*(n)}{n} &= \sum_{d\le x}\frac{h(d)}{d}\sum_{m\le x/d}\frac{f(m)}{m} \\ &= \sum_{d\le(\log x)^6}\frac{h(d)}{d}\sum_{m\le x/d}\frac{f(m)}{m} + O\Big(\log x\sum_{d>(\log x)^6}\frac{|h(d)|}{d}\Big).\end{aligned} \tag{4.1}$$

Since $h(p)=0$ and $|h(p^k)|\le 2$ for $k\ge2$ we see that

$$\sum_{d>(\log x)^6}\frac{|h(d)|}{d} \le (\log x)^{-2}\sum_{d\ge1}\frac{|h(d)|}{d^{\frac{2}{3}}} \ll (\log x)^{-2}. \tag{4.2}$$

[1] The Dickman function is defined as $\rho(u)=1$ for $u\le1$, and $\rho(u)=(1/u)\int_{u-1}^{u}\rho(t)dt$ for $u\ge1$.

Further, for $d \le (\log x)^6$, we have (writing $F(t) = \frac{1}{t}\sum_{n\le t} f(n)$ as in section 3)

$$\sum_{x/d\le n\le x} \frac{f(n)}{n} = F(x) - F(x/d) + \int_{x/d}^{x} \frac{F(t)}{t} dt = \frac{\log d}{x} \sum_{n\le x} f(n) + O\Big(\frac{1}{(\log x)^{\frac{1}{5}}}\Big),$$

using (3.2). Using the above in (4.1) we deduce that

$$\sum_{n\le x} \frac{f^*(n)}{n} = \Big(\sum_{n\le x}\frac{f(n)}{n}\Big) \sum_{d\le (\log x)^6} \frac{h(d)}{d} - \frac{1}{x}\sum_{n\le x} f(n) \sum_{d\le (\log x)^6} \frac{h(d)\log d}{d} + O\Big(\frac{1}{(\log x)^{\frac{1}{5}}}\Big).$$

Arguing as in (4.2) we may extend the sums over d above to all d, incurring a negligible error. Thus we conclude that

$$\sum_{n\le x} \frac{f^*(n)}{n} = H_0 \sum_{n\le x} \frac{f(n)}{n} + H_1 \frac{1}{x} \sum_{n\le x} f(n) + O\Big(\frac{1}{(\log x)^{\frac{1}{5}}}\Big),$$

with

$$H_0 = \sum_{d=1}^{\infty} \frac{h(d)}{d}, \qquad \text{and} \qquad H_1 = -\sum_{d=1}^{\infty} \frac{h(d)\log d}{d}.$$

Note that $H_0 = \prod_p (1 + h(p)/p + h(p^2)/p^2 + \ldots) \ge 0$, and that $H_0, |H_1| \ll 1$.

We now use Proposition 3.1, keeping the notation there. We deduce that

$$\sum_{n\le x} \frac{f^*(n)}{n} = H_0 \frac{1}{x} \sum_{n\le x} g(n) + \Big((1-\gamma)H_0 + H_1\Big) \frac{1}{x} \sum_{n\le x} f(n) + O\Big(\frac{1}{(\log x)^{\frac{1}{5}}}\Big). \tag{4.3}$$

If $H_0 \ge (\log x)^{-\frac{1}{20}}$ then we may argue as in section 3, using (3.5) and (3.6). In that case, we see that $\sum_{n\le x} f^*(n)/n \ge -1/(\log\log x)^{\frac{3}{5}}$. Henceforth we suppose that $H_0 \le (\log x)^{-\frac{1}{20}}$. Since

$$H_0 \asymp 1 + \frac{h(2)}{2} + \frac{h(2^2)}{2^2} + \ldots \asymp 1 + \frac{f^*(2)}{2} + \frac{f^*(2^2)}{2^2} + \ldots,$$

we deduce that (note $h(2) = 0$)

$$\sum_{k=2}^{\infty} \frac{2 + h(2^k)}{2^k} \asymp \sum_{k=1}^{\infty} \frac{1 + f^*(2^k)}{2^k} \ll (\log x)^{-\frac{1}{20}}. \tag{4.4}$$

This proves the middle assertion of Theorem 2.

Writing $d = 2^k \ell$ with ℓ odd,

$$\begin{aligned} H_1 &= -\sum_{\ell \text{ odd}} \frac{h(\ell)}{\ell} \sum_{k=0}^{\infty} \frac{h(2^k)}{2^k}(k\log 2 + \log \ell) \\ &= -\log 2 \Big(\sum_{k=1}^{\infty} \frac{k h(2^k)}{2^k}\Big) \sum_{\ell \text{ odd}} \frac{h(\ell)}{\ell} + O((\log x)^{-\frac{1}{20}}) \\ &= 3\log 2 \prod_{p\ge 3} \Big(1 + \frac{h(p)}{p} + \frac{h(p^2)}{p^2} + \ldots\Big) + O\Big(\frac{\log\log x}{(\log x)^{\frac{1}{20}}}\Big), \end{aligned}$$

where we have used (4.4) and that $\sum_{k=1}^{\infty} kh(2^k)/2^k = -3 + O(\log\log x/(\log x)^{\frac{1}{20}})$. Using these observations in (4.3) we obtain that

(4.5)
$$\sum_{n\le x}\frac{f^*(n)}{n} = H_0\frac{1}{x}\sum_{n\le x} g(n) + 3\log 2\prod_{p\ge 3}\Big(1+\frac{h(p)}{p}+\frac{h(p^2)}{p^2}+\dots\Big)\frac{1}{x}\sum_{n\le x} f(n) + o(1)$$
$$\ge 3\log 2\prod_{p\ge 3}\Big(1+\frac{h(p)}{p}+\frac{h(p^2)}{p^2}+\dots\Big)\frac{1}{x}\sum_{n\le x} f(n) + o(1).$$

Let $r(\cdot)$ be the completely multiplicative function with $r(p) = 1$ for $p \le \log x$, and $r(p) = f(p)$ otherwise. Then Proposition 4.4 of [**GS01**] shows that

$$\frac{1}{x}\sum_{n\le x} f(n) = \prod_{p\le \log x}\Big(1-\frac{1}{p}\Big)\Big(1-\frac{f(p)}{p}\Big)^{-1}\frac{1}{x}\sum_{n\le x} r(n) + O\Big(\frac{1}{(\log x)^{\frac{1}{20}}}\Big).$$

Since $f(2) = -1 + O(H_0)$ we deduce from (4.5) and the above that

$$\sum_{n\le x}\frac{f^*(n)}{n} \ge \log 2\prod_{p\ge 3}\Big(1-\frac{1}{p}\Big)\Big(1+\frac{f^*(p)}{p}+\frac{f^*(p^2)}{p^2}+\dots\Big)\frac{1}{x}\sum_{n\le x} r(n) + o(1). \tag{4.6}$$

One of the main results of [**GS01**] (see Corollary 1 there) shows that

$$\frac{1}{x}\sum_{n\le x} r(n) \ge 1-2\log(1+\sqrt{e})+4\int_1^{\sqrt{e}}\frac{\log t}{t+1}dt+o(1) = -0.656999\ldots+o(1), \tag{4.7}$$

and that equality here holds if and only if

$$\sum_{p\le x^{1/(1+\sqrt{e})}}\frac{1-r(p)}{p} + \sum_{x^{1/(1+\sqrt{e})}\le p\le x}\frac{1+r(p)}{p} = o(1). \tag{4.8}$$

Since the product in (4.6) lies between 0 and 1 we conclude that

$$\sum_{n\le x}\frac{f^*(n)}{n} \ge \Big(1-2\log(1+\sqrt{e})+4\int_1^{\sqrt{e}}\frac{\log t}{t+1}dt\Big)\log 2 + o(1), \tag{4.9}$$

and for equality to be possible here we must have (4.8), and in addition that the product in (4.6) is $1+o(1)$. These conditions may be written as

$$\sum_{3\le p\le x^{1/(1+\sqrt{e})}}\sum_{k=1}^{\infty}\frac{1-f^*(p^k)}{p^k} + \sum_{x^{1/(1+\sqrt{e})}\le p\le x}\frac{1-f^*(p)}{p} = o(1).$$

If the above condition holds then, by (3.5), $\sum_{n\le x} g(n) \gg x\log x$ and so for equality to hold in (4.5) we must have $H_0 = o(1/\log x)$. Thus equality in (4.9) is only possible if

$$\Big(\sum_{k=1}^{\infty}\frac{1+f^*(2^k)}{2^k}\Big)\log x + \sum_{3\le p\le x^{1/(1+\sqrt{e})}}\sum_{k=1}^{\infty}\frac{1-f^*(p^k)}{p^k} + \sum_{x^{1/(1+\sqrt{e})}\le p\le x}\frac{1-f^*(p)}{p} = o(1).$$

Conversely, if the above is true then equality holds in (4.5), (4.6), and (4.7) giving equality in (4.9). This proves Theorem 2.

References

[BFM] P. Borwein, R. Ferguson & M. Mossinghoff – "Sign changes in sums of the Liouville function", preprint.

[GS01] A. Granville & K. Soundararajan – "The spectrum of multiplicative functions", *Ann. of Math. (2)* **153** (2001), no. 2, p. 407–470.

[GS03] ———, "Decay of mean values of multiplicative functions", *Canad. J. Math.* **55** (2003), no. 6, p. 1191–1230.

[Has58] C. B. Haselgrove – "A disproof of a conjecture of Pólya", *Mathematika* **5** (1958), p. 141–145.

[Hil87] A. Hildebrand – "Quantitative mean value theorems for nonnegative multiplicative functions. II", *Acta Arith.* **48** (1987), no. 3, p. 209–260.

[HT91] R. R. Hall & G. Tenenbaum – "Effective mean value estimates for complex multiplicative functions", *Math. Proc. Cambridge Philos. Soc.* **110** (1991), no. 2, p. 337–351.

Départment de Mathématiques et Statistique, Université de Montréal, CP 6128 succ Centre-Ville, Montréal, QC H3C 3J7, Canada

E-mail address: andrew@dms.umontreal.ca

Department of Mathematics, Stanford University, Bldg. 380, 450 Serra Mall, Stanford, CA 94305-2125, USA

E-mail address: ksound@math.stanford.edu

Clay Mathematics Proceedings
Volume 7, 2007

Long arithmetic progressions of primes

Ben Green

Abstract. This is an article for a general mathematical audience on the author's work, joint with Terence Tao, establishing that there are arbitrarily long arithmetic progressions of primes.

1. Introduction and history

This is a description of recent work of the author and Terence Tao [**GTc**] on primes in arithmetic progression. It is based on seminars given for a general mathematical audience in a variety of institutions in the UK, France, the Czech Republic, Canada and the US.

Perhaps curiously, the order of presentation is much closer to the order in which we discovered the various ingredients of the argument than it is to the layout in [**GTc**]. We hope that both expert and lay readers might benefit from contrasting this account with [**GTc**] as well as the expository accounts by Kra [**Kra06**] and Tao [**Tao06a, Tao06b**].

As we remarked, this article is based on lectures given to a general audience. It was often necessary, when giving these lectures, to say things which were not strictly speaking true for the sake of clarity of exposition. We have retained this style here. However, it being undesirable to commit false statements to print, we have added numerous footnotes alerting readers to points where we have oversimplified, and directing them to places in the literature where fully rigorous arguments can be found.

Our result is:

Theorem 1.1 (G.–Tao). *The primes contain arbitrarily long arithmetic progressions.*

Let us start by explaining that the truth of this statement is not in the least surprising. For a start, it is rather easy to write down a progression of five primes (for example $5, 11, 17, 23, 29$), and in 2004 Frind, Jobling and Underwood produced

2000 *Mathematics Subject Classification.* Primary 11N13, Secondary 11B25.

the example

$$56211383760397 + 44546738095860k; \quad k = 0, 1, \ldots, 22.$$

of 23 primes in arithmetic progression. A very crude heuristic model for the primes may be developed based on the prime number theorem, which states that $\pi(N)$, the number of primes less than or equal to N, is asymptotic to $N/\log N$. We may alternatively express this as

$$\mathbb{P}\big(x \text{ is prime} \mid 1 \leqslant x \leqslant N\big) \sim 1/\log N.$$

Consider now the collection of all arithmetic progressions

$$x, x+d, \ldots, x+(k-1)d$$

with $x, d \in \{1, \ldots, N\}$. Select x and d at random from amongst the N^2 possible choices, and write E_j for the event that $x + jd$ is prime, for $j = 0, 1, \ldots, k-1$. The prime number theorem tells us that

$$\mathbb{P}(E_j) \approx 1/\log N.$$

If the events E_j were independent we should therefore have

$$\mathbb{P}(x, x+d, \ldots, x+(k-1)d \text{ are all prime}) = \mathbb{P}\Big(\bigwedge_{j=0}^{k-1} E_j\Big) \approx 1/(\log N)^k.$$

We might then conclude that

$$\#\{x, d \in \{1, \ldots, N\} : x, x+d, \ldots, x+(k-1)d \text{ are all prime }\} \approx \frac{N^2}{(\log N)^k}.$$

For fixed k, and in fact for k nearly as large as $2\log N/\log\log N$, this is an increasing function of N. This suggests that there are infinitely many k-term arithmetic progressions of primes for any fixed k, and thus arbitrarily long such progressions.

Of course, the assumption that the events E_j are independent was totally unjustified. If E_0, E_1 and E_2 all hold then one may infer that x is odd and d is even, which increases the chance that E_3 also holds by a factor of two. There are, however, more sophisticated heuristic arguments available, which take account of the fact that the primes $> q$ fall only in those residue classes $a (\operatorname{mod} q)$ with a coprime to q. There are very general conjectures of Hardy-Littlewood which derive from such heuristics, and a special case of these conjectures applies to our problem. It turns out that the extremely naïve heuristic we gave above only misses the mark by a constant factor:

Conjecture 1.2 (Hardy-Littlewood conjecture on k-term APs). *For each k we have*

$$\#\{x, d \in \{1, \ldots, N\} : x, x+d, \ldots, x+(k-1)d \text{ are all prime }\} = \frac{\gamma_k N^2}{(\log N)^k}(1+o(1)),$$

where

$$\gamma_k = \prod_p \alpha_p^{(k)}$$

is a certain product of "local densities" which is rapidly convergent and positive.

We have

$$\alpha_p^{(k)} = \begin{cases} \frac{1}{p}\left(\frac{p}{p-1}\right)^{k-1} & \text{if } p \leqslant k \\ \left(1-\frac{k-1}{p}\right)\left(\frac{p}{p-1}\right)^{k-1} & \text{if } p \geqslant k. \end{cases}$$

In particular we compute[1]

$$\gamma_3 = 2\prod_{p\geqslant 3}\left(1 - \frac{1}{(p-1)^2}\right) \approx 1.32032$$

and

$$\gamma_4 = \frac{9}{2}\prod_{p\geqslant 5}\left(1 - \frac{3p-1}{(p-1)^3}\right) \approx 2.85825.$$

What we actually prove is a somewhat more precise version of Theorem 1.1, which gives a lower bound falling short of the Hardy-Littlewood conjecture by just a constant factor.

THEOREM 1.3 (G.–Tao). *For each $k \geqslant 3$ there is a constant $\gamma'_k > 0$ such that*

$$\#\{x, d \in \{1, \dots, N\} : x, x+d, \dots, x+(k-1)d \text{ are all prime }\} \geqslant \frac{\gamma'_k N^2}{(\log N)^k}$$

for all $N > N_0(k)$.

The value of γ'_k we obtain is very small indeed, especially for large k.

Let us conclude this introduction with a little history of the problem. Prior to our work, the conjecture of Hardy-Littlewood was known only in the case $k = 3$, a result due to Van der Corput [**vdC39**] (see also [**Cho44**]) in 1939. For $k \geqslant 4$, even the existence of infinitely many k-term progressions of primes was not previously known. A result of Heath-Brown from 1981 [**HB81**] comes close to handling the case $k = 4$; he shows that there are infinitely many 4-tuples $q_1 < q_2 < q_3 < q_4$ in arithmetic progression, where three of the q_i are prime and the fourth is either prime or a product of two primes. This has been described as "infinitely many $3\frac{1}{2}$-term arithmetic progressions of primes".

2. The relative Szemerédi strategy

A number of people have noted that [**GTc**] manages to avoid using any deep facts about the primes. Indeed the only serious number-theoretical input is a zero-free region for ζ of "classical type", and this was known to Hadamard and de la Vallée Poussin over 100 years ago. Even this is slightly more than absolutely necessary; one can get by with the information that ζ has an isolated pole at 1 [**Taoa**].

Our main advance, then, lies not in our understanding of the primes but rather in what we can say about *arithmetic progressions*. Let us begin this section by telling a little of the story of the study of arithmetic progressions from the combinatorial point of view of Erdős and Turán [**ET36**].

[1]For a tabulation of values of γ_k, $3 \leqslant k \leqslant 20$, see [**GH79**]. As $k \to \infty$, $\log \gamma_k \sim k \log\log k$.

Definition 2.1. Fix an integer $k \geqslant 3$. We define $r_k(N)$ to be the largest cardinality of a subset $A \subseteq \{1, \ldots, N\}$ which does not contain k distinct elements in arithmetic progression.

Erdős and Turán asked simply: what is $r_k(N)$? To this day our knowledge on this question is very unsatisfactory, and in particular we do not know the answer to

Question 2.2. Is it true that $r_k(N) < \pi(N)$ for $N > N_0(k)$?

If this is so then the primes contain k-term arithmetic progressions on density grounds alone, irrespective of any additional structure that they might have. I do not know of anyone who seriously doubts the truth of this conjecture, and indeed all known lower bounds for $r_k(N)$ are much smaller than $\pi(N)$. The most famous such bound is Behrend's assertion [**Beh46**] that

$$r_3(N) \gg Ne^{-c\sqrt{\log N}};$$

slightly superior lower bounds are known for $r_k(N)$, $k \geqslant 4$ (cf. [**ŁL, Ran61**]).

The question of Erdős and Turán became, and remains, rather notorious for its difficulty. It soon became clear that even seemingly modest bounds should be regarded as great achievements in combinatorics. The first really substantial advance was made by Klaus Roth, who proved

Theorem 2.3 (Roth, [**Rot53**]). *We have* $r_3(N) \ll N(\log\log N)^{-1}$.

The key feature of this bound is that $\log\log N$ tends to infinity with N, albeit slowly[2]. This means that if one fixes some small positive real number, such as 0.0001, and then takes a set $A \subseteq \{1, \ldots, N\}$ containing at least $0.0001N$ integers, then provided N is sufficiently large this set A will contain three distinct elements in arithmetic progression.

The generalisation of this statement to general k remained unproven until Szemerédi clarified the issue in 1969 for $k = 4$ and then in 1975 for general k. His result is one of the most celebrated in combinatorics.

Theorem 2.4 (Szemerédi [**Sze69, Sze75**]). *We have* $r_k(N) = o(N)$ *for any fixed* $k \geqslant 3$.

Szemerédi's theorem is one of many in this branch of combinatorics for which the bounds, if they are ever worked out, are almost unimaginably weak. Although it is in principle possible to obtain an explicit function $\omega_k(N)$, tending to zero as $N \to \infty$, for which

$$r_k(N) \leqslant \omega_k(N)N,$$

to my knowledge no-one has done so. Such a function would certainly be worse than $1/\log_* N$ (the number of times one must apply the log function to N in order to get a number less than 2), and may even be slowly-growing compared to the inverse of the Ackermann function.

The next major advance in the subject was another proof of Szemerédi's theorem by Furstenberg [**Fur77**]. Furstenberg used methods of ergodic theory, and

[2]cf. the well-known quotation "$\log\log\log N$ has been proved to tend to infinity with N, but has never been observed to do so".

his argument is relatively short and conceptual. The methods of Furstenberg have proved very amenable to generalisation. For example in [**BL96**] Bergelson and Leibman proved a version of Szemerédi's theorem in which arithmetic progressions are replaced by more general configurations $(x + p_1(d), \ldots, x + p_k(d))$, where the p_i are polynomials with $p_i(\mathbb{Z}) \subseteq \mathbb{Z}$ and $p_i(0) = 0$. A variety of multidimensional versions of the theorem are also known. A significant drawback[3] of Furstenberg's approach is that it uses the axiom of choice, and so does not give *any* explicit function $\omega_k(N)$.

Rather recently, Gowers [**Gow98, Gow01**] made a major breakthrough in giving the first "sensible" bounds for $r_k(N)$.

Theorem 2.5 (Gowers). *Let $k \geqslant 3$ be an integer. Then there is a constant $c_k > 0$ such that*

$$r_k(N) \ll N(\log \log N)^{-c_k}.$$

This is still a long way short of the conjecture that $r_k(N) < \pi(N)$ for N sufficiently large. However, in addition to coming much closer to this bound than any previous arguments, Gowers succeeded in introducing methods of harmonic analysis to the problem for the first time since Roth. Since harmonic analysis (in the form of the circle method of Hardy and Littlewood) has been the most effective tool in tackling additive problems involving the primes, it seems fair to say that it was the work of Gowers which first gave us hope of tackling long progressions of primes. The ideas of Gowers will feature fairly substantially in this exposition, but in our paper [**GTc**] much of what is done is more in the ergodic-theoretic spirit of Furstenberg and of more recent authors in that area such as Host–Kra [**HK05**] and Ziegler [**Zie**].

To conclude this discussion of Szemerédi's theorem we mention a variant of it which is far more useful in practice. This applies to *functions*[4] $f : \mathbb{Z}/N\mathbb{Z} \to [0, 1]$ rather than just to (characteristic functions of) sets. It also guarantees *many* arithmetic progressions of length k. This version does, however, follow from the earlier formulation by some fairly straightforward averaging arguments due to Varnavides [**Var59**].

Proposition 2.6 (Szemerédi's theorem, II). *Let $k \geqslant 3$ be an integer, and let $\delta \in (0, 1]$ be a real number. Then there is a constant $c(k, \delta) > 0$ such that for any function $f : \mathbb{Z}/N\mathbb{Z} \to [0, 1]$ with $\mathbb{E}f = \delta$ we have the bound*[5]

$$\mathbb{E}_{x,d \in \mathbb{Z}/N\mathbb{Z}} f(x)f(x + d) \ldots f(x + (k - 1)d) \geqslant c(k, \delta).$$

We do not, in [**GTc**], prove any new bounds for $r_k(N)$. Our strategy is to prove a *relative Szemerédi theorem.* To describe this we consider, for brevity of exposition, only the case $k = 4$. Consider the following table.

[3] A discrete analogue of Furstenberg's argument has now been found by Tao [**Taob**]. It does give an explicit function $\omega_k(N)$, but once again it tends to zero incredibly slowly.

[4] When discussing additive problems it is often convenient to work in the context of a finite abelian group G. For problems involving $\{1, \ldots, N\}$ there are various technical tricks which allow one to work in $\mathbb{Z}/N'\mathbb{Z}$, for some $N' \approx N$. In this expository article we will not bother to distinguish between $\{1, \ldots, N\}$ and $\mathbb{Z}/N\mathbb{Z}$. For examples of the technical trickery required here, see [**GTc**, Definition 9.3], or the proof of Theorem 2.6 in [**Gow01**].

[5] We use this very convenient conditional expectation notation repeatedly. $\mathbb{E}_{x \in A} f(x)$ is defined to equal $|A|^{-1} \sum_{x \in A} f(x)$.

Szemerédi	Relative Szemerédi
$\{1,\dots,N\}$	?
$A \subseteq \{1,\dots,N\}$ $\lvert A\rvert \geqslant 0.0001N$	$\mathcal{P}_N$ $=$ primes $\leqslant N$
Szemerédi's theorem: A contains many 4-term APs.	Green–Tao theorem: $\mathcal{P}_N$ contains many 4-term APs.

On the left-hand side of this table is Szemerédi's theorem for progressions of length 4, stated as the result that a set $A \subseteq \{1,\dots,N\}$ of density 0.0001 contains many 4-term APs if N is large enough. On the right is the result we wish to prove. Only one thing is missing: we must find an object to play the rôle of $\{1,\dots,N\}$. We might try to place the primes inside some larger set $\mathcal{P}'_N$ in such a way that $|\mathcal{P}_N| \geqslant 0.0001|\mathcal{P}'_N|$, and hope to prove an analogue of Szemerédi's theorem for $\mathcal{P}'_N$.

A natural candidate for $\mathcal{P}'_N$ might be the set of *almost primes*; perhaps, for example, we could take $\mathcal{P}'_N$ to be the set of integers in $\{1,\dots,N\}$ with at most 100 prime factors. This would be consistent with the intuition, coming from sieve theory, that almost primes are much easier to deal with than primes. It is relatively easy to show, for example, that there are long arithmetic progressions of almost primes [**Gro80**].

This idea does not quite work, but a variant of it does. Instead of a *set* $\mathcal{P}'_N$ we instead consider what we call a *measure*[6] $\nu : \{1,\dots,N\} \to [0,\infty)$. Define the *von Mangoldt function* Λ by

$$\Lambda(n) := \begin{cases} \log p & \text{if } n = p^k \text{ is prime} \\ 0 & \text{otherwise.} \end{cases}$$

The function Λ is a weighted version of the primes; note that the prime number theorem is equivalent to the fact that $\mathbb{E}_{1\leqslant n\leqslant N}\Lambda(n) = 1 + o(1)$. Our measure ν will satisfy the following two properties.

(i) (ν majorises the primes) We have $\Lambda(n) \leqslant 10000\nu(n)$ for all $1 \leqslant n \leqslant N$.
(ii) (primes sit inside ν with positive density) We have $\mathbb{E}_{1\leqslant n\leqslant N}\nu(n) = 1 + o(1)$.

These two properties are very easy to satisfy, for example by taking $\nu = \Lambda$, or by taking ν to be a suitably normalised version of the almost primes. Remember, however, that we intend to prove a Szemerédi theorem relative to ν. In order to do that it is reasonable to suppose that ν will need to meet more stringent conditions. The conditions we use in [**GTc**] are called the *linear forms condition* and the *correlation condition*. We will not state them here in full generality, referring the reader to [**GTc**, §3] for full details. We remark, however, that verifying these conditions is of the same order of difficulty as obtaining asymptotics for, say,

$$\sum_{n\leqslant N} \nu(n)\nu(n+2).$$

[6]Actually, ν is just a function but we use the term "measure" to distinguish it from other functions appearing in our work.

For this reason there is no chance that we could simply take $\nu = \Lambda$, since if we could do so we would have solved the twin prime conjecture.

We call a measure ν which satisfies the linear forms and correlation conditions *pseudorandom*.

To succeed with the relative Szemerédi strategy, then, our aim is to find a pseudorandom measure ν for which conditions (i) and (ii) and the are satisfied. Such a function[7] comes to us, like the almost primes, from the idea of using a sieve to bound the primes. The particular sieve we had recourse to was the Λ^2-sieve of Selberg. Selberg's great idea was as follows.

Fix a parameter R, and let $\lambda = (\lambda_d)_{d=1}^R$ be any sequence of real numbers with $\lambda_1 = 1$. Then the function

$$\sigma_\lambda(n) := (\sum_{\substack{d|n \\ d \leqslant R}} \lambda_d)^2$$

majorises the primes greater than R. Indeed if $n > R$ is prime then the truncated divisor sum over $d|n$, $d \leqslant R$ contains just one term corresponding to $d = 1$.

Although this works for any sequence λ, some choices are much better than others. If one wishes to minimise

$$\sum_{n \leqslant N} \sigma_\lambda(n)$$

then, provided that R is a bit smaller than $\sqrt{N}$, one is faced with a minimisation problem involving a certain quadratic form in the λ_ds. The optimal weights λ_d^{SEL}, Selberg's weights, have a slightly complicated form, but roughly we have

$$\lambda_d^{\mathrm{SEL}} \approx \lambda_d^{\mathrm{GY}} := \mu(d)\frac{\log(R/d)}{\log R},$$

where $\mu(d)$ is the Möbius function. These weights were considered by Goldston and Yıldırım [**GY**] in some of their work on small gaps between primes (and earlier, in other contexts, by others including Heath-Brown). It seems rather natural, then, to define a function ν by

$$\nu(n) := \begin{cases} \log N & n \leqslant R \\ \dfrac{1}{\log R}\Bigl(\sum\limits_{\substack{d|n \\ d \leqslant R}} \lambda_d^{\mathrm{GY}}\Bigr)^2 & n > R. \end{cases}$$

The weight $1/\log R$ is chosen for normalisation purposes; if $R < N^{1/2-\epsilon}$ for some $\epsilon > 0$ then we have $\mathbb{E}_{1 \leqslant n \leqslant N}\nu(n) = 1 + o(1)$.

One may more-or-less read out of the work of Goldston and Yıldırım a proof of properties (i) and (ii) above, as well as pseudorandomness, for this function ν.

[7] Actually, this is a lie. There is no pseudorandom measure which majorises the primes themselves. One must first use a device known as the W-trick to remove biases in the primes coming from their irregular distribution in residue classes to small moduli. This is discussed in §3.

One requires that $R < N^c$ where c is sufficiently small. These verifications use the classical zero-free region for the ζ-function and classical techniques of contour integration.

Goldston and Yıldırım's work was part of their long-term programme to prove that

$$\liminf_{n\to\infty} \frac{p_{n+1} - p_n}{\log n} = 0, \tag{1}$$

where p_n is the nth prime. We have recently learnt that this programme has been successful. Indeed together with J. Pintz they have used weights coming from a higher-dimensional sieve in order to establish (1). It is certain that without the earlier preprints of Goldston and Yıldırım our work would have developed much more slowly, at the very least.

Let us conclude this section by remarking that ν will not play a great rôle in the subsequent exposition. It plays a substantial rôle in [**GTc**], but in a relatively non-technical exposition like this it is often best to merely remark that the measure ν and the fact that it is pseudorandom is used all the time in proofs of the various statements that we will describe.

3. Progressions of length three and linear bias

Let G be a finite abelian group with cardinality N. If $f_1, \ldots, f_k : G \to \mathbb{C}$ are any functions we write

$$T_k(f_1, \ldots, f_k) := \mathbb{E}_{x,d\in G} f_1(x) f_2(x+d) \ldots f_k(x+(k-1)d)$$

for the normalised count of k-term APs involving the f_i. When all the f_i are equal to some function f, we write

$$T_k(f) := T_k(f, \ldots, f).$$

When f is equal to 1_A, the characteristic function of a set $A \subseteq G$, we write

$$T_k(A) := T_k(1_A) = T_k(1_A, \ldots, 1_A).$$

This is simply the number of k-term arithmetic progressions in the set A, divided by N^2.

Let us begin with a discussion of 3-term arithmetic progressions and the trilinear form T_3. If $A \subseteq G$ is a set, then clearly $T_3(A)$ may vary between 0 (when $A = \emptyset$) and 1 (when $A = G$). If, however, one places some restriction on the cardinality of A then the following question seems natural:

Question 3.1. Let $\alpha \in (0, 1)$, and suppose that $A \subseteq G$ is a set with cardinality αN. What is $T_3(A)$?

To think about this question, we consider some examples.

Example 1 (Random set). Select a set $A \subseteq G$ by picking each element $x \in G$ to lie in A independently at random with probability α. Then with high probability $|A| \approx \alpha N$. Also, if $d \neq 0$, the arithmetic progression $(x, x+d, x+2d)$ lies in G with probability α^3. Thus we expect that $T_3(A) \approx \alpha^3$, and indeed it can be shown using simple large deviation estimates that this is so with high probability.

Write $E_3(\alpha) := \alpha^3$ for the *expected* normalised count of three-term progressions in the random set of Example 1. One might refine Question 3.1 by asking:

QUESTION 3.2. Let $\alpha \in (0, 1)$, and suppose that $A \subseteq G$ is a set with cardinality αN. Is $T_3(A) \approx E_3(\alpha)$?

It turns out that the answer to this question is "no", as the next example illustrates.

Example 2 (Highly structured set, I). Let $G = \mathbb{Z}/N\mathbb{Z}$, and consider the set $A = \{1, \dots, \lfloor \alpha N \rfloor\}$, an interval. It is not hard to check that if $\alpha < 1/2$ then $T_3(A) \approx \frac{1}{4}\alpha^2$, which is much bigger than $E_3(\alpha)$ for small α.

These first two examples do not rule out a positive answer to the following question.

QUESTION 3.3. Let $\alpha \in (0, 1)$, and suppose that $A \subseteq G$ is a set with cardinality αN. Is $T_3(A) \geqslant E_3(\alpha)$?

If this question did have an affirmative answer, the quest for progressions of length three in sets would be a fairly simple one (the primes would trivially contain many three-term progressions on density grounds alone, for example). Unfortunately, there are counterexamples.

Example 3 (Highly structured set, II). Let $G = \mathbb{Z}/N\mathbb{Z}$. Then there are sets $A \subseteq G$ with $|A| = \lfloor \alpha N \rfloor$, yet with $T_3(A) \ll \alpha^{10000}$. We omit the details of the construction, remarking only that such sets can be constructed[8] as unions of intervals of length $\gg_\alpha N$ in $\mathbb{Z}/N\mathbb{Z}$.

Our discussion so far seems to be rather negative, in that our only conclusion is that none of Questions 3.1, 3.2 and 3.3 have particularly satisfactory answers. Note, however, that the three examples we have mentioned are all consistent with the following dichotomy.

DICHOTOMY 3.4 (Randomness vs Structure for 3-term APs). Suppose that $A \subseteq G$ has size αN. Then **either**

- $T_3(A) \approx E_3(\alpha)$ **or**
- A has *structure*.

It turns out that one may clarify, in quite a precise sense, what is meant by *structure* in this context. The following proposition may be proved by fairly straightforward harmonic analysis. We use the Fourier transform on G, which is defined as follows. If $f : G \to \mathbb{C}$ is a function and $\gamma \in \widehat{G}$ a character (i.e., a homomorphism from G to $\mathbb{C}^\times$), then

$$f^\wedge(\gamma) := \mathbb{E}_{x \in G} f(x)\gamma(x).$$

PROPOSITION 3.5 (Too many/few 3APs implies linear bias). *Let $\alpha, \eta \in (0, 1)$. Then there is $c(\alpha, \eta) > 0$ with the following property. Suppose that $A \subseteq G$ is a set with $|A| = \alpha N$, and that*

$$|T_3(A) - E_3(\alpha)| \geqslant \eta.$$

[8]Basically one considers a set $S \subseteq \mathbb{Z}^2$ formed as the product of a Behrend set in $\{1, \dots, M\}$ and the interval $\{1, \dots, L\}$, for suitable M and L, and then one projects this set linearly to $\mathbb{Z}/N\mathbb{Z}$.

Then there is some character $\gamma \in \widehat{G}$ *with the property that*

$$|(1_A - \alpha)^\wedge(\gamma)| \geqslant c(\alpha, \eta).$$

Note that when $G = \mathbb{Z}/N\mathbb{Z}$ every character γ has the form $\gamma(x) = e(rx/N)$. It is the occurrence of the linear function $x \mapsto rx/N$ here which gives us the name *linear bias.*

It is an instructive exercise to compare this proposition with Examples 1 and 2 above. In Example 2, consider the character $\gamma(x) = e(x/N)$. If α is reasonably small then all the vectors $e(x/N)$, $x \in A$, have large positive real part and so when the sum

$$(1_A - \alpha)^\wedge(\gamma) = \mathbb{E}_{x \in \mathbb{Z}/N\mathbb{Z}} \widehat{1}_A(x) e(x/N)$$

is formed there is very little cancellation, with the result that the sum is large.

In Example 1, by contrast, there is (with high probability) considerable cancellation in the sum for $(1_A - \alpha)^\wedge(\gamma)$ for every character γ.

4. Linear bias and the primes

What use is Dichotomy 3.4 for thinking about the primes? One might hope to use Proposition 3.5 in order to count 3-term APs in some set $A \subseteq G$ by showing that A does not have linear bias. One would then know that $T_3(A) \approx E_3(\alpha)$, where $|A| = \alpha N$.

Let us imagine how this might work in the context of the primes. We have the following proposition[9], which is an analogue of Proposition 3.5. In this proposition[10], $\nu : \mathbb{Z}/N\mathbb{Z} \to [0, \infty)$ is the Goldston-Yıldırım measure constructed in §2.

PROPOSITION 4.1. *Let* $\alpha, \eta \in (0, 2]$. *Then there is* $c(\alpha, \eta) > 0$ *with the following propety. Let* $f : \mathbb{Z}/N\mathbb{Z} \to \mathbb{R}$ *be a function with* $\mathbb{E}f = \alpha$ *and such that* $0 \leqslant f(x) \leqslant 10000\nu(x)$ *for all* $x \in \mathbb{Z}/N\mathbb{Z}$, *and suppose that*

$$|T_3(f) - E_3(\alpha)| \geqslant \eta.$$

Then

$$|\mathbb{E}_{x \in \mathbb{Z}/N\mathbb{Z}}(f(x) - \alpha) e(rx/N)| \geqslant c(\alpha, \eta) \tag{2}$$

for some $r \in \mathbb{Z}/N\mathbb{Z}$.

This proposition may be applied with $f = \Lambda$ and $\alpha = 1 + o(1)$. If we could rule out (2), then we would know that $T_3(\Lambda) \approx E_3(1) = 1$, and would thus have an asymptotic for 3-term progressions of primes.

[9]There are two ways of proving this proposition. One uses classical harmonic analysis. For pointers to such a proof, which would involve establishing an L^p-restriction theorem for ν for some $p \in (2, 3)$, we refer the reader to [**GT06**]. This proof uses more facts about ν than mere pseudorandomness. Alternatively, the result may be deduced from Proposition 3.5 by a transference principle using the machinery of [**GTc**, §6–8]. For details of this approach, which is far more amenable to generalisation, see [**GTb**]. Note that Proposition 4.1 does not feature in [**GTc**] and is stated here for pedagogical reasons only.

[10]Recall that we are being very hazy in distinguishing between $\{1, \dots, N\}$ and $\mathbb{Z}/N\mathbb{Z}$.

Sadly, (2) does hold. Indeed if N is even and $r = N/2$ then, observing that most primes are odd, it is easy to confirm that

$$\mathbb{E}_{x \in \mathbb{Z}/N\mathbb{Z}}(\Lambda(x) - 1)e(rx/N) = -1 + o(1).$$

That is, the primes *do* have linear bias.

Fortunately, it is possible to modify the primes so that they have no linear bias using a device that we refer to as the W-trick. We have remarked that most primes are odd, and that as a result $\Lambda - 1$ has considerable linear bias. However, if one takes the odd primes

$$3, 5, 7, 11, 13, 17, 19, \ldots$$

and then rescales by the map $x \mapsto (x-1)/2$, one obtains the set

$$1, 2, 3, 5, 6, 8, 9, \ldots$$

which does not have substantial $(\bmod 2)$ bias (this is a consequence of the fact that there are roughly the same number of primes congruent to 1 and $3 (\bmod 4)$). Furthermore, if one can find an arithmetic progression of length k in this set of rescaled primes, one can certainly find such a progression in the primes themselves. Unfortunately this set of rescaled primes still has linear bias, because it contains only one element $\equiv 1 (\bmod 3)$. However, a similar rescaling trick may be applied to remove this bias too, and so on.

Here, then, is the W-trick. Take a slowly growing function $w(N) \to \infty$, and set $W := \prod_{p < w(N)} p$. Define the rescaled von Mangoldt function $\widetilde{\Lambda}$ by

$$\widetilde{\Lambda}(n) := \frac{\phi(W)}{W}\Lambda(Wn + 1).$$

The normalisation has been chosen so that $\mathbb{E}\widetilde{\Lambda} = 1 + o(1)$. $\widetilde{\Lambda}$ does not have substantial bias in any residue class to modulus $q < w(N)$, and so there is at least hope of applying a suitable analogue of Proposition 4.1 to it.

Now it is a straightforward matter to define a new pseudorandom measure $\widetilde{\nu}$ which majorises $\widetilde{\Lambda}$. Specifically, we have

(i) ($\widetilde{\nu}$ majorises the modified primes) We have $\widetilde{\lambda}(n) \leqslant 10000\widetilde{\nu}(n)$ for all $1 \leqslant n \leqslant N$.
(ii) (modified primes sit inside $\widetilde{\nu}$ with positive density) We have $\mathbb{E}_{1 \leqslant n \leqslant N}\widetilde{\nu}(n) = 1 + o(1)$.

The following modified version of Proposition 4.1 may be proved:

PROPOSITION 4.2. *Let $\alpha, \eta \in (0, 2]$. Then there is $c(\alpha, \eta) > 0$ with the following property. Let $f : \mathbb{Z}/N\mathbb{Z} \to \mathbb{R}$ be a function with $\mathbb{E}f = \alpha$ and such that $0 \leqslant f(x) \leqslant 10000\widetilde{\nu}(x)$ for all $x \in \mathbb{Z}/N\mathbb{Z}$, and suppose that*

$$|T_3(f) - E_3(\alpha)| \geqslant \eta.$$

Then

$$|\mathbb{E}_{x \in \mathbb{Z}/N\mathbb{Z}}(f(x) - \alpha)e(rx/N)| \geqslant c(\alpha, \eta) \tag{3}$$

for some $r \in \mathbb{Z}/N\mathbb{Z}$. □

This may be applied with $f = \widetilde{\Lambda}$ and $\alpha = 1 + o(1)$. Now, however, condition (3) does not so obviously hold. In fact, one has the estimate

$$\sup_{r \in \mathbb{Z}/N\mathbb{Z}} |\mathbb{E}_{x \in \mathbb{Z}/N\mathbb{Z}} (\widetilde{\Lambda}(x) - 1) e(rx/N)| = o(1). \tag{4}$$

To prove this requires more than simply the good distribution of $\widetilde{\Lambda}$ in residue classes to small moduli. It is, however, a fairly standard consequence of the Hardy-Littlewood circle method as applied to primes by Vinogradov. In fact, the whole theme of linear bias in the context of additive questions involving primes may be traced back to Hardy and Littlewood.

Proposition 4.2 and (4) imply that $T_3(\widetilde{\Lambda}) \approx E_3(1) = 1$. Thus there are infinitely many three-term progressions in the modified (W-tricked) primes, and hence also in the primes themselves[11].

5. Progressions of length four and quadratic bias

We return now to the discussion of §3. There we were interested in counting 3-term arithmetic progressions in a set $A \subseteq G$ with cardinality αN. In this section our interest will be in 4-term progressions.

Suppose then that $A \subseteq G$ is a set, and recall that

$$T_4(A) := \mathbb{E}_{x,d \in G} 1_A(x) 1_A(x+d) 1_A(x+2d) 1_A(x+3d)$$

is the normalised count of four-term arithmetic progressions in A. One may, of course, ask the analogue of Question 3.1:

QUESTION 5.1. Let $\alpha \in (0,1)$, and suppose that $A \subseteq G$ is a set with cardinality αN. What is $T_4(A)$?

Examples 1,2 and 3 make perfect sense here, and we see once again that there is no immediately satisfactory answer to Question 5.1. With high probability the random set of Example 1 has about $E_4(\alpha) := \alpha^4$ four-term APs, but there are structured sets with substantially more or less than this number of APs. As in §3, these examples are consistent with a dichotomy of the following type:

DICHOTOMY 5.2 (Randomness vs Structure for 4-term APs). Suppose that $A \subseteq G$ has size αN. Then **either**

- $T_4(A) \approx E_4(\alpha)$ **or**
- A has *structure*.

Taking into account the three examples we have so far, it is quite possible that this dichotomy takes *exactly* the form of that for 3-term APs. That is to say "A has structure" could just mean that A has linear bias:

QUESTION 5.3. Let $\alpha, \eta \in (0,1)$. Suppose that $A \subseteq G$ is a set with $|A| = \alpha N$, and that

$$|T_4(A) - E_4(\alpha)| \geqslant \eta.$$

[11] In fact, this analysis does not have to be pushed much further to get a proof of Conjecture 1.2 for $k = 3$, that is to say an asymptotic for 3-term progressions of primes. One simply counts progressions $x, x+d, x+2d$ by splitting into residue classes $x \equiv b \pmod W$, $d \equiv b' \pmod W$ and using a simple variant of Proposition 4.2.

Must there exist some $c = c(\alpha, \eta) > 0$ and some character $\gamma \in \widehat{G}$ with the property that

$$|(1_A - \alpha)^\wedge(\gamma)| \geqslant c(\alpha, \eta)?$$

That the answer to this question is no, together with the nature of the counterexample, is one of the key themes of our whole work. This phenomenon was discovered, in the context of ergodic theory, by Furstenberg and Weiss [**FW96**] and then again, in the discrete setting, by Gowers [**Gow01**].

Example 4 (Quadratically structured set). Define $A \subseteq \mathbb{Z}/N\mathbb{Z}$ to be the set of all x such that $x^2 \in [-\alpha N/2, \alpha N/2]$. It is not hard to check using estimates for Gauss sums that $|A| \approx \alpha N$, and also that

$$\sup_{r \in \mathbb{Z}/N\mathbb{Z}} |\mathbb{E}_{x \in \mathbb{Z}/N\mathbb{Z}}(1_A(x) - \alpha)e(rx/N)| = o(1),$$

that is to say A does not have linear bias. (In fact, the largest Fourier coefficient of $1_A - \alpha$ is just $N^{-1/2+\epsilon}$.) Note, however, the relation

$$x^2 - 3(x+d)^2 + 3(x+2d)^2 + (x+3d)^2 = 0,$$

valid for arbitrary $x, d \in \mathbb{Z}/N\mathbb{Z}$. This means that if $x, x+d, x+2d \in A$ then automatically we have

$$(x+3d)^2 \in [-7\alpha N/2, 7\alpha N/2].$$

It seems, then, that if we know that $x, x+d$ and $x+2d$ lie in A there is a very high chance that $x+3d$ also lies in A. This observation may be made rigorous, and it does indeed transpire that $T_4(A) \geqslant c\alpha^3$.

How can one rescue the randomness-structure dichotomy in the light of this example? Rather remarkably, "quadratic" examples like Example 4 are the *only* obstructions to having $T_4(A) \approx E_4(\alpha)$. There is an analogue of Proposition 3.5 in which characters γ are replaced by "quadratic" objects[12].

PROPOSITION 5.4 (Too many/few 4APs implies quadratic bias). *Let $\alpha, \eta \in (0,1)$. Then there is $c(\alpha, \eta) > 0$ with the following property. Suppose that $A \subseteq G$ is a set with $|A| = \alpha N$, and that*

$$|T_4(A) - E_4(\alpha)| \geqslant \eta.$$

Then there is some quadratic object $q \in \mathcal{Q}(\kappa)$, where $\kappa \geqslant \kappa_0(\alpha, \eta)$, with the property that

$$|\mathbb{E}_{x \in G}(1_A(x) - \alpha)q(x)| \geqslant c(\alpha, \eta).$$

We have not, of course, said what we mean by the set of *quadratic objects* $\mathcal{Q}(\kappa)$. To give the exact definition, even for $G = \mathbb{Z}/N\mathbb{Z}$, would take us some time, and we refer to [**GTa**] for a full discussion. In the light of Example 4, the reader will not be surprised to hear that quadratic exponentials such as $q(x) = e(x^2/N)$ are members of $\mathcal{Q}$. However, $\mathcal{Q}(\kappa)$ also contains rather more obscure objects[13] such as

$$q(x) = e(x\sqrt{2}\{x\sqrt{3}\})$$

[12]The proof of this proposition is long and difficult and may be found in [**GTa**]. It is heavily based on the arguments of Gowers [**Gow98, Gow01**]. This proposition has no place in [**GTc**], and it is once again included for pedagogical reasons only. It played an important rôle in the development of our ideas.

[13]We are thinking of these as defined on $\{1, \dots, N\}$ rather than $\mathbb{Z}/N\mathbb{Z}$.

and
$$q(x) = e(x\sqrt{2}\{x\sqrt{3}\} + x\sqrt{5}\{x\sqrt{7}\} + x\sqrt{11}),$$
where $\{x\}$ denotes fractional part. The parameter κ governs the complexity of the expressions which are allowed: smaller values of κ correspond to more complicated expressions. The need to involve these "generalised" quadratics in addition to "genuine" quadratics such as $e(x^2/N)$ was first appreciated by Furstenberg and Weiss in the ergodic theory context, and the matter also arose in the work of Gowers.

6. Quadratic bias and the primes

It is possible to prove[14] a version of Proposition 5.4 which might be applied to primes. The analogue of Proposition 4.1 is true but not useful, for the same reason as before: the primes exhibit significant bias in residue classes to small moduli. As before, this bias may be removed using the W-trick.

PROPOSITION 6.1. *Let $\alpha, \eta \in (0, 2]$. Then there are $c(\alpha, \eta)$ and $\kappa_0(\alpha, \eta) > 0$ with the following propety. Let $f : \mathbb{Z}/N\mathbb{Z} \to \mathbb{R}$ be a function with $\mathbb{E}f = \alpha$ and such that $0 \leqslant f(x) \leqslant 10000\widetilde{\nu}(x)$ for all $x \in \mathbb{Z}/N\mathbb{Z}$, and suppose that*
$$|T_4(f) - E_4(\alpha)| \geqslant \eta.$$
Then we have
$$|\mathbb{E}_{x\in\mathbb{Z}/N\mathbb{Z}}(f(x) - \alpha)q(x)| \geqslant c(\alpha, \eta) \qquad (5)$$
for some quadratic object $q \in \mathcal{Q}(\kappa)$ with $\kappa \geqslant \kappa_0(\alpha, \eta)$.

One is interested, of course, in applying this with $f = \widetilde{\Lambda}$. If we could verify that (5) does not hold, that is to say the primes do not have quadratic bias, then it would follow that $T_4(\widetilde{\Lambda}) \approx E_4(1) = 1$. This means that the modified (W-tricked) primes have many 4-term progressions, and hence so do the primes themselves[15].

One wishes to show, then, that for fixed κ one has
$$\sup_{q\in\mathcal{Q}(\kappa)} |\mathbb{E}_{x\in\mathbb{Z}/N\mathbb{Z}}(\widetilde{\Lambda}(x) - 1)q(x)| = o(1). \qquad (6)$$
Such a result is certainly not a consequence of the classical Hardy-Littlewood circle method[16]. Generalised quadratic phases such as $q(x) = e(x\sqrt{2}\{x\sqrt{3}\})$ are particularly troublesome. Although we do now have a proof of (6), it is very long and complicated. See [**GTd**] for details.

In the next section we explain how our original paper [**GTc**] managed to avoid the need to prove (6).

[14]As with Proposition 4.1, this proposition does not appear in [**GTc**], though it motivated our work and a variant of it is used in our later work [**GTb**]. Once again there are two proofs. One is based on a combination of harmonic analysis and the work of Gowers, is difficult, and requires more facts about ν than mere pseudorandomness. This was our original argument. It is also possible to proceed by a transference principle, deducing the result from Proposition 5.4 using the machinery of [**GTc**, §6–8]. See [**GTb**] for more details.

[15]in fact, just as for progressions of length 3, this allows one to obtain a proof of Conjecture 1.2 for $k = 4$, that is to say an asymptotic for prime progressions of length 4. See [**GTb**].

[16]Though reasonably straightforward extensions of the circle method do permit one to handle genuine quadratic phases such as $q(x) = e(x^2\sqrt{2})$.

7. Quotienting out the bias - the energy increment argument

Our paper [**GTc**] failed to rule out the possibility that $\widetilde{\Lambda} - 1$ correlates with some quadratic function $q \in \mathcal{Q}(\kappa)$. For that reason we did not obtain a proof of Conjecture 1.2, getting instead the weaker statement of Theorem 1.3. In this section[17] we outline the *energy increment* argument of [**GTc**], which allowed us to deal with the possibility that $\widetilde{\Lambda} - 1$ does correlate with a quadratic.

We begin by writing

$$\widetilde{\Lambda} := 1 + f_0. \tag{7}$$

Proposition 6.1 tells us that $T_4(\widetilde{\Lambda}) \approx 1$, unless f_0 correlates with some quadratic $q_0 \in \mathcal{Q}$. Suppose, then, that

$$|\mathbb{E}_{x \in \mathbb{Z}/N\mathbb{Z}} f_0(x) q_0(x)| \geqslant \eta.$$

Then we revise the decomposition (7) to

$$\widetilde{\Lambda} := F_1 + f_1, \tag{8}$$

where F_1 is a function defined using q_0. In fact, F_1 is basically the average of $\widetilde{\Lambda}$ over approximate level sets of q_0. That is, one picks an appropriate scale[18] $\epsilon = 1/J$, and then defines

$$F_1 := \mathbb{E}(\widetilde{\Lambda}|\mathcal{B}_0),$$

where $\mathcal{B}_0$ is the σ-algebra generated by the sets $x : q_0(x) \in [j/J, (j+1)/J)$.

A variant of Proposition 6.1 implies a new dichotomy: either $T_4(\widetilde{\Lambda}) \approx T_4(F_1)$, or else f_1 correlates with some quadratic $q_1 \in \mathcal{Q}$. Suppose then that

$$|\mathbb{E}_{x \in \mathbb{Z}/N\mathbb{Z}} f_1(x) q_1(x)| \geqslant \eta.$$

We then further revise the decomposition (8) to

$$\widetilde{\Lambda} := F_2 + f_2,$$

where now

$$F_2 := \mathbb{E}(\widetilde{\Lambda}|\mathcal{B}_0 \wedge \mathcal{B}_1),$$

the σ-algebra being defined by the joint level sets of q_0 and q_1.

We repeat this process. It turns out that the algorithm stops in a finite number s of steps, bounded in terms of η. The reason for this is that each new assumption

$$|\mathbb{E}_{x \in \mathbb{Z}/N\mathbb{Z}} f_j(x) q_j(x)| \geqslant \eta$$

[17]The exposition in this section is rather looser than in other sections. To make the argument rigorous, one must introduce various technical devices, such as the exceptional sets which feature in [**GTc**, §7,8]. We are also being rather vague about the meaning of terms such as "correlate", and the parameter κ involved in the definition of quadratic object. Note also that the argument of [**GTc**] uses *soft* quadratic objects rather than the genuine ones which we are discussing here for expositional purposes. See §8 for a brief discussion of these.

[18]As we remarked, the actual situation is more complicated. There is an averaging over possible decompositions of $[0, 1]$ into intervals of length ϵ, to ensure that the level sets look pleasant. There is also a need to consider exceptional sets, which unfortunately makes the argument look rather messy.

implies an increased lower bound for the *energy* of $\widetilde{\Lambda}$ relative to the σ-algebra $\mathcal{B}_0 \wedge \cdots \wedge \mathcal{B}_{j-1}$, that is to say the quantity

$$E_j := \|\mathbb{E}(\widetilde{\Lambda}|\mathcal{B}_0 \wedge \cdots \wedge \mathcal{B}_{j-1})\|_2.$$

The fact that $\widetilde{\Lambda}$ is dominated by $\widetilde{\nu}$ does, however, provide a universal bound for the energy, by dint of the evident inequality

$$E_j \leqslant 10000\|\mathbb{E}(\widetilde{\nu}|\mathcal{B}_0 \wedge \cdots \wedge \mathcal{B}_{j-1})\|_2.$$

The pseudorandomness of $\widetilde{\nu}$ allows one[19] to bound the right-hand side here by $O(1)$.

At termination, then, we have a decomposition

$$\widetilde{\Lambda} = F_s + f_s,$$

where

$$\sup_{q \in \mathcal{Q}} |\mathbb{E}_{x \in \mathbb{Z}/N\mathbb{Z}} f_s(x) q(x)| < \eta, \tag{9}$$

and F_s is defined by

$$F_s := \mathbb{E}(\widetilde{\Lambda}|\mathcal{B}_0 \wedge \mathcal{B}_1 \wedge \cdots \wedge \mathcal{B}_{s-1}). \tag{10}$$

A variant of Proposition 6.1 implies, together with (9), that

$$T_4(\widetilde{\Lambda}) \approx T_4(F_s). \tag{11}$$

What can be said about $T_4(F_s)$? Let us note two things about the function F_s. First of all the definition (10) implies that

$$\mathbb{E}F_s = \mathbb{E}\widetilde{\Lambda} = 1 + o(1). \tag{12}$$

Secondly, F_s is not too large pointwise; this is again an artifact of $\widetilde{\Lambda}$ being dominated by $\widetilde{\nu}$. We have, of course,

$$\|F_s\|_\infty = \|\mathbb{E}(\widetilde{\Lambda}|\mathcal{B}_0 \wedge \mathcal{B}_1 \wedge \cdots \wedge \mathcal{B}_{s-1})\|_\infty \leqslant 10000\|\mathbb{E}(\widetilde{\nu}|\mathcal{B}_0 \wedge \mathcal{B}_1 \wedge \cdots \wedge \mathcal{B}_{s-1})\|_\infty.$$

The pseudorandomness of $\widetilde{\nu}$ can again be used[20] to show that the right-hand side here is $10000 + o(1)$; that is,

$$\|F_s\|_\infty \leqslant 10000 + o(1). \tag{13}$$

The two properties (12) and (13) together mean that F_s behaves rather like the characteristic function of a subset of $\mathbb{Z}/N\mathbb{Z}$ with density at least $1/10000$. This suggests the use of Szemerédi's theorem to bound $T_4(F_s)$ below. The formulation of that theorem given in Proposition 2.6 applies to exactly this situation, and it tells us that

$$T_4(F_s) > c$$

for some absolute constant $c > 0$. Together with (11) this implies a similar lower bound for $T_4(\widetilde{\Lambda})$, which means that there are infinitely many 4-term arithmetic progressions of primes.

---

[19]This deduction uses the machinery of the Gowers U^3-norm, which we do not discuss in this survey. See [**GTc**, §6] for a full discussion. Of specific relevance is the fact that $\|\widetilde{\nu}\|_{U^3} = o(1)$, which is a consequence of the pseudorandomness of $\widetilde{\nu}$.

[20]Again, the machinery of the Gowers U^3-norm is used.

Let us conclude this section with an overview of what it is we have proved. The only facts about $\widetilde{\Lambda}$ that we used were that it is dominated pointwise by $10000\widetilde{\nu}$, and that $\mathbb{E}\widetilde{\Lambda}$ is not too small. The argument sketched above applies equally well in the general context of functions with these properties, and in the context of an arbitrary pseudorandom measure (not just the Goldston-Yıldırım measure).

PROPOSITION 7.1 (Relative Szemerédi Theorem). *Let $\delta \in (0,1]$ be a real number and let ν be a psuedorandom measure. Then there is a constant $c'(4,\delta) > 0$ with the following property. Suppose that $f : \mathbb{Z}/N\mathbb{Z} \to \mathbb{R}$ is a function such that $0 \leqslant f(x) \leqslant \nu(x)$ pointwise, and for which $\mathbb{E}f \geqslant \delta$. Then we have the estimate*

$$T_4(f) \geqslant c'(4,\delta).$$

In [**GTc**] we prove the same[21] theorem for progressions of any length $k \geqslant 3$.

Proposition 7.1 captures the spirit of our argument quite well. We first deal with arithmetic progressions in a rather general context. Only upon completion of that study do we concern ourselves with the primes, and this is simply a matter of constructing an appropriate pseudorandom measure. Note also that Szemerédi's theorem is used as a "black box". We do not need to understand the proof of it, or to have good bounds for it.

Observe that one consequence of Proposition 7.1 is a *Szemerédi theorem relative to the primes*: any subset of the primes with positive relative density contains progressions of arbitrary length. Applying this to the set of primes congruent to $1 \pmod 4$, we see that there are arbitrarily long progressions of numbers which are sums of two squares.

8. Soft obstructions

Readers familiar with [**GTc**] may have been confused by our exposition thus far, since "quadratic objects" play essentially no rôle in that paper. The purpose of this brief section is to explain why this is so, and to provide a bridge between this survey and our paper. Further details and discussion may be found in [**GTc**, §6].

Let us start by recalling §3, where a set of "obstructions" to a set $A \subseteq G$ having roughly $E_3(\alpha)$ three-term APs was obtained. This was just the collection of characters $\gamma \in \widehat{G}$, and we used the term *linear bias* to describe correlation with one of these characters.

Let $f : G \to \mathbb{C}$ be a function with $\|f\|_\infty \leqslant 1$. Now we observe the formula

$$\mathbb{E}_{a,b \in G}\overline{f(x+a)f(x+b)}f(x+a+b) = \sum_{\gamma \in \widehat{G}} |\widehat{f}(\gamma)|^2 \overline{\widehat{f}(\gamma)}\overline{\gamma(x)},$$

which may be verified by straightforward harmonic analysis on G. Coupled with the fact that

$$\sum_{\gamma \in \widehat{G}} |\widehat{f}(\gamma)|^2 \leqslant 1,$$

[21]Note, however, that the definition of pseudorandom measure is strongly dependent on k.

a consequence of Parseval's identity, this means that the[22] "dual function"

$$\mathcal{D}_2 f := \mathbb{E}_{a,b\in G}\overline{f(x+a)f(x+b)}f(x+a+b)$$

can be approximated by the weighted sum of a few characters. Every character is actually equal to a dual function; indeed we clearly have $\mathcal{D}_2(\gamma) = \overline{\gamma}$.

We think of the dual functions $\mathcal{D}_2(f)$ as *soft linear obstructions*. They may be used in the iterative argument of §7 in place of the genuinely linear functions, after one has established certain algebraic closure properties of these functions (see [**GTc**, Proposition 6.2])

The great advantage of these soft obstructions is that it is reasonably obvious how they should be generalised to give objects appropriate for the study of longer arithmetic progressions. We write $\mathcal{D}_3(f)$ for

$$\mathbb{E}_{a,b,c}\overline{f(x+a)f(x+b)f(x+c)}f(x+a+b)f(x+a+c)f(x+b+c)\overline{f(x+a+b+c)}.$$

This is a kind of sum of f over parallelepipeds (minus one vertex), whereas $\mathcal{D}_2(f)$ was a sum over parallelograms (minus one vertex). This we think of as a *soft quadratic obstruction*. Gone are the complications of having to deal with explicit generalised quadratic functions which, rest assured, only become worse when one deals with progressions of length 5 and longer.

The idea of using these soft obstructions came from the ergodic-theory work of Host and Kra [**HK05**], where very similar objects are involved.

We conclude by emphasising that soft obstructions lead to relatively soft results, such as Theorem 1.3. To get a proof of Conjecture 1.2 it will be necessary to return to generalised quadratic functions and their higher-order analogues.

9. Acknowledgements

I would like to thank James Cranch for reading the manuscript and advice on using Mathematica, and Terry Tao for several helpful comments.

References

[Beh46] F. A. Behrend – "On sets of integers which contain no three terms in arithmetical progression", *Proc. Nat. Acad. Sci. U. S. A.* **32** (1946), p. 331–332.

[BL96] V. Bergelson & A. Leibman – "Polynomial extensions of van der Waerden's and Szemerédi's theorems", *J. Amer. Math. Soc.* **9** (1996), no. 3, p. 725–753.

[Cho44] S. Chowla – "There exists an infinity of 3—combinations of primes in A. P", *Proc. Lahore Philos. Soc.* **6** (1944), no. 2, p. 15–16.

[ET36] P. Erdős, & P. Turán – "On some sequences of integers", *J. London Math. Soc.* **11** (1936), p. 261–264.

[Fur77] H. Furstenberg – "Ergodic behavior of diagonal measures and a theorem of Szemerédi on arithmetic progressions", *J. Analyse Math.* **31** (1977), p. 204–256.

[FW96] H. Furstenberg & B. Weiss – "A mean ergodic theorem for $(1/N)\sum_{n=1}^{N} f(T^n x)g(T^{n^2}x)$", in *Convergence in ergodic theory and probability (Columbus, OH, 1993)*, Ohio State Univ. Math. Res. Inst. Publ., vol. 5, de Gruyter, Berlin, 1996, p. 193–227.

[22] The subscript 2 refers to the Gowers U^2-norm, which is relevant to the study of progressions of length 3.

[GH79] E. Grosswald & P. Hagis, Jr. – "Arithmetic progressions consisting only of primes", *Math. Comp.* **33** (1979), no. 148, p. 1343–1352.

[Gow98] W. T. Gowers – "A new proof of Szemerédi's theorem for arithmetic progressions of length four", *Geom. Funct. Anal.* **8** (1998), no. 3, p. 529–551.

[Gow01] ———, "A new proof of Szemerédi's theorem", *GAFA* **11** (2001), p. 465–588.

[Gro80] E. Grosswald – "Arithmetic progressions of arbitrary length and consisting only of primes and almost primes", *J. Reine Angew. Math.* **317** (1980), p. 200–208.

[GTa] B. J. Green & T. C. Tao – "An inverse theorem for the Gowers U^3-norm, with applications", to appear in Proc. Edinbrugh Math. Soc.

[GTb] ———, "Linear equations in primes", `math.NT/0606088`.

[GTc] ———, "The primes contain arbitrarily long arithmetic progressions", to appear in Ann. of Math.

[GTd] ———, "Quadratic uniformity of the Möbius function", `math.NT/0606087`.

[GT06] ———, "Restriction theory of Selberg's sieve, with applications", *J. Théorie des Nombres de Bordeaux* **18** (2006), p. 147–182.

[GY] D. Goldston & C. Y. Yildirim – "Small gaps between primes, I", `math.NT/0504336`.

[HB81] D. R. Heath-Brown – "Three primes and an almost-prime in arithmetic progression", *J. London Math. Soc. (2)* **23** (1981), no. 3, p. 396–414.

[HK05] B. Host & B. Kra – "Nonconventional ergodic averages and nilmanifolds", *Ann. of Math. (2)* **161** (2005), no. 1, p. 397–488.

[Kra06] B. Kra – "The Green-Tao theorem on arithmetic progressions in the primes: an ergodic point of view", *Bull. Amer. Math. Soc. (N.S.)* **43** (2006), no. 1, p. 3–23 (electronic).

[ŁL] I. Łaba & M. Lacey – "On sets of integers not containing long arithmetic progressions", `math.CO/0108155`.

[Ran61] R. A. Rankin – "Sets of integers containing not more than a given number of terms in arithmetical progression", *Proc. Roy. Soc. Edinburgh Sect. A* **65** (1960/1961), p. 332–344 (1960/61).

[Rot53] K. F. Roth – "On certain sets of integers", *J. London Math. Soc.* **28** (1953), p. 104–109.

[Sze69] E. Szemerédi – "On sets of integers containing no four elements in arithmetic progression", *Acta Math. Acad. Sci. Hungar.* **20** (1969), p. 89–104.

[Sze75] ———, "On sets of integers containing no k elements in arithmetic progression", *Acta Arith.* **27** (1975), p. 199–245, Collection of articles in memory of Juriĭ Vladimirovič Linnik.

[Taoa] T. C. Tao – "A note on Goldston-Yıldırım correlation estimates", unpublished.

[Taob] ———, "A quantitative ergodic theory proof of Szemerédi's theorem", preprint.

[Tao06a] ———, "Arithmetic progressions and the primes", *Collectanea Mathematica* **extra volume** (2006), p. 37–88, Proceedings, 7th International Conference on Harmonic Analysis and Partial Differential Equations.

[Tao06b] ———, "Obstructions to uniformity, and arithmetic patterns in the primes", *Quart. J. Pure App. Math.* **2** (2006), p. 199–217, special issue in honour of John H. Coates.

[Var59] P. Varnavides – "On certain sets of positive density", *J. London Math. Soc.* **34** (1959), p. 358–360.

[vdC39] J. G. van der Corput – "Über Summen von Primzahlen und Primzahlquadraten", *Math. Ann.* **116** (1939), p. 1–50.

[Zie] T. Ziegler – "Universal characteristic factors and Furstenberg averages", to appear in J. Amer. Math. Soc.

School of Mathematics, University Walk, Bristol BS8 1TW, England
E-mail address: `b.j.green@bristol.ac.uk`

Clay Mathematics Proceedings
Volume 7, 2007

Heegner points and non-vanishing of Rankin/Selberg L-functions

Philippe Michel and Akshay Venkatesh

ABSTRACT. We discuss the nonvanishing of central values $L(\frac{1}{2}, f \otimes \chi)$, where f is a fixed automorphic form on GL(2) and χ varies through class group characters of an imaginary quadratic field $K = \mathbb{Q}(\sqrt{-D})$, as D varies; we prove results of the nature that at least $D^{1/5000}$ such twists are nonvanishing. We also discuss the related question of the rank of a fixed elliptic curve $E/\mathbb{Q}$ over the Hilbert class field of $\mathbb{Q}(\sqrt{-D})$, as D varies. The tools used are results about the distribution of Heegner points, as well as subconvexity bounds for L-functions.

1. Introduction

The problem of studying the non-vanishing of central values of automorphic L-functions arise naturally in several contexts ranging from analytic number theory, quantum chaos and arithmetic geometry and can be approached by a great variety of methods (ie. via analytic, geometric spectral and ergodic techniques or even a blend of them).

Amongst the many interesting families that may occur, arguably one of the most attractive is the family of (the central values of) *twists by class group characters*: Let f be a modular form on PGL(2) over $\mathbb{Q}$ and K a quadratic field of discriminant D. If χ is a ring class character associated to K, we may form the L-function $L(s, f \otimes \chi)$: the Rankin-Selberg convolution of f with the θ-series $g_\chi(z) = \sum_{\{0\} \neq \mathfrak{a} \subset O_K} \chi(\mathfrak{a}) e(N(\mathfrak{a})z)$. Here g_χ is a holomorphic Hecke-eigenform of weight 1 on $\Gamma_0(D)$ with Nebentypus χ_K and a cusp form iff χ is not a quadratic character[1].

2000 *Mathematics Subject Classification.* Primary 11F66, Secondary 11F67, 11M41.

Key words and phrases. Automorphic L-functions, Central Values, Subconvexity, Equidistribution.

The research of the first author is partially supported by the RMT-network "Arithmetic Algebraic Geometry" and by the "RAP" network of the Région Languedoc-Roussillon.

The second author was supported by the Clay Mathematics Institute and also acknowledges support through NSF grants 02045606 and NSF Grants DMS0111298. He thanks the Institute of Advanced Study for providing excellent working conditions.

[1]Equivalently, one can define $L(s, f \otimes \chi)$ as $L(s, \Pi_f \otimes \chi)$, where Π_f is the base-change to K of the automorphic representation underlying f, and χ is regarded as a character of $\mathbb{A}_K^\times / K^\times$.

We will always assume that the conductor of f is coprime to the discriminant of K. In that case the sign of the functional equation equals $\pm\left(\frac{-D}{N}\right)$, where one takes the $+$ sign in the case when f is Maass, and the $-$ sign if f is weight 2 holomorphic (these are the only cases that we shall consider).

Many lovely results have been proved in this context: we refer the reader to §1.3 for a review of some of these results. A common theme is the use, implicit or explicit, of the equidistribution properties of special points. The purpose of this paper is to give an informal exposition (see §1.1) as well as some new applications of this idea. Since our goal is merely to illustrate what can be obtained along these lines we have not tried to reach the most general results that can be obtained and, in particular, we limit ourselves to the non-vanishing problem for the family of unramified ring class characters of an imaginary quadratic field $K = \mathbb{Q}(\sqrt{-D})$ of large discriminant D.

We prove

THEOREM 1. *Let $f(z)$ be a weight 0, even, Maass (Hecke-eigen) cuspform on the modular surface $X_0(1)$; then, for any $0 < \delta < 1/2700$, one has the lower bound*

$$\left|\{\chi \in \widehat{\mathrm{Cl}_K},\ L(f \otimes \chi, 1/2) \neq 0\}\right| \gg_{\delta,f} D^{\delta}$$

THEOREM 2. *Let q be a prime and $f(z)$ be a holomorphic Hecke-eigen cuspform of weight 2 on $\Gamma_0(q)$ such that q remains inert in K; then, for any $0 < \delta < 1/2700$, one has the lower bound*

$$\left|\{\chi \in \widehat{\mathrm{Cl}_K},\ L(f \otimes \chi, 1/2) \neq 0\}\right| \gg_{\delta,f} D^{\delta}$$

for any $\delta < 1/2700$.

The restriction to either trivial or prime level in the theorems above is merely for simplification (to avoid the occurrence of oldforms in our analysis) and extending these results to more general levels is just a technical matter. Another arguably more interesting generalization consists in considering levels q and quadratic fields K such that the sign of the functional equation is -1: then one expects that the number of χ such that the first derivative $L'(f \otimes \chi, 1/2) \neq 0$ is $\gg D^{\delta}$ for some positive absolute δ. This can be proven along the above lines at least when f is holomorphic of weight 2 by using the Gross/Zagier formulas; the proof however is significantly more difficult and will be dealt with elsewhere; interestingly the proof combines the two types of equidistribution results encountered in the proof of Theorems 1 and 2 above. In the present paper, we give, for the sake of diversity, an entirely different, purely geometric, argument of such a generalization when f corresponds to an elliptic curve. For technical reasons we need to assume a certain hypothesis "$S_{\beta,\theta}$" that guarantees there are enough small split primes in K. This is a fairly common feature of such problems (cf. [**DFI95**], [**EY03**]) and we regard it as almost orthogonal to the main issues we are considering. Given $\theta > 0$ and $\alpha \in]0, 1]$ we consider

HYPOTHESIS $S_{\beta,\theta}$. *The number of primitive[2] integral ideals $\mathfrak{n}$ in O_K with* $\mathrm{Norm}(\mathfrak{n}) \leqslant D^{\theta}$ *is* $\gg D^{\beta\theta}$.

Actually, in a sense it is remarkable that Theorems 1 and 2 above *do not* require such a hypothesis. It should be noted that $S_{\beta,\theta}$ is always true under the generalized

[2]That is, not divisible by any nontrivial ideal of the form (m), with $m \in \mathbb{Z}$.

Lindelöf hypothesis and can be established unconditionally with any $\alpha \in]0, 1/3[$ for those Ds whose largest prime factor is a sufficiently small power of D by the work of Graham/Ringrose [**GR90**](see [**DFI95**] for more details).

THEOREM 3. *Assume $S_{\beta,\theta}$. Let E be an elliptic curve over $\mathbb{Q}$ of squarefree conductor N, and suppose D is odd, coprime to N, and so that all primes dividing N split in the quadratic extension $\mathbb{Q}(\sqrt{-D})$. Then the Mordell-Weil rank of E over the Hilbert class field of $\mathbb{Q}(\sqrt{-D})$ is $\gg_\epsilon D^{\delta-\epsilon}$, where $\delta = \min(\beta\theta, 1/2 - 4\theta)$.*

Neither the statement nor the proof of Theorem 3 make any use of automorphic forms; but (in view of the Gross/Zagier formula) the proof actually demonstrates that the number of nonvanishing central derivatives $L'(f_E \otimes \chi, 1/2)$ is $\gg D^\alpha$, where f_E is the newform associated to E. Moreover, we use the ideas of the proof to give another proof (conditional on $S_{\beta,\theta}$) of Thm. 1.

We conclude the introduction by describing the main geometric issues that intervene in the proof of these Theorems. Let us consider just Theorem 1 for clarity. In that case, one has a collection of Heegner points in $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbf{H}$ with discriminant $-D$, parameterized by Cl_K. The collection of values $L(\frac{1}{2}, f \otimes \chi)$ reflects – for a fixed Maass form f, varying χ through $\widehat{\mathrm{Cl}_K}$ – the distribution of Heegner points. More precisely, it reflects the way in which the distribution of these Heegner points interacts with the subgroup structure of Cl_K. For example, if there existed a subgroup $H \subset \mathrm{Cl}_K$ such that points in the same H-coset also tend to cluster together on $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbf{H}$, this would cause the L-values to be distributed unusually. Thus, in a sense, whatever results we are able to prove about these values are (geometrically speaking) assertions that the group structure on Cl_K does not interact at all with the "proximity structure" that arises from its embedding into $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbf{H}$.

REMARK 1.1. Denote by $\mathrm{Cl}_K = \mathrm{Pic}(O_K)$ the class group of O_K and by $\widehat{\mathrm{Cl}_K}$ its dual group. We write $h_K = |\mathrm{Cl}_K| = |\widehat{\mathrm{Cl}_K}|$ for the class number of O_K. By Siegel's theorem one has

$$h_K \gg_\varepsilon D^{1/2-\varepsilon} \tag{1}$$

(where the constant implied is not effective) so the lower bounds of Theorems 1 and 2 are far from giving a constant proportion of nonvanishing values. (In the case where f is Eisenstein, Blomer has obtained much better results: see Sec. 1.3). Moreover, both proofs make use of (1) so the constants implied are ineffective.

1.1. Nonvanishing of a single twist. Let us introduce some of the main ideas of the present paper in the most direct way, by sketching two very short proofs that *at least one* twist is nonvanishing in the context of Theorem 1. We denote by $\mathbf{H}$ the upper-half plane. To the quadratic field $K = \mathbb{Q}(\sqrt{-D})$ – where we always assume that $-D$ is a fundamental discriminant – and each ideal class x of the maximal order O_K of $\mathbb{Q}(\sqrt{-D})$ there is associated a Heegner point $[x] \in \mathrm{SL}_2(\mathbb{Z})\backslash\mathbf{H}$. [3]

One can describe the collection $He_K := \{[x] : x \in \mathrm{Cl}_K\}$ using the moduli description of $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbf{H}$: if one identifies $z \in \mathrm{SL}_2(\mathbb{Z})\backslash\mathbf{H}$ with the isomorphism

[3]Namely, $[x]$ is represented by the point $\frac{-b+\sqrt{-D}}{2a}$, where $au^2 + buv + cv^2$ is a quadratic form of discriminant $-D$ corresponding to the ideal class x, i.e. there exists a fractional ideal $\mathfrak{J}$ in the class x and a $\mathbb{Z}$-basis α, β for $\mathfrak{J}$ so that $\mathrm{Norm}(u\alpha + v\beta) = \mathrm{Norm}(\mathfrak{J})(au^2 + buv + cv^2)$.

class of elliptic curves over $\mathbb{C}$, via $z \in \mathbf{H} \to \mathbb{C}/(\mathbb{Z} + z\mathbb{Z})$, then He_K is identified with the set of elliptic curves with CM by O_K.

If f is a Maass form and χ a character of Cl_K, one has associated a twisted L-function $L(s, f \times \chi)$, and it is known, from the work of Waldspurger and Zhang [**Zha01, Zha04**] that

$$L(f \otimes \chi, 1/2) = \frac{2}{\sqrt{D}} \Big| \sum_{x \in \mathrm{Cl}_K} \overline{\chi}(x) f([x]) \Big|^2. \tag{2}$$

In other words: the values $L(\frac{1}{2}, f \otimes \chi)$ are the squares of the "Fourier coefficients" of the function $x \mapsto f([x])$ on the finite abelian group Cl_K. The Fourier transform being an isomorphism, in order to show that there exists *at least one* $\chi \in \widehat{\mathrm{Cl}_K}$ such that $L(1/2, f \otimes \chi)$ is nonvanishing, it will suffice to show that $f([x]) \neq 0$ for at least one $x \in \mathrm{Cl}_K$. There are two natural ways to approach this (for D large enough):

(1) Probabilistically: show this is true for a random x. It is known, by a theorem of Duke, that the points $\{[x] : x \in \mathrm{Cl}_K\}$ become equidistributed (as $D \to \infty$) w.r.t. the Riemannian measure on Y; thus $f([x])$ is nonvanishing for a random $x \in \mathrm{Cl}_K$.
(2) Deterministically: show this is true for a special x. The class group Cl_K has a distinguished element, namely the identity $e \in \mathrm{Cl}_K$; and the corresponding point $[e]$ looks very special: it lives very high in the cusp. Therefore $f([e]) \neq 0$ for obvious reasons (look at the Fourier expansion!)

Thus we have given two (fundamentally different) proofs of the fact that there exists χ such that $L(\frac{1}{2}, f \otimes \chi) \neq 0$! Soft as they appear, these simple ideas are rather powerful. The main body of the paper is devoted to quantifying these ideas further, i.e. pushing them to give that *many* twists are nonvanishing.

Remark 1.2. The first idea is the standard one in analytic number theory: to prove that a family of quantities is nonvanishing, compute their average. It is an emerging philosophy that many averages in analytic number theory are connected to equidistribution questions and thus often to ergodic theory.

Of course we note that, in the above approach, one does not really need to know that $\{[x] : x \in \mathrm{Cl}_K\}$ become equidistributed as $D \to \infty$; it suffices to know that this set is becoming *dense*, or even just that it is not contained in the nodal set of f. This remark is more useful in the holomorphic setting, where it means that one can use *Zariski dense* as a substitute for *dense*. See [**Cor02**].

In considering the second idea, it is worth keeping in mind that $f([e])$ is *extremely* small – of size $\exp(-\sqrt{D})$! We can therefore paraphrase the proof as follows: the L-function $L(\frac{1}{2}, f \otimes \chi)$ admits a certain canonical square root, which is not positive; then the sum of all these square roots is very small but known to be nonzero!

This seems of a different flavour from any analytic proof of nonvanishing known to us. Of course the central idea here – that there is always a Heegner point (in fact many) that is very high in the cusp – has been utilized in various ways before. The first example is Deuring's result [**Deu33**] that the failure of the Riemann hypothesis (for ζ) would yield an effective solution to Gauss' class number one problem; another particularly relevant application of this idea is Y. André's lovely proof [**And98**] of the André–Oort conjecture for products of modular surfaces.

ACKNOWLEDGEMENTS. We would like to thank Peter Sarnak for useful remarks and comments during the elaboration of this paper.

1.2. Quantification: nonvanishing of many twists. As we have remarked, the main purpose of this paper is to give quantitative versions of the proofs given in §1.1. A natural benchmark in this question is to prove that a *positive proportion* of the L-values are nonzero. At present this seems out of reach in our instance, at least for general D. We can compute the first but not the second moment of $\{L(\frac{1}{2}, f\otimes\chi) : \chi \in \widehat{\mathrm{Cl}_K}\}$ and the problem appears resistant to the standard analytic technique of "mollification." Nevertheless we will be able to prove that $\gg D^\alpha$ twists are nonvanishing for some positive α.

We now indicate how both of the ideas indicated in the previous section can be quantified to give a lower bound on the number of χ for which $L(\frac{1}{2}, f\otimes\chi) \neq 0$. In order to clarify the ideas involved, let us consider the *worst case*, that is, if $L(\frac{1}{2}, f\otimes\chi)$ was only nonvanishing for a single character χ_0. Then, in view of the Fourier-analytic description given above, the function $x \mapsto f([x])$ is a linear multiple of χ_0, i.e. $f([x]) = a_0\chi_0(x)$, some $a_0 \in \mathbb{C}$. There is no shortage of ways to see that this is impossible; let us give two of them that fit naturally into the "probabilistic" and the "deterministic" framework and will be most appropriate for generalization.

(1) Probabilistic: Let us show that in fact $f([x])$ cannot behave like $a_0\chi_0(x)$ for "most" x. Suppose to the contrary. First note that the constant a_0 cannot be too small: otherwise $f(x)$ would take small values everywhere (since the $[x] : x \in \mathrm{Cl}_K$ are equidistributed). We now observe that the twisted average $\sum f([x])\overline{\chi_0(x)}$ must be "large": but, as discussed above, this will force $L(\frac{1}{2}, f\otimes\chi_0)$ to be large. As it turns out, a *subconvex* bound on this L-function is precisely what is needed to rule out such an event. [4]
(2) Deterministic: Again we will use the properties of certain distinguished points. However, the identity $e \in \mathrm{Cl}_K$ will no longer suffice by itself. Let $\mathfrak{n}$ be an integral ideal in O_K of small norm (much smaller than $D^{1/2}$). Then the point $[\mathfrak{n}]$ is still high in the cusp: indeed, if we choose a representative z for $[\mathfrak{n}]$ that belongs to the standard fundamental domain, we have $\Im(z) \asymp \frac{D^{1/2}}{\mathrm{Norm}(\mathfrak{n})}$. The Fourier expansion now shows that, under some mild assumption such as $\mathrm{Norm}(\mathfrak{n})$ being odd, the sizes of $|f([e])|$ and $|f([\mathfrak{n}])|$ must be wildly different. This contradicts the assumption that $f([x]) = a_0\chi(x)$.

As it turns out, both of the approaches above can be pushed to give that a large number of twists $L(\frac{1}{2}, f\otimes\chi)$ are nonvanishing. However, as is already clear from the discussion above, the "deterministic" approach will require some auxiliary ideals of O_K of small norm.

[4]Here is another way of looking at this. Fix some element $y \in \mathrm{Cl}_K$. If it were true that the function $x \mapsto f([x])$ behaved like $x \mapsto \chi_0(x)$, it would in particular be true that $f([xy]) = f([x])\chi_0(y)$ for all x. This could not happen, for instance, if we knew that the collection $\{[x], [xy]\}_{x\in\mathrm{Cl}_d} \subset Y^2$ was equidistributed (or even dense). Actually, this is evidently not true for all y (for example $y = e$ or more generally y with a representative of small norm) but one can prove enough in this direction to give a proof of many nonvanishing twists if one has enough small split primes. Since the deterministic method gives this anyway, we do not pursue this.

1.3. Connection to existing work. As remarked in the introduction, a considerable amount of work has been done on nonvanishing for families $L(f\otimes\chi,1/2)$ (or the corresponding family of derivatives). We note in particular:

(1) Duke/Friedlander/Iwaniec and subsequently Blomer considered the case where $f(z)=E(z,1/2)$ is the standard non-holomorphic Eisenstein series of level 1 and weight 0 and $\Xi=\widehat{\mathrm{Cl}_K}$ is the group of unramified ring class characters (ie. the characters of the ideal class group) of an imaginary quadratic field K with large discriminant (the central value then equals $L(g_\chi,1/2)^2=L(K,\chi,1/2)^2$). In particular, Blomer [**Blo04**], building on the earlier results of [**DFI95**], used the mollification method to obtain the lower bound

$$|\{\chi\in\widehat{\mathrm{Cl}_K},\ L(K,\chi,1/2)\neq 0\}|\gg\prod_{p|D}(1-\frac{1}{p})\widehat{\mathrm{Cl}_K}\text{ for }|\mathrm{disc}(K)|\to+\infty. \tag{3}$$

This result is evidently much stronger than Theorem 1.

Let us recall that the mollification method requires the asymptotic evaluation of the first and second (twisted) moments

$$\sum_{\chi\in\widehat{\mathrm{Cl}_K}}\chi(\mathfrak{a})L(g_\chi,1/2),\quad\sum_{\chi\in\widehat{\mathrm{Cl}_K}}\chi(\mathfrak{a})L(g_\chi,1/2)^2$$

(where $\mathfrak{a}$ denotes an ideal of O_K of relatively small norm) which is the main content of [**DFI95**]. The evaluation of the second moment is by far the hardest; for it, Duke/Friedlander/Iwaniec started with an integral representation of the $L(g_\chi,1/2)^2$ as a double integral involving two copies of the theta series $g_\chi(z)$ which they averaged over χ; then after several tranformations, they reduced the estimation to an equidistribution property of the Heegner points (associated with O_K) on the modular curve $X_0(N_{K/\mathbb{Q}}(\mathfrak{a}))(\mathbb{C})$ which was proven by Duke [**Duk88**].

(2) On the other hand, Vatsal and Cornut, motivated by conjectures of Mazur, considered a nearly orthogonal situation: namely, fixing f a holomorphic cuspidal newform of weight 2 of level q, and K an imaginary quadratic field with $(q,\mathrm{disc}(K))=1$ and fixing an auxiliary unramified prime p, they considered the non-vanishing problem for the central values

$$\{L(f\otimes\chi,1/2),\ \chi\in\Xi_K(p^n)\}$$

(or for the first derivative) for $\Xi_K(p^n)$, the ring class characters of K of exact conductor p^n (the primitive class group characters of the order O_{K,p^n} of discriminant $-Dp^{2n}$) and for $n\to+\infty$ [**Vat02, Vat03, Cor02**]. Amongst other things, they proved that if $p\nmid 2q\mathrm{disc}(K)$ and if n is large enough – where "large enough" depends on f,K,p – then $L(f\otimes\chi,1/2)$ or $L'(f\otimes\chi,1/2)$ (depending on the sign of the functional equation) is non-zero for *all* $\chi\in\Xi_K(p^n)$.

The methods of [**Cor02, Vat02, Vat03**] look more geometric and arithmetic by comparison with that of [**Blo04, DFI95**]. Indeed they combine the expression of the central values as (the squares of) suitable periods on Shimura curves, with some equidistribution properties of CM points which are obtained through ergodic arguments (i.e. a special case of Ratner's theory on the classification of measures invariant under unipotent orbits), reduction and/or congruence arguments to pass from the "definite case" to the "indefinite case" (i.e. from the non-vanishing of central values to the non-vanishing of the first derivative at 1/2) together with the invariance property of non-vanishing of central values under Galois conjugation.

1.4. Subfamilies of characters; real qudratic fields. There is another variant of the nonvanishing question about which we have said little: given a subfamily $\mathscr{S} \subset \widehat{\mathrm{Cl}_K}$, can one prove that there is a nonvanishing $L(\frac{1}{2}, f \otimes \chi)$ for some $\chi \in \mathscr{S}$? Natural examples of such $\mathscr{S}$ arise from cosets of subgroups of $\widehat{\mathrm{Cl}_K}$. We indicate below some instances in which this type of question arises naturally.

(1) If f is holomorphic, the values $L(\frac{1}{2}, f \otimes \chi)$ have arithmetic interpretations; in particular, if $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, then $L(\frac{1}{2}, f^\sigma \otimes \chi^\sigma)$ is vanishing if and only if $L(\frac{1}{2}, f \otimes \chi)$ is vanishing. In particular, if one can show that one value $L(\frac{1}{2}, f \otimes \chi)$ is nonvanishing, when χ varies through the $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(f))$-orbit of some fixed character χ_0, then they are *all* nonvanishing.

This type of approach was first used by Rohrlich, [**Roh84**]; this is also essentially the situation confronted by Vatsal. In Vatsal's case, the Galois orbits of χ in question are precisely cosets of subgroups, thus reducing us to the problem mentioned above.

(2) Real quadratic fields: One can ask questions similar to those considered here but replacing K by a *real* quadratic field. It will take some preparation to explain how this relates to cosets of subgroups as above.

Firstly, the question of whether there exists a class group character $\chi \in \widehat{\mathrm{Cl}_K}$ such that $L(\frac{1}{2}, f \otimes \chi) \neq 0$ is evidently not as well-behaved, because the size of the class group of K may fluctuate wildly. A suitable analogue to the imaginary case can be obtained by replacing Cl_K by the *extended class group*, $\widetilde{\mathrm{Cl}}_K := \mathbb{A}_K^\times/\mathbb{R}^* U K^\times$, where $\mathbb{R}^*$ is embedded in $(K \otimes \mathbb{R})^\times$, and U is the maximal compact subgroup of the finite ideles of K. This group fits into an exact sequence $\mathbb{R}^*/O_K^\times \to \widetilde{\mathrm{Cl}_K} \to \mathrm{Cl}_K$. Its connected component is therefore a torus, and its component group agrees with Cl_K up to a possible $\mathbb{Z}/2$-extension.

Given $\chi \in \widehat{\widetilde{\mathrm{Cl}_K}}$, there is a unique $s_\chi \in \mathbb{R}$ such that χ restricted to the $\mathbb{R}_+^*$ is of the form $x \mapsto x^{is_\chi}$. The "natural analogue" of our result for imaginary quadratic fields, then, is of the following shape: For a fixed automorphic form f and sufficiently large D, there exist χ with $|s_\chi| \leqslant C$ – a constant depending only on f – and $L(\frac{1}{2}, f \otimes \chi) \neq 0$.

One may still ask, however, the question of whether $L(\frac{1}{2}, f \otimes \chi) \neq 0$ for $\chi \in \widehat{\mathrm{Cl}_K}$ if K is a real quadratic field which happens to have large class group – for instance, $K = \mathbb{Q}(\sqrt{n^2+1})$. We now see that this *is* a question of the flavour of that discussed above: we can prove nonvanishing in the large family $L(\frac{1}{2}, f \otimes \chi)$, where $\chi \in \widehat{\widetilde{\mathrm{Cl}_K}}$, and wish to pass to nonvanishing for the subgroup $\widehat{\mathrm{Cl}_K}$.

(3) The split quadratic extension: to make the distinction between $\widetilde{\mathrm{Cl}_K}$ and Cl_K even more clear, one can degenerate the previous example to the split extension $K = \mathbb{Q} \oplus \mathbb{Q}$.

In that case the analogue of the θ-series χ is given simply by an Eisenstein series of trivial central character; the analogue of the L-functions $L(\frac{1}{2}, f\otimes\chi)$ are therefore $|L(\frac{1}{2}, f\otimes\psi)|^2$, where ψ is just a usual Dirichlet character over $\mathbb{Q}$.

Here one can see the difficulty in a concrete fashion: even the asymptotic as $N\to\infty$ for the square moment

$$\sum_{\psi} |L(\frac{1}{2}, f\otimes\psi)|^2, \tag{4}$$

where the sum is taken over Dirichlet characters ψ of conductor N, is not known in general; however, if one adds a small auxiliary t-averaging and considers instead

$$\sum_{\psi} \int_{|t|\ll 1} |L(\frac{1}{2}+it, f\otimes\psi)|^2 dt. \tag{5}$$

then the problem becomes almost trivial.[5]

The difference between (4) and (5) is precisely the difference between the family $\chi\in \mathrm{Cl}_K$ and $\chi\in\widehat{\mathrm{Cl}_K}$.

2. Proof of Theorem 1

Let f be a primitive even Maass Hecke-eigenform (of weight 0) on $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbf{H}$ (normalized so that its first Fourier coefficient equals 1); the proof of theorem 1 starts with the expression (2) of the central value $L(f\otimes\chi, 1/2)$ as the square of a twisted period of f over H_K. From that expresssion it follows that

$$\sum_{\chi} L(f\otimes\chi, 1/2) = \frac{2h_K}{\sqrt{D}} \sum_{\sigma\in\mathrm{Cl}_K} |f([\sigma])|^2.$$

Now, by a theorem of Duke [**Duk88**] the set $He_K = \{[x] : x\in \mathrm{Cl}_K\}$ becomes equidistributed on $X_0(1)(\mathbb{C})$ with respect to the hyperbolic measure of mass one $d\mu(z) := (3/\pi)dxdy/y^2$, so that since the function $z\to|f(z)|^2$ is a smooth, square-integrable function, one has

$$\frac{1}{h_K}\sum_{\sigma\in\mathrm{Cl}_K} |f([\sigma])|^2 = (1+o_f(1))\int_{X_0(1)(\mathbb{C})} |f(z)|^2 d\mu(z) = \langle f, f\rangle(1+o_f(1))$$

as $D\to+\infty$ (notice that the proof of the equidistribution of Heegner points uses Siegel's theorem, in particular the term $o_f(1)$ is not effective). Hence, we have

$$\sum_{\chi} L(f\otimes\chi, 1/2) = 2\frac{h_K^2}{\sqrt{D}}\langle f, f\rangle(1+o_f(1)) \gg_{f,\varepsilon} D^{1/2-\varepsilon}$$

by (1). In particular this proves that for D large enough, there exists $\chi\in\widehat{\mathrm{Cl}_K}$ such that $L(f\otimes\chi, 1/2)\neq 0$. In order to conclude the proof of Theorem 1, it is sufficient to prove that for any $\chi\in\widehat{\mathrm{Cl}_K}$

$$L(f\otimes\chi, 1/2) \ll_f D^{1/2-\delta},$$

for some absolute $\delta > 0$. Such a bound is known as a *subconvex* bound, as the corresponding bound with $\delta = 0$ is known and called the convexity bound (see [**IS00**]). When χ is a quadratic character, such a bound is an indirect consequence

[5]We thank K. Soundararajan for an enlightening discussion of this problem.

of [**Duk88**] and is essentially proven in [**DFI93**] (see also [**Har03, Mic04**]). When χ is not quadratic, this bound is proven in [**HM06**].

REMARK 2.1. The theme of this section was to reduce a question about the average $L(\frac{1}{2}, f \otimes \chi)$ to equidistribution of Heegner points (and therefore to subconvexity of $L(\frac{1}{2}, f \otimes \chi_K)$, where χ_K is the Dirichlet character associated to K). This reduction can be made precise, and this introduces in a natural way triple product L-functions:

$$(6)\quad \frac{1}{h_K} \sum_{\chi \in \widehat{\mathrm{Cl}_K}} L(1/2, f \otimes \chi) \sim \frac{1}{h_K} \sum_{x \in \mathrm{Cl}_K} |f([x])|^2 = \int_{\mathrm{SL}_2(\mathbb{Z})\backslash \mathbf{H}} |f(z)|^2 dz + \sum_g \langle f^2, g\rangle \sum_{x \in \mathrm{Cl}_K} g([x])$$

Here $\sim$ means an equality up to a constant of size $D^{\pm\varepsilon}$, and, in the second term, the sum over g is over a basis for $L^2_0(\mathrm{SL}_2(\mathbb{Z})\backslash\mathbf{H})$. Here L^2_0 denotes the orthogonal complement of the constants. This g-sum should strictly include an integral over the Eisenstein spectrum; we suppress it for clarity. By Cauchy-Schwarz we have a majorization of the second term (continuing to suppress the Eisenstein spectrum):

$$(7)\quad \left|\sum_g \langle f^2, g\rangle \sum_{x \in \mathrm{Cl}_K} g([x])\right|^2 \leqslant \sum_g \left|\langle f^2, g\rangle\right|^2 \left|\sum_{x \in \mathrm{Cl}_K} g([x])\right|^2$$

where the g-sum is taken over $L^2_0(\mathrm{SL}_2(\mathbb{Z})\backslash\mathbf{H})$, again with suppression of the continuous spectrum. Finally, the summand corresponding to g in the right-hand side can be computed by period formulae: it is roughly of the shape (by Watson's identity, Waldspurger/Zhang formula (2), and factorization of the resulting L-functions)

$$\frac{L(1/2, \mathrm{sym}^2 f \otimes g) L(1/2, g)^2 L(1/2, g \otimes \chi_K)}{\langle g, g\rangle^2 \langle f, f\rangle}.$$

By use of this formula, one can, for instance, make explicit the dependence of Theorem (1) on the level q of f: one may show that there is a nonvanishing twist as soon as $q < D^A$, for some explicit A. Upon GLH, $q < D^{1/2}$ suffices. There seems to be considerable potential for exploiting (7) further; we hope to return to this in a future paper. We note that similar identities have been exploited in the work of Reznikov [**Rez05**].

One can also prove the following twisted variant of (6): let $\sigma_{\mathfrak{l}} \in \mathrm{Cl}_K$ be the class of an integral ideal $\mathfrak{l}$ of O_K coprime with D. Then one can give an asymptotic for $\sum_\chi \chi(\sigma_{\mathfrak{l}}) L(f \otimes \chi, 1/2)$, when the norm of $\mathfrak{l}$ is a sufficiently small power of D. This again uses equidistribution of Heegner points of discriminant D, but at level $\mathrm{Norm}(\mathfrak{l})$.

3. Proof of Theorem 2

The proof of Theorem (2) is in spirit identical to the proof of Theorem (1) that was presented in the previous section. The only difference is that the L-function is the square of a period on a quaternion algebra instead of $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbf{H}$. We will try to set up our notation to emphasize this similarity.

For the proof of Theorem (2) we need to recall some more notations; we refer to [**Gro87**] for more background. Let q be a prime and B_q be the definite quaternion algebra ramified at q and ∞. Let O_q be a choice of a maximal order. Let S be the set of classes for B_q, i.e. the set of classes of left ideals for O_q. To each $s \in S$ is associated an ideal I and another maximal order, namely, the right order $R_s := \{\lambda \in B_q : I\lambda \subset I\}$. We set $w_s = \#R_s^\times/2$. We endow S with the measure ν in which each $\{s\}$ has mass $1/w_s$. This is not a probability measure.

The space of functions on S becomes a Hilbert space via the norm $\langle f, f\rangle^2 = \int |f|^2 d\nu$. Let $S_2^B(q)$ be the orthogonal complement of the constant function. It is endowed with an action of the Hecke algebra $\mathbf{T}^{(q)}$ generated by the Hecke operators T_p $p \nmid q$ and as a $\mathbf{T}^{(q)}$-module $S_2^B(q)$ is isomorphic with $S_2(q)$, the space of weight 2 holomorphic cusp newforms of level q. In particular to each Hecke newform $f \in S_2(q)$ there is a corresponding element $\tilde{f} \in S_2^B(q)$ such that

$$T_n\tilde{f} = \lambda_f(n)\cdot\tilde{f}, \quad (n, q) = 1.$$

We normalize $\tilde{f}$ so that $\langle\tilde{f}, \tilde{f}\rangle = 1$.

Let K be an imaginary quadratic field such that q is inert in K. Once one fixes a special point associated to K, one obtains for each $\sigma \in G_K$ a "special point" $x_\sigma \in S$, cf. discussion in [**Gro87**] of "x_a" after [**Gro87**, (3.6)].

One has the Gross formula [**Gro87**, Prop 11.2]: for each $\chi \in \widehat{\mathrm{Cl}_K}$,

$$L(f\otimes\chi, 1/2) = \frac{\langle f, f\rangle}{u^2\sqrt{D}}\left|\sum_{\sigma\in\mathrm{Cl}_K}\tilde{f}(x_\sigma)\chi(\sigma)\right|^2 \tag{8}$$

Here u is the number of units in the ring of integers of K. Therefore,

$$\sum_{\chi\in\widehat{\mathrm{Cl}_K}} L(f\otimes\chi, 1/2) = \frac{h_K\langle f, f\rangle}{u^2\sqrt{D}}\sum_{\sigma\in\mathrm{Cl}_K}\left|\tilde{f}(x_\sigma)\right|^2$$

Now we use the fact that the Cl_K-orbit $\{x_\sigma,\ \sigma \in \mathrm{Cl}_K\}$ becomes equidistributed, as $D \to \infty$, with respect to the (probability) measure $\frac{\nu}{\nu(S)}$: this is a consequence of the main theorem of [**Iwa87**] (see also [**Mic04**] for a further strengthening) and deduce that

$$h_K^{-1}\sum_\sigma\left|\tilde{f}(x_\sigma)\right|^2 = (1 + o_q(1))\frac{1}{\nu(S)}\int|\tilde{f}|^2 d\nu \tag{9}$$

In particular, it follows from (1) that, for all $\varepsilon > 0$

$$\sum_\chi L(f\otimes\chi, 1/2) \gg_{f,\varepsilon} D^{1/2-\varepsilon}.$$

Again the proof of theorem 2 follows from the subconvex bound

$$L(f\otimes\chi, 1/2) \ll_f D^{1/2-\delta}$$

for any $0 < \delta < 1/1100$, which is proven in [**Mic04**].

4. Quantification using the cusp; a conditional proof of Theorem 1 and Theorem 3 using the cusp.

Here we elaborate on the second method of proof discussed in Section 1.1.

4.1. Proof of Theorem 1 using the cusp. We note that $S_{\beta,\theta}$ implies that there are $\gg D^{\beta\theta-\epsilon}$ distinct primitive ideals with odd norms with norm $\leqslant D^{\theta}$. Indeed $S_{\beta,\theta}$ provides many such ideals without the restriction of odd norm; just take the "odd part" of each such ideal. The number of primitive ideals with norm $\leqslant X$ and the same odd part is easily verified to be $O(\log X)$, whence the claim.

Proposition 4.1. *Assume hypothesis $S_{\beta,\theta}$, and let f be an even Hecke-Maass cusp form on* $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbf{H}$. *Then $\gg D^{\delta-\epsilon}$ twists $L(\frac{1}{2}, f\otimes\chi)$ are nonvanishing, where $\delta = \min(\beta\theta, 1/2-4\theta)$.*

Proof. Notations being as above, fix any $\alpha < \delta$, and suppose that precisely $k-1$ of the twisted sums

$$\sum_{x\in\mathrm{Cl}_K} f([x])\chi(x) \tag{10}$$

are nonvanishing, where $k < D^{\alpha}$. In particular, $k < D^{\beta\theta}$. We will show that this leads to a contradiction for large enough D.

Let $1/4+\nu^2$ be the eigenvalue of f. Then f has a Fourier expansion of the form

$$f(x+iy) = \sum_{n\geqslant 1} a_n (ny)^{1/2} K_{i\nu}(2\pi ny)\cos(2\pi nx), \tag{11}$$

where the Fourier coefficients $|a_n|$ are polynomially bounded. We normalize so that $a_1 = 1$; moreover, in view of the asymptotic $K_{i\nu}(y) \sim (\frac{\pi}{2y})^{1/2}e^{-y}(1+O_{\nu}(y^{-1}))$, we obtain an asymptotic expansion for f near the cusp. Indeed, if $z_0 = x_0+iy_0$ belongs to the standard fundamental domain for $\mathrm{SL}_2(\mathbb{Z})$, the standard asymptotics show that – with an appropriate normalization –

$$f(z) = \text{const.}\cos(2\pi x)\exp(-2\pi y)(1+O(y^{-1})) + O(e^{-4\pi y}) \tag{12}$$

Let $\mathfrak{p}_j, \mathfrak{q}_j$ be primitive integral ideals of O_K for $1 \leqslant j \leqslant k$, all with odd norm, so that $\mathfrak{p}_j$ are mutually distinct and the $\mathfrak{q}_j$ are mutually distinct; and, moreover that

$$\mathrm{Norm}(\mathfrak{p}_1) < \mathrm{Norm}(\mathfrak{p}_2) < \cdots < \mathrm{Norm}(\mathfrak{p}_k) < D^{\theta} \tag{13}$$

$$D^{\theta} > \mathrm{Norm}(\mathfrak{q}_1) > \mathrm{Norm}(\mathfrak{q}_2) > \cdots > \mathrm{Norm}(\mathfrak{q}_k). \tag{14}$$

The assumption on the size of k and the hypothesis $S_{\beta,\theta}$ guarantees that we may choose such ideals, at least for sufficiently large D.

If $\mathfrak{n}$ is any primitive ideal with norm $< \sqrt{D}$, it corresponds to a reduced binary quadratic form $ax^2+bxy+cy^2$ with $a = \mathrm{Norm}(\mathfrak{n})$ and $b^2-4ac = -D$; the corresponding Heegner point $[\mathfrak{n}]$ has as representative $\frac{-b+\sqrt{-D}}{2\mathrm{Norm}(\mathfrak{n})}$. We note that if $a = \mathrm{Norm}(\mathfrak{n})$ is odd, then

$$\left|\cos(2\pi\cdot\left(\frac{-b}{2\mathrm{Norm}(\mathfrak{n})}\right))\right| \gg \mathrm{Norm}(\mathfrak{n})^{-1}. \tag{15}$$

Then the functions $x \mapsto f([x\mathfrak{p}_j])$ – considered as belonging to the vector space of maps $\mathrm{Cl}_K \to \mathbb{C}$ – are necessarily linearly dependent for $1 \leqslant j \leqslant k$, because of the assumption on the sums (10). Evaluating these functions at the $[\mathfrak{q}_j]$ shows that the matrix $f([\mathfrak{p}_i\mathfrak{q}_j])_{1\leqslant i,j\leqslant k}$ must be singular. We will evaluate the determinant of this matrix and show it is nonzero, obtaining a contradiction. The point here is that, because all the entries of this matrix differ enormously from each other in absolute value, there is one term that dominates when one expands the determinant via permutations.

Thus, if $\mathfrak{n}$ is a primitive integral ideal of odd norm $< c_0\sqrt{D}$, for some suitable, sufficiently large, absolute constant c_0, (12) and (15) show that one has the bound – for some absolute c_1, c_2 –

$$c_1 e^{-\pi\sqrt{D}/\mathrm{Norm}(\mathfrak{n})} \geqslant |f([\mathfrak{n}])| \geqslant c_2 D^{-1} e^{-\pi\sqrt{D}/\mathrm{Norm}(\mathfrak{n})}.$$

Expanding the determinant of $f([\mathfrak{p}_i\mathfrak{q}_j])_{1\leqslant i,j\leqslant k}$ we get

$$\det = \sum_{\sigma\in S_k}\prod_{i=1}^{k} f([\mathfrak{p}_i\mathfrak{q}_{\sigma(i)}])\mathrm{sign}(\sigma) \tag{16}$$

Now, in view of the asymptotic noted above, we have

$$\prod_{i=1}^{k} f([\mathfrak{p}_i\mathfrak{q}_{\sigma(i)}]) = c_3 \exp\left(-\pi\sqrt{D}\sum_i \frac{1}{\mathrm{Norm}(\mathfrak{p}_i\mathfrak{q}_{\sigma(i)})}\right)$$

where the constant c_2 satisfies $c_3 \in [(c_2/D)^k, c_1^k]$. Set $a_\sigma = \sum_i \frac{1}{\mathrm{Norm}(\mathfrak{p}_i)\mathrm{Norm}(\mathfrak{q}_{\sigma(i)})}$. Then a_σ is maximized – in view of (13) and (14) – for the identity permutation $\sigma = \mathrm{Id}$, and, moreover, it is simple to see that $a_{Id} - a_\sigma \geqslant \frac{1}{D^{4\theta}}$ for any σ other than the identity permutation. It follows that the determinant of (16) is bounded below, in absolute value, by

$$\exp(a_{Id})\left((c_2/D)^k - c_1^k k! \exp(-\pi D^{1/2-4\theta})\right)$$

Since $k < D^\alpha$ and $\alpha < 1/2 - 4\theta$, this expression is nonzero if D is sufficiently large, and we obtain a contradiction. □

4.2. Variant: the derivative of L-functions and the rank of elliptic curves over Hilbert class fields of $\mathbb{Q}(\sqrt{-D})$. We now prove Thm. 3. For a short discussion of the idea of the proof, see the paragraph after (18).

Take $\Phi_E : X_0(N) \to E$ a modular parameterization, defined over $\mathbb{Q}$, with N squarefree. If f is the weight 2 newform corresponding to E, the map

$$\Phi_E : z \mapsto \int_\tau f(w)dw, \tag{17}$$

where τ is any path that begins at ∞ and ends at z, is well-defined up to a lattice $L \subset \mathbb{C}$ and descends to a well-defined map $X_0(N) \to \mathbb{C}/L \cong E(\mathbb{C})$; this sends the cusp at ∞ to the origin of the elliptic curve E and arises from a map defined over $\mathbb{Q}$.

The space $X_0(N)$ parameterizes (a compactification) of the space of cyclic N-isogenies $E \to E'$ between two elliptic curves. We refer to [**GZ86**, II. §1] for further background on Heegner points; for now we just quote the facts we need. If $\mathfrak{m}$ is any ideal of O_K and $\mathfrak{n}$ any integral ideal with $\mathrm{Norm}(\mathfrak{n}) = N$, then $\mathbb{C}/\mathfrak{m} \to \mathbb{C}/\mathfrak{m}\mathfrak{n}^{-1}$ defines a Heegner point on $X_0(N)$ which depends on $\mathfrak{m}$ only through its ideal class, equivalently, depends only on the point $[\mathfrak{m}] \in \mathrm{SL}_2(\mathbb{Z})\backslash\mathbf{H}$. Thus Heegner points are parameterized by such pairs $([\mathfrak{m}], \mathfrak{n})$ and their total number is $|\mathrm{Cl}_K| \cdot \nu(N)$, where $\nu(N)$ is the number of divisors of N.

Fix any $\mathfrak{n}_0$ with $\mathrm{Norm}(\mathfrak{n}_0) = N$ and let P be the Heegner point corresponding to $([e], \mathfrak{n}_0)$. Then P is defined over H, the Hilbert class field of $\mathbb{Q}(\sqrt{-D})$, and we can apply any element $x \in \mathrm{Cl}_K$ (which is identified with the Galois group of H/K) to P to get P^x, which is the Heegner point corresponding to $([x], \mathfrak{n}_0)$.

Suppose $\mathfrak{m}$ is an ideal of O_K of norm m, prime to N. We will later need an explicit representative in $\mathbb{H}$ for $P^{\mathfrak{m}\mathfrak{n}_0} = ([\mathfrak{m}\mathfrak{n}_o], \mathfrak{n}_0)$. (Note that the correspondence between $z \in \Gamma_0(N)\backslash\mathbf{H}$ and elliptic curve isogenies sends z to $\mathbb{C}/\langle 1, z\rangle \mapsto \mathbb{C}/\langle 1/N, z\rangle$.) This representative (cf. [**GZ86**, eq. (1.4–1.5)]) can be taken to be

$$z = \frac{-b + \sqrt{-D}}{2a}, \tag{18}$$

where $a = \mathrm{Norm}(\mathfrak{m}\mathfrak{n}_0)$, and $\mathfrak{m}\mathfrak{n}_o = \langle a, \frac{b+\sqrt{-D}}{2}\rangle$, $\mathfrak{m} = \langle aN^{-1}, \frac{b+\sqrt{-D}}{2}\rangle$.

Let us explain the general idea of the proof. Suppose, first, that $E(H)$ had rank *zero*. We denote by $\#E(H)_{tors}$ the order of the torsion subgroup of $E(H)$. This would mean, in particular, that $\Phi(P)$ was a torsion point on $E(H)$; in particular $\#E(H)_{tors}.\Phi(P) = 0$. In view of (17), and the fact that P is very close to the cusp of $X_0(N)$ the point $\Phi(P) \in \mathbb{C}/L$ is represented by a nonzero element $z_P \in \mathbb{C}$ very close to 0. It is then easy to see that $\#E(H)_{tors} \cdot z_P \notin L$, a contradiction. Now one can extend this idea to the case when $E(H)$ has higher rank. Suppose it had rank *one*, for instance. Then Cl_K must act on $E(H) \otimes \mathbb{Q}$ through a character of order 2. In particular, if $\mathfrak{p}$ is any integral ideal of K, then $\Phi(P^{\mathfrak{p}})$ equals $\pm\Phi(P)$ in $E(H) \otimes \mathbb{Q}$. Suppose, say, that $\Phi(P^{\mathfrak{p}}) = \Phi(P)$ in $E(H) \otimes \mathbb{Q}$. One again verifies that, if the norm of $\mathfrak{p}$ is sufficiently small, then $\Phi(P^{\mathfrak{p}}) - \Phi(P) \in \mathbb{C}/L$ is represented by a nonzero $z \in \mathbb{C}$ which is sufficiently close to zero that $\#E(H)_{tors}.z \notin L$.

The $\mathbb{Q}$-vector space $V := E(H) \otimes \mathbb{Q}$ defines a $\mathbb{Q}$-representation of $\mathrm{Gal}(H/K) = \mathrm{Cl}_K$, and we will eventually want to find certain elements in the group algebra of $\mathrm{Gal}(H/K)$ which annihilate this representation, and on the other hand do not have coefficients that are too large. This will be achieved in the following two lemmas.

LEMMA 4.1. *Let A be a finite abelian group and W a k-dimensional $\mathbb{Q}$-representation of A. Then there exists a basis for W with respect to which the elements of A act by integral matrices, all of whose entries are $\leqslant C^{k^2}$ in absolute value. Here C is an absolute constant.*

PROOF. We may assume that W is irreducible over $\mathbb{Q}$. The group algebra $\mathbb{Q}\cdot A$ decomposes as a certain direct sum $\oplus_j K_j$ of number fields K_j; these K_j exhaust the $\mathbb{Q}$-irreducible representations of A.

Each of these number fields has the property that it is generated, as a $\mathbb{Q}$-vector space, by the roots of unity contained in it (namely, take the images of elements of A under the natural projection $\mathbb{Q}.A \to K_j$). The roots of unity in each K_j form a group, necessarily cyclic; so all the K_j are of the form $\mathbb{Q}[\zeta]$ for some root of unity ζ; and each $a \in A$ acts by multiplication by some power of ζ.

Thus let ζ be a kth root of unity, so $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(k)$ and $\mathbb{Q}(\zeta)$ is isomorphic to $\mathbb{Q}[x]/p_k(x)$, where p_k is the kth cyclotomic polynomial. Then multiplication by x on $\mathbb{Q}[x]/p_k(x)$ is represented, w.r.t. the natural basis $\{1, x, \dots, x^{\varphi(k)-1}\}$, by a matrix all of whose coefficients are integers of size $\leqslant A$, where A is the absolute value of the largest coefficient of p_k. Since any coefficient of A is a symmetric function in $\{\zeta^i\}_{(i,k)=1}$, one easily sees that $A \leqslant 2^k$.

For any $k \times k$ matrix M, let $\|M\|$ denote the largest absolute value of any entry of M. Then one easily checks that $\|M.N\| \leqslant k\|M\|\|N\|$ and, by induction, $\|M^r\| \leqslant k^{r-1}\|M\|^r$. Thus any power of ζ acts on $\mathbb{Q}(\zeta)$, w.r.t. the basis $\{1, \zeta, \dots, \zeta^{\varphi(k)-1}\}$, by an integral matrix all of whose entries have size $\leqslant k^k \cdot 2^{k^2} \leqslant C^{k^2}$ for some absolute C. $\square$

LEMMA 4.2. *Let assumptions and notations be as in the previous lemma; let $S \subset A$ have size $|S| = 2k$. Then there exist integers $n_s \in \mathbb{Z}$, not all zero, such that the element $\sum n_s s \in \mathbb{Z}[A]$ annihilates the A-module W. Moreover, we may choose n_s so that $|n_s| \ll C_2^{k^2}$, for some absolute constant C_2.*

PROOF. This follows from Siegel's lemma. Indeed, consider all choices of n_s when $|n_s| \leqslant N$ for all $s \in S$; there are at least N^{2k} such choices. Let $\{w_i\}_{1\leqslant i\leqslant k}$ be the basis for W provided by the previous lemma. For each i_0, the element $(\sum n_s s)\cdot w_{i_0}$ can be expanded in terms of the basis w_i with integral coefficients of size $\leqslant (2k)C^{k^2}N$. So the number of possibilities for the collection $\{(\sum n_s s)\, w_j\}_{1\leqslant j\leqslant k}$ is $\ll C_2^{k^3}N^k$, for some suitable absolute constant C_2. It follows that if $N \gg C_2^{k^2}$ two of these must coincide. $\square$

We are now ready to prove Theorem 3.

PROOF. (of Thm. 3). Fix $\alpha < \delta = \min(\beta\theta, 1/2-4\theta)$ and suppose that the rank of $E(H)\otimes\mathbb{Q}$ is k, where $k < D^\alpha$. We will show that this leads to a contradiction for D sufficiently large.

Choose $\{\mathfrak{p}_1, \dots, \mathfrak{p}_{2k}, \mathfrak{q}_1, \dots, \mathfrak{q}_{2k}\}$ satisfying the same conditions (13) and (14) as in the proof of Prop. 4.1. We additionally assume that all $\mathfrak{p}_j, \mathfrak{q}_j$ have norms coprime to N; it is easy to see that this is still possible for sufficiently large D. Recall we have fixed an integral ideal $\mathfrak{n}_0$ of norm N. Lem. 4.2 shows that there are integers n_i $(1 \leqslant i \leqslant 2k)$ such that the element

$$\Upsilon := \sum_{i=1}^{2k} n_i \cdot \mathfrak{p}_i\mathfrak{n}_0 \in \mathbb{Z}[\mathrm{Cl}_K] \tag{19}$$

annihilates $E(H)\otimes\mathbb{Q}$ and moreover $|n_i| \ll C_2^{k^2}$. In particular

$$\Upsilon \cdot \Phi_E(P^{\mathfrak{q}_j}) = 0 \quad (1 \leqslant j \leqslant k) \tag{20}$$

But $\Phi_E(P^{\mathfrak{p}_i\mathfrak{q}_j\mathfrak{n}_0})$ is the image under the map Φ_E (see (17)) of a point $z_{P,i,j} \in \mathbf{H}$ whose y-coordinate is given by (cf. (18)) $y_{P,i,j} = \frac{\sqrt{D}}{2\mathrm{Norm}(\mathfrak{p}_i\mathfrak{q}_j\mathfrak{n}_0)}$. In particular this satisfies $y_{P,i,j} \gg D^{1/2-2\theta}$.

The weight 2 form f has a q-expansion in the neighbourhood of ∞ of the form

$$f(z) = e^{2\pi iz} + \sum_{n\geqslant 2} a_n e^{2\pi inz}$$

where the a_n are integers satisfying $|a_n| \ll n^{1/2+\epsilon}$. In particular, there exists a contour C from ∞ to $z_{P,i,j}$ so that

$$\left|\int_C f(\tau)d\tau\right| = \frac{1}{2\pi i}\exp(-\pi\frac{\sqrt{D}}{\mathrm{Norm}(\mathfrak{p}_i\mathfrak{q}_j\mathfrak{n}_0)})\left(1 + O(\exp(-\pi D^{1/2-2\theta}))\right)$$

Thus the image of the Heegner point $P^{\mathfrak{p}_i\mathfrak{q}_j\mathfrak{n}_0}$ on $E(\mathbb{C}) = \mathbb{C}/L$ is represented by $z_{ij} \in \mathbb{C}$ satisfying $|z_{ij}| = \frac{1}{2\pi i}\exp(-\pi\frac{\sqrt{D}}{\mathrm{Norm}(\mathfrak{p}_i\mathfrak{q}_j\mathfrak{n}_0)})\left(1 + O(\exp(-\pi D^{1/2-2\theta}))\right)$. The relation (20) shows that

$$\#E(H)_{tors} \cdot \sum n_i z_{ij} \in L.$$

Note that $\#E(H)_{tors}$ is bounded by a polynomial in D, by reducing modulo primes of H that lie above inert primes in K. Since $|n_i| \ll C_2^{k^2}$ and $k < D^\alpha$, this forces $\sum n_i z_{ij} = 0$ for sufficiently large D. This implies that the matrix $(z_{ij})_{1\leqslant i,j\leqslant 2k}$ is *singular*, and one obtains a contradiction by computing determinants, as in Sec. 4.1. □

References

[And98] Y. André – "Finitude des couples d'invariants modulaires singuliers sur une courbe algébrique plane non modulaire", *J. Reine Angew. Math.* **505** (1998), p. 203–208.

[Blo04] V. Blomer – "Non-vanishing of class group L-functions at the central point", *Ann. Inst. Fourier (Grenoble)* **54** (2004), no. 4, p. 831–847 (English, with English and French summaries).

[Cor02] C. Cornut – "Mazur's conjecture on higher Heegner points", *Invent. Math.* **148** (2002), no. 3, p. 495–523.

[Deu33] M. Deuring – "Imaginäre quadratische Zahlkörper mit der Klassenzahl 1", *Math. Z.* **37** (1933), no. 1, p. 405–415.

[DFI93] W. Duke, J. Friedlander & H. Iwaniec – "Bounds for automorphic L-functions", *Invent. Math.* **112** (1993), no. 1, p. 1–8.

[DFI95] ———, "Class group L-functions", *Duke Math. J.* **79** (1995), no. 1, p. 1–56.

[Duk88] W. Duke – "Hyperbolic distribution problems and half-integral weight Maass forms", *Invent. Math.* **92** (1988), no. 1, p. 73–90.

[EY03] B. Edixhoven & A. Yafaev – "Subvarieties of Shimura varieties", *Ann. of Math. (2)* **157** (2003), no. 2, p. 621–645.

[GR90] S. W. Graham & C. J. Ringrose – "Lower bounds for least quadratic nonresidues", in *Analytic number theory (Allerton Park, IL, 1989)* (Boston, MA), Progr. Math., vol. 85, Birkhäuser Boston, 1990, p. 269–309.

[Gro87] B. Gross – "Heights and the special values of L-series", in *Number theory (Montreal, Que., 1985)*, CMS Conf. Proc., vol. 7, Amer. Math. Soc., 1987, p. 115–187.

[GZ86] B. Gross & D. Zagier – "Heegner points and derivatives of L-series", *Invent. Math.* **84** (1986), no. 2, p. 225–320.

[Har03] G. Harcos – "An additive problem in the Fourier coefficients of cusp forms", *Math. Ann.* **326** (2003), no. 2, p. 347–365.

[HM06] G. Harcos & P. Michel – "The subconvexity problem for Rankin-Selberg L-functions and equidistribution of heegner points II", *Invent. Math.* **163** (2006), p. 581–655.

[IS00] H. Iwaniec & P. Sarnak – "Perspectives on the analytic theory of L-functions", *Geom. Funct. Anal.* (2000), no. Special Volume, p. 705–741, GAFA 2000 (Tel Aviv, 1999).

[Iwa87] H. Iwaniec – "Fourier coefficients of modular forms of half-integral weight", *Invent. Math.* **87** (1987), no. 2, p. 385–401.

[Mic04] P. Michel – "The subconvexity problem for Rankin-Selberg L-functions and equidistribution of Heegner points", *Ann. of Math. (2)* **160** (2004), no. 1, p. 185–236.

[Rez05] A. Reznikov – "Rankin-Selberg without unfolding", 2005.

[Roh84] D. Rohrlich – "On L-functions of elliptic curves and cyclotomic towers", *Invent. Math.* **75** (1984), no. 3, p. 409–423.

[Vat02] V. Vatsal – "Uniform distribution of Heegner points", *Invent. Math.* **148** (2002), no. 1, p. 1–46.

[Vat03] ———, "Special values of anticyclotomic L-functions", *Duke Math. J.* **116** (2003), no. 2, p. 219–261.

[Zha01] S. Zhang – "Gross-Zagier formula for GL_2", *Asian J. Math.* **5** (2001), no. 2, p. 183–290.

[Zha04] ———, "Gross-zagier formula for GL_2. II", in *Heegner points and Rankin L-series*, Math. Sci. Res. Inst. Publ., vol. 49, Cambridge Univ. Press, 2004, p. 191–214.

I3M, UMR 5149 CNRS, cc 051 Universit de Montpellier II, Place E. Bataillon, 34095 Montpellier Cedex 5, FRANCE

Institute for Advanced Study, 1 Einstein Drive, Princeton, NJ 08540
Current address: Courant Institute of Mathematical Sciences, New York University

Clay Mathematics Proceedings
Volume 7, 2007

Singular moduli generating functions for modular curves and surfaces

Ken Ono

Abstract. Zagier [**Zag02**] proved that the generating functions for the traces of singular moduli are often weight 3/2 modular forms. Here we investigate the modularity of generating functions of Maass singular moduli, as well as traces of singular moduli on Hilbert modular surfaces.

1. Introduction and Statement of Results

Let $j(z)$ be the usual modular function for $\mathrm{SL}_2(\mathbb{Z})$

$$j(z) = q^{-1} + 744 + 196884q + 21493760q^2 + \cdots ,$$

where $q = e^{2\pi iz}$. The values of modular functions such as $j(z)$ at imaginary quadratic arguments in $\mathfrak{h}$, the upper half of the complex plane, are known as *singular moduli*. Singular moduli are algebraic integers which play many roles in number theory. For example, they generate class fields of imaginary quadratic fields, and they parameterize isomorphism classes of elliptic curves with complex multiplication.

This expository article describes the author's recent joint works with Bringmann, Bruinier, Jenkins, and Rouse [**BO, BOR05, BJO06**] on generating functions for traces of singular moduli. To motivate these results, we begin by comparing the classical evaluations

$$\frac{j\left(\frac{-1+\sqrt{-3}}{2}\right) - 744}{3} = -248, \qquad \frac{j(i) - 744}{2} = 492, \qquad j\left(\frac{1+\sqrt{-7}}{2}\right) - 744 = -4119,$$

with the Fourier coefficients of the modular form

(1.1)

$$g(z) := -\frac{\eta(z)^2 \cdot E_4(4z)}{\eta(2z)\eta(4z)^6} = -q^{-1} + 2 - 248q^3 + 492q^4 - 4119q^7 + 7256q^8 - \cdots ,$$

where $E_4(z) = 1 + 240\sum_{n=1}^{\infty}\sigma_3(n)q^n$ is the usual weight 4 Eisenstein series, and $\eta(z) = q^{1/24}\prod_{n=1}^{\infty}(1-q^n)$ is Dedekind's eta-function. The appearance of singular

---

2000 *Mathematics Subject Classification.* Primary 11F37, Secondary 11F30, 11F41.

The author thanks the National Science Foundation for their generous support, and he is grateful for the support of the David and Lucile Packard, H. I. Romnes, and John S. Guggenheim Fellowships.

moduli as the initial coefficients of the modular form $g(z)$ is not a coincidence. In a recent groundbreaking paper [**Zag02**], Zagier established that $g(z)$ is indeed the generating function for the "traces" of the $j(z)$ singular moduli. In this important paper, Zagier employs such results to give a new proof of Borcherds' famous theorem on the infinite product expansions of integer weight modular forms on $\mathrm{SL}_2(\mathbb{Z})$ with Heegner divisor (for example, see [**Bor95a, Bor95b**]).

Here we survey three recent papers inspired by Zagier's work. First we revisit his work from the context of Maass-Poincaré series. This uniform approach gives many of his results as special cases of a single theorem, and, as an added bonus, gives exact formulas for traces of singular moduli. Our first general result (see Theorem 1.1) establishes that the coefficients of certain half-integral weight Maass forms have the property that their coefficients are traces of singular moduli. These works are described in [**BO, BJO06**]. Secondly, we obtain generalizations [**BOR05**] for Hilbert modular surfaces (see Theorem 1.2).

Before we state these results, we first recall some of Zagier's results. For integers λ, let $M^!_{\lambda+\frac{1}{2}}$ be the space of weight $\lambda+\frac{1}{2}$ *weakly holomorphic modular forms* on $\Gamma_0(4)$ satisfying the "Kohnen plus-space" condition. Recall that a meromorphic modular form is weakly holomorphic if its poles (if there are any) are supported at the cusps, and it satisfies Kohnen's plus-space condition if its q-expansion has the form

$$\sum_{(-1)^\lambda n\equiv 0,1 \pmod 4} a(n)q^n. \tag{1.2}$$

Throughout, let $d\equiv 0,3 \pmod 4$ be a positive integer, let $H(d)$ be the Hurwitz-Kronecker class number for the discriminant $-d$, and let $\mathcal{Q}_d$ be the set of positive definite integral binary quadratic forms (including imprimitive forms)

$$Q(x,y)=[a,b,c]=ax^2+bxy+cy^2$$

with discriminant $D_Q=-d=b^2-4ac$. For each Q, let τ_Q be the unique root in $\mathfrak{h}$ of $Q(x,1)=0$. The singular modulus $f(\tau_Q)$, for any modular invariant $f(z)$, depends only on the equivalence class of Q under the action of $\Gamma:=\mathrm{PSL}_2(\mathbb{Z})$. If $\omega_Q\in\{1,2,3\}$ is given by

$$\omega_Q:=\begin{cases}2 & \text{if } Q\sim_\Gamma [a,0,a],\\ 3 & \text{if } Q\sim_\Gamma [a,a,a],\\ 1 & \text{otherwise,}\end{cases}$$

then, for a modular invariant $f(z)$, define the trace $\mathrm{Tr}(f;d)$ by

$$\mathrm{Tr}(f;d):=\sum_{Q\in\mathcal{Q}_d/\Gamma}\frac{f(\tau_Q)}{\omega_Q}. \tag{1.3}$$

Theorems 1 and 5 of [**Zag02**] imply the following.

Theorem. (Zagier)
If $f(z)\in\mathbb{Z}[j(z)]$ has a Fourier expansion with constant term 0, then there is a finite principal part $A_f(z)=\sum_{n\le 0}a_f(n)q^n$ for which

$$A_f(z)+\sum_{0<d\equiv 0,3 \pmod 4}\mathrm{Tr}(f;d)q^d\in M^!_{\frac{3}{2}}.$$

REMARK. The earlier claim about the modular form $g(z)$ is the $f(z) = J_1(z) = j(z) - 744$ case of this theorem.

REMARK. Using Poincaré series constructed [**BJO06**] by Bruinier, Jenkins and the author, Duke [**Duk06**] and Jenkins [**Jen**] have provided new proofs of this theorem by combining earlier results of Niebur [**Nie73**] with facts about Kloosterman-Salié sums.

Zagier gave several generalizations of this result. Here we highlight two of these; the first concerns "twisted traces". For fundamental discriminants D_1, let χ_{D_1} denote the associated genus character for positive definite binary quadratic forms whose discriminants are multiples of D_1. If λ is an integer and D_2 is a non-zero integer for which $(-1)^\lambda D_2 \equiv 0, 1 \pmod 4$ and $(-1)^\lambda D_1 D_2 < 0$, then define the twisted trace of a modular invariant $f(z)$, say $\mathrm{Tr}_{D_1}(f; D_2)$, by

$$\mathrm{Tr}_{D_1}(f; D_2) := \sum_{Q \in \mathcal{Q}_{|D_1 D_2|}/\Gamma} \frac{\chi_{D_1}(Q) f(\tau_Q)}{\omega_Q}. \tag{1.4}$$

If $f \in \mathbb{Z}[j(z)]$ has a Fourier expansion with constant term 0, then Zagier proved that these traces are coefficients of weight 3/2 forms (see Theorem 6 of [**Zag02**]). The second generalization involves $\mathrm{Tr}(f; d)$ for special non-holomorphic modular functions $f(z)$. In these cases, the corresponding generating functions have weight $\lambda + \frac{1}{2}$, where $\lambda \in \{-6, -4, -3, -2, -1\}$ (see Theorems 10 and 11 of [**Zag02**]).

REMARK. Kim [**Kim04, Kim**] has established the modularity for traces of singular moduli on certain genus zero congruence subgroups. Using theta lifts, Bruinier and Funke [**BF06**] (see Theorem 3.1) have recently proven a more general theorem which holds for modular functions on modular curves of arbitrary genus. Their result plays an important role in the proof of Theorem 1.2, our result for Hilbert modular surfaces.

Generalizing the arguments of Duke and Jenkins alluded to above, we show that the coefficients of certain half-integral weight Maass-Poincaré series are traces of singular moduli. This result includes the results of Zagier described above, and, as an added bonus, gives exact formulas for these traces. To construct these series, let $k := \lambda + \frac{1}{2}$, where λ is an arbitrary integer, and let $M_{\nu,\mu}(z)$ be the usual M-Whittaker function. For $s \in \mathbb{C}$ and $y \in \mathbb{R} - \{0\}$, we define

$$\mathcal{M}_s(y) := |y|^{-\frac{k}{2}} M_{\frac{k}{2}\,\mathrm{sgn}(y),\, s-\frac{1}{2}}(|y|).$$

Suppose that $m \geq 1$ is an integer with $(-1)^{\lambda+1} m \equiv 0, 1 \pmod 4$. Define $\varphi_{-m,s}(z)$ by

$$\varphi_{-m,s}(z) := \mathcal{M}_s(-4\pi m y) e(-mx),$$

where $z = x + iy$, and $e(w) := e^{2\pi i w}$. Furthermore, let

$$\Gamma_\infty := \left\{ \pm \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \ : \ n \in \mathbb{Z} \right\}$$

denote the translations within $\mathrm{SL}_2(\mathbb{Z})$. Using this notation, define the Poincaré series

$$\mathcal{F}_\lambda(-m, s; z) := \sum_{A \in \Gamma_\infty \backslash \Gamma_0(4)} (\varphi_{-m,s} \mid_k A)(z) \tag{1.5}$$

for $\mathrm{Re}(s) > 1$. Here $|_k$ denotes the usual half-integral weight k "slash operator" (see Shimura's seminal paper [**Shi73**]). If pr_λ is Kohnen's projection operator (see page 250 of [**Koh85**]) to the weight $\lambda + \frac{1}{2}$ plus-space for $\Gamma_0(4)$, then for $\lambda \notin \{0, 1\}$ define $F_\lambda(-m; z)$ by

$$(1.6) \qquad F_\lambda(-m;z) := \begin{cases} \frac{3}{2}\mathcal{F}_\lambda\left(-m, \frac{k}{2}; z\right) \mid \mathrm{pr}_\lambda & \text{if } \lambda \geq 2, \\ \frac{3}{2(1-k)\Gamma(1-k)}\mathcal{F}_\lambda\left(-m, 1-\frac{k}{2}; z\right) \mid \mathrm{pr}_\lambda & \text{if } \lambda \leq -1. \end{cases}$$

REMARK. For $\lambda = 0$ or 1 we also have series $F_\lambda(-m; z)$. Their construction requires more care. For $\lambda = 1$ this is carried out in [**BJO06**], and for $\lambda = 0$ see [**BO**].

By Theorem 3.5 of [**BJO06**], if $\lambda \geq -6$ with $\lambda \neq -5$, then $F_\lambda(-m; z) \in M^!_{\lambda+\frac{1}{2}}$. For such λ, we denote the corresponding Fourier expansions by

$$(1.7) \qquad F_\lambda(-m;z) = q^{-m} + \sum_{\substack{n\geq 0 \\ (-1)^\lambda n \equiv 0,1 \pmod 4}} b_\lambda(-m;n)q^n \in M^!_{\lambda+\frac{1}{2}}.$$

For other λ, namely $\lambda = -5$ or $\lambda \leq -7$, it turns out that the $F_\lambda(-m; z)$ are weak Maass forms of weight $\lambda + \frac{1}{2}$ (see Section 2.1). We denote their expansions by

$$(1.8) \qquad F_\lambda(-m;z) = B_\lambda(-m;z) + q^{-m} + \sum_{\substack{n\geq 0 \\ (-1)^\lambda n \equiv 0,1 \pmod 4}} b_\lambda(-m;n)q^n,$$

where $B_\lambda(-m; z)$ is the "non-holomorphic" part of $F_\lambda(-m; z)$.

EXAMPLE. If $\lambda = 1$ and $-m = -1$, then we have the modular form in (1.1)

$$-F_1(-1;z) = g(z) = -q^{-1} + 2 - 248q^3 + 492q^4 - 4119q^7 + 7256q^8 - \cdots.$$

Generalizing Zagier's results, we show that the coefficients $b_\lambda(-m; n)$ of the $F_\lambda(-m; z)$ are traces of singular moduli for functions defined by Niebur [**Nie73**]. If $I_s(x)$ denotes the usual I-Bessel function, and if $\lambda > 1$, then let

$$(1.9) \qquad \mathfrak{F}_\lambda(z) := \pi \sum_{A\in\Gamma_\infty\backslash \mathrm{SL}_2(\mathbb{Z})} \mathrm{Im}(Az)^{\frac{1}{2}} I_{\lambda-\frac{1}{2}}(2\pi \mathrm{Im}(Az))e(-\mathrm{Re}(Az)).$$

REMARK. For $\lambda = 1$, Niebur's [**Nie73**] shows that $\mathfrak{F}_1(z) = \frac{1}{2}(j(z) - 744)$, where this function is the analytic continuation, as $s \to 1$ from the right, of

$$-12 + \pi \sum_{A\in\Gamma_\infty\backslash \mathrm{SL}_2(\mathbb{Z})} \mathrm{Im}(Az)^{\frac{1}{2}} I_{s-\frac{1}{2}}(2\pi \mathrm{Im}(Az))e(-\mathrm{Re}(Az)).$$

Arguing as in [**BJO06, Duk06, Jen**], Bringmann and the author have proved [**BO**] the following:

THEOREM 1.1. (Bringmann and Ono; Theorem 1.2 of [**BO**])
If $\lambda, m \geq 1$ are integers for which $(-1)^{\lambda+1}m$ is a fundamental discriminant (which includes 1), then for each positive integer n with $(-1)^\lambda n \equiv 0, 1 \pmod 4$ we have

$$b_\lambda(-m;n) = \frac{2(-1)^{[(\lambda+1)/2]} n^{\frac{\lambda}{2}-\frac{1}{2}}}{m^{\frac{\lambda}{2}}} \cdot \mathrm{Tr}_{(-1)^{\lambda+1}m}\left(\mathfrak{F}_\lambda; n\right).$$

REMARK. A version of Theorem 1.1 holds for integers $\lambda \leq 0$. This follows from a beautiful duality (see Theorem 1.1 of [**BO**]) which generalizes an observation of Zagier. Suppose that $\lambda \geq 1$, and that m is a positive integer for which $(-1)^{\lambda+1}m \equiv 0, 1 \pmod 4$. For every positive integer n with $(-1)^{\lambda}n \equiv 0, 1 \pmod 4$, this duality asserts that

$$b_\lambda(-m; n) = -b_{1-\lambda}(-n; m).$$

REMARK. For $\lambda = 1$, Theorem 1.1 relates $b_1(-m; n)$ to traces and twisted traces of $\mathfrak{F}_1(z) = \frac{1}{2}(j(z) - 744)$. These are Theorems 1 and 6 of Zagier's paper [**Zag02**].

Theorem 1.1 is obtained by reformulating, as traces of singular moduli, exact expressions for the coefficients $b_\lambda(-m; n)$. We shall sketch the proof of this in Section 2. These exact formulas often lead to nice number theoretic consequences. Here we mention one such application which is related to the classical observation that

$$e^{\pi\sqrt{163}} = 262537412640768743.9999999999992\ldots \tag{1.10}$$

is nearly an integer.

To make this precise, we recall some classical facts. A primitive positive definite binary quadratic form Q is *reduced* if $|B| \leq A \leq C$, and $B \geq 0$ if either $|B| = A$ or $A = C$. If $-d < -4$ is a fundamental discriminant, then there are $H(d)$ reduced forms with discriminant $-d$. The set of such reduced forms, say $\mathcal{Q}_d^{\mathrm{red}}$, is a complete set of representatives for $\mathcal{Q}_d/\Gamma$. Moreover, each such reduced form has $1 \leq A \leq \sqrt{d/3}$ (see page 29 of [**Cox89**]), and has the property that τ_Q lies in the usual fundamental domain for the action of $\mathrm{SL}_2(\mathbb{Z})$

$$\mathcal{F} = \left\{-\frac{1}{2} \leq \Re(z) < \frac{1}{2} \text{ and } |z| > 1\right\} \cup \left\{-\frac{1}{2} \leq \Re(z) \leq 0 \text{ and } |z| = 1\right\}. \tag{1.11}$$

Since $J_1(z) := j(z) - 744 = q^{-1} + 196884q + \cdots$, it follows that if $G^{\mathrm{red}}(d)$ is defined by

$$G^{\mathrm{red}}(d) = \sum_{Q=(A,B,C)\in\mathcal{Q}_d^{\mathrm{red}}} e^{\pi Bi/A} \cdot e^{\pi\sqrt{d}/A}, \tag{1.12}$$

then $\mathrm{Tr}(d) - G^{\mathrm{red}}(d)$ is "small", where $\mathrm{Tr}(d) := \mathrm{Tr}(J_1; d)$. In other words, q^{-1} provides a good approximation for $J_1(z)$ for most points z. This is illustrated by (1.10) where $H(163) = 1$.

It is natural to investigate the "average value"

$$\frac{\mathrm{Tr}(d) - G^{\mathrm{red}}(d)}{H(d)},$$

which for $d = 163$ is $-0.0000000000008\ldots$. Armed with the exact formulas for $\mathrm{Tr}(d)$, it turns out that a uniform picture emerges for a slightly perturbed average, one including some non-reduced quadratic forms. For each positive integer A, let $\mathcal{Q}_{A,d}^{\mathrm{old}}$ denote the set

$$\mathcal{Q}_{A,d}^{\mathrm{old}} = \{Q = (A, B, C) \ : \text{ non-reduced with } D_Q = -d \text{ and } |B| \leq A\}. \tag{1.13}$$

Define $G^{\mathrm{old}}(d)$ by

$$G^{\mathrm{old}}(d) = \sum_{\substack{\sqrt{d}/2 \le A \le \sqrt{d/3} \\ Q \in \mathcal{Q}^{\mathrm{old}}_{A,d}}} e^{\pi B i/A} \cdot e^{\pi\sqrt{d}/A}. \tag{1.14}$$

The non-reduced forms Q contributing to $G^{\mathrm{old}}(d)$ are those primitive discriminant $-d$ forms for which τ_Q is in the bounded region obtained by connecting the two endpoints of the lower boundary of $\mathcal{F}$ with a horizontal line. The following data is quite suggestive:

$$\frac{\mathrm{Tr}(d) - G^{\mathrm{red}}(d) - G^{\mathrm{old}}(d)}{H(d)} = \begin{cases} -24.672\ldots & \text{if } d = 1931, \\ -24.483\ldots & \text{if } d = 2028, \\ -23.458\ldots & \text{if } d = 2111. \end{cases}$$

Recently, Duke has proved [**Duk06**] a result which implies the following theorem.

THEOREM. (Duke [**Duk06**])
As $-d$ ranges over negative fundamental discriminants, we have

$$\lim_{-d \to -\infty} \frac{\mathrm{Tr}(d) - G^{\mathrm{red}}(d) - G^{\mathrm{old}}(d)}{H(d)} = -24.$$

In Section 2 we shall give an explanation of the constant -24 in this theorem. We shall see that it makes a surprising appearance in the exact formulas for $\mathrm{Tr}(d)$.

We shall also describe some generalizations of Theorem 1.1 for Hilbert modular surfaces. Using the groundbreaking work of Hirzebruch and Zagier [**HZ76**] on the intersection theory of Hilbert modular surfaces as a prototype, we consider analogs of Theorem 1.1 for Hilbert modular surfaces defined over $\mathbb{Q}(\sqrt{p})$, where $p \equiv 1 \pmod 4$ is prime. As usual, let $\mathcal{O}_K := \mathbb{Z}\left[\frac{1+\sqrt{p}}{2}\right]$ be the ring of integers of the real quadratic field $K := \mathbb{Q}(\sqrt{p})$. The group $\mathrm{SL}_2(\mathcal{O}_K)$ acts on $\mathfrak{h} \times \mathfrak{h}$ by

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \circ (z_1, z_2) := \left(\frac{\alpha z_1 + \beta}{\gamma z_1 + \delta}, \frac{\alpha' z_2 + \beta'}{\gamma' z_2 + \delta'} \right).$$

Here ν' denotes the conjugate of ν in $\mathbb{Q}(\sqrt{p})$. The quotient $X_p := (\mathfrak{h} \times \mathfrak{h})/\mathrm{SL}_2(\mathcal{O}_K)$ is a non-compact surface with finitely many singularities which can be compactified by adding finitely many points (i.e. cusps). Hirzebruch showed [**Hir73**] how to resolve the singularities introduced by adding cusps using cyclic configurations of rational curves. The resulting modular surface Y_p is a nearly smooth compact algebraic surface with quotient singularities supported at those points in $\mathfrak{h} \times \mathfrak{h}$ with a non-trivial isotropy subgroup within $\mathrm{PSL}_2(\mathcal{O}_K)$.

Hirzebruch and Zagier introduced [**HZ76**] a sequence of algebraic curves

$$Z_1^{(p)}, Z_2^{(p)}, \cdots \subset X_p,$$

and studied the generating functions for their intersection numbers. They proved the striking fact that these generating functions are weight 2 modular forms, an observation which allowed them to identify spaces of modular forms with certain homology groups for Y_p. To define these curves, for a positive integer N, consider the points $(z_1, z_2) \in \mathfrak{h} \times \mathfrak{h}$ satisfying an equation of the form

$$A z_1 z_2 \sqrt{p} + \lambda z_1 - \lambda' z_2 + B\sqrt{p} = 0, \tag{1.15}$$

where $A, B \in \mathbb{Z}$, $\lambda \in \mathcal{O}_K$, and $\lambda\lambda' + ABp = N$. Each such equation defines a curve in $\mathfrak{h} \times \mathfrak{h}$ isomorphic to $\mathfrak{h}$, and their union is invariant under $\mathrm{SL}_2(\mathcal{O}_K)$. The *Hirzebruch-Zagier divisor* $Z_N^{(p)}$ is defined to be the image of this union in X_p.

REMARK. If $\left(\frac{N}{p}\right) = -1$, then one easily sees from (1.15) that $Z_N^{(p)}$ is empty.

We let $\widetilde{Z_N^{(p)}}$ denote the closure of $Z_N^{(p)}$ in Y_p. If $(\widetilde{Z_m^{(p)}}, \widetilde{Z_n^{(p)}})$ denotes the intersection number of $\widetilde{Z_m^{(p)}}$ and $\widetilde{Z_n^{(p)}}$ in Y_p, then Hirzebruch and Zagier proved in [**HZ76**], for every positive integer m, that

$$\Phi_m^{(p)}(z) := a_m^{(p)}(0) + \sum_{n=1}^{\infty} (\widetilde{Z_m^{(p)}}, \widetilde{Z_n^{(p)}}) q^n \tag{1.16}$$

is a holomorphic weight 2 modular form on $\Gamma_0(p)$ with Nebentypus $\left(\frac{\cdot}{p}\right)$. Here $a_m^{(p)}(0)$ is a simple constant arising from a volume computation. More precisely, $\Phi_m^{(p)}(z)$ is in the *plus space* $M_2^+\left(\Gamma_0(p), \left(\frac{\cdot}{p}\right)\right)$, the space of holomorphic weight 2 modular forms $F(z) = \sum_{n=0}^{\infty} a(n) q^n$ on $\Gamma_0(p)$ with Nebentypus $\left(\frac{\cdot}{p}\right)$, with the additional property that

$$a(n) = 0 \quad \text{if } \left(\frac{n}{p}\right) = -1. \tag{1.17}$$

Our generalization of Theorem 1.1 to these surfaces is also a generalization of this result of Hirzebruch and Zagier, one which involves forms in $\mathcal{M}_2\left(\Gamma_0(p), \left(\frac{\cdot}{p}\right)\right)$, the space of weakly holomorphic modular forms of weight 2 on $\Gamma_0(p)$ with Nebentypus $\left(\frac{\cdot}{p}\right)$, and $\mathcal{M}_2^+\left(\Gamma_0(p), \left(\frac{\cdot}{p}\right)\right)$, the subspace of those forms in $\mathcal{M}_2\left(\Gamma_0(p), \left(\frac{\cdot}{p}\right)\right)$ that satisfy (1.17).

To explain this, we first note that the "geometric part" of the proof of the modularity of (1.16) gives a concrete description of the intersection points $Z_m^{(p)} \cap Z_n^{(p)}$ in terms of CM points which are the "roots" of $\Gamma_0(m)$ equivalence classes of binary quadratic forms with negative discriminants of the form $-(4mn - x^2)/p$. In this context, it is natural to consider the traces of singular moduli over the points constituting $Z_m^{(p)} \cap Z_n^{(p)}$.

To state our result, suppose that $\ell = 1$ or that ℓ is an odd prime with $\left(\frac{\ell}{p}\right) \neq -1$, and let $\Gamma_0^*(\ell)$ be the projective image of the extension of $\Gamma_0(\ell)$ by the Fricke involution $W_\ell = \left(\begin{smallmatrix} 0 & -1 \\ \ell & 0 \end{smallmatrix}\right)$ in $\mathrm{PSL}_2(\mathbb{R})$. Suppose that $f(z) = \sum_{n \gg -\infty} a(n) q^n \in \mathcal{M}_0(\Gamma_0^*(\ell))$, the space of weakly holomorphic modular functions with respect to $\Gamma_0^*(\ell)$, and suppose that $a(0) = 0$. We define the "trace" of $f(z)$ over $Z_\ell^{(p)} \cap Z_n^{(p)}$ by

$$(Z_\ell^{(p)}, Z_n^{(p)})_f^{\mathrm{tr}} := \sum_{\tau \in Z_\ell^{(p)} \cap Z_n^{(p)}} \frac{f(\tau)}{\#\Gamma_0^*(\ell)_\tau}, \tag{1.18}$$

where $\Gamma_0^*(\ell)_\tau$ is the stabilizer of τ in $\Gamma_0^*(\ell)$. We consider their generating functions

$$\Phi_{\ell,f}^{(p)}(z) := A_{\ell,f}^{(p)}(z) + B_{\ell,f}^{(p)}(z) + \sum_{n=1}^{\infty} (Z_\ell^{(p)}, Z_n^{(p)})_f^{\mathrm{tr}} q^n, \tag{1.19}$$

where

$$A_{\ell,f}^{(p)}(z) := -\epsilon(\ell)\sum_{m,n\geq 1} ma(-mn)\left(\sum_{\substack{x\in\mathbb{Z}\\ x^2\equiv m^2p \pmod{2\ell}}} q^{\frac{x^2-m^2p}{4\ell}} + \sum_{\substack{x\in\mathbb{Z}\\ x\equiv m \pmod 2}} q^{\frac{x^2\ell-m^2p\ell}{4}}\right),$$

$$B_{\ell,f}^{(p)}(z) := 2\epsilon(\ell)\sum_{n\geq 1}(\sigma_1(n)+\ell\sigma_1(n/\ell))a(-n)\sum_{x\in\mathbb{Z}} q^{\ell x^2},$$

and where $\epsilon(\ell) = 1/2$ for $\ell = 1$, and is 1 otherwise. As usual, $\sigma_1(x)$ denotes the sum of the positive divisors of x if x is an integer, and is zero if x is not an integer.

Bringmann, Rouse and the author have shown [**BOR05**] that these generating functions are also modular forms of weight 2. In particular, we obtain a linear map:

$$\Phi_{\ell,\star}^{(p)} : \mathcal{M}_0(\Gamma_0^*(\ell)) \to \mathcal{M}_2\left(\Gamma_0(p\ell^2), \left(\frac{\cdot}{p}\right)\right)$$

(where the map is defined for the subspace of those functions with constant term 0).

THEOREM 1.2. (Bringmann, Ono and Rouse; Theorem 1.1 of [**BOR05**]) *Suppose that* $p \equiv 1 \pmod 4$ *is prime, and that* $\ell = 1$ *or is an odd prime with* $\left(\frac{\ell}{p}\right) \neq -1$. *If* $f(z) = \sum_{n\gg-\infty} a(n)q^n \in \mathcal{M}_0(\Gamma_0^*(\ell))$ *, with* $a(0) = 0$*, then the generating function* $\Phi_{\ell,f}^{(p)}(z)$ *is in* $\mathcal{M}_2\left(\Gamma_0(p\ell^2), \left(\frac{\cdot}{p}\right)\right)$.

In Section 3 we combine the geometry of these surfaces with recent work of Bruinier and Funke [**BF06**] to sketch the proof of Theorem 1.2. In this section we characterize these modular forms $\Phi_{\ell,f}^{(p)}(z)$ when $f(z) = J_1(z) := j(z) - 744$. In terms of the classical Weber functions

$$\mathfrak{f}_1(z) = \frac{\eta(z/2)}{\eta(z)} \quad \text{and} \quad \mathfrak{f}_2(z) = \sqrt{2}\cdot\frac{\eta(2z)}{\eta(z)}, \tag{1.20}$$

we have the following exact description.

THEOREM 1.3. (Bringmann, Ono and Rouse; Theorem 1.2 of [**BOR05**]) *If* $p \equiv 1 \pmod 4$ *is prime, then*

$$\Phi_{1,J_1}^{(p)}(z) = \frac{\eta(2z)\eta(2pz)E_4(pz)\mathfrak{f}_2(2z)^2\mathfrak{f}_2(2pz)^2}{4\eta(pz)^6}\cdot\left(\mathfrak{f}_1(4z)^4\mathfrak{f}_2(z)^2 - \mathfrak{f}_1(4pz)^4\mathfrak{f}_2(pz)^2\right).$$

Although Theorem 1.3 gives a precise description of the forms $\Phi_{1,J_1}^{(p)}(z)$, it is interesting to note that they are intimately related to Hilbert class polynomials, the polynomials given by

$$H_D(x) = \prod_{\tau\in\mathcal{C}_D}(x - j(\tau)) \in \mathbb{Z}[x], \tag{1.21}$$

where $\mathcal{C}_D$ denotes the equivalence classes of CM points with discriminant $-D$. Each $H_D(x)$ is an irreducible polynomial in $\mathbb{Z}[x]$ which generates a class field extension of $\mathbb{Q}(\sqrt{-D})$. Define $N_p(z)$ as the "multiplicative norm" of $\Phi_{1,J_1}(z)$

$$N_p(z) := \prod_{M\in\Gamma_0(p)\backslash\mathrm{SL}_2(\mathbb{Z})} \Phi_{1,J_1}^{(p)}|M. \tag{1.22}$$

If $N_p^*(z)$ is the normalization of $N_p(z)$ with leading coefficient 1, then we have

$$N_p^*(z) = \begin{cases} \Delta(z)H_{75}(j(z)) & \text{if } p=5, \\ E_4(z)\Delta(z)^2H_3(j(z))H_{507}(j(z)) & \text{if } p=13, \\ \Delta(z)^3H_4(j(z))H_{867}(j(z)) & \text{if } p=17, \\ \Delta(z)^5H_7(j(z))^2H_{2523}(j(z)) & \text{if } p=29, \end{cases}$$

where $\Delta(z) = \eta(z)^{24}$ is the usual Delta-function. These examples illustrate a general phenomenon in which $N_p^*(z)$ is essentially a product of certain Hilbert class polynomials.

To state the general result, define integers $a(p)$, $b(p)$, and $c(p)$ by

$$a(p) := \frac{1}{2}\left(\left(\frac{3}{p}\right)+1\right), \tag{1.23}$$

$$b(p) := \frac{1}{2}\left(\left(\frac{2}{p}\right)+1\right), \tag{1.24}$$

$$c(p) := \frac{1}{6}\left(p-\left(\frac{3}{p}\right)\right), \tag{1.25}$$

and let $\mathcal{D}_p$ be the negative discriminants $-D \neq -3, -4$ of the form $\frac{x^2-4p}{16f^2}$ with $x, f \geq 1$.

Theorem 1.4. (Bringmann, Ono and Rouse; Theorem 1.3 of [**BOR05**]) *Assume the notation above. If* $p \equiv 1 \pmod 4$ *is prime, then*

$$N_p^*(z) = (E_4(z)H_3(j(z)))^{a(p)} \cdot H_4(j(z))^{b(p)} \cdot \Delta(z)^{c(p)} \cdot H_{3\cdot p^2}(j(z)) \cdot \prod_{-D\in\mathcal{D}_p} H_D(j(z))^2.$$

The remainder of this survey is organized as follows. In Section 2 we compute the coefficients of the Maass-Poincaré series $F_\lambda(-m;z)$, and we sketch the proof of Theorem 1.1 by employing facts about Kloosterman-Salié sums. Moreover, we give a brief discussion of Duke's theorem on the "average values"

$$\frac{\mathrm{Tr}(d) - G^{\mathrm{red}}(d) - G^{\mathrm{old}}(d)}{H(d)}.$$

In Section 3 we sketch the proof of Theorems 1.2, 1.3 and 1.4.

Acknowledgements

The author thanks Yuri Tschinkel and Bill Duke for organizing the exciting Gauss-Dirichlet Conference, and for inviting him to speak on singular moduli.

2. Maass-Poincaré series and the proof of Theorem 1.1

In this section we sketch the proof of Theorem 1.1. We first recall the construction of the forms $F_\lambda(-m;z)$, and we then give exact formulas for the coefficients $b_\lambda(-m;n)$. The proof then follows from classical observations about Kloosterman-Salié sums and their reformulation as Poincaré series.

2.1. Maass-Poincaré series. Here we give more details on the Poincaré series $F_\lambda(-m;z)$ (see [**Bru02, BO, BJO06, Hir73**] for more on such series). Suppose that λ is an integer, and that $k := \lambda + \frac{1}{2}$. For each $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Gamma_0(4)$, let

$$j(A,z) := \left(\frac{\gamma}{\delta}\right)\epsilon_\delta^{-1}(\gamma z+\delta)^{\frac{1}{2}}$$

be the factor of automorphy for half-integral weight modular forms. If $f : \mathfrak{h} \to \mathbb{C}$ is a function, then for $A \in \Gamma_0(4)$ we let

$$(f \mid_k A)(z) := j(A,z)^{-2\lambda-1} f(Az). \tag{2.1}$$

As usual, let $z = x + iy$, and for $s \in \mathbb{C}$ and $y \in \mathbb{R} - \{0\}$, we let

$$\mathcal{M}_s(y) := |y|^{-\frac{k}{2}} M_{\frac{k}{2}\operatorname{sgn}(y),\, s-\frac{1}{2}}(|y|), \tag{2.2}$$

where $M_{\nu,\mu}(z)$ is the standard M-Whittaker function which is a solution to the differential equation

$$\frac{\partial^2 u}{\partial z^2} + \left(-\frac{1}{4} + \frac{\nu}{z} + \frac{\frac{1}{4}-\mu^2}{z^2}\right) u = 0.$$

If m is a positive integer, and $\varphi_{-m,s}(z)$ is given by

$$\varphi_{-m,s}(z) := \mathcal{M}_s(-4\pi m y) e(-mx),$$

then recall from the introduction that

$$\mathcal{F}_\lambda(-m,s;z) := \sum_{A \in \Gamma_\infty \backslash \Gamma_0(4)} (\varphi_{-m,s} \mid_k A)(z). \tag{2.3}$$

It is easy to verify that $\varphi_{-m,s}(z)$ is an eigenfunction, with eigenvalue

$$s(1-s) + (k^2-2k)/4, \tag{2.4}$$

of the weight k hyperbolic Laplacian

$$\Delta_k := -y^2\left(\frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2}\right) + iky\left(\frac{\partial}{\partial x} + i\frac{\partial}{\partial y}\right).$$

Since $\varphi_{-m,s}(z) = O\left(y^{\operatorname{Re}(s)-\frac{k}{2}}\right)$ as $y \to 0$, it follows that $\mathcal{F}_\lambda(-m,s;z)$ converges absolutely for $\operatorname{Re}(s) > 1$, is a $\Gamma_0(4)$-invariant eigenfunction of the Laplacian, and is real analytic.

Special values, in s, of these series provide examples of half-integral weight weak Maass forms. A *weak Maass form of weight* k for the group $\Gamma_0(4)$ is a smooth function $f : \mathfrak{h} \to \mathbb{C}$ satisfying the following:

(1) For all $A \in \Gamma_0(4)$ we have
$$(f \mid_k A)(z) = f(z).$$
(2) We have $\Delta_k f = 0$.
(3) The function $f(z)$ has at most linear exponential growth at all the cusps.

In particular, the discussion above implies that the special s-values at $k/2$ and $1-k/2$ of $\mathcal{F}_\lambda(-m,s;z)$ are weak Maass forms of weight $k = \lambda + \frac{1}{2}$ when the series is absolutely convergent. If $\lambda \notin \{0,1\}$ and $m \geq 1$ is an integer for which $(-1)^{\lambda+1}m \equiv 0,1 \pmod 4$, then this implies that the Kohnen projections $F_\lambda(-m;z)$, from the introduction, are weak Maass forms of weight $k = \lambda + \frac{1}{2}$ on $\Gamma_0(4)$ in Kohnen's plus space.

If $\lambda = 1$ and m is a positive integer for which $m \equiv 0, 1 \pmod 4$, then define $F_1(-m; z)$ by

$$F_1(-m;z) := \frac{3}{2}\mathcal{F}_1\left(-m, \frac{3}{4}; z\right) \mid \mathrm{pr}_1 + 24\delta_{\Box,m}G(z). \tag{2.5}$$

The function $G(z)$ is given by the Fourier expansion

$$G(z) := \sum_{n=0}^{\infty} H(n)q^n + \frac{1}{16\pi\sqrt{y}} \sum_{n=-\infty}^{\infty} \beta(4\pi n^2 y)q^{-n^2},$$

where $H(0) = -1/12$ and

$$\beta(s) := \int_1^{\infty} t^{-\frac{3}{2}} e^{-st} dt.$$

Proposition 3.6 of [**BJO06**] establishes that each $F_1(-m; z)$ is in $M^!_{\frac{3}{2}}$.

Remark. The function $G(z)$ plays an important role in the work of Hirzebruch and Zagier [**HZ76**] which is intimately related to Theorems 1.2, 1.3 and 1.4.

Remark. An analogous argument is used to define the series $F_0(-m; z) \in M^!_{\frac{1}{2}}$.

2.2. Exact formulas for the coefficients $b_\lambda(-m; n)$. Here we give exact formulas for the $b_\lambda(-m; n)$, the coefficients of the holomorphic parts of the Maass-Poincaré series $F_\lambda(-m; z)$. These coefficients are given as explicit infinite sums in half-integral weight Kloosterman sums weighted by Bessel functions. To define these Kloosterman sums, for odd δ let

$$\epsilon_\delta := \begin{cases} 1 & \text{if } \delta \equiv 1 \pmod 4, \\ i & \text{if } \delta \equiv 3 \pmod 4. \end{cases} \tag{2.6}$$

If λ is an integer, then we define the $\lambda + \frac{1}{2}$ weight Kloosterman sum $K_\lambda(m, n, c)$ by

$$K_\lambda(m,n,c) := \sum_{v \pmod{c}^*} \left(\frac{c}{v}\right) \epsilon_v^{2\lambda+1} e\left(\frac{m\bar{v} + nv}{c}\right). \tag{2.7}$$

In the sum, v runs through the primitive residue classes modulo c, and $\bar{v}$ denotes the multiplicative inverse of v modulo c. In addition, for convenience we define $\delta_{\Box,m} \in \{0, 1\}$ by

$$\delta_{\Box,m} := \begin{cases} 1 & \text{if } m \text{ is a square}, \\ 0 & \text{otherwise}. \end{cases} \tag{2.8}$$

Finally, for integers c define $\delta_{\mathrm{odd}}(c)$ by

$$\delta_{\mathrm{odd}}(c) := \begin{cases} 1 & \text{if } c \text{ is odd}, \\ 0 & \text{otherwise}. \end{cases}$$

Theorem 2.1. *Suppose that λ is an integer, and suppose that m is a positive integer for which $(-1)^{\lambda+1}m \equiv 0, 1 \pmod 4$. Furthermore, suppose that n is a non-negative integer for which $(-1)^\lambda n \equiv 0, 1 \pmod 4$.*

(1) *If $\lambda \geq 2$, then $b_\lambda(-m;0)=0$, and for positive n we have*

$$b_\lambda(-m;n) = (-1)^{[(\lambda+1)/2]}\pi\sqrt{2}(n/m)^{\frac{\lambda}{2}-\frac{1}{4}}(1-(-1)^\lambda i) \times \sum_{\substack{c>0 \\ c\equiv 0 \pmod 4}} (1+\delta_{\mathrm{odd}}(c/4))\frac{K_\lambda(-m,n,c)}{c}\cdot I_{\lambda-\frac{1}{2}}\left(\frac{4\pi\sqrt{mn}}{c}\right).$$

(2) *If $\lambda \leq -1$, then*

$$b_\lambda(-m;0) = (-1)^{[(\lambda+1)/2]}\pi^{\frac{3}{2}-\lambda}2^{1-\lambda}m^{\frac{1}{2}-\lambda}(1-(-1)^\lambda i) \times \frac{1}{(\frac{1}{2}-\lambda)\Gamma(\frac{1}{2}-\lambda)}\sum_{\substack{c>0 \\ c\equiv 0 \pmod 4}} (1+\delta_{\mathrm{odd}}(c/4))\frac{K_\lambda(-m,0,c)}{c^{\frac{3}{2}-\lambda}},$$

and for positive n we have

$$b_\lambda(-m;n) = (-1)^{[(\lambda+1)/2]}\pi\sqrt{2}(n/m)^{\frac{\lambda}{2}-\frac{1}{4}}(1-(-1)^\lambda i) \times \sum_{\substack{c>0 \\ c\equiv 0 \pmod 4}} (1+\delta_{\mathrm{odd}}(c/4))\frac{K_\lambda(-m,n,c)}{c}\cdot I_{\frac{1}{2}-\lambda}\left(\frac{4\pi\sqrt{mn}}{c}\right).$$

(3) *If $\lambda = 1$, then $b_1(-m;0) = -2\delta_{\Box,m}$, and for positive n we have*

$$b_1(-m;n) = 24\delta_{\Box,m}H(n) - \pi\sqrt{2}(n/m)^{\frac{1}{4}}(1+i) \times \sum_{\substack{c>0 \\ c\equiv 0 \pmod 4}} (1+\delta_{\mathrm{odd}}(c/4))\frac{K_1(-m,n,c)}{c}\cdot I_{\frac{1}{2}}\left(\frac{4\pi\sqrt{mn}}{c}\right).$$

(4) *If $\lambda = 0$, then $b_0(-m;0)=0$, and for positive n we have*

$$b_0(-m;n) = -24\delta_{\Box,n}H(m) + \pi\sqrt{2}(m/n)^{\frac{1}{4}}(1-i) \times \sum_{\substack{c>0 \\ c\equiv 0 \pmod 4}} (1+\delta_{\mathrm{odd}}(c/4))\frac{K_0(-m,n,c)}{c}\cdot I_{\frac{1}{2}}\left(\frac{4\pi\sqrt{mn}}{c}\right).$$

Remark. For positive integers m and n, the formulas for $b_\lambda(-m;n)$ are nearly uniform in λ. In fact, this uniformity may be used to derive a nice duality (see Theorem 1.1 of [**BO**]) for these coefficients. More precisely, suppose that $\lambda \geq 1$, and that m is a positive integer for which $(-1)^{\lambda+1}m \equiv 0,1 \pmod 4$. For every positive integer n with $(-1)^\lambda n \equiv 0,1 \pmod 4$, this duality asserts that

$$b_\lambda(-m;n) = -b_{1-\lambda}(-n;m).$$

The proof of Theorem 2.1 requires some further preliminaries. For $s\in\mathbb{C}$ and $y\in\mathbb{R}-\{0\}$, we let

$$\mathcal{W}_s(y) := |y|^{-\frac{k}{2}}W_{\frac{k}{2}\,\mathrm{sgn}(y),\,s-\frac{1}{2}}(|y|), \tag{2.9}$$

where $W_{\nu,\mu}$ denotes the usual W-Whittaker function. For $y>0$, we have the relations

$$\mathcal{M}_{\frac{k}{2}}(-y) = e^{\frac{y}{2}}, \tag{2.10}$$

$$\mathcal{W}_{1-\frac{k}{2}}(y) = \mathcal{W}_{\frac{k}{2}}(y) = e^{-\frac{y}{2}}, \tag{2.11}$$

and

$$\mathcal{W}_{1-\frac{k}{2}}(-y) = \mathcal{W}_{\frac{k}{2}}(-y) = e^{\frac{y}{2}}\Gamma\left(1-k, y\right), \tag{2.12}$$

where

$$\Gamma(a,x) := \int_x^\infty e^{-t}t^a \frac{dt}{t}$$

is the incomplete Gamma function. For $z \in \mathbb{C}$, the functions $M_{\nu,\mu}(z)$ and $M_{\nu,-\mu}(z)$ are related by the identity

$$W_{\nu,\mu}(z) = \frac{\Gamma(-2\mu)}{\Gamma(\frac{1}{2}-\mu-\nu)}M_{\nu,\mu}(z) + \frac{\Gamma(2\mu)}{\Gamma(\frac{1}{2}+\mu-\nu)}M_{\nu,-\mu}(z).$$

From these facts, we easily find, for $y > 0$, that

$$\mathcal{M}_{1-\frac{k}{2}}(-y) = (k-1)e^{\frac{y}{2}}\Gamma(1-k,y) + (1-k)\Gamma(1-k)e^{\frac{y}{2}}. \tag{2.13}$$

Sketch of the proof of Theorem 2.1. For simplicity, suppose that $\lambda \notin \{0,1\}$, and suppose that m is a positive integer for which $(-1)^{\lambda+1}m \equiv 0, 1 \pmod 4$. Computing the Fourier expansion requires the integral

$$\int_{-\infty}^{\infty} z^{-k}\mathcal{M}_s\left(-4\pi m\frac{y}{c^2|z|^2}\right)e\left(\frac{mx}{c^2|z|^2} - nx\right)dx,$$

which may be found on p. 357 of [**Hir73**]. This calculation implies that $\mathcal{F}_\lambda(-m,s;z)$ has a Fourier expansion of the form

$$\mathcal{F}_\lambda(-m,s;z) = \mathcal{M}_s(-4\pi my)e(-mx) + \sum_{n\in\mathbb{Z}} c(n,y,s)e(nx).$$

If $J_s(x)$ is the usual Bessel function of the first kind, then the coefficients $c(n,y,s)$ are given as follows. If $n < 0$, then

$$c(n,y,s) := \frac{2\pi i^{-k}\Gamma(2s)}{\Gamma(s-\frac{k}{2})}\left|\frac{n}{m}\right|^{\frac{\lambda}{2}-\frac{1}{4}} \sum_{\substack{c>0\\ c\equiv 0 \pmod 4}} \frac{K_\lambda(-m,n,c)}{c} J_{2s-1}\left(\frac{4\pi\sqrt{|mn|}}{c}\right)\mathcal{W}_s(4\pi ny).$$

If $n > 0$, then

$$c(n,y,s) := \frac{2\pi i^{-k}\Gamma(2s)}{\Gamma(s+\frac{k}{2})}(n/m)^{\frac{\lambda}{2}-\frac{1}{4}} \sum_{\substack{c>0\\ c\equiv 0 \pmod 4}} \frac{K_\lambda(-m,n,c)}{c} I_{2s-1}\left(\frac{4\pi\sqrt{mn}}{c}\right)\mathcal{W}_s(4\pi ny).$$

Lastly, if $n = 0$, then

$$c(0,y,s) := \frac{4^{\frac{3}{4}-\frac{\lambda}{2}}\pi^{\frac{3}{4}+s-\frac{\lambda}{2}}i^{-k}m^{s-\frac{\lambda}{2}-\frac{1}{4}}y^{\frac{3}{4}-s-\frac{\lambda}{2}}\Gamma(2s-1)}{\Gamma(s+\frac{k}{2})\Gamma(s-\frac{k}{2})} \sum_{\substack{c>0\\ c\equiv 0 \pmod 4}} \frac{K_\lambda(-m,0,c)}{c^{2s}}.$$

The Fourier expansion defines an analytic continuation of $\mathcal{F}_\lambda(-m,s;z)$ to $\mathrm{Re}(s) > 3/4$. For $\lambda \geq 2$, the presence of the Γ-factor above implies that the Fourier coefficients $c(n,y,s)$ vanish for negative n. Therefore, $\mathcal{F}_\lambda(-m,\frac{k}{2};z)$ is a weakly holomorphic modular form on $\Gamma_0(4)$. Applying Kohnen's projection operator (see page 250 of [**Koh85**]) to these series gives Theorem 2.1 (1).

As we have seen, if $\lambda \leq -1$, then $\mathcal{F}_\lambda(-m, 1-\frac{k}{2}; z)$ is a weak Maass form of weight $k = \lambda + \frac{1}{2}$ on $\Gamma_0(4)$. Using (2.12) and (2.13), we find that its Fourier expansion has the form

$$\begin{aligned}(2.14)\qquad &\mathcal{F}_\lambda\left(-m, 1-\frac{k}{2}; z\right)\\ &\quad = (k-1)\left(\Gamma(1-k, 4\pi m y) - \Gamma(1-k)\right) q^{-m} + \sum_{n\in\mathbb{Z}} c(n,y) e(nz),\end{aligned}$$

where the coefficients $c(n, y)$, for $n < 0$, are given by

$$2\pi i^{-k}(1-k)\left|\frac{n}{m}\right|^{\frac{\lambda}{2}-\frac{1}{4}} \Gamma(1-k, 4\pi|n|y). \sum_{\substack{c>0\\ c\equiv 0 \pmod 4}} \frac{K_\lambda(-m,n,c)}{c} J_{\frac{1}{2}-\lambda}\left(\frac{4\pi}{c}\sqrt{|mn|}\right).$$

For $n \geq 0$, (2.11) allows us to conclude that the $c(n, y)$ are given by

$$\begin{cases} 2\pi i^{-k}\Gamma(2-k)(n/m)^{\frac{\lambda}{2}-\frac{1}{4}} \displaystyle\sum_{\substack{c>0\\ c\equiv 0 \pmod 4}} \frac{K_\lambda(-m,n,c)}{c} \cdot I_{\frac{1}{2}-\lambda}\left(\frac{4\pi}{c}\sqrt{mn}\right), & n>0,\\ 4^{\frac{3}{4}-\frac{\lambda}{2}}\pi^{\frac{3}{2}-\lambda} i^{-k} m^{\frac{1}{2}-\lambda} \displaystyle\sum_{\substack{c>0\\ c\equiv 0 \pmod 4}} \frac{K_\lambda(-m,0,c)}{c^{\frac{3}{2}-\lambda}}. & n=0.\end{cases}$$

One easily checks that the claimed formulas for $b_\lambda(-m; n)$ are obtained from these formulas by applying Kohnen's projection operator pr_λ. □

Remark. In addition to those $\lambda \geq 0$, if $\lambda \in \{-6, -4, -3, -2, -1\}$, then the functions $F_\lambda(-m; z)$ are in $M^!_{\lambda+\frac{1}{2}}$, and their q-expansions are of the form

$$F_\lambda(-m; z) = q^{-m} + \sum_{\substack{n\geq 0\\ (-1)^\lambda n \equiv 0,1 \pmod 4}} b_\lambda(-m; n) q^n. \tag{2.15}$$

This claim is equivalent to the vanishing of the non-holomorphic terms appearing in the proof of Theorem 2.1 for these λ. This vanishing is proved in Section 2 of [**BO**].

2.3. Sketch of the proof of Theorem 1.1. Here we sketch the proof of Theorem 1.1. Armed with Theorem 2.1, this proof reduces to classical facts relating half-integral weight Kloosterman sums to Salié sums. To define these sums, suppose that $0 \neq D_1 \equiv 0, 1 \pmod 4$. If λ is an integer, $D_2 \neq 0$ is an integer for which $(-1)^\lambda D_2 \equiv 0, 1 \pmod 4$, and N is a positive multiple of 4, then define the generalized Salié sum $S_\lambda(D_1, D_2, N)$ by

(2.16)

$$S_\lambda(D_1, D_2, N) := \sum_{\substack{x \pmod N\\ x^2 \equiv (-1)^\lambda D_1 D_2 \pmod N}} \chi_{D_1}\left(\frac{N}{4}, x, \frac{x^2 - (-1)^\lambda D_1 D_2}{N}\right) e\left(\frac{2x}{N}\right),$$

where $\chi_{D_1}(a, b, c)$, for a binary quadratic form $Q = [a, b, c]$, is given by

(2.17)

$$\chi_{D_1}(a,b,c) := \begin{cases} 0 & \text{if } (a,b,c,D_1) > 1,\\ \left(\frac{D_1}{r}\right) & \text{if } (a,b,c,D_1) = 1 \text{ and } Q \text{ represents } r \text{ with } (r, D_1) = 1.\end{cases}$$

REMARK. If $D_1 = 1$, then χ_{D_1} is trivial. Therefore, if $(-1)^\lambda D_2 \equiv 0, 1 \pmod 4$, then

$$S_\lambda(1, D_2, N) = \sum_{\substack{x \pmod N \\ x^2 \equiv (-1)^\lambda D_2 \pmod N}} e\left(\frac{2x}{N}\right).$$

Half-integral weight Kloosterman sums are essentially equal to such Salié sums, a fact which plays a fundamental role throughout the theory of half-integral weight modular forms. The following proposition is due to Kohnen (see Proposition 5 of [**Koh85**]).

PROPOSITION 2.2. *Suppose that N is a positive multiple of 4. If λ is an integer, and D_1 and D_2 are non-zero integers for which $D_1, (-1)^\lambda D_2 \equiv 0, 1 \pmod 4$, then*

$$N^{-\frac{1}{2}}(1-(-1)^\lambda i)(1+\delta_{\mathrm{odd}}(N/4)) \cdot K_\lambda((-1)^\lambda D_1, D_2, N) = S_\lambda(D_1, D_2, N).$$

As a consequence, we may rewrite the formulas in Theorem 2.1 using Salié sums. The following proposition, well known to experts, then describes these Salié sums as Poincaré-type series over CM points.

PROPOSITION 2.3. *Suppose that λ is an integer, and that D_1 is a fundamental discriminant. If D_2 is a non-zero integer for which $(-1)^\lambda D_2 \equiv 0, 1 \pmod 4$ and $(-1)^\lambda D_1 D_2 < 0$, then for every positive integer a we have*

$$S_\lambda(D_1, D_2, 4a) = 2 \sum_{Q \in \mathcal{Q}_{|D_1 D_2|}/\Gamma} \frac{\chi_{D_1}(Q)}{\omega_Q} \sum_{\substack{A \in \Gamma_\infty \backslash \mathrm{SL}_2(\mathbb{Z}) \\ \mathrm{Im}(A\tau_Q) = \frac{\sqrt{|D_1 D_2|}}{2a}}} e\left(-\mathrm{Re}\left(A\tau_Q\right)\right).$$

PROOF. For every integral binary quadratic form

$$Q(x, y) = ax^2 + bxy + cy^2$$

of discriminant $(-1)^\lambda D_1 D_2$, let $\tau_Q \in \mathfrak{h}$ be as before. Clearly τ_Q is equal to

$$\tau_Q = \frac{-b + i\sqrt{|D_1 D_2|}}{2a}, \tag{2.18}$$

and the coefficient b of Q solves the congruence

$$b^2 \equiv (-1)^\lambda D_1 D_2 \pmod{4a}. \tag{2.19}$$

Conversely, every solution of (2.19) corresponds to a quadratic form with an associated CM point thereby providing a one-to-one correspondence between the solutions of

$$b^2 - 4ac = (-1)^\lambda D_1 D_2 \qquad (a, b, c \in \mathbb{Z}, a, c > 0)$$

and the points of the orbits

$$\bigcup_Q \left\{ A\tau_Q : \ A \in \mathrm{SL}_2(\mathbb{Z})/\Gamma_{\tau_Q} \right\},$$

where Γ_{τ_Q} denotes the isotropy subgroup of τ_Q in $\mathrm{SL}_2(\mathbb{Z})$, and where Q varies over the representatives of $\mathcal{Q}_{|D_1 D_2|}/\Gamma$. The group Γ_∞ preserves the imaginary part of such a CM point τ_Q, and preserves (2.19). However, it does not preserve the middle coefficient b of the corresponding quadratic forms modulo $4a$. It identifies the congruence classes $b, b+2a \pmod{4a}$ appearing in the definition of $S_\lambda(D_1, D_2, 4a)$. Since $\chi_{D_1}(Q)$ is fixed under the action of Γ_∞, the corresponding summands for such pairs of congruence classes are equal. Proposition 2.3 follows since $\#\Gamma_{\tau_Q} = 2\omega_Q$, and since both Γ_{τ_Q} and Γ_∞ contain the negative identity matrix. $\square$

Sketch of the proof of Theorem 1.1. Here we prove the cases where $\lambda \geq 2$. The argument when $\lambda = 1$ is identical. For $\lambda \geq 2$, Theorem 2.1 (1) implies that

$$b_\lambda(-m;n) = (-1)^{[(\lambda+1)/2]}\pi\sqrt{2}(n/m)^{\frac{\lambda}{2}-\frac{1}{4}}(1-(-1)^\lambda i) \times \sum_{\substack{c>0 \\ c\equiv 0 \pmod 4}} (1+\delta_{\text{odd}}(c/4))\frac{K_\lambda(-m,n,c)}{c}\cdot I_{\lambda-\frac{1}{2}}\left(\frac{4\pi\sqrt{mn}}{c}\right).$$

Using Proposition 2.2, where $D_1 = (-1)^{\lambda+1}m$ and $D_2 = n$, for integers $N = c$ which are positive multiples of 4, we have

$$c^{-\frac{1}{2}}(1-(-1)^\lambda i)(1+\delta_{\text{odd}}(c/4))\cdot K_\lambda(-m,n,c) = S_\lambda((-1)^{\lambda+1}m,n,c).$$

These identities, combined with the change of variable $c = 4a$, give

$$b_\lambda(-m;n) = \frac{(-1)^{[(\lambda+1)/2]}\pi}{\sqrt{2}}(n/m)^{\frac{\lambda}{2}-\frac{1}{4}}\sum_{a=1}^{\infty}\frac{S_\lambda((-1)^{\lambda+1}m,n,4a)}{\sqrt{a}}\cdot I_{\lambda-\frac{1}{2}}\left(\frac{\pi\sqrt{mn}}{a}\right).$$

Using Proposition 2.3, this becomes

$$b_\lambda(-m;n) = \frac{2(-1)^{[(\lambda+1)/2]}\pi}{\sqrt{2}}(n/m)^{\frac{\lambda}{2}-\frac{1}{4}}\sum_{Q\in\mathcal{Q}_{nm}/\Gamma}\frac{\chi_{(-1)^{\lambda+1}m}(Q)}{\omega_Q} \sum_{a=1}^{\infty}\sum_{\substack{A\in\Gamma_\infty\backslash\mathrm{SL}_2(\mathbb{Z}) \\ \mathrm{Im}(A\tau_Q)=\frac{\sqrt{mn}}{2a}}}\frac{I_{\lambda-\frac{1}{2}}(2\pi\mathrm{Im}(A\tau_Q))}{\sqrt{a}}\cdot e(-\mathrm{Re}(A\tau_Q)).$$

The definition of $\mathfrak{F}_\lambda(z)$ in (1.9), combined with the obvious change of variable relating $1/\sqrt{a}$ to $\mathrm{Im}(A\tau_Q)^{\frac{1}{2}}$, gives

$$\begin{aligned} b_\lambda(-m;n) &= \frac{2(-1)^{[(\lambda+1)/2]}n^{\frac{\lambda}{2}-\frac{1}{2}}}{m^{\frac{\lambda}{2}}}\cdot\pi\sum_{Q\in\mathcal{Q}_{nm}/\Gamma}\frac{\chi_{(-1)^{\lambda+1}m}(Q)}{\omega_Q} \\ &\quad \sum_{A\in\Gamma_\infty\backslash\mathrm{SL}_2(\mathbb{Z})}\mathrm{Im}(A\tau_Q)^{\frac{1}{2}}\cdot I_{\lambda-\frac{1}{2}}(2\pi\mathrm{Im}(A\tau_Q))e(-\mathrm{Re}(A\tau_Q)) \\ &= \frac{2(-1)^{[(\lambda+1)/2]}n^{\frac{\lambda}{2}-\frac{1}{2}}}{m^{\frac{\lambda}{2}}}\cdot\mathrm{Tr}_{(-1)^{\lambda+1}m}(\mathfrak{F}_\lambda;n). \end{aligned}$$

$\square$

2.4. The "24 Theorem". Here we explain the source of -24 in the limit

$$\lim_{-d\to-\infty}\frac{\mathrm{Tr}(d)-G^{\text{red}}(d)-G^{\text{old}}(d)}{H(d)} = -24. \tag{2.20}$$

Combining Theorems 1.1 and 2.1 with Proposition 2.2, we find that

$$\mathrm{Tr}(d) = -24H(d) + \sum_{\substack{c>0 \\ c\equiv 0 \pmod 4}} S(d,c)\sinh(4\pi\sqrt{d}/c),$$

where $S(d,c)$ is the Salié sum

$$S(d,c)=\sum_{x^2\equiv -d \pmod{c}} e(2x/c).$$

The constant -24 arises from (2.5). It is not difficult to show that the "24 Theorem" is equivalent to the assertion that

$$\sum_{\substack{c>\sqrt{d/3}\\ c\equiv 0\ (4)}} S(d,c)\sinh\left(\frac{4\pi}{c}\sqrt{d}\right)=o\left(H(d)\right).$$

This follows from the fact the sum over $c\leq\sqrt{d/3}$ is essentially $G^{\mathrm{red}}(d)+G^{\mathrm{old}}(d)$. The sinh factor contributes the size of q^{-1} in the Fourier expansion of a singular modulus, and the summands in the Kloosterman sum provides the corresponding "angles". The contribution $G^{\mathrm{old}}(d)$ arises from the fact that the Kloosterman sum cannot distinguish between reduced and non-reduced forms. In view of Siegel's theorem that $H(d)\gg_{\epsilon} d^{\frac{1}{2}-\epsilon}$, (2.20) follows from a bound for such sums of the form $\ll d^{\frac{1}{2}-\gamma}$, for some $\gamma>0$. Such bounds are implicit in Duke's proof of this result [**Duk06**].

3. Traces on Hilbert modular surfaces

In this section we sketch the proofs of Theorems 1.2, 1.3 and 1.4. In the first subsection we recall the arithmetic of the intersection points on the relevant Hilbert modular surfaces, and in the second subsection we recall recent work of Bruinier and Funke concerning traces of singular moduli on more generic modular curves. In the last subsection we sketch the proofs of the theorems.

3.1. Intersection points on Hilbert modular surfaces. Here we provide (for $\ell=1$ or an odd prime with $\left(\frac{\ell}{p}\right)\neq -1$) an interpretation of $Z_{\ell}^{(p)}\cap Z_n^{(p)}$ as a union of $\Gamma_0^*(\ell)$ equivalence classes of CM points. As before, for $-D\equiv 0,1 \pmod 4$ with $D>0$, we let $\mathcal{Q}_D$ be the set of all (not necessarily primitive) binary quadratic forms

$$Q(x,y)=[a,b,c](x,y):=ax^2+bxy+cy^2$$

with discriminant $b^2-4ac=-D$. To each such form Q, we let the CM point τ_Q be as before. For $\ell=1$ or an odd prime and $D>0$, $-D\equiv 0,1 \pmod 4$ we define $\mathcal{Q}_D^{[\ell]}$ to be the subset of $\mathcal{Q}_D$ with the additional condition that $\ell|a$. It is easy to show that $\mathcal{Q}_D^{[\ell]}$ is invariant under $\Gamma_0^*(\ell)$.

If $\ell=1$ or ℓ is an odd prime with $\left(\frac{\ell}{p}\right)\neq -1$, then there is a prime ideal $\mathfrak{p}\subseteq\mathcal{O}_K$ with norm ℓ. Define

$$\mathrm{SL}_2(\mathcal{O}_K,\mathfrak{p}):=\left\{\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}\in\mathrm{SL}_2(K):\alpha,\delta\in\mathcal{O}_K,\gamma\in\mathfrak{p},\beta\in\mathfrak{p}^{-1}\right\}.$$

In this case there is a matrix $A\in\mathrm{GL}_2^+(K)$ such that $A^{-1}\mathrm{SL}_2(\mathcal{O}_K,\mathfrak{p})A=\mathrm{SL}_2(\mathcal{O}_K)$. Define

$$\phi:(\mathfrak{h}\times\mathfrak{h})/\mathrm{SL}_2(\mathcal{O}_K,\mathfrak{p})\to(\mathfrak{h}\times\mathfrak{h})/\mathrm{SL}_2(\mathcal{O}_K)$$

by

$$\phi((z_1,z_2)):=(Az_1,A'z_2).$$

Let Γ be the stabilizer of $\{(z,z) : z \in \mathfrak{h}\} \subseteq \mathfrak{h}\times\mathfrak{h}$ in $\mathrm{SL}_2(\mathcal{O}_K,\mathfrak{p})$. Then $\Gamma = \Gamma_0(\ell)$ if $\ell \neq p$ and $\Gamma = \Gamma_0^*(\ell)$ if $\ell = p$. The image of $\{(z,z) : z \in \mathfrak{h}\}$ under ϕ is $Z_\ell^{(p)}$. Hence, we have a natural map $\psi : \mathfrak{h}/\Gamma \to Z_\ell^{(p)}$. By the work of Hirzebruch and Zagier [**HZ76**], if $\ell = 1$ or an odd prime with $\left(\frac{\ell}{p}\right) \neq -1$, and $n \geq 1$, then we may define

$$Z_\ell^{(p)} \cap Z_n^{(p)} := \bigcup_{\substack{x\in\mathbb{Z}\\ x^2<4\ell n\\ x^2\equiv 4\ell n \pmod p}} \left\{\tau_Q : Q \in \mathcal{Q}^{[\ell]}_{(4\ell n - x^2)/p} \,/\, \Gamma_0^*(\ell)\right\}. \tag{3.1}$$

Here the repetition of x and $-x$ indicates that $Z_\ell^{(p)} \cap Z_n^{(p)}$ is a multiset where a CM point τ_Q occurs twice if $Q \in \mathcal{Q}^{[\ell]}_{(4\ell n-x^2)/p}$ for $x \neq 0$. In addition, if $\ell > 1$ and $\ell | n$, then we include

$$\bigcup_{\substack{x\in\mathbb{Z}\\ x^2<4n/\ell\\ x^2\equiv 4n/\ell \pmod p}} \left\{\tau_Q : Q \in \mathcal{Q}^{[\ell]}_{(4n/\ell - x^2)/p} \,/\, \Gamma_0^*(\ell)\right\},$$

where each point with non-zero x is taken with multiplicity 2ℓ, and a point where $x = 0$ is taken with multiplicity ℓ.

To justify our definition we argue as follows. Hirzebruch and Zagier ([**HZ76**], p. 66) show that if $t \in \mathfrak{h}$, $n \geq 1$ and $\psi(t) \in Z_\ell^{(p)} \cap Z_n^{(p)}$, then

$$a\ell t^2 + \frac{\ell\lambda - \ell\lambda'}{\sqrt{p}} t + b = 0$$

for $(a,b,\lambda) \in \mathbb{Z}\oplus\mathbb{Z}\oplus\mathfrak{p}^{-1}$ with $\ell\lambda\lambda' + abp = n$. This follows as a result of considering the inverse image $\phi^{-1}(Z_\ell^{(p)}) \subseteq (\mathfrak{h}\times\mathfrak{h})/\mathrm{SL}_2(\mathcal{O}_K,\mathfrak{p})$.

Write $\ell\lambda = c + d\frac{1+\sqrt{p}}{2}$, for $c, d \in \mathbb{Z}$. We have that the discriminant of the equation above is $d^2 - 4ab\ell$. However, this implies that

$$\frac{(2c+d)^2 - 4n\ell}{p} = d^2 - 4ab\ell.$$

Thus, the discriminant is of the form $(x^2 - 4n\ell)/p$. From Hirzebruch and Zagier's Theorem 3 ([**HZ76**], p. 77), computing the number of transverse intersections of $Z_\ell^{(p)}$ and $Z_n^{(p)}$, we see that each $z \in \mathfrak{h}$ with discriminant of the form $(x^2 - 4n\ell)/p$ occurs with the appropriate multiplicity.

3.2. Traces of singular moduli on modular curves aprés Bruinier and Funke. Throughout, we let ℓ be 1 or an odd prime. Recently, Bruinier and Funke [**BF06**] have generalized Zagier's results on the modularity of generating functions for traces of singular moduli, and they have obtained results for groups which do not necessarily possess a Hauptmodul. A particularly elegant example of their work applies to modular functions on $\Gamma_0^*(\ell)$. Suppose that $f(z) = \sum_{n\gg-\infty} a(n)q^n \in \mathcal{M}_0(\Gamma_0^*(\ell))$ has constant term $a(0) = 0$. The discriminant $-D$ trace is given by

$$t_f^*(D) := \sum_{Q\in\mathcal{Q}_{D,\ell}/\Gamma_0^*(\ell)} \frac{1}{\#\Gamma_0^*(\ell)_Q} \cdot f(\tau_Q). \tag{3.2}$$

Here $\Gamma_0^*(\ell)_Q$ is the stabilizer of Q in $\Gamma_0^*(\ell)$. Following Kohnen [**Koh82**], we let, for $\epsilon \in \{\pm1\}$, $\mathcal{M}^{+,\epsilon}_{k+\frac{1}{2}}(\Gamma_0(4\ell))$ be the space of those weight $k + \frac{1}{2}$ weakly holomorphic modular forms $f(z) = \sum_{n\gg-\infty} a(n)q^n$ on $\Gamma_0(4\ell)$ whose Fourier coefficients satisfy

$$a(n) = 0 \quad \text{whenever} \quad (-1)^k n \equiv 2,3 \pmod 4 \quad \text{or} \quad \left(\frac{(-1)^k n}{\ell}\right) = -\epsilon. \tag{3.3}$$

THEOREM 3.1. (Bruinier and Funke; Theorem 1.1 of [**BF06**])
If $\ell = 1$ *or is an odd prime and* $f(z) = \sum_{n\gg-\infty} a(n)q^n \in \mathcal{M}_0(\Gamma_0^*(\ell))$, *with* $a(0) = 0$, *then*

$$G_\ell(f,z) := -\sum_{m,n\geq 1} ma(-mn)q^{-m^2} + \sum_{n\geq 1} (\sigma_1(n) + \ell\sigma_1(n/\ell))\, a(-n) + \sum_{D>0} t_f^*(D)q^D$$

is an element of $\mathcal{M}^{+,+}_{\frac{3}{2}}(\Gamma_0(4\ell))$.

3.3. Traces on Hilbert modular surfaces. We are now in a position to sketch the proofs of Theorems 1.2, 1.3, and 1.4.

SKETCH OF THE PROOF OF THEOREM 1.2. It is well known that the Jacobi theta function

$$\Theta(z) = \sum_{x\in\mathbb{Z}} q^{x^2} = 1 + 2q + 2q^4 + 2q^9 + \cdots. \tag{3.4}$$

is a weight 1/2 holomorphic modular form on $\Gamma_0(4)$. Suppose that

$$f(z) = \sum_{n\gg-\infty} a(n)q^n \in \mathcal{M}_0(\Gamma_0^*(\ell))$$

satisfies the hypotheses of Theorem 1.2. By (3.1) and Theorem 3.1, an easy calculation reveals that

$$\Phi^{(p)}_{\ell,f}(z) = \epsilon(\ell)\,(G_\ell(f,pz)\Theta(z)) \mid U(4) \mid (U(\ell) + \ell V(\ell)), \tag{3.5}$$

where for $d \geq 1$ the operators $U(d)$ and $V(d)$ are defined on formal power series by

$$\left(\sum a(n)q^n\right) \mid U(d) := \sum a(dn)q^n, \tag{3.6}$$

and

$$\left(\sum a(n)q^n\right) \mid V(d) := \sum a(n)q^{dn}. \tag{3.7}$$

The proof now follows from generalizations of classical facts about the U and V operators to spaces of weakly holomorphic modular forms. □

SKETCH OF THE PROOF OF THEOREM 1.3. We work directly with (1.1). We recall the following classical theta function identities:

$$\Theta(z) = \frac{\eta(2z)^5}{\eta(z)^2\eta(4z)^2} = \sum_{x\in\mathbb{Z}} q^{x^2} = 1 + 2q + 2q^4 + \cdots, \tag{3.8}$$

$$\Theta_0(z) = \frac{\eta(z)^2}{\eta(2z)} = \sum_{x\in\mathbb{Z}} (-1)^x q^{x^2} = 1 - 2q + 2q^4 - 2q^9 + \cdots, \tag{3.9}$$

and

$$\Theta_{\mathrm{odd}}(z) = \frac{\eta(16z)^2}{\eta(8z)} = \sum_{x\geq 0} q^{(2x+1)^2} = q + q^9 + q^{25} + q^{49} + \cdots. \tag{3.10}$$

By (1.1), (3.5), and (3.9), we have that

$$\begin{aligned}\Phi^{(p)}_{1,J_1}(z) &= -\left(g_1(pz)\Theta(z)\right) \mid U(4)\\ &= -\left(\frac{\Theta_0(pz)E_4(4pz)}{\eta(4pz)^6}\cdot\Theta(z)\right) \mid U(4).\end{aligned}$$

For integers v, we have the identities $E_4(p(z+\nu)) = E_4(pz)$ and

$$\eta(p(z+\nu))^6 = i^{\nu}\eta(pz)^6,$$

which when inserted into the definition of $U(4)$ gives

$$\Phi^{(p)}_{1,J_1}(z) = -\frac{E_4(pz)}{4\eta(pz)^6}\sum_{\nu=0}^{3} i^{-\nu}\Theta_0(p(z+\nu)/4)\Theta((z+\nu)/4).$$

By (3.9) and (3.10), one finds that

$$\Phi^{(p)}_{1,J_1}(z) = -\frac{E_4(pz)}{4\eta(pz)^6}\cdot\sum_{x,y\in\mathbb{Z}} q^{(px^2+y^2)/4}\cdot(-1)^x\left(\sum_{\nu=0}^{3} i^{p\nu x^2+y^2\nu-\nu}\right).$$

Since we have that

$$\sum_{\nu=0}^{3} i^{p\nu x^2+y^2\nu-\nu} = \begin{cases} 0 & \text{if } x\equiv y \pmod 2,\\ 4 & \text{if } x\not\equiv y \pmod 2,\end{cases}$$

it follows that

$$\begin{aligned}\Phi^{(p)}_{1,J_1}(z) &= -\frac{E_4(pz)}{\eta(pz)^6}\cdot\left(\sum_{x,y\in\mathbb{Z}} q^{((2y+1)^2+4px^2)/4} - \sum_{x,y\in\mathbb{Z}} q^{(4y^2+(2x+1)^2p)/4}\right)\\ &= -\frac{2E_4(pz)}{\eta(pz)^6}\cdot\left(\Theta(pz)\Theta_{\text{odd}}(z/4) - \Theta(z)\Theta_{\text{odd}}(pz/4)\right).\end{aligned}$$

The claimed formula now follows easily from (1.20), (3.8), and (3.10). □

Sketch of the proof of Theorem 1.4. If $p\equiv 1 \pmod 4$ is prime, then a lengthy, but straightforward calculation, reveals that

$$N^*_p(z) = E_4(z)^{a(p)}\cdot\Delta(z)^{c(p)}\cdot F_p(j(z)), \tag{3.11}$$

where $F_p(x)\in\mathbb{Z}[x]$ is a monic polynomial with

$$\deg(F_p(x)) = \begin{cases} (5p-5)/12 & \text{if } p\equiv 1 \pmod{12},\\ (5p-1)/12 & \text{if } p\equiv 5 \pmod{12}.\end{cases}$$

Hence it suffices to compute the factorization of $F_p(x)$ over $\mathbb{Z}[x]$.

Loosely speaking, $F_p(x)$ captures the divisor of the modular form $N^*_p(z)$ in $\mathfrak{h}$. To compute the points in the divisor, we shall make use of Theorem 1.3. Since $\eta(z)$ is non-vanishing on $\mathfrak{h}$, the factors of $F_p(x)$ only arise from the zeros of the "norm" of $E_4(pz)$ and of

$$\mathfrak{f}_1(4z)^4\mathfrak{f}_2(z)^2 - \mathfrak{f}_1(4pz)^4\mathfrak{f}_2(pz)^2.$$

To determine these zeros and their corresponding multiplicities, we require classical facts about class numbers and the Eichler-Selberg trace formula. To begin, first observe that $E_4(\omega)=0$, where $\omega := e^{2\pi/3} = \frac{-1+\sqrt{-3}}{2}$. Hence it follows that

$E_4(pz)$ is zero for $z_p := \omega/p$. Since z_p has discriminant $-3p^2$, the irreducibility of $H_{3\cdot p^2}(x)$ implies that $H_{3\cdot p^2}(x) \mid F_p(x)$ in $\mathbb{Z}[x]$. Therefore, we may conclude that

$$F_p(x) = H_{3\cdot p^2}(x) \cdot I_p(x),$$

where $I_p(x) \in \mathbb{Z}[x]$ has

$$\deg(I_p(x)) = \begin{cases} (p-1)/12 & \text{if } p \equiv 1 \pmod{12}, \\ (p-5)/12 & \text{if } p \equiv 5 \pmod{12}. \end{cases}$$

To complete the proof, it suffices to determine the polynomial $I_p(x)$. To this end, observe that $I_p(x)$ is the polynomial which encodes the divisor of the norm of

$$\mathfrak{f}_1(4z)^4\mathfrak{f}_2(z)^2 - \mathfrak{f}_1(4pz)^4\mathfrak{f}_2(pz)^2.$$

To study this divisor, one notes that if $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ with $b \equiv c \equiv 0 \pmod 4$ and $g(z) := \mathfrak{f}_1(4z)^4\mathfrak{f}_2(z)^2$, then $g\left(\frac{az+b}{cz+d}\right) = g(z)$. The proof is complete once we establish that

$$I_p(x) = H_3(x)^{a(p)} \cdot H_4(x)^{b(p)} \prod_{-D \in \mathcal{D}_p} H_D(x)^2.$$

To prove this assertion, we note that the modular transformation above implies that $z \in \mathfrak{h}$ is a root of $g(z) - g(pz)$ if $\frac{az+b}{cz+d} = pz$ for $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ with $b \equiv c \equiv 0 \pmod 4$. This leads to the quadratic equation

$$\frac{pc}{4}z^2 + \frac{pd-a}{4}z - \frac{b}{4} = 0.$$

Using some class number relations, and the fact that Hilbert class polynomials are irreducible, we simply need to show that for a negative discriminant of the form $-D := \frac{x^2-4p}{16f^2}$ with $x, f \in \mathbb{Z}$ that there are two integral binary quadratic forms

$$\begin{aligned} Q_1 &:= \frac{pc_1}{4f}x^2 + \frac{pd_1 - a_1}{4f}xy - \frac{b_1}{4f}y^2 \\ Q_2 &:= \frac{pc_2}{4f}x^2 + \frac{pd_2 - a_2}{4f}xy - \frac{b_2}{4f}y^2, \end{aligned}$$

which are inequivalent under $\Gamma_0(p)$ with discriminants $-D$ such that $\left(\begin{smallmatrix} a_1 & b_1 \\ c_1 & d_1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} a_2 & b_2 \\ c_2 & d_2 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ with $b_1 \equiv b_2 \equiv c_1 \equiv c_2 \equiv 0 \pmod 4$. This is an easy exercise. ☐

References

[BF06] J. H. Bruinier & J. Funke – "Traces of CM values of modular functions", *J. Reine Angew. Math.* **594** (2006), p. 1–33.

[BJO06] J. H. Bruinier, P. Jenkins & K. Ono – "Hilbert class polynomials and traces of singular moduli", *Math. Ann.* **334** (2006), no. 2, p. 373–393.

[BO] K. Bringmann & K. Ono – "Arithmetic properties of half-integral weight Maass-Poincaré series", accepted for publication.

[Bor95a] R. E. Borcherds – "Automorphic forms on $\mathrm{O}_{s+2,2}(\mathbf{R})$ and infinite products", *Invent. Math.* **120** (1995), no. 1, p. 161–213.

[Bor95b] ———, "Automorphic forms on $\mathrm{O}_{s+2,2}(\mathbf{R})^+$ and generalized Kac-Moody algebras", in *Proceedings of the International Congress of Mathematicians, Vol. 1, 2 (Zürich, 1994)* (Basel), Birkhäuser, 1995, p. 744–752.

[BOR05] K. Bringmann, K. Ono & J. Rouse – "Traces of singular moduli on Hilbert modular surfaces", *Int. Math. Res. Not.* (2005), no. 47, p. 2891–2912.

[Bru02] J. H. Bruinier – *Borcherds products on O(2, l) and Chern classes of Heegner divisors*, Lecture Notes in Mathematics, vol. 1780, Springer-Verlag, Berlin, 2002.

[Cox89] D. A. Cox – *Primes of the form* x^2+ny^2, A Wiley-Interscience Publication, John Wiley & Sons Inc., New York, 1989, Fermat, class field theory and complex multiplication.

[Duk06] W. Duke – "Modular functions and the uniform distribution of CM points", *Math. Ann.* **334** (2006), no. 2, p. 241–252.

[Hir73] F. E. P. Hirzebruch – "Hilbert modular surfaces", *Enseignement Math. (2)* **19** (1973), p. 183–281.

[HZ76] F. Hirzebruch & D. Zagier – "Intersection numbers of curves on Hilbert modular surfaces and modular forms of Nebentypus", *Invent. Math.* **36** (1976), p. 57–113.

[Jen] P. Jenkins – "Kloosterman sums and traces of singular moduli", *J. Number Th.*, to appear.

[Kim] C. H. Kim – "Traces of singular values and Borcherds products", preprint.

[Kim04] ———, "Borcherds products associated with certain Thompson series", *Compos. Math.* **140** (2004), no. 3, p. 541–551.

[Koh82] W. Kohnen – "Newforms of half-integral weight", *J. Reine Angew. Math.* **333** (1982), p. 32–72.

[Koh85] ———, "Fourier coefficients of modular forms of half-integral weight", *Math. Ann.* **271** (1985), no. 2, p. 237–268.

[Nie73] D. Niebur – "A class of nonanalytic automorphic functions", *Nagoya Math. J.* **52** (1973), p. 133–145.

[Shi73] G. Shimura – "On modular forms of half integral weight", *Ann. of Math. (2)* **97** (1973), p. 440–481.

[Zag02] D. Zagier – "Traces of singular moduli", in *Motives, polylogarithms and Hodge theory, Part I (Irvine, CA, 1998)*, Int. Press Lect. Ser., vol. 3, Int. Press, Somerville, MA, 2002, p. 211–244.

Department of Mathematics, University of Wisconsin, Madison, Wisconsin 53706
E-mail address: ono@math.wisc.edu

Clay Mathematics Proceedings
Volume 7, 2007

Rational points of bounded height on threefolds

Per Salberger

ABSTRACT. Let $n_{e,f}(B)$ be the number of non-trivial positive integer solutions $x_0, x_1, x_2, y_0, y_1, y_2 \leq B$ to the simultaneous equations

$$x_0^e + x_1^e + x_2^e = y_0^e + y_1^e + y_2^e, \qquad x_0^f + x_1^f + x_2^f = y_0^f + y_1^f + y_2^f.$$

We show that $n_{1,4}(B) = O_\varepsilon(B^{85/32+\varepsilon}), n_{1,5}(B) = O_\varepsilon(B^{51/20+\varepsilon})$ and that $n_{e,f}(B) = O_{e,f,\varepsilon}(B^{5/2+\varepsilon})$ if $ef \geq 6$ and $f \geq 4$. These estimates are deduced from general upper bounds for the number of rational points of bounded height on projective threefolds over $\mathbb{Q}$.

Introduction

This paper deals with the number $N(X, B)$ of rational points of height at most B on projective threefolds $X \subset \mathbb{P}^n$ over $\mathbb{Q}$. To define the height $H(x)$ of a rational point x on $\mathbb{P}^n$, we choose a primitive integral $(n+1)$-tuple $(x_0, ..., x_n)$ representing x and let $H(x) = \max(|x_0|, ..., |x_n|)$. Our main result is the following.

THEOREM 0.1. *Let $X \subset \mathbb{P}^n$ be a geometrically integral projective threefold over $\mathbb{Q}$ of degree d and let X' be the complement of the union of all planes on X. Then*

$$N(X', B) = \begin{cases} O_{n,\varepsilon}(B^{15\sqrt{3}/16+5/4+\varepsilon}) & \text{if } \; d = 3, \\ O_{n,\varepsilon}(B^{1205/448+\varepsilon}) & \text{if } \; d = 4, \\ O_{n,\varepsilon}(B^{51/20+\varepsilon}) & \text{if } \; d = 5, \\ O_{d,n,\varepsilon}(B^{5/2+\varepsilon}) & \text{if } \; d \geq 6. \end{cases}$$

If $n = d = 4$ and X is not a cone of a Steiner surface, then

$$N(X', B) = O_{n,\varepsilon}(B^{85/32+\varepsilon}).$$

This bound is better than the bound $O_{d,n,\varepsilon}(B^{11/4+\varepsilon} + B^{5/2+5/3d+\varepsilon})$ in [**Salc**], §8. An important special case is the following.

THEOREM 0.2. *Let $(a_0, \ldots, a_5)$ and $(b_0, \ldots, b_5)$ be two sextuples of rational numbers all different from zero and $e < f$ be positive integers. Let $X \subset \mathbb{P}^5$ be the threefold defined by the two equations $a_0x_0^e + \ldots + a_5x_5^e = 0$ and $b_0x_0^f + \ldots + b_5x_5^f = 0$. Then there are only finitely many planes on X if $f \geq 3$. Moreover, if $X' \subset X$ is*

2000 *Mathematics Subject Classification.* Primary 14G08, Secondary 11G35.

the complement of these planes in X, then

$$N(X',B) = \begin{cases} O_\varepsilon(B^{15\sqrt{3}/16+5/4+\varepsilon}) & \text{if } \; e=1 \text{ and } f=3, \\ O_\varepsilon(B^{85/32+\varepsilon}) & \text{if } \; e=1 \text{ and } f=4, \\ O_\varepsilon(B^{51/20+\varepsilon}) & \text{if } \; e=1 \text{ and } f=5, \\ O_{e,f,\varepsilon}(B^{5/2+\varepsilon}) & \text{if } \; ef \geq 6. \end{cases}$$

As a corollary we obtain from Lemma 1 in [**BHB**] the following result on pairs of simultaneous equal sums of three powers.

COROLLARY 0.3. Let $n_{e,f}(B)$, $e < f$ be the number of solutions in positive integers x_i, $y_i \leq B$ to the two polynomial equations

$$\begin{aligned} x_0^e + x_1^e + x_2^e &= y_0^e + y_1^e + y_2^e \\ x_0^f + x_1^f + x_2^f &= y_0^f + y_1^f + y_2^f \end{aligned}$$

where $(x_0, x_1, x_2) \neq (y_i, y_j, y_k)$ for all six permutations of (i,j,k) of $(0,1,2)$. Then,

$$\begin{aligned} & n_{1,4}(B) = O_\varepsilon(B^{85/32+\varepsilon}) \\ & n_{1,5}(B) = O_\varepsilon(B^{51/20+\varepsilon}) \\ & n_{e,f}(B) = O_{e,f,\varepsilon}(B^{5/2+\varepsilon}) \quad \text{if } \; ef \geq 6 \text{ and } f \geq 4. \end{aligned}$$

Previously, it has been shown by Greaves [**Gre97**] that $n_{1,f}(B) = O_\varepsilon(B^{17/6+\varepsilon})$ and by Skinner-Wooley[**SW97**] that $n_{1,f}(B) = O_\varepsilon(B^{8/3+1/(f-1)+\varepsilon})$. Moreover, work of Wooley [**Woo96**] shows that $n_{2,3}(B) = O_\varepsilon(B^{7/3+\varepsilon})$ and Tsui and Wooley [**TW99**] have shown that $n_{2,4}(B) = O_\varepsilon(B^{36/13+\varepsilon})$. Finally, one may find the estimate

$$n_{e,f}(B) = O_{e,f,\varepsilon}(B^{11/4+\varepsilon} + B^{5/2+5/3ef+\varepsilon})$$

in the paper of Browning and Heath-Brown [**BHB**]. Our estimate for $n_{e,f}(B)$ is superior to the previous estimates when $f \geq 4$.

The main idea of the proof of Theorem 0.1 is to use hyperplane sections to reduce to counting problems for surfaces. For the geometrically integral hyperplane sections we use thereby the new sharp estimates for surfaces in [**Sala**].

I would like to thank T. Browning for his comments on an earlier version of this paper.

1. The hyperplane sections given by Siegel's lemma

Let $G_r(\mathbb{P}^n)$ be the Grassmannian of r-planes on $\mathbb{P}^n$. It is embedded into $\mathbb{P}^{\binom{n+1}{r+1}-1}$ by the Plücker embedding. In particular, if $r = n-1$, then we may identify $G_r(\mathbb{P}^n)$ with the dual projective space $\mathbb{P}^{n\vee}$. The height $H(\Lambda)$ of a rational r-plane $\Lambda \subset \mathbb{P}^n$ is by definition the height of its Plücker coordinates. In particular, if $r = n-1$ then the height of a hyperplane $\Lambda \subset \mathbb{P}^n$ defined by $c_0x_0 + \ldots + c_nx_n = 0$, is the height of the rational point $(c_0, \ldots, c_n)$ in $\mathbb{P}^{n\vee}$.

In order to prove Theorem 0.1 for hypersurfaces in $\mathbb{P}^4$, we shall need the following two lemmas from the geometry of numbers. See [**Sch91**], Chap I, for example.

LEMMA 1.1. *Let x be a rational point of height $\leq B$ on $\mathbb{P}^4$. Then x lies on a hyperplane Π of height $H(\Pi) \leq (5B)^{1/4}$.*

LEMMA 1.2. *There is an absolute constant κ such that $H(\Pi) \leq \kappa H(\Lambda)^{1/3}$ for any rational hyperplane Π of minimal height containing a given line $\Lambda \subset \mathbb{P}^4$.*

We now introduce the following notation for a geometrically integral hypersurface $X \subset \mathbb{P}^4$.

NOTATION 1.3. (i) *X' is the complement of the union of all planes on X.*
(ii) *$S(X, B)$ is the set of all rational points of height at most B on X.*
(iii) *$P(X, B)$ is the set of all rational planes $\Theta \subset X$ which are spanned by their rational points of height $\leq B$ and which are contained in a rational hyperplane $\Pi \subset \mathbb{P}^4$ of height $H(\Pi) \leq (5B)^{1/4}$.*
(iv) *$\widetilde{S}(X, B)$ is the set of all rational points of height at most B on X, which do not lie on a plane $\Theta \subset X$ in $P(X, B)$.*
(v) *$N(X, B) = \#S(X, B)$ and $\widetilde{N}(X, B) = \#\widetilde{S}(X, B)$.*

2. The hyperplane sections which are not geometrically integral

We shall in this section estimate the contribution to $\widetilde{N}(X, B)$ from the hyperplane sections $\Pi \cap X$, which are not geometrically integral.

LEMMA 2.1. *Let $X \subset \mathbb{P}^4$ be a geometrically integral projective threefold of degree $d \geq 2$ over some field. Let $\mathbb{P}^{4\vee}$ be the dual projective space parameterising hyperplanes $\Pi \subset \mathbb{P}^4$ and let $c < d$ be a positive integer. Then the following holds.*

a) *There is a closed subscheme $W_{c,d} \subset \mathbb{P}^{4\vee}$ which parameterises the hyperplanes Π such that $\Pi \cap X$ contains a surface of degree c. The sum of the degrees of the irreducible components of $W_{c,d}$ is bounded in terms of d.*
b) $\dim W_{c,d} \leq 2$.
c) *If there is a plane on $W_{c,d} \subset \mathbb{P}^{4\vee}$, then X is a cone over a curve.*

PROOF. a) See [**Sal05**], Lemma 3.3.

(b) There exists by the theorem of Bertini a hyperplane $\Pi_0 \subset \mathbb{P}^{4\vee}$ and a plane $\Theta \subset \Pi_0$ such that $\Pi_0 \cap X$ and $\Theta \cap X$ are geometrically integral. Let $\Pi_0^\vee$ be the dual projective 3-space of Π_0 which parameterises all planes in Π_0 and $f : W_{c,d} \to \Pi_0^\vee$ be the linear morphism which sends the Grassmann point of $\Pi \subset \mathbb{P}^4$ to the Grassmann points of $\Pi \cap \Pi_0 \subset \Pi_0$. Then f must be finite since otherwise one of the fibres of f would contain a line passing through the Grassmann point of $\Pi_0 \subset \mathbb{P}^4$. Also, f is not surjective since Θ cannot be of the form $\Pi \cap \Pi_0$ for any hyperplane $\Pi \subset \mathbb{P}^4$ parameterised by a point in $W_{c,d}$. Hence $\dim W_{c,d} = \dim f(W_{c,d}) \leq \dim \Pi_0 - 1 = 2$.

(c) Let $\Gamma \subset \mathbb{P}^{4\vee}$ be a plane, $\Lambda \subset \mathbb{P}^4$ the dual line, $\pi : Z \to \mathbb{P}^4$ the blow-up at Λ and $\widetilde{X} = \pi^{-1}(X)$. Let $p : \mathbb{P}^4 \backslash \Lambda \to \mathbb{P}^2$ be a linear projection from Λ and $q : Z \to \mathbb{P}^2$ the morphism induced by p. If $q(\widetilde{X}) \neq \mathbb{P}^2$, then X is a cone over a curve with Λ as vertex. If $q(\widetilde{X}) = \mathbb{P}^2$, then we apply the theorem of Bertini to the restriction of q to $\widetilde{X}$. This implies that $q^{-1}(L) \cap \widetilde{X}$ is geometrically integral for a generic line $L \subset \mathbb{P}^2$. Let $\Pi \subset \mathbb{P}^4$ be the hyperplane given by the closure of $p^{-1}(L)$. Then $\Pi \cap X$ is geometrically integral since $q^{-1}(L) \cap \widetilde{X}$ is mapped birationally onto $\Pi \cap X$ under π. But as $\Pi \supset \Lambda$, this hyperplane is parameterised by a point on $\Gamma \backslash W_{c,d}$. In particular, Γ is not contained in $W_{c,d}$. This completes the proof. □

The following result is a minor extension of Theorem 2.1 in [**Sal05**].

THEOREM 2.2. *Let $W \subset \mathbb{P}^n$ be a closed subscheme defined over $\mathbb{Q}$ where all irreducible components are of dimension at most two. Let D be the sum of the degrees of all irreducible components of W. Then,*

$$N(W, B) = O_{D,n}(B^3)\,.$$

If W does not contain any plane spanned by its rational points of height at most B, then

$$N(W,B) = O_{D,n,\varepsilon}(B^{2+\varepsilon}).$$

PROOF. One reduces immediately to the case where W is integral and then to the case where W is geometrically integral by the arguments in the proof of Theorem 2.1 in [**Sal05**]. It is also shown there that Theorem 2.2 holds if W is geometrically integral and not a plane. It remains to prove Theorem 2.2 for a rational plane W. Then the rational points of height $\leq B$ on W span an r-plane Λ, $r \leq 2$ where $N(W,B) = N(\Lambda,B) = O_n(B^{\dim \Lambda})$ if $N(W,B) \geq 1$, ([**HB02**], Lemma 1(iii)). This completes the proof. □

LEMMA 2.3. *Let $X \subset \mathbb{P}^4$ be a geometrically integral projective threefold over $\mathbb{Q}$ of degree $d \geq 2$. Then there are $O_{d,\varepsilon}(B^{11/4+\varepsilon})$ points $x \in \widetilde{S}(X,B)$ for which there is a rational hyperplane $\Pi \subset \mathbb{P}^4$ of height at most $(5B)^{1/4}$ containing x such that $\Pi \cap X$ is not geometrically integral. If X is not a cone over a curve then there are $O_{d,\varepsilon}(B^{5/2+\varepsilon})$ such points $x \in \widetilde{S}(X,B)$.*

PROOF. It suffices to establish this bound under the extra hypothesis that $\Pi \in W_{c,d}(\mathbb{Q})$ for some fixed integer $c < d$. By Lemma 2.1 and Theorem 2.2 we have $N(W_{c,d},(5B)^{1/4}) = O_{d,\varepsilon}(B^{3/4})$ in general and $N(W_{c,d},(5B)^{1/4}) = O_{d,\varepsilon}(B^{1/2+\varepsilon})$ if X is not a cone over a curve. We may also apply Theorem 2.2 to the closure W in $\Pi \cap X$ of the complement of all rational planes in $\Pi \cap X$ spanned by its rational points of height $\leq B$. We then get that there are $O_{d,\varepsilon}(B^{2+\varepsilon})$ points in $\widetilde{S}(X,B) \cap \Pi(\mathbb{Q})$ for any hyperplane $\Pi \subset \mathbb{P}^4$. The desired result follows by summing over all $\Pi \in W_{c,d}(\mathbb{Q})$ in the statement of the lemma and over all c. □

3. The points outside the lines

We shall in this section count the points outside the lines on hypersurfaces X in $\mathbb{P}^4$.

DEFINITION 3.1. A surface $X \subset \mathbb{P}^3$ is said to be a Steiner surface if there is a morphism $\pi : \mathbb{P}^2 \to \mathbb{P}^3$ of projective degree 2 which maps $\mathbb{P}^2$ birationally onto X.

It follows immediately from the definition that a Steiner surface is of degree 4. The following result is proved but not stated in [**Sala**].

THEOREM 3.2. *Let $X \subset \mathbb{P}^3$ be a geometrically integral projective surface over $\mathbb{Q}$ of degree $d \geq 3$. Suppose that X is not a Steiner surface. Then there exists a set of $O_{d,\varepsilon}(B^{3/2\sqrt{d}+\varepsilon})$ rational lines on X such that there are*

$$O_{d,\varepsilon}(B^{3/\sqrt{d}+\varepsilon} + B^{3/2\sqrt{d}+2/3+\varepsilon} + B^{1+\varepsilon})$$

rational points of height $\leq B$ not lying on these lines. If $X \subset \mathbb{P}^3$ is a Steiner surface, then there are

$$O_{d,\varepsilon}(B^{43/28+\varepsilon})$$

rational points of height $\leq B$ not lying on the lines.

PROOF. There exists by Theorem 0.5 in [**Sala**] a set Γ of $O_{d,\varepsilon}(B^{3/2\sqrt{d}+\varepsilon})$ geometrically integral curves of degree $O_{d,\varepsilon}(1)$ on X such that all but $O_{d,\varepsilon}(B^{3/\sqrt{d}+\varepsilon})$ rational points of height $\leq B$ on X lie on the union of these curves. Hence, by [**HB02**], th.5, there are $O_{d,\varepsilon}(B^{3/2\sqrt{d}+2/3+\varepsilon})$ rational points of height $\leq B$ on the union of all curves in Γ of degree ≥ 3. It thus only remains to estimate the total contribution from the conics. But it is proved in [**Sala**], 5.4, that this contribution is $O_{d,\varepsilon}(B^{1+3/2\sqrt{d}-3\sqrt{d}/16+\varepsilon}+B^{1+\varepsilon})$ if X does not contain a two-dimensional family of conics and $O_{d,\varepsilon}(B^{43/28+\varepsilon})$ if X contains such a family. To complete the proof, we use the fact that a geometrically integral surface $X \subset \mathbb{P}^3$ of degree $d \geq 3$ contains a two-dimensional family of conics if and only if it is a Steiner surface (cf. [**SR49**], pp. 157-8 or [**Sha99**], p.74). □

THEOREM 3.3. *Let $X \subset \mathbb{P}^4$ be a geometrically integral projective threefold over $\mathbb{Q}$ of degree $d \geq 3$, which is not a cone of a Steiner surface. Then there exists a set of $O_{d,\varepsilon}(B^{45/32\sqrt{d}+5/4+\varepsilon})$ rational lines on X such that there are $O_{d,\varepsilon}(B^{45/16\sqrt{d}+5/4+\varepsilon}+B^{5/2+\varepsilon})$ rational points in $\widetilde{S}(X,B)$ not lying on any of these lines. If X is a cone of a Steiner surface, then there exists a set of $O_{d,\varepsilon}(B^{45/64+5/4+\varepsilon})$ rational lines on X such that there are $O_{d,\varepsilon}(B^{1205/448+\varepsilon})$ rational points on X not lying on any of these lines.*

PROOF. We follow the proof of Lemma 5.1 in [**Sal05**] to which we refer for more details. To each hyperplane $\Pi \subset \mathbb{P}^4$ we introduce new coordinates (y_1, y_2, y_3, y_4) for Π with the following properties for the rational points P_j, $1 \leq j \leq 4$ on Π defined by $y_i(P_j) = \delta_{ij}$ for $1 \leq j \leq 4$.

(3.4)
- (i) $H(P_1) \leq H(P_2) \leq H(P_3) \leq H(P_4)$
- (ii) $H(\Pi) \ll H(P_1)H(P_2)H(P_3)H(P_4) \ll H(\Pi)$
- (iii) Any rational point P on Π is represented by a primitive integral quadruple (y_1, y_2, y_3, y_4) such that $|y_i| \ll H(P)/H(P_i)$ for $1 \leq i \leq 4$.

The heights in (3.4) are defined with respect to the original coordinates for $\mathbb{P}^4$.

Now let $g(d) = \max\ (3/\sqrt{d}, 3/2\sqrt{d} + 2/3, 1)$ if X is not a cone of a Steiner surface. In this case no hyperplane section of X is a Steiner surface by [**Rog94**], Lemma 12. If X is a cone of a Steiner surface, let $g(d) = 43/28$. Then, by Theorem 3.2 and (3.4)(iii) the following assertion holds for any hyperplane $\Pi \subset \mathbb{P}^4$ such that $\Pi \cap X$ is geometrically integral.

(3.5) There exists a set of $\ll_{d,\varepsilon} (B/H(P_1))^{3/2\sqrt{d}+\varepsilon}$ lines on $\Pi \cap X$ such that there are $\ll_{d,\varepsilon} (B/H(P_1))^{g(d)+\varepsilon}$ rational points of height $\leq B$ on $\Pi \cap X$ outside these lines.

Now let $1 \leq C_1 \leq C_2 \leq C_3 \leq C_4$ and $C_1C_2C_3C_4 \ll B^{1/4}$ and let us consider the hyperplanes spanned by quadruples (P_1, P_2, P_3, P_4) of rational points as above and such that $C_j \leq H(P_j) \leq 2C_j$, $1 \leq j \leq 4$. It follows from the proof of Lemma 5.1 in [**Sal05**], that there are $\ll C_1^8(C_2C_3C_4)^4$ such hyperplanes. Also, for any such hyperplane Π where $\Pi \cap X$ is geometrically integral, there exists by Theorem 3.2 a set of $\ll_{d,\varepsilon} (B/C_1)^{3/2\sqrt{d}+\varepsilon}$ lines on $\Pi \cap X$ such that there are $\ll_{d,\varepsilon} (B/C_1)^{g(d)+\varepsilon}$ rational points of height $\leq B$ on $\Pi \cap X$ outside these lines. This implies just as in (op. cit.) that we have a set of $\ll_{d,\varepsilon} B^{3/2\sqrt{d}+\varepsilon}C_1^{8-3/2\sqrt{d}}(C_2C_3C_4)^4$ rational lines on the union V of these hyperplane sections such that there $\ll_{d,\varepsilon}$ $B^{g(d)+\varepsilon}C_1^{8-g(d)}(C_2C_3C_4)^4$ rational points of height $\leq B$ on V outside all these lines. Now as $3/2\sqrt{d} \leq 4$ and $g(d) \leq 4$ we get from the assumptions on C_j, $1 \leq$

$j \leq 4$ that $C_1^{8-3/2\sqrt{d}}(C_2C_3C_4)^4 \leq (C_1C_2C_3C_4)^{5-3/8\sqrt{d}}$ and $C_1^{8-g(d)}(C_2C_3C_4)^4 \leq (C_1C_2C_3C_4)^{5-g(d)/4}$. Hence if we sum over all dyadic intervals $[C_j, 2C_j], 1 \leq j \leq 4$ for 2-powers C_j as above and argue as in (op. cit.), we will get a set of $\ll_{d,\varepsilon} B^{15(3/2\sqrt{d})/16+5/4+\varepsilon}$ rational lines on X such that there are $O_{d,\varepsilon}(B^{15g(d)/16+5/4+\varepsilon})$ rational points of height $\leq B$ on the union of all geometrically integral hyperplane sections $\Pi \cap X$ with $H(\Pi) \leq (5B)^{1/4}$ which do not lie on these lines.

We now combine this with (1.1) and (2.3). Then we conclude that there are $\ll_{d,\varepsilon} B^{15g(d)/16+5/4+\varepsilon} + B^{5/2+\varepsilon}$ points in $\widetilde{S}(X,B)$ outside these lines if X is not a cone of a Steiner surface and $\ll_{\varepsilon} B^{15g(d)/16+5/4+\varepsilon} + B^{11/4+\varepsilon}$ such points if X is a cone of a Steiner surface. To finish the proof, note that $\max(15g(d)/16+5/4, 5/2) = \max(45/16\sqrt{d}+5/4, 5/2)$ in the first case and that $\max(15g(d)/16+5/4, 11/4) = 1205/448$ in the second case. $\square$

4. The points on the lines

We shall in this section estimate the contribution to $N(X', B)$ from the lines in Theorem 3.3.

LEMMA 4.1. *$X \subset \mathbb{P}^4$ be a geometrically integral projective threefold over $\mathbb{Q}$ of degree $d \geq 2$. Let M be a set of $O_{d,\varepsilon}(B^{5/2+\varepsilon})$ rational lines Λ on X each contained in some hyperplane $\Pi \subset \mathbb{P}^4$ of height $\leq (5B)^{1/4}$ and $\widetilde{N}(\cup_{\Lambda\in M}\Lambda, B)$ be the number of points in $\widetilde{S}(X,B) \cap (\cup_{\Lambda\in M}\Lambda(\mathbb{Q}))$. Then the following holds.*

(a) $\widetilde{N}(\cup_{\Lambda\in M}\Lambda, B) = O_{d,\varepsilon}(B^{11/4+\varepsilon} + B^{5/2+3/2d+\varepsilon})$.
(b) $\widetilde{N}(\cup_{\Lambda\in M}\Lambda, B) = O_{d,\varepsilon}(B^{5/2+3/2d+\varepsilon})$ *if X is not a cone over a curve.*
(c) $\widetilde{N}(\cup_{\Lambda\in M}\Lambda, B) = O_{d,\varepsilon}(B^{5/2+\varepsilon} + B^{9/4+3/2d+\varepsilon})$ *if there are only finitely many planes on X.*

PROOF. We shall for each $\Lambda \in M$ choose a hyperplane $\Pi(\Lambda) \subset \mathbb{P}^4$ of minimal height containing Λ . Then, $H(\Pi(\Lambda)) \leq \kappa H(\Lambda)^{1/3}$ for some absolute constant κ by (1.2). The contribution to $\widetilde{N}(\cup_{\Lambda\in M}\Lambda, B)$ from all $\Lambda \in M$ where $\Pi(\Lambda) \cap X$ is not geometrically integral is $O_{d,\varepsilon}(B^{11/4+\varepsilon})$ in general and $O_{d,\varepsilon}(B^{5/2+\varepsilon})$ if X is not a cone over a curve (see (2.3)). The contribution from the lines $\Lambda \in M$ with $N(\Lambda, B) \leq 1$ is $O_{d,\varepsilon}(B^{5/2+\varepsilon})$. We may and shall therefore in the sequel assume that $\Pi(\Lambda) \cap X$ is geometrically integral and $N(\Lambda, B) \geq 2$ for all $\Lambda \in M$. From $N(\Lambda, B) \geq 2$ we deduce that $H(\Lambda) \leq 2B^2$, $N(\Lambda, B) \ll B^2/H(\Lambda)$ and

$$N(\cup_{\Lambda\in M}\Lambda, B) \leq \sum_{\Lambda\in M} N(\Lambda, B) \ll B^2 \sum_{\Lambda\in M} H(\Lambda)^{-1} \tag{4.2}$$

It is therefore sufficient to prove that:

$$\sum_{\Lambda\in M} H(\Lambda)^{-1} = O_{d,\varepsilon}(B^{1/2+3/2d+\varepsilon}) \tag{4.3}$$

in general and that

$$\sum_{\Lambda\in M} H(\Lambda)^{-1} = O_{d,\varepsilon}(B^{1/2+\varepsilon} + B^{1/4+3/2d+\varepsilon}) \tag{4.4}$$

if there are only finitely many planes on X.

A proof of (4.3) may be found in the proofs of Lemma 3.2.2 and Lemma 3.2.3 in [**BS04**]. It is therefore enough to show (4.4).

Let $M_1 \subseteq M$ be the subset of rational lines Λ such that $\Pi(\Lambda) \cap X$ contains only finitely many lines. Then it is known and easy to show using Hilbert schemes that there is a uniform upper bound depending only on d for the number of lines on such $\Pi(\Lambda) \cap X$. There can therefore only be $O_d(B^{5/4})$ lines $\Lambda \in M_1$ as there are only $O(B^{5/4})$ possibilities for $\Pi(\Lambda)$. The contribution to $\sum_{\Lambda \in M_1} H(\Lambda)^{-1}$ from lines of height $\geq B^{3/4}$ is thus $O_d(B^{1/2})$.

Now let $[R, 2R]$ be a dyadic interval with $1 \leq R \leq B^{3/4}$. Then $H(\Pi(\Lambda)) \ll H(\Lambda)^{1/3} \ll R^{1/3}$ for Λ with $H(\Lambda) \in [R, 2R]$ so that there are only $O(R^{5/3})$ possibilities for $\Pi(\Lambda)$ and $O_d(R^{5/3})$ such lines Λ. The contribution to $\sum_{\Lambda \in M_1} H(\Lambda)^{-1}$ from the lines of height $H(\Lambda) \in [R, 2R]$ is thus $O_d(R^{2/3})$. Hence if we sum over all $O(\log B)$ dyadic intervals $[R, 2R]$ with $R \leq B^{3/4}$ we get that lines of height $\leq B^{3/4}$ contribute with $O_d(B^{1/2}(\log B))$ to $\sum\limits_{\Lambda \in M_1} H(\Lambda)^{-1}$ so that

$$\sum_{\Lambda \in M_1} H(\Lambda)^{-1} = O_d(B^{1/2}(\log B)). \tag{4.5}$$

We now consider the subset $M_2 \subseteq M$ of rational lines Λ where $\Pi(\Lambda) \cap X$ contains infinitely many lines. This is equivalent to $(\Pi(\Lambda) \cap X)(\bar{\mathbb{Q}})$ being a union of its lines (see [**Salb**], 7.4).

There exists therefore by [**Salb**], 7.8 a hypersurface $W \subset \mathbb{P}^{4\vee}$ of degree $O_d(1)$ such that any hyperplane $\Pi \subset \mathbb{P}^4$ where $\Pi \cap X$ contains infinitely many lines is parameterised by a point on W. There are thus $O_d(B)$ such hyperplanes of height $\leq (5B)^{1/4}$. If $R \geq 1$, then $H(\Pi(\Lambda)) \ll H(\Lambda)^{1/3} \ll R^{4/3}$ for lines Λ of height $\leq 2R$. There are therefore $O_d(R^{4/3})$ possibilities for $\Pi(\Lambda)$ among all lines of height $\leq 2R$. There are also by the proof of lemma 3.2.2 in [**BS04**] $O_{d,\varepsilon}(R^{2/d+\varepsilon})$ rational lines of height $\leq 2R$ on each geometrically integral hyperplane section. There are thus $\ll_{d,\varepsilon} \min(BR^{2/d+\varepsilon}, R^{4/3+2/d+\varepsilon})$ rational lines of height $\leq 2R$ in M_2. Hence if $R \geq 1$, the contribution from all rational lines of height $H(\Lambda) \in [R, 2R]$ to $\sum_{\Lambda \in M_2} H(\Lambda)^{-1}$ will be $\ll_{d,\varepsilon} \min(BR^{-1+2/d+\varepsilon}, R^{1/3+2/d+\varepsilon}) \leq B^{1/4+3/2d}R^{\varepsilon}$. If we cover $[1, 2B^2]$ by $O(\log B)$ dyadic intervals with $1 \leq R \leq B^2$, we obtain

$$\sum_{\Lambda \in M_2} H(\Lambda)^{-1} = O_d(B^{1/4+3/2d+\varepsilon}) \ . \tag{4.6}$$

If we combine (4.5) and (4.6), then we get (4.4). This completes the proof. □

5. Proof of the theorems

We shall in this section prove Theorems 0.1 and 0.2.

THEOREM 5.1. *Let $X \subset \mathbb{P}^4$ be a geometrically integral projective hypersurface over $\mathbb{Q}$ of degree $d \geq 3$. Then,*

$$\widetilde{N}(X, B) = O_{d,\varepsilon}(B^{11/4+\varepsilon} + B^{3/2d+5/2+\varepsilon}) \ .$$

If X is not a cone over a curve, then,

$$\widetilde{N}(X, B) = O_{d,\varepsilon}(B^{45/16\sqrt{d}+5/4+\varepsilon} + B^{3/2d+5/2+\varepsilon}) \ .$$

If there are only finitely many planes on $X \subset \mathbb{P}^4$, then

$$\widetilde{N}(X,B) = \begin{cases} O_\varepsilon(B^{45/16\sqrt{d}+5/4+\varepsilon}) & \text{if } d=3 \text{ or } 4 \text{ and } X \text{ is not a cone of a Steiner surface} \\ O_\varepsilon(B^{1205/448+\varepsilon}) & \text{if} d=4 \\ O_\varepsilon(B^{51/20+\varepsilon}) & \text{if } d=5 \\ O_{d,\varepsilon}(B^{5/2+\varepsilon}) & \text{if } d \geq 6. \end{cases}$$

PROOF. Let $h(d) = \max(45/16\sqrt{d} + 5/4, 5/2)$ if X is not a cone of a Steiner surface and $h(d) = 1205/448$ if X is a cone of a Steiner surface. Then it is shown in Theorem 3.3 that there is a set M of $O_{d,\varepsilon}(B^{45/32\sqrt{d}+5/4+\varepsilon})$ rational lines on X such that all but $O_{d,\varepsilon}(B^{h(d)+\varepsilon})$ points in $\widetilde{S}(X,B)$ lie on the union of these lines. To count the points in $\widetilde{S}(X,B) \cap (\cup_{\Lambda \in M} \Lambda(\mathbb{Q}))$, we note that $\#M = O_{d,\varepsilon}(B^{5/2+\varepsilon})$ and apply Lemma 4.1. We then get that $\widetilde{N}(X,B) = O_{d,\varepsilon}(B^{h(d)+\varepsilon} + B^{11/4+\varepsilon} + B^{3/2d+5/2+\varepsilon})$ in general. Further, if X is not a cone over a curve, then $\widetilde{N}(X,B) = O_{d,\varepsilon}(B^{h(d)+\varepsilon} + B^{3/2d+5/2+\varepsilon})$ while $\widetilde{N}(X,B) = O_{d,\varepsilon}(B^{h(d)+\varepsilon} + B^{3/2d+9/4+\varepsilon} + B^{5/2+\varepsilon})$ in the more special case when there are only finitely many planes on $X \subset \mathbb{P}^4$. It is now easy to complete the proof by comparing all the exponents that occur. □

COROLLARY 5.2. Let $X \subset \mathbb{P}^4$ be a geometrically integral projective hypersurface over $\mathbb{Q}$ of degree $d \geq 3$. Then, $N(X,B) = O_{d,\varepsilon}(B^{3+\varepsilon})$.

PROOF. This follows from the first assertion in Theorem 5.1 and [**BS04**], Lemma 3.1.1. (The result was first proved for $d \geq 4$ in [**BS04**] and then for $d = 3$ in [**BHB05**].) □

THEOREM 5.3. *Let $X \subset \mathbb{P}^n$ be a geometrically integral projective threefold over $\mathbb{Q}$ of degree d. Let X' be the complement of the union of all planes on X. Then,*

$$N(X',B) = \begin{cases} O_{n,\varepsilon}(B^{15\sqrt{3}/16+5/4+\varepsilon}) & \text{if } d=3, \\ O_{n,\varepsilon}(B^{1205/448+\varepsilon}) & \text{if } d=4, \\ O_{n,\varepsilon}(B^{51/20+\varepsilon}) & \text{if } d=5, \\ O_{d,n,\varepsilon}(B^{5/2+\varepsilon}) & \text{if } d \geq 6\ . \end{cases}$$

If $n = d = 4$ and X is not a cone of a Steiner surface, then

$$N(X',B) = O_{n,\varepsilon}(B^{85/32+\varepsilon})\ .$$

PROOF. If $n = 4$ and there are only finitely many planes on $X \subset \mathbb{P}^4$, then this follows from Theorem 5.1 since $N(X',B) \leq \widetilde{N}(X,B)$. If there are infinitely many planes on X, then X' is empty [**Salb**], 7.4 and $N(X',B) = 0$. To prove Theorem 5.3 for $n > 4$, we reduce to the case $n = 4$ by means of a birational projection argument (see [**Salc**], 8.3). □

PROPOSITION 5.4. *Let k be an algebraically closed field of characteristic 0 and $(a_0,\ldots,a_5)$, $(b_0,\ldots,b_5)$ be two sextuples in $k^* = k \setminus \{0\}$ and $X \subset \mathbb{P}^5$ be the closed subscheme defined by the two equations $a_0x_0^e + \ldots + a_5x_5^e = 0$ and $b_0x_0^f + \ldots + b_5x_5^f = 0$ where $e < f$. Then the following holds*

(a) *There are only finitely many singular points on X,*
(b) *X is a normal integral scheme of degree ef,*
(c) *There are only finitely many planes on X if $f \geq 3$,*
(d) *X is not a cone over a Steiner surface.*

PROOF. (a) Let $(x_0, \ldots, x_5)$ be a singular point on X with at least two non-zero coordinates x_i, x_j. Then it follows from the Jacobian criterion that $a_i b_j x_i^{e-1} x_j^{f-1} = a_j b_i x_j^{e-1} x_i^{f-1}$ and hence that $a_i b_j x_j^{f-e} = a_j b_i x_i^{f-e}$. Hence there are only $f - e$ possible values for x_j/x_i for any two non-zero coordinates x_i, x_j of a singular point. This implies that there only finitely many singular points on X.

(b) The forms $a_0 x_0^e + \ldots + a_5 x_5^e$ and $b_0 x_0^f + \ldots + b_5 x_5^f$ are irreducible for $(a_0, \ldots, a_5)$, $(b_0, \ldots, b_5)$ as above and define integral hypersurfaces $Y_a \subset \mathbb{P}^5$ and $Y_b \subset \mathbb{P}^5$ of different degrees. Therefore, $X \subset \mathbb{P}^5$ is a complete intersection of codimension two of degree ef. In particular, Y_b is a Cohen-Macaulay scheme and $X \subset Y_b$ a closed subscheme which is regularly immersed. Hence, as the singular locus of X is of codimension ≥ 2, we obtain from [**AK70**], VII 2.14, that X is normal. As X is of finite type over k, it is thus integral if and only if it is connected. To show that X is connected, use Exercise II.8.4 in [**Har77**].

(c) It is known that there are only finitely many planes on non-singular hypersurfaces of degree ≥ 3 in $\mathbb{P}^5$ (see [**Sta06**] where it is attributed to Debarre). There are thus only finitely many planes on Y and hence also on X.

(d) It is well known that a Steiner surface has three double lines. The singular locus of a cone of Steiner surface is thus two-dimensional. Hence X cannot be such a cone by (a). □

Parts (a) and (c) of the previous proposition were used already in [**Kon02**] and [**BHB**].

THEOREM 5.5. *Let $(a_0, \ldots, a_5)$ and $(b_0, \ldots, b_5)$ be two sextuples of rational numbers different from zero and $e < f$ be positive integers with $f \geq 3$. Let $X \subset \mathbb{P}^5$ be the threefold defined by the two equations $a_0 x_0^e + \ldots + a_5 x_5^e = 0$ and $b_0 x_0^f + \ldots + b_5 x_5^f = 0$. Then there are only finitely many planes on X. If $X' \subset X$ is the complement of these planes in X, then*

$$\begin{aligned} N(X', B) &= O_\varepsilon(B^{45/16\sqrt{ef}+5/4+\varepsilon}) && \text{if } ef = 3 \text{ or } 4, \\ N(X', B) &= O_\varepsilon(B^{51/20+\varepsilon}) && \text{if } ef = 5, \\ N(X', B) &= O_{e,f,\varepsilon}(B^{5/2+\varepsilon}) && \text{if } ef \geq 6\,. \end{aligned}$$

PROOF. This follows from Theorems 5.3 and 5.4. □

References

[AK70] A. ALTMAN & S. KLEIMAN – *Introduction to Grothendieck duality theory*, Lecture Notes in Mathematics, Vol. 146, Springer-Verlag, Berlin, 1970.

[BHB] T. D. BROWNING & D. R. HEATH-BROWN – "Simultaneous equal sums of three powers", Proc. of the session on Diophantine geometry (Pisa, 1st April-30th July , 2005), to appear.

[BHB05] ______, "Counting rational points on hypersurfaces", *J. Reine Angew. Math.* **584** (2005), p. 83–115.

[BS04] N. BROBERG & P. SALBERGER – "Counting rational points on threefolds", in *Arithmetic of higher-dimensional algebraic varieties (Palo Alto, CA, 2002)*, Progr. Math., vol. 226, Birkhäuser Boston, Boston, MA, 2004, p. 105–120.

[Gre97] G. GREAVES – "Some Diophantine equations with almost all solutions trivial", *Mathematika* **44** (1997), no. 1, p. 14–36.

[Har77] R. HARTSHORNE – *Algebraic geometry*, Springer-Verlag, New York, 1977, Graduate Texts in Mathematics, No. 52.

[HB02] D. R. HEATH-BROWN – "The density of rational points on curves and surfaces", *Ann. of Math. (2)* **155** (2002), no. 2, p. 553–595.

[Kon02] A. Kontogeorgis – "Automorphisms of Fermat-like varieties", *Manuscripta Math.* **107** (2002), no. 2, p. 187–205.

[Rog94] E. Rogora – "Varieties with many lines", *Manuscripta Math.* **82** (1994), no. 2, p. 207–226.

[Sala] P. Salberger – "Counting rational points on projective varieties", preprint.

[Salb] ______, "On the density of rational and integral points on algebraic varieties", to appear in J. Reine und Angew. Math., (see www.arxiv.org 2005).

[Salc] ______, "Rational points of bounded height on projective surfaces", submitted.

[Sal05] P. Salberger – "Counting rational points on hypersurfaces of low dimension", *Ann. Sci. École Norm. Sup. (4)* **38** (2005), no. 1, p. 93–115.

[Sch91] W. M. Schmidt – *Diophantine approximations and Diophantine equations*, Lecture Notes in Mathematics, vol. 1467, Springer-Verlag, Berlin, 1991.

[Sha99] I. R. Shafarevich (ed.) – *Algebraic geometry. V*, Encyclopaedia of Mathematical Sciences, vol. 47, Springer-Verlag, Berlin, 1999, Fano varieties, A translation of *Algebraic geometry. 5* (Russian), Ross. Akad. Nauk, Vseross. Inst. Nauchn. i Tekhn. Inform., Moscow, Translation edited by A. N. Parshin and I. R. Shafarevich.

[SR49] J. G. Semple & L. Roth – *Introduction to Algebraic Geometry*, Oxford, at the Clarendon Press, 1949.

[Sta06] J. M. Starr – "Appendix to the paper: *The density of rational points on non-singular hypersurfaces, II* by T.D. Browning and R. Heath-Brown", *Proc. London Math. Soc.* **93** (2006), p. 273–303.

[SW97] C. M. Skinner & T. D. Wooley – "On the paucity of non-diagonal solutions in certain diagonal Diophantine systems", *Quart. J. Math. Oxford Ser. (2)* **48** (1997), no. 190, p. 255–277.

[TW99] W. Y. Tsui & T. D. Wooley – "The paucity problem for simultaneous quadratic and biquadratic equations", *Math. Proc. Cambridge Philos. Soc.* **126** (1999), no. 2, p. 209–221.

[Woo96] T. D. Wooley – "An affine slicing approach to certain paucity problems", in *Analytic number theory, Vol. 2 (Allerton Park, IL, 1995)*, Progr. Math., vol. 139, Birkhäuser Boston, Boston, MA, 1996, p. 803–815.

Department of Mathematics, Chalmers University of Technology, SE-41296 Göteborg, Sweden

E-mail address: salberg@math.chalmers.se

Clay Mathematics Proceedings
Volume 7, 2007

Reciprocal Geodesics

Peter Sarnak

ABSTRACT. The closed geodesics on the modular surface which are equivalent to themselves when their orientation is reversed have recently arisen in a number of different contexts.We examine their relation to Gauss' ambiguous binary quadratic forms and to elements of order four in his composition groups.We give a parametrization of these geodesics and use this to count them asymptotically and to investigate their distribution.

This note is concerned with parametrizing, counting and equidistribution of conjugacy classes of infinite maximal dihedral subgroups of $\Gamma = PSL(2,\mathbb{Z})$ and their connection to Gauss' ambiguous quadratic forms. These subgroups feature in the recent work of Connolly and Davis on invariants for the connect sum problem for manifolds [**CD**]. They also come up in [**PR04**] (also see the references therein) in connection with the stability of kicked dynamics of torus automorphisms as well as in the theory of quasimorphisms of Γ. In [**GS80**] they arise when classifying codimension one foliations of torus bundles over the circle. Apparently they are of quite wide interest. As pointed out to me by Peter Doyle, these conjugacy classes and the corresponding reciprocal geodesics, are already discussed in a couple of places in the volumes of Fricke and Klein ([**FK**], Vol. I, page 269, Vol II, page 165). The discussion below essentially reproduces a (long) letter that I wrote to Jim Davis (June, 2005).

Denote by $\{\gamma\}_\Gamma$ the conjugacy class in Γ of an element $\gamma \in \Gamma$. The elliptic and parabolic classes (i.e., those with $t(\gamma) \leq 2$ where $t(\gamma) = |\text{trace } \gamma|$) are well-known through examining the standard fundamental domain for Γ as it acts on $\mathbb{H}$. We restrict our attention to hyperbolic γ's and we call such a γ primitive (or prime) if it is not a proper power of another element of Γ. Denote by P the set of such elements and by Π the corresponding set of conjugacy classes. The primitive elements generate the maximal hyperbolic cyclic subgroups of Γ. We call a $p \in P$ reciprocal if $p^{-1} = S^{-1}pS$ for some $S \in \Gamma$. In this case, $S^2 = 1$ (proofs of this and further claims are given below) and S is unique up to multiplication on the left by $\gamma \in \langle p \rangle$. Let R denote the set of such reciprocal elements. For $r \in R$ the group $D_r = \langle r, S \rangle$, depends only on r and it is a maximal infinite dihedral subgroup of

2000 *Mathematics Subject Classification.* Primary 11F06, Secondary 11M36.
Key words and phrases. Number theory, binary quadratic forms, modular surface.
Supported in part by the NSF Grant No. DMS0500191 and a Veblen Grant from the IAS.

Γ. Moreover, all of the latter arise in this way. Thus, the determination of the conjugacy classes of these dihedral subgroups is the same as determining ρ, the subset of Π consisting of conjugacy classes of reciprocal elements. Geometrically, each $p \in P$ gives rise to an oriented primitive closed geodesic on $\Gamma\backslash\mathbb{H}$, whose length is $\log N(p)$ where $N(p) = \left[\left(t(p) + \sqrt{t(p)^2 - 4}\right)/2\right]^2$. Conjugate elements give rise to the same oriented closed geodesic. A closed geodesic is equivalent to itself with its orientation reversed iff it corresponds to an $\{r\} \in \rho$.

The question as to whether a given γ is conjugate to γ^{-1} in Γ is reflected in part in the corresponding local question. If $p \equiv 3 \pmod 4$, then $c = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ is not conjugate to c^{-1} in $SL(2, \mathbb{F}_p)$, on the other hand, if $p \equiv 1 \pmod 4$ then every $c \in SL(2, \mathbb{F}_p)$ is conjugate to c^{-1}. This difficulty of being conjugate in $G(\bar{F})$ but not in $G(F)$ does not arise if $G = GL_n$ (F a field) and it is the source of a basic general difficulty associated with conjugacy classes in G and the (adelic) trace formula and its stabilization [**Lan79**]. For the case at hand when working over $\mathbb{Z}$, there is the added issue associated with the lack of a local to global principle and in particular the class group enters. In fact, certain elements of order dividing four in Gauss' composition group play a critical role in the analysis of the reciprocal classes.

In order to study ρ it is convenient to introduce some other set theoretic involutions of Π. Let ϕ_R be the involution of Γ given by $\phi_R(\gamma) = \gamma^{-1}$. Let $\phi_w(\gamma) = w^{-1}\gamma w$ where $w = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \in PGL(2, \mathbb{Z})$ (modulo inner automorphism ϕ_w generates the outer automorphisms of Γ coming from $PGL(2, \mathbb{Z})$). ϕ_R and ϕ_w commute and set $\phi_A = \phi_R \circ \phi_w = \phi_w \circ \phi_R$. These three involutions generate the Klein group G of order 4. The action of G on Γ preserves P and Π. For H a subgroup of G, let $\Pi_H = \{\{p\} \in \Pi : \phi(\{p\}) = \{p\} \text{ for } \phi \in H\}$. Thus $\Pi_{\{e\}} = \Pi$ and $\Pi_{\langle \phi_R \rangle} = \rho$. We call the elements in $\Pi_{\langle \phi_A \rangle}$ ambiguous classes (we will see that they are related to Gauss' ambiguous classes of quadratic forms) and of $\Pi_{\langle \phi_w \rangle}$, inert classes. Note that the involution $\gamma \to \gamma^t$ is, up to conjugacy in Γ, the same as ϕ_R, since the contragredient satisfies ${}^t g^{-1} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} g \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$. Thus $p \in P$ is reciprocal iff p is conjugate to p^t.

To give an explicit parametrization of ρ let

$$(1) \qquad C = \left\{(a,b) \in \mathbb{Z}^2 : (a,b) = 1,\, a > 0,\, d = 4a^2 + b^2 \text{ is not a square}\right\}.$$

To each $(a,b) \in C$ let (t_0, u_0) be the least solution with $t_0 > 0$ and $u_0 > 0$ of the Pell equation

$$(2) \qquad t^2 - du^2 = 4\,.$$

Define $\psi : C \longrightarrow \rho$ by

$$(3) \qquad (a,b) \longrightarrow \left\{ \begin{bmatrix} \dfrac{t_0 - bu_0}{2} & au_0 \\ au_0 & \dfrac{t_0 + bu_0}{2} \end{bmatrix} \right\}_\Gamma ,$$

It is clear that $\psi((a,b))$ is reciprocal since an $A \in \Gamma$ is symmetric iff $S_0^{-1} A S_0 = A^{-1}$ where $S_0 = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$. Our central assertion concerning parametrizing ρ is;

Proposition 1. *$\psi : C \longrightarrow \rho$ is two-to-one and onto.* *

There is a further stratification to the correspondence (3). Let

(4) $$\mathcal{D} = \{m \,|\, m > 0\,,\, m \equiv 0,1 \pmod 4\,, m \text{ not a square}\}\,.$$

Then

$$C = \bigcup_{d \in \mathcal{D}} C_d$$

where

(5) $$C_d = \left\{(a,b) \in C \,|\, 4a^2 + b^2 = d\right\}\,.$$

Elementary considerations concerning proper representations of integers as a sum of two squares shows that C_d is empty unless d has only prime divisors p with $p \equiv 1 \pmod 4$ or the prime 2 which can occur to exponent $\alpha = 0, 2$ or 3. Denote this subset of $\mathcal{D}$ by $\mathcal{D}_R$. Moreover for $d \in \mathcal{D}_R$,

(6) $$|C_d| = 2\,\nu(d)$$

where for any $d \in \mathcal{D}, \nu(d)$ is the number of genera of binary quadratic forms of discriminant d ((6) is not a coincidence as will be explained below). Explicitly $\nu(d)$ is given as follows: If $d = 2^\alpha D$ with D odd and if λ is the number of distinct prime divisors of D then

(6′) $$\nu(d) = \begin{cases} 2^{\lambda-1} & \text{if} \quad \alpha = 0 \\ 2^{\lambda-1} & \text{if} \quad \alpha = 2 \quad \text{and} \quad D \equiv 1 \pmod 4 \\ 2^{\lambda} & \text{if} \quad \alpha = 2 \quad \text{and} \quad D \equiv 3 \pmod 4 \\ 2^{\lambda} & \text{if} \quad \alpha = 3 \quad \text{or} \quad 4 \\ 2^{\lambda+1} & \text{if} \quad \alpha \geq 5\,. \end{cases}$$

Corresponding to (5) we have

(7) $$\rho = \bigsqcup_{d \in \mathcal{D}_R} \rho_d\,,$$

with $\rho_d = \psi(C_d)$. In particular, $\psi : C_d \longrightarrow \rho_d$ is two-to-one and onto and hence

(8) $$|\rho_d| = \nu(d) \text{ for } d \in \mathcal{D}_R\,.$$

Local considerations show that for $d \in \mathcal{D}$ the Pell equation

(9) $$t^2 - du^2 = -4\,,$$

can only have a solution if $d \in \mathcal{D}_R$. When $d \in \mathcal{D}_R$ it may or may not have a solution. Let $\mathcal{D}_R^-$ be those d's for which (9) has a solution and $\mathcal{D}_R^+$ the set of $d \in \mathcal{D}_R$ for which (9) has no integer solution. Then

(i) For $d \in \mathcal{D}_R^+$ none of the $\{r\} \in \rho_d$, are ambiguous.
(ii) For $d \in \mathcal{D}_R^-$, every $\{r\} \in \rho_d$ is ambiguous.

*Part of this Proposition is noted in ([**FK**], Vol. I, pages 267-269).

In this last case (ii) we can choose an explicit section of the two-to-one map (3). For $d \in \mathcal{D}_R^-$ let $C_d^- = \{(a,b) : b < 0\}$, then $\psi : C_d^- \longrightarrow \rho_d$ is a bijection.†

Using these parameterizations as well as some standard techniques from the spectral theory of $\Gamma\backslash\mathbb{H}$ one can count the number of primitive reciprocal classes. We order the primes $\{p\} \in \Pi$ by their trace $t(p)$ (this is equivalent to ordering the corresponding prime geodesics by their lengths). For H a subgroup of G and $x > 2$ let

$$\Pi_H(x) := \sum_{\substack{\{p\} \in \Pi_H \\ t(p) \leq x}} 1\,. \tag{10}$$

THEOREM 2. *As $x \longrightarrow \infty$ we have the following asymptotics:*

$$\Pi_{\{1\}}(x) \sim \frac{x^2}{2\log x}\,, \tag{11}$$

$$\Pi_{\langle\phi_A\rangle}(x) \sim \frac{97}{8\pi^2}\, x(\log x)^2\,, \tag{12}$$

$$\Pi_{\langle\phi_R\rangle}(x) \sim \frac{3}{8}\, x\,, \tag{13}$$

$$\Pi_{\langle\phi_w\rangle}(x) \sim \frac{x}{2\log x} \tag{14}$$

and

$$\Pi_G(x) \sim \frac{21}{8\pi}\, x^{1/2} \log x\,. \tag{15}$$

(All of these are established with an exponent saving for the remainder).

In particular, roughly the square root of all the primitive classes are reciprocal while the fourth root of them are simultaneously reciprocal ambiguous and inert.

We turn to the proofs of the above statements as well as a further discussion connecting ρ with elements of order dividing four in Gauss' composition groups.

We begin with the implication $S^{-1}pS = p^{-1} \Longrightarrow S^2 = 1$. This is true already in $PSL(2,\mathbb{R})$. Indeed, in this group p is conjugate to $\pm\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$ with $\lambda > 1$. Hence $Sp^{-1} = pS$ with $S = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \Longrightarrow a = d = 0$, i.e., $S = \pm\begin{bmatrix} 0 & \beta \\ -\beta^{-1} & 0 \end{bmatrix}$ and so $S^2 = 1$. If S and S_1 satisfy $x^{-1}px = p^{-1}$ then $SS_1^{-1} \in \Gamma_p$ the centralizer of p in Γ. But $\Gamma_p = \langle p \rangle$ and hence $S = \beta S_1$ with $\beta \in \langle p \rangle$. Now every element $S \in \Gamma$ whose order is two (i.e., an elliptic element of order 2) is conjugate in Γ to $S_0 = \pm\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$. Hence any $r \in R$ is conjugate to an element $\gamma \in \Gamma$ for which $S_0^{-1}\gamma S_0 = \gamma^{-1}$. The last is equivalent to γ being symmetric. Thus each $r \in R$ is conjugate to a $\gamma \in R$ with $\gamma = \gamma^t$. (15′)

We can be more precise:

LEMMA 3. *Every $r \in R$ is conjugate to exactly four γ's which are symmetric.*

†For a general $d \in \mathcal{D}_R^+$ it appears to be difficult to determine explicitly a one-to-one section of ψ.

To see this associate to each S satisfying

(16) $$S^{-1}rS = r^{-1}$$

the two solutions γ_S and γ'_S (here $\gamma'_S = S\gamma_S$) of

(17) $$\gamma^{-1}S\gamma = S_0 .$$

Then

(18) $\gamma_S^{-1}\, r\gamma_S = ((\gamma'_S)^{-1}\, r\gamma'_S)^{-1}$ and both of these are symmetric.

Thus each S satisfying (17) affords a conjugation of r to a pair of inverse symmetric matrices. Conversely every such conjugation of r to a symmetric matrix is induced as above from a γ_S. Indeed if $\beta^{-1}r\beta$ is symmetric then $S_0^{-1}\,\beta^{-1}\, r\beta S_0 = \beta^{-1}\, r^{-1}\beta$ and so $\beta S_0^{-1}\,\beta^{-1} = S$ for an S satisfying (17). Thus to establish (16) it remains to count the number of distinct images $\gamma_S^{-1}\, r\gamma_S$ and its inverse that we get as we vary over all S satisfying (17). Suppose then that

(19) $$\gamma_S^{-1}\, r\gamma_S = \gamma_{S'}^{-1}\, r\gamma_{S'} .$$

Then

(20) $$\gamma_{S'}\,\gamma_S^{-1} = b \in \Gamma_r = \langle r\rangle .$$

Also from (18)

(21) $$\gamma_S^{-1}\, S\gamma_S = \gamma_{S'}^{-1}\, S'\,\gamma_{S'}$$

or

(22) $$\gamma_{S'}\,\gamma_S^{-1}\, S\,\gamma_S\,\gamma_{S'}^{-1} = S' .$$

Using (21) in (23) yields

(23) $$b^{-1}\, Sb = S' .$$

But bS satisfies (17), hence $bSbS = 1$. Putting this relation in (24) yields

(24) $$S' = b^{-2}S .$$

These steps after (22) may all be reversed and we find that (20) holds iff $S = b^2S'$ for some $b \in \Gamma_r$. Since the solutions of (17) are parametrized by bS with $b \in \Gamma_r$(and S a fixed solution) it follows that as S runs over solutions of (17), $\gamma_S^{-1}\, r\gamma_S$ and $(\gamma'_S)^{-1}r(\gamma'_S)$ run over exactly four elements. This completes the proof of (16). This argument should be compared with the one in ([**Cas82**], p. 342) for counting the number of ambiguous classes of forms. Peter Doyle notes that the four primitive symmetric elements which are related by conjugacy can be described as follows: If A is positive, one can write A as $\gamma'\gamma$ with $\gamma \in \Gamma$ (the map $\gamma \longrightarrow \gamma'\gamma$ is onto such); then A, A^{-1}, B, B^{-1}, with $B = \gamma\gamma'$, are the four such elements.

To continue we make use of the explicit correspondence between Π and classes of binary quadratic forms (see [**Sar**] and also ([**Hej83**], pp. 514-518). [‡] An integral binary quadratic form $f = [a, b, c]$ (i.e. $ax^2 + bxy + xy^2$) is primitive if $(a, b, c) = 1$. Let F denote the set of such forms whose discriminant $d = b^2 - 4ac$ is in $\mathcal{D}$. Thus

(25) $$F = \bigsqcup_{d\in\mathcal{D}} F_d .$$

with F_d consisting of the forms of discriminant d. The symmetric square representation of PGL_2 gives an action $\sigma(\gamma)$ on F for each $\gamma \in \Gamma$. It is given by $\sigma(\gamma)f = f'$

[‡]This seems to have been first observed in ([**FK**], Vol., page 268)

where $f'(x,y) = f((x,y)\gamma)$. Following Gauss we decompose F into equivalence classes under this action $\sigma(\Gamma)$. The class of f is denoted by $\bar{f}$ or Φ and the set of classes by $\mathcal{F}$. Equivalent forms have a common discriminant and so

$$\mathcal{F} = \bigsqcup_{d\in\mathcal{D}} \mathcal{F}_d\,. \tag{26}$$

Each $\mathcal{F}_d$ is finite and its cardinality is denoted by $h(d)$ - the class number. Define a map n from P to F by

$$p = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \xrightarrow{\,n\,} f(p) = \frac{1}{\delta}\,\mathsf{sgn}\,(a+d)\,[b, d-a, -c]\,. \tag{27}$$

where $\delta = \gcd(a, d-a, c) \geq 1$ and n satisfies the following

(i) n is a bijection from Π to F.
(ii) $n(\gamma p \gamma^{-1}) = (\det\gamma)\,\sigma(\gamma)\,n(p)$ for $\gamma \in PGL(2,\mathbb{Z})$.
(iii) $n(p^{-1}) = -n(p)$
(iv) $n(w^{-1}pw) = n(p)^*$
(v) $n(w^{-1}p^{-1}w) = n(p)'$

where

$$[a,b,c]^* = [-a,b,-c] \tag{28}$$

and

$$[a,b,c]' = [a,-b,c]\,. \tag{29}$$

The proof is a straight-forward verification except for n being onto, which relies on the theory of Pell's equation (2). If $f = [a,b,c] \in F$ and has discriminant d and if (t_d, u_d) is the fundamental positive solution to (2) (we also let $\epsilon_d := \frac{t_d + \sqrt{d}\,u_d}{2}$) and if

$$p = \begin{bmatrix} \frac{t_d - u_d b}{2} & a u_d \\ -c u_d & \frac{t_d + u_d b}{2} \end{bmatrix} \tag{30}$$

then $p \in P$ and $n(p) = f$. That p is primitive follows from the well-known fact (see [**Cas82**], p. 291) that the group of automorphs of f, $\mathsf{Aut}_\Gamma(f)$ satisfies
(31)

$$\mathsf{Aut}_\Gamma(f) := \{\gamma \in \Gamma : \sigma(\gamma) f = f\} = \left\{ \begin{pmatrix} \frac{t-bu}{2} & au \\ -cu & \frac{t+bu}{2} \end{pmatrix} : t^2 - du^2 = 4 \right\} \Big/ \pm 1$$

More generally

$$Z(f) := \{\gamma \in PGL(2,\mathbb{Z}) |\, \sigma(\gamma) f = (\det\gamma) f\}$$

$$= \left\{ \begin{pmatrix} \frac{t-bu}{2} & au \\ -cu & \frac{t+bu}{2} \end{pmatrix} : t^2 - du^2 = \pm 4 \right\} \Big/ \pm 1\,. \tag{32}$$

$Z(f)$ is cyclic with a generator η_f corresponding to the fundamental solution $\eta_d = (t_1 + \sqrt{d}\,u_1)/2$, $t_1 > 0$, $u_1 > 0$ of

$$t^2 - du^2 = \pm 4\,. \tag{33}$$

If (9) has a solution, i.e. $d \in \mathcal{D}_R^-$ then η_d corresponds to a solution of (9) and $\epsilon_d = \eta_d^2$. If (9) doesn't have a solution then $\eta_d = \epsilon_d$. Note that $Z(f)$ has elements with $\det \gamma = -1$ iff $d_f \in \mathcal{D}_R^-$. (35)

From (ii) of the properties of the correspondence n we see that $Z(f)$ is the centralizer of p in $PGL(2, \mathbb{Z})$, where $n(p) = f$. (36)

Also from (ii) it follows that n preserves classes and gives a bijection between Π and $\mathcal{F}$. Moreover, from (iii), (iv) and (v) we see that the action of $G = \{1, \phi_w, \phi_A, \phi_R)\}$ corresponds to that of $\tilde{G} = \{1, *, \prime, -\}$ on $\mathcal{F}, \tilde{G}$ preserves the decomposition (27) and we therefore examine the fixed points of $g \in \tilde{G}$ on $\mathcal{F}_d$.

Gauss [**Gau**] determined the number of fixed points of $\prime$ in $\mathcal{F}_d$. He discovered that $\mathcal{F}_d$ forms an abelian group under his law of composition. In terms of the group law, $\Phi' = \Phi^{-1}$ for $\Phi \in \mathcal{F}_d$. Hence the number of fixed points of $\prime$ (which he calls ambiguous forms) in $\mathcal{F}_d$ is the number of elements of order (dividing) 2. Furthermore $\mathcal{F}_d/\mathcal{F}_d^2$ is isomorphic to the group of genera (the genera are classes of forms with equivalence being local integral equivalence at all places). Thus the number of fixed points of $\prime$ in $\mathcal{F}_d$ is equal to the number of genera, which in turn he showed is equal to the number $\nu(d)$ defined earlier. For an excellent modern treatment of all of this see [**Cas82**].

Consider next the involution $*$ on $\mathcal{F}_d$. If $b \in \mathbb{Z}$ and $b \equiv d \pmod 2$ then the forms $[-1, b, \frac{d-b^2}{4}]$ are all equivalent and this defines a class $J \in \mathcal{F}_d$. Using composition one sees immediately that $J^2 = 1$, that is J is ambiguous. Also, applying composition one finds that

$$J\,\overline{[a,b,c]} = \overline{[-a,b,-c]} = \overline{[a,b,c]}^* . \tag{37}$$

That is, the action of $*$ on $\mathcal{F}_d$ is given by translation in the composition group; $\Phi \to \Phi J$. Thus $*$ has a fixed point in $\mathcal{F}_d$ iff $J = 1$, in which case all of $\mathcal{F}_d$ is fixed by $*$. To analyze when $J = 1$ we first determine when J and 1 are in the same genus (i.e. the principal genus). Since $[1, b, \frac{b^2-d}{4}]$ and $[1, -b, \frac{b^2-d}{4}]$ are in the same genus (they are even equivalent) it follows that J and 1 are in the same genus iff $f = [1, b, \frac{b^2-d}{4}]$ and $-f$ are in the same genus. An examination of the local genera (see [**Cas82**], p. 33) shows that there is an f of discriminant d which is in the same genus as $-f$ iff $d \in \mathcal{D}_R$. Thus J is in the principal genus iff $d \in \mathcal{D}_R$. (38)

To complete the analysis of when $J = 1$, note that this happens iff $[1, b, \frac{b^2-d}{4}] \sim [-1, b\,\frac{d-b^2}{4}]$. That is, $[1, b, \frac{b^2-d}{4}] \sim (\det w)\,\sigma(w)[1, b, \frac{b^2-d}{4}]$. Alternatively, $J = 1$ iff $f = (\det \gamma)\,\sigma(\gamma) f$ with $f = [1, b, \frac{b^2-d}{4}]$ and $\det \gamma = -1$. According to (35) this is equivalent to $d \in \mathcal{D}_R^-$. Thus $*$ fixes $\mathcal{F}_d$ iff $J = 1$ iff $d \in \mathcal{D}_R^-$ and otherwise $*$ has no fixed points in $\mathcal{F}_d$. (39)

We turn to the case of interest, that is, the fixed points of $-$ on $\mathcal{F}_d$. Since $-$ is the (mapping) composite of $*$ and $\prime$ we see from the discussion above that the action $\Phi \longrightarrow -\Phi$ on $\mathcal{F}_d$ when expressed in terms of (Gauss) composition on $\mathcal{F}_d$ is given by

$$\Phi \longrightarrow J\,\Phi^{-1} . \tag{40}$$

Thus the reciprocal forms in $\mathcal{F}_d$ are those Φ's satisfying

$$\Phi^2 = J . \tag{41}$$

Since $J^2 = 1$, these Φ's have order dividing 4. Clearly, the number of solutions to (41) is either 0 or $\#\{B | B^2 = 1\}$, that is, it is either 0 or the number of ambiguous classes, which we know is $\nu(d)$. According to (38) if $d \notin \mathcal{D}_R$ then J is not in the principal genus and since Φ^2 is in the principal genus for every $\Phi \in \mathcal{F}_d$, it follows that if $d \notin \mathcal{D}_R$ then (41) has no solutions. On the other hand, if $d \in \mathcal{D}_R$ then we remarked earlier that $d = 4a^2 + b^2$ with $(a, b) = 1$. In fact there are $2\nu(d)$ such representations with $a > 0$. Each of these yields a form $f = [a, b, -a]$ in $\mathcal{F}_d$ and each of these is reciprocal by S_0. Hence for each such $f, \Phi = \bar{f}$ satisfies (41), which of course can also be checked by a direct calculation with composition. Thus for $d \in \mathcal{D}_R$, (41) has exactly $\nu(d)$ solutions. In fact, the $2\nu(d)$ forms $f = [a, b, -a]$ above project onto the $\nu(d)$ solutions in a two-to-one manner. To see this, recall (15′), which via the correspondence n, asserts that every reciprocal g is equivalent to an $f = [a, b, c]$ with $a = c$. Moreover, since $[a, b, -a]$ is equivalent to $[-a, -b, a]$ it follows that every reciprocal class has a representative form $f = [a, b, -a]$ with $(a, b) \in C_d$. That is $(a, b) \longrightarrow \overline{[a, b, -a]}$ from C_d to $\mathcal{F}_d$ maps onto the $\nu(d)$ reciprocal forms. That this map is two-to-one follows immediately from (16) and the correspondence n. This completes our proof of (3) and (8). In fact (15′) and (16) give a direct counting argument proof of (3) and (8) which does not appeal to the composition group or Gauss' determination of the number of ambiguous classes. The statements (i) and (ii) follow from (41) and (39). If $d \in \mathcal{D}_R^-$ then $J = 1$ and from (41) the reciprocal and ambiguous classes coincide. If $d \in \mathcal{D}_R^+$ then $J \neq 1$ and according to (14) the reciprocal classes constitute a fixed (non-identity) coset of the group A of ambiguous classes in $\mathcal{F}_d$.

To summarize we have the following: The primitive hyperbolic conjugacy classes are in 1-1 correspondence with classes of forms of discriminants $d \in \mathcal{D}$. To each such d, there are $h(d) = |\mathcal{F}_d|$ such classes all of which have a common trace t_d and norm ϵ_d^2. The number of ambiguous classes for any $d \in \mathcal{D}$ is $\nu(d)$. Unless $d \in \mathcal{D}_R$ there are no reciprocal classes in $\mathcal{F}_d$ while if $d \in \mathcal{D}_R$ then there are $\nu(d)$ such classes and they are parametrized by C_d in a two-to-one manner. If $d \notin \mathcal{D}_R^-$, there are no inert classes. If $d \in \mathcal{D}_R^-$ every class is inert and every ambiguous class is reciprocal and vice-versa. For $d \in \mathcal{D}_R^-$, C_d^- parametrizes the G fixed classes.

Here are some examples:

(i) If $d \in \mathcal{D}_R$ and $\mathcal{F}_d$ has no elements of order four, then $d \in \mathcal{D}_R^-$ (this fact seems to be first noted in [Re1]). For if $d \in \mathcal{D}_R^+$ then $J \neq 1$ and hence any one of our $\nu(d)$ reciprocal classes is of order four. In particular, if $d = p \equiv 1 \pmod 4$, then $h(d)$ is odd (from the definition of ambiguous forms it is clear that $h(d) \equiv \nu(d) \pmod 2$) and hence $d \in \mathcal{D}_R^-$. That is, $t^2 - pu^2 = -4$ has a solution (this is a well-known result of Legendre).

(ii) $d = 85 = 17 \times 5$. $\eta_{85} = \frac{9+\sqrt{85}}{2}$, $\epsilon_{85} = \frac{83+9\sqrt{85}}{2}$, $85 \in \mathcal{D}_R^-$ and $\nu(85) = h(85) = 2$. The distinct classes are $\overline{[1, 9, -1]}$ and $\overline{[3, 7, -3]}$. Both are ambiguous reciprocal and inert. The corresponding classes in ρ are

$$\left\{ \begin{bmatrix} 1 & 9 \\ 9 & 82 \end{bmatrix} \right\}_\Gamma \quad \text{and} \quad \left\{ \begin{bmatrix} 10 & 27 \\ 27 & 73 \end{bmatrix} \right\}_\Gamma .$$

(iii) $d = 221 = 13 \times 17$. $\eta_{221} = \epsilon_{221} = \frac{15+\sqrt{221}}{2}$ so that $221 \in \mathcal{D}_R^+$. $\nu(221) = 2$ while $h(221) = 4$. The distinct classes are $\overline{[1, 13, -13]}$, $\overline{[-1, 13, 13]}$, $\overline{[5, 11, -5]} = \overline{[7, 5, -7]}$, $\overline{[-5, 11, 5]} = \overline{[-7, 5, 7]}$. The first two classes 1 and J are the ambiguous ones while the last two are the reciprocal ones. There are no inert classes. The composition group is cyclic of order four with generator either of the reciprocal classes. The two genera consist of the ambiguous classes in one genus and the reciprocal classes in the other. The corresponding classes in ρ_{221} are

$$\left\{ \begin{bmatrix} 2 & 5 \\ 5 & 13 \end{bmatrix} \right\}_\Gamma \quad \text{and} \quad \left\{ \begin{bmatrix} 13 & 5 \\ 5 & 2 \end{bmatrix} \right\}_\Gamma .$$

The two-to-one correspondence from C_{221} to ρ_{221} has $(5, 11)$ and $(7, 5)$ going to the first class and $(5, 11)$ and $(7, -5)$ going to the second class.

(iv)[§] $d = 1885 = 5 \times 13 \times 29$. $\eta_{1885} = \epsilon_{1885} = (1042 + 24\sqrt{1885}/2)$ so that $1885 \in \mathcal{D}_R^+$. $\nu(1885) = 4$ and $h(1885) = 8$. The 8 distinct classes are

$$\mathbf{1} = \overline{[1, 43, -9]},\ \overline{[-1, 43, 9]} = J,\ \overline{[7, 31, -33]},\ \overline{[-7, 31, 33]},$$
$$\overline{[21, 11, -21]} = \overline{[-19, 21, 19]},\ \overline{[-21, 11, 21]} = \overline{[19, 21, -19]},$$
$$\overline{[3, 43, -3]} = \overline{[17, 27, -17]},\ \overline{[-3, 43, 3]} = [-17, 27, 17].$$

The first four are ambiguous and the last four reciprocal. The composition group $\mathcal{F}_{1885} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4$ and the group of genera is equal to $\mathcal{F}_{1885}/\{\mathbf{1}, J\}$. The corresponding classes in ρ_{1885} are

$$\left\{ \begin{bmatrix} 389 & 504 \\ 504 & 653 \end{bmatrix} \right\}_\Gamma , \quad \left\{ \begin{bmatrix} 653 & 504 \\ 504 & 389 \end{bmatrix} \right\}_\Gamma ,$$

$$\left\{ \begin{bmatrix} 5 & 72 \\ 72 & 1037 \end{bmatrix} \right\}_\Gamma , \quad \left\{ \begin{bmatrix} 1037 & 72 \\ 72 & 5 \end{bmatrix} \right\}_\Gamma .$$

The two-to-one correspondence from C_{1885} to ρ_{1885} has the pairs $(21, 11)$ and $(19, -21)$, $(21, -11)$ and $(19, 21)$, $(3, 43)$ and $(17, 27)$, $(3, -43)$ and $(17, -27)$ going to each of the reciprocal classes.

[§]The classes of forms of this discriminant as well as all others for $d < 2000$ were computed using Gauss reduced forms, in Kwon [**Kwo**].

(v) Markov discovered an infinite set of elements of II all of which project entirely into the set $\mathcal{G}_{3/2}$, where for $a > 1\, \mathcal{G}_a = \{z \in \mathcal{G};\, y < a\}$ and $\mathcal{G}$ is the standard fundamental domain for Γ. These primitive geodesics are parametrized by positive integral solutions $m = (m_0, m_1, m_2)$ of

$$m_0^2 + m_1^2 + m_2^2 = 3\, m_0 m_1 m_2\,. \tag{41$'$}$$

All such solutions can be gotten from the solution $(1, 1, 1)$ by repeated application of the transformation $(m_0, m_1, m_2) \to (3m_1m_2 - m_0, m_1, m_2)$ and permutations of the coordinates. The set of solutions to $(41')$ is very sparse [**Zag82**]. For a solution m of $(41')$ with $m_0 \geq m_1 \geq m_2$ let u_0 be the (unique) integer in $(0, m_0/2]$ which is congruent to $\epsilon \bar{m}_1 m_2 \pmod{m_0}$ where $\epsilon = \pm 1$ and $\bar{m}_1 m_1 \equiv 1 \pmod{m_0}$. Let v_0 be defined by $u_0^2 + 1 = m_0 v_0$, it is an integer since $(\bar{m}_1 m_2)^2 \equiv -1 \mod m_0$, from $(41')$. Set f_m to be $[m_0, 3m_0 - 2u_0, v_0 - 3u_0]$ if m_0 is odd and $\frac{1}{2}[m_0, 3m_0 - 2u_0, v_0 - 3u_0]$ if m_0 is even. Then $f_m \in F$ and let $\Phi_m = \bar{f}_m \in \mathcal{F}$. Its discriminant d_m is $9m_0^2 - 4$ if m_0 is odd and $(9m_0^2 - 4)/4$ if m_0 is even. The fundamental unit is given by $\epsilon_{d_m} = (3m + \sqrt{d_m})/2$ and the corresponding class in Π is $\{p_m\}_\Gamma$ with

$$p_m = \begin{bmatrix} u_0 & m_0 \\ 3u_0 - v_0 & 3m_0 - u_0 \end{bmatrix}. \tag{41$''$}$$

The basic fact about these geodesics is that they are the only complete geodesics which project entirely into $\mathcal{G}_{3/2}$ and what is of interest to us here, these $\{p_m\}_\Gamma$ are all reciprocal (see [**CF89**] p. 20 for proofs).

$m = (1, 1, 1)$ gives $\Phi_{(1,1,1)} = \overline{[1, 1, -1]}$, $d_{(1,1,1)} = 5$, $\epsilon_5 = (3 + \sqrt{5})/2$ while $\eta_5 = (1 + \sqrt{5})/2$. Hence $d_5 \in \mathcal{D}_R^-$ and $\Phi_{(1,1,1)}$ is ambiguous and reciprocal. The same is true for $m = (2, 1, 1)$ and $\Phi_{(2,1,1)} = \overline{[1, 2, -1]}$.

$m = (5, 2, 1)$ gives $\Phi_{(5,2,1)} = [5, 11, -5]$ and $d_{(5,2,1)} = 221$. This is the case considered in (iv) above. $\Phi_{(5,2,1)}$ is one of the two reciprocal classes of discriminant 221. It is not ambiguous.

For $m \neq (1, 1, 1)$ or $(2, 1, 1)$, $\eta_{d_m} = \epsilon_{d_m}$ and since Φ_m is reciprocal we have that $d_m \in \mathcal{D}_R^+$ and since Φ_m is not ambiguous, it has order 4 in $\mathcal{F}_{d_m}$.

We turn to counting the primes $\{p\} \in \Pi_H$, for the subgroups H of G. The cases $H = \{e\}$ and $\langle \phi_w \rangle$ are similar in that they are connected with the prime geodesic theorems for $\Gamma = PSL(2,\mathbb{Z})$ and $PGL(2,\mathbb{Z})$ [**Hej83**].

Since $t(p) \sim (N(p))^{1/2}$ as $t(p) \longrightarrow \infty$,

$$\Pi_{\{e\}}(x) = \sum_{\substack{t(p) \le x \\ \{p\} \in \Pi}} 1 \sim \sum_{\substack{N(p) \le x^2 \\ \{p\} \in \Pi}} 1\,. \tag{42}$$

According to our parametrization we have

$$\sum_{\substack{N(p) \le x^2 \\ \{p\} \in \Pi}} 1 = \sum_{\substack{d \in \mathcal{D} \\ \epsilon_d \le x}} h(d)\,. \tag{43}$$

The prime geodesic theorem for a general lattice in $PSL(2,\mathbb{R})$ is proved using the trace formula, however for $\Gamma = PSL(2,\mathbb{Z})$ the derivation of sharpest known remainder makes use of the Petersson-Kuznetzov formula and is established in [**LS95**]. It reads

$$\sum_{\substack{N(p) \le x \\ \{p\} \in \Pi}} 1 = Li(x) + O(x^{7/10})\,. \tag{44}$$

Hence

$$\Pi_{\{e\}}(x) \sim \sum_{\substack{d \in \mathcal{D} \\ \epsilon_d \le x}} h(d) \sim \frac{x^2}{2\log x}\ \text{, as } x \longrightarrow \infty\,. \tag{45}$$

We examine $H = \langle \phi_w \rangle$ next. As $x \longrightarrow \infty$,

$$\Pi_{\langle \phi_w \rangle}(x) = \sum_{\substack{t(p) \le x \\ \{p\} \in \Pi_{\langle \phi_w \rangle}}} 1 \sim \sum_{\substack{N(p) \le x^2 \\ \{p\} \in \Pi_{\langle \phi_w \rangle}}} 1\,. \tag{46}$$

Again according to our parametrization,

$$\sum_{\substack{N(p) \le x^2 \\ \{p\} \in \Pi_{\langle \phi_w \rangle}}} 1 = \sum_{\substack{d \in \mathcal{D}_R^- \\ \epsilon_d \le x}} h(d)\,. \tag{47}$$

Note that if $p \in P$ and $\phi_w(\{p\}) = \{p\}$ then $w^{-1} p\, w = \delta^{-1} p \delta$ for some $\delta \in \Gamma$. Hence $w\,\delta^{-1}$ is in the centralizer of p in $PGL(2,\mathbb{Z})$ and $\det(w\delta^{-1}) = -1$. From (36) it follows that there is a unique primitive $h \in PGL(2,\mathbb{Z})$, $\det h = -1$, such that $h^2 = p$. Moreover, every primitive h with $\det h = -1$ arises this way and if p_1 is conjugate to p_2 in Γ then h_1 is Γ conjugate to h_2. That is,

$$\sum_{\substack{N(p) \le x^2 \\ \{p\} \in \Pi_{\langle \phi_w \rangle}}} 1 = \sum_{\substack{N(h) \le x \\ \{h\}_\Gamma \\ \det h = -1}} 1\,, \tag{48}$$

where the last sum is over all primitive hyperbolic elements in $PGL(2,\mathbb{Z})$ with $\det h = -1$, $\{h\}_\Gamma$ denotes Γ conjugacy and $N(h) = \sqrt{N(h^2)}$. The right hand side of (48) can be studied via the trace formula for the even and odd part of the spectrum of $\Gamma\backslash\mathbb{H}$ ([**Ven82**], pp. 138-143). Specifically, it follows from ([**Efr93**], p. 210) and an analysis of the zeros and poles of the corresponding Selberg zeta functions $Z_+(s)$ and $Z_-(s)$ that

$$B(s) := \prod_{\substack{\{h\}_\Gamma,\ \det h = -1 \\ h \text{ primitive}}} \left(\frac{1 - N(h)^{-s}}{1 + N(h)^{-s}} \right) \tag{49}$$

has a simple zero at $s = 1$ and is homomorphic and otherwise non-vanishing in $\Re(s) > 1/2$.

Using this and standard techniques it follows that

$$\sum_{\substack{N(h) \le x \\ \det h = -1 \\ \{\gamma\}_\Gamma}} 1 \sim \frac{1}{2} \frac{x}{\log x} \quad \text{as } x \longrightarrow \infty\,. \tag{50}$$

Thus

$$\Pi_{\langle \phi_w \rangle}(x) \sim \sum_{\substack{d \in \mathcal{D}_R^- \\ \epsilon_d \le x}} h(d) \sim \frac{x}{2 \log x} \quad \text{as } x \longrightarrow \infty\,. \tag{51}$$

The asymptotics for $\Pi_{\langle \phi_R \rangle}$, $\Pi_{\langle \phi_A \rangle}$ and Π_G all reduce to counting integer points lying on a quadric and inside a large region. These problems can be handled for quite general homogeneous varieties ([**DRS93**], [**EM93**]), though two of the three cases at hand are singular so we deal with the counting directly.

$$\Pi_{\langle \phi_R \rangle}(x) = \sum_{\substack{\{\gamma\} \in \Pi_{\langle \phi_R \rangle} \\ t(\gamma) \le x}} 1 = \sum_{\substack{t_d \le x \\ d \in \mathcal{D}_R}} \nu(d)\,. \tag{52}$$

According to (16) every $\gamma \in R$ is conjugate to exactly 4 primitive symmetric $\gamma \in \Gamma$. So

$$\begin{aligned} \Pi_{\langle \phi_R \rangle}(x) &= \tfrac{1}{4} \sum_{\substack{t(\gamma) \le x \\ \gamma \in P \\ \gamma = \gamma^t}} 1 \\ &\sim \tfrac{1}{4} \sum_{\substack{N(\gamma) \le x^2 \\ \gamma \in P \\ \gamma = \gamma^t}} 1\,. \end{aligned} \tag{53}$$

Now if $\gamma \in P$ and $\gamma = \gamma^t$, then for $k \ge 1$, $\gamma^k = (\gamma^k)^t$ and conversely if $\beta \in \Gamma$ with $\beta = \beta^t$, β hyperbolic and $\beta = \gamma_1^k$ with $\gamma_1 \in P$ and $k \ge 1$, then $\gamma_1 = \gamma_1^t$. Thus we have the disjoint union

$$\bigsqcup_{k=1}^{\infty} \{\gamma^k : \gamma \in P, \gamma = \gamma^t\}$$

$$= \left\{ \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma : t(\gamma) > 2 , \gamma = \gamma^t \right\}$$

$$= \left\{ \begin{pmatrix} a & b \\ b & d \end{pmatrix} : ad - b^2 = 1 , 2 < a + d, a, b, d \in \mathbb{Z} \right\} . \tag{54}$$

Hence as $y \longrightarrow \infty$ we have,

$$\psi(y) := \# \left\{ \gamma = \begin{pmatrix} a & b \\ b & d \end{pmatrix} \in \Gamma : 2 < t(\gamma) \leq y \right\}$$

$$\sim \# \left\{ \gamma = \begin{pmatrix} a & b \\ b & d \end{pmatrix} \in \Gamma : 1 < N(\gamma) \leq y^2 \right\}$$

$$= \sum_{k=1}^{\infty} \# \left\{ \gamma \in P : \gamma = \gamma^t , N(\gamma) \leq y^{2/k} \right\}$$

$$= \#\{\gamma \in P : \gamma = \gamma^t , N(\gamma) \leq y^2\} + O(\psi(y) \log y)) . \tag{55}$$

Now $\gamma \longrightarrow \gamma^t \gamma$ maps Γ onto the set of $\begin{bmatrix} a & b \\ b & d \end{bmatrix}$, $ad - b^2 = 1$ and $a + d \geq 2$, in a two-to-one manner. Hence

$$\psi(y) = \frac{1}{2} \left| \left\{ \gamma \in \Gamma : \text{ trace } (\gamma^t \gamma) \leq y \right\} \right| - 1 . \tag{56}$$

This last is just the hyperbolic lattice point counting problem (for Γ and $z_0 = i$) see ([**Iwa95**], p. 192) from which we conclude that as $y \longrightarrow \infty$,

$$\psi(y) = \frac{3}{2} y + O(y^{2/3}) . \tag{57}$$

Combining this with (55) and (53) we get that as $x \longrightarrow \infty$

$$\Pi_{\langle \phi_R \rangle}(x) \sim \sum_{\substack{d \in \mathcal{D}_R \\ \epsilon_d \leq x}} \nu(d) \sim \frac{3}{8} x . \tag{58}$$

The case $H = \langle \phi_A \rangle$ is similar but singular. Firstly one shows as in (16) (this is done in ([**Cas82**], p. 341) where he determines the number of ambiguous forms and classes) that every $p \in P$ which is ambiguous is conjugate to precisely 4 primitive p's which are either of the form

$$w^{-1} p\, w = p^{-1} \tag{59}$$

or

$$w_1^{-1}\, p\, w_1 \;=\; p^{-1} \quad \text{with} \quad w_1 \;=\; \begin{bmatrix} 1 & 0 \\ 1 & -1 \end{bmatrix}, \tag{60}$$

called of the first and second kind respectively.

Correspondingly we have

$$\sum_{\substack{d \,\in\, \mathcal{D} \\ \epsilon_d \,\le\, x}} \nu(d) \;\sim\; \Pi_{\langle \phi_A \rangle}(x) \;=\; \Pi^{(1)}_{\langle \phi_A \rangle}(x) \;+\; \Pi^{(2)}_{\langle \phi_A \rangle}(x)\,. \tag{61}$$

An analysis as above leads to

$$\Pi^{(1)}_{\langle \phi_A \rangle}(x) \;\sim\; \frac{1}{4}\,\#\left\{a^2 - bc \;=\; 1\,;\, 1 \;<\; a \;<\; \frac{x}{2}\right\} \;=\; \frac{1}{2} \sum_{1<a<\frac{x}{2}} \tau(a^2-1) \tag{62}$$

where $\tau(m) \;=\; \#$ of divisors of m.

The asymptotics on the r.h.s. of (62) may be derived elementarily as in Ingham [**Ing27**] (for a power saving in the remainder see [**DFI94**]) and one finds that

$$\Pi^{(1)}_{\langle \phi_A \rangle}(x) \;\sim\; \frac{3}{2\pi^2}\, x(\log x)^2 \;\text{ as }\; x \longrightarrow \infty\,. \tag{63}$$

$\Pi^{(2)}_{\langle \phi_A \rangle}(x)$ is a bit messier and reduces to counting

$$\frac{1}{4}\,\#\left\{(m,n,c) :\; m^2 - 4 \;=\; n(n-4c)\,,\; 2 < m \;\le\; x\right\}\,. \tag{64}$$

This is handled in the same way though it is a bit tedious, yielding

$$\Pi^{(2)}_{\langle \phi_A \rangle}(x) \;\sim\; \frac{85}{8\pi^2}\, x(\log x)^2\,. \tag{65}$$

Putting these together gives

$$\sum_{\substack{d \,\in\mathcal{D} \\ \epsilon_d \,\le\, x}} \nu(d) \;\sim\; \Pi_{\langle \phi_A \rangle}(x) \;\sim\; \frac{97}{8\pi^2}\, x(\log x)^2 \;\text{ as }\; x \longrightarrow \infty\,. \tag{66}$$

Finally we consider $H = G$. According to the parametrization we have

$$\Pi_G(x) \;=\; \sum_{\substack{\{p\} \,\in \Pi_G \\ t(p) \,\le\, x}} 1 \;=\; \sum_{\substack{d \,\in \mathcal{D}_R^- \\ t_d \,\le\, x}} \nu(d) \;\sim\; \sum_{\substack{d \,\in\, \mathcal{D}_R^- \\ \epsilon_d \,\le\, x}} \nu(d)\,. \tag{67}$$

As in the analysis of $\Pi_{\langle \phi_R \rangle}$ and $\Pi_{\langle \phi_A \rangle}$ we conclude that

(68)

$$\Pi_G(x) \;\sim\; \frac{1}{4}\,\#\left\{\gamma \;=\; \begin{bmatrix} a & b \\ b & c \end{bmatrix} \in PGL(2,\mathbb{Z});\, \det\gamma \;=\; -1\,,\;\; 2 < a + c \;\le\; \sqrt{x}\right\}\,.$$

Or, what is equivalent, after a change of variables:

$$\Pi_G(x) \;\sim\; \frac{1}{4} \sum_{m \,\le\, \sqrt{x}} r_f(m^2+4) \tag{69}$$

where $r_f(t)$ is the number of representations of t by $f(x_1, x_2) \;=\; x_1^2 + 4x_2^2$. This asymptotics can be handled as before and gives

$$\sum_{\substack{d \,\in \mathcal{D}_R^- \\ \epsilon_d \,\le\, x}} \nu(d) \;\sim\; \Pi_G(x) \;\sim\; \frac{21}{8\pi}\sqrt{x}\, \log x\,. \tag{70}$$

This completes the proof of Theorem 2.

Returning to our enumeration of geodesics, note that one could order the elements of Π according to the discriminant d in their parametrization and ask about the corresponding asymptotics. This is certainly a natural question and one that was raised in Gauss (see [**Gau**], §304).

For H a subgroup of G define the counting functions ψ_H corresponding to Π_H by

$$\psi_H(x) = \sum_{\substack{d \in \mathcal{D} \\ d \le x}} \#\{\Phi \in \mathcal{F}_d : h(\Phi) = \Phi, h \in H\} . \tag{71}$$

Thus according to our analysis

$$\psi_{\{e\}}(x) = \sum_{\substack{d \in \mathcal{D} \\ d \le x}} h(d) \tag{72}$$

$$\psi_{\langle \phi_A \rangle}(x) = \sum_{\substack{d \in \mathcal{D} \\ d \le x}} \nu(d) \tag{73}$$

$$\psi_{\langle \phi_R \rangle}(x) = \sum_{\substack{d \in \mathcal{D}_R \\ d \le x}} \nu(d) \tag{74}$$

$$\psi_{\langle \phi_w \rangle}(x) = \sum_{\substack{d \in \mathcal{D}_R^- \\ d \le x}} h(d) \tag{75}$$

$$\psi_G(x) = \sum_{d \in \mathcal{D}_R^-, d \le x} \nu(d) . \tag{76}$$

The asymptotics here for the ambiguous classes was determined by Gauss ([**Gau**], §301), though note that he only deals with forms $[a, 2b, c]$ and so his count is smaller than (73). One finds that

$$\psi_{\langle \phi_A \rangle}(x) \sim \frac{3}{2\pi^2} x \log x , \text{ as } x \longrightarrow \infty . \tag{77}$$

As far as (74) goes, it is immediate from (1) that

$$\psi_{\langle \phi_R \rangle}(x) \sim \frac{3}{4\pi} x , \text{ as } x \longrightarrow \infty . \tag{78}$$

The asymptotics for (72) and (75) are notoriously difficult problems. They are connected with the phenomenon that the normal order of $h(d)$ in this ordering appears to be not much larger than $\nu(d)$. There are Diophantine heuristic arguments that explain why this is so [**Hoo84**], [**Sar85**]; however as far as I am aware, all that is known are the immediate bounds

$$(1 + o(1)) \frac{3}{2\pi^2} x \log x \le \psi_{\{e\}}(x) \ll \frac{x^{3/2}}{\log x} . \tag{79}$$

The lower bound coming from (77) and the upper bound from the asymptotics in [**Sie44**],

$$\sum_{\substack{d \in \mathcal{D} \\ d \le x}} h(d) \log \epsilon_d = \frac{\pi^2}{18\zeta(3)} x^{3/2} + O(x \log x) .$$

In [Ho] a more precise conjecture is made:

$$\psi_{\{e\}}(x) \sim c_2\, x(\log x)^2\,. \tag{80}$$

Kwon [**Kwo**] has recently investigated this numerically. To do so she makes an ansatz for the lower order terms in (80) in the form: $\psi_{\{e\}}(x) = x[c_2(\log x)^2 + c_1(\log x) + c_0] + O(x^\alpha)$ with $\alpha < 1$. The computations were carried out for $x < 10^7$ and she finds that for $x > 10^4$ the ansatz is accurate with $c_0 \simeq 0.06, c_1 \simeq -0.89$ and $c_2 \simeq 4.96$. It would be interesting to extend these computations and also to extend Hooley's heuristics to see if they lead to the ansatz.

The difficulty with (76) lies in the delicate issue of the relative density of $\mathcal{D}_R^-$ in $\mathcal{D}_R$. See the discussions in [**Lag80**] and [**Mor90**] concerning the solvability of (9). In [**R3́6**], the two-component of $\mathcal{F}_d$ is studied and used to get lower bounds of the form: Fix t a large integer, then

$$\sum_{\substack{d\,\in\mathcal{D}_R^+\\ d\,\le\,x}} 1 \ \text{ and } \sum_{\substack{d\,\in\,\mathcal{D}_R^-\\ d\,\le\,x}} 1 \gg_t \frac{x(\log\log x)^t}{\log x}\,. \tag{81}$$

On the other hand each of these is bounded above by $\sum_{\substack{d\,\in\mathcal{D}_R\\ d\,\le\,x}} 1$, which by Landau's thesis or the half-dimensional sieve is asymptotic to $c_3\, x\big/\sqrt{\log x}$. (81) leads to a corresponding lower bound for $\psi_G(x)$. The result [**R3́6**] leading to (81) suggests strongly that the proportion of $d \in \mathcal{D}_R$ which lie in $\mathcal{D}_R^-$ is in $\left(\frac{1}{2}, 1\right)$ (In [**Ste93**] a conjecture for the exact proportion is put forth together with some sound reasoning). It seems therefore quite likely that

$$\frac{\psi_G(x)}{\psi_{\langle \phi_R\rangle}(x)} \longrightarrow c_4 \quad \text{as} \quad x \longrightarrow \infty\,, \quad \text{with} \quad \frac{1}{2} < c_4 < 1\,. \tag{82}$$

It follows from (78) and (79) that it is still the case that zero percent of the classes in Π are reciprocal when ordered by discriminant, though this probability goes to zero much slower than when ordering by trace. On the other hand, according to (82) a positive proportion, even perhaps more than 1/2, of the reciprocal classes are ambiguous in this ordering, unlike when ordering by trace.

We end with some comments about the question of the equidistribution of closed geodesics as well as some comments about higher dimensions. To each primitive closed $p \in \Pi$ we associate the measure μ_p on $X = \Gamma\backslash\mathbb{H}$ (or better still, the corresponding measure on the unit tangent bundle $\Gamma\backslash SL(2,\mathbb{R})$) which is arc length supported on the closed geodesic. For a positive finite measure μ let $\bar{\mu}$ denote the corresponding normalized probability measure. For many p's (almost all of them in the sense of density, when ordered by length) $\bar{\mu}_p$ becomes equidistributed with respect to $\overline{dA} = \frac{3}{\pi}\,\frac{dxdy}{y^2}$ as $\ell(p) \to \infty$. However, there are at the same time many closed geodesics which don't equidistribute w.r.t. $\overline{dA}$ as their length goes to infinity. The Markov geodesics $(41'')$ are supported in $\mathcal{G}_{3/2}$ and so cannot equidistribute with respect to $\overline{dA}$. Another example of singularly distributed closed geodesics is that of the principal class 1_d ($\in \Pi$), for $d \in \mathcal{D}$ of the form $m^2 - 4$, $m \in \mathbb{Z}$. In this case $\epsilon_d = (m + \sqrt{d})/2$ and it is easily seen that $\bar{\mu}_{1_d} \to 0$ as $d \to \infty$ (that is, all the mass of the measure corresponding to the principal class escapes in the cusp of X).

On renormalizing one finds that for K and L compact geodesic balls in X,

$$\lim_{d\to\infty} \frac{\mu_{1_d}(L)}{\mu_{1_d}(K)} \to \frac{\mathsf{Length}(g \cap L)}{\mathsf{Length}(g \cap K)},$$

where g is the infinite geodesics from i to $i\infty$.

Equidistribution is often restored when one averages over naturally defined sets of geodesics. If S is a finite set of (primitive) closed geodesics, set

$$\bar{\mu}_S = \frac{1}{\ell(S)} \sum_{p \in S} \mu_p$$

where $\ell(S) = \sum_{p\in S} \ell(p)$.

We say that an infinite set S of closed geodesics is equidistributed with respect to μ when ordered by length (and similarly for ordering by discriminant) if $\bar{\mu}_{S_x} \to \mu$ as $x \to \infty$ where $S_x = \{p \in S : \ell(p) \leq x\}$. A fundamental theorem of Duke [**Duk88**] asserts that the measures $\mu_{\mathcal{F}_d}$ for $d \in \mathcal{D}$ become equidistributed with respect to $\overline{dA}$ as $d \to \infty$. From this, it follows that the measures

$$\sum_{\substack{t(p) = t \\ p\in\Pi}} \mu_p = \sum_{\substack{t_d = t \\ d\in\mathcal{D}}} \mu_{\mathcal{F}_d}$$

become equidistributed with respect to $\overline{dA}$ as $t \to \infty$. In particular the set Π of all primitive closed geodesics as well as the set of all inert closed geodesics become equidistributed as the length goes to infinity. However, the set of ambiguous geodesics as well as the G-fixed closed geodesics don't become equidistributed in $\Gamma\backslash PSL(2,\mathbb{R})$ as their length go to infinity. The extra logs in the asymptotics (63) and (70) are responsible for this singular behaviour. Specifically, in both cases a fixed positive proportion of their mass escapes in the cusp. One can see this in the ambiguous case by considering the closed geodesics corresponding to $[a, 0, -c]$ with $4ac = t^2 - 4$ and $t \leq T$. Fix $y_0 > 1$ then such a closed geodesic with $\sqrt{c/a} \geq y_0$ spends at least $\log\,(\sqrt{c/a}/y_0)$ if its length in $\mathcal{G}_{y_0} = \{z \in \mathcal{G}; \Im(z) > y_0\}$. An elementary count of the number of such geodesics with $t \leq T$, yields a mass of at least $c_0 T(\log T)^3$ as $T \longrightarrow \infty$, with $c_0 > 0$ and independent of y_0. This is a positive proportion of the total mass $\sum_{\substack{t(\{\gamma\}) \leq T \\ \gamma\in\pi_{\langle\phi_A\rangle}}} \ell(\{\gamma\})$, and, since it is independent of y_0, the claim follows. The argument for the case of G-fixed geodesics is similar.

We expect that the reciprocal geodesics are equidistributed with respect to dg in $\Gamma\backslash PSL(2,\mathbb{R})$, when ordered by length. One can show that there is $c_1 > 0$ such that for any compact set $\Omega \subset \Gamma\ PSL(2,\mathbb{R})$

$$\liminf_{x\longrightarrow\infty} \overline{\mu}_{\rho_x}(\Omega) \geq c_1 \mathrm{Vol}(\Omega)\,. \tag{83}$$

This establishes a substantial part of the expected equidistribution. To prove (83) consider the contribution from the reciprocal geodesics corresponding to $[a, b, -a]$ with $4a^2 + b^2 = t^2 - 4$, $t \leq T$. Each such geodesic has length $2\log((t+\sqrt{t^2-4})/2)$. The equidistribution in question may be rephrased in terms of the Γ action on the space of geodesics as follows. Let V be the one-sheeted hyperboloid $\{(\alpha, \beta, \gamma) : \beta^2 - 4\alpha\gamma = 1\}$. Then $\rho(PSL(2,\mathbb{R}))$ acts on the right on V by the symmetric square representation and it preserves a Haar measure dv on V. For $\xi \in V$ let Γ_ξ be the stabilizer in Γ of ξ. If the orbit $\{\xi\rho(\gamma) : \gamma \in \Gamma_\xi\backslash\Gamma\}$ is discrete in V then $\sum_{\gamma\in\Gamma_\xi\backslash\Gamma} \delta_{\xi\rho(\gamma)}$ defines a locally finite $\rho(\Gamma)$-invariant measure on V. The equidistribution question is that of showing that ν_T becomes equidistributed with respect to dv, locally in V, where

$$\nu_T := \sum_{4<t\leq T} \sum_{4a^2+b^2=t^2-4} \sum_{\gamma\in\Gamma_{\xi(a,b)}\backslash\Gamma} \delta_{\xi(a,b)\,\rho(\gamma)} \tag{84}$$

and $\xi(a,b) = \left(\frac{a}{\sqrt{t^2-4}}\,,\ \frac{b}{\sqrt{t^2-4}}\,,\ \frac{-a}{\sqrt{t^2-4}}\right)$.

Let Ω be a nice compact subset of V (say a ball) and fix $\gamma\in\Gamma$, then using the spectral method [**DRS93**] for counting integral points in regions on the two-sheeted hyperboloid $4a^2+b^2-t^2=-4$ one can show that

$$\sum_{4<t\leq T} \sum_{\substack{4a^2+b^2=t^2-4 \\ \gamma\notin i\,\Gamma_{\xi(a,b)}}} \delta_{\xi(a,b)\,\rho(\gamma)}\,(\Omega) \;=\; c(\gamma,\Omega)T \;+\; 0\left(T^{1-\delta}\parallel\gamma\parallel^A\right) \tag{85}$$

where $\delta>0$ and $A<\infty$ are fixed, $c(\gamma,\Omega)\geq 0$ and $\parallel\gamma\parallel=\sqrt{\mathrm{tr}(\gamma'\gamma)}$. The c's satisfy

$$\sum_{\|\gamma\|\leq\xi} c(\gamma,\Omega) \gg \mathrm{Vol}(\Omega)\log\xi \quad \text{as } \xi\longrightarrow\infty\,. \tag{86}$$

Hence, summing (85) over γ with $\parallel\gamma\parallel\leq T^{\epsilon_0}$ for $\epsilon_0>0$ small enough but fixed, we get that

$$\nu_T(\Omega) \gg \mathrm{Vol}(\Omega)\,T\log T\,. \tag{87}$$

On the other hand for any compact $B\subset V$, $\nu_T(B) = O(T\log T)$ and hence (83) follows.

In this connection we mention the recent work [**ELMV**] in which they revisit Linnik's methods and give a proof along those lines of Duke's theorem mentioned on the previous page. They show further that for a subset of $\mathcal{F}_d$ of size d^{ϵ_0} with $\epsilon_0>0$ and fixed, any probability measure which is a weak-star limit of the measures associated with such closed geodesics has positive entropy.

The distribution of these sets of geodesics is somewhat different when we order them by discriminant. Indeed, at least conjecturally they should be equidistributed with respect to $d\bar{A}$. We assume the following normal order conjecture for $h(d)$ which is predicted by various heuristics [**Sar85**], [**Hoo84**]; For $\alpha>0$ there is $\epsilon>0$ such that

$$\#\{d\in\mathcal{D} :\, d\leq x \text{ and } h(d)\geq d^\alpha\} = O\left(x^{1-\epsilon}\right)\,. \tag{88}$$

According to the recent results of [**Pop**] and [**HM**], if $h(d)\leq d^{\alpha_0}$ with $\alpha_0 = 1/5297$ then *every* closed geodesic of discriminant d becomes equidistributed with respect to $d\bar{A}$ as $d\longrightarrow\infty$. From this and Conjecture (88) it follows that each of our sets of closed geodesics, including the set of principal ones, becomes equidistributed with respect to $d\bar{A}$, when ordered by discriminant.

An interesting question is whether the set of Markov geodesics is equidistributed with respect to some measure ν when ordered by length (or equivalently by discriminant). The support of such a ν would be one-dimensional (Hausdorff). One can also ask about arithmetic equidistribution (e.g. congruences) for Markov forms and triples.

The dihedral subgroups of $PSL(2,\mathbb{Z})$ are the maximal elementary noncyclic subgroups of this group (an elementary subgroup is one whose limit set in $\mathbb{R} \cup \{\infty\}$ consists of at most 2 points). In this form one can examine the problem more generally. Consider for example the case of the Bianchi groups $\Gamma_d = PSL(2, O_d)$ where O_d is the ring of integers in $\mathbb{Q}(\sqrt{d})$, $d < 0$. In this case, besides the issue of the conjugacy classes of maximal elementary subgroups, one can investigate the conjugacy classes of the maximal Fuchsian subgroups (that is, subgroups whose limit sets are circles or lines in $\mathbb{C} \cup \{\infty\}$ = boundary of hyperbolic 3-space $\mathbb{H}^3$). Such classes correspond precisely to the primitive totally geodesic hyperbolic surfaces of finite area immersed in $\Gamma_d \backslash \mathbb{H}^3$. As in the case of $PSL(2,\mathbb{Z})$, these are parametrized by orbits of integral orthogonal groups acting on corresponding quadrics (see Maclachlan and Reid [**MR91**]). In this case one is dealing with an indefinite integral quadratic form f in four variables and their arithmetic is much more regular than that of ternary forms. The parametrization is given by orbits of the orthogonal group $O_f(\mathbb{Z})$ acting on $V_t = \{x : f(x) = t\}$ where the sign of t is such that the stabilizer of an $x (\in V_t(\mathbb{R}))$ in $O_f(\mathbb{R})$ is not compact. As is shown in [**MR91**] using Siegel's mass formula (or using suitable local to global principles for spin groups in four variables (see [**JM96**]) the number of such orbits is bounded independently of t (for $d = -1$, there are 1,2 or 3 orbits depending on congruences satisfied by t). The mass formula also gives a simple formula in terms of t for the areas of the corresponding hyperbolic surface. Using this, it is straight-forward to give an asymptotic count for the number of such totally geodesic surfaces of area at most x, as $x \to \infty$ (i.e., a "prime geodesic surface theorem"). It takes the form of this number being asymptotic to $c.x$ with c positive constant depending on Γ_d. Among these, those surfaces which are noncompact are fewer in number, being asymptotic to $c_1 x/\sqrt{\log x}$.

Another regularizing feature which comes with more variables is that each such immersed geodesic surface becomes equidistributed in the hyperbolic manifold $X_d = \Gamma_d \backslash \mathbb{H}^3$ with respect to $d\tilde{\mathrm{V}}\mathrm{ol}$, as its area goes to infinity. There are two ways to see this. The first is to use Maass' theta correspondence together with bounds towards the Ramanujan Conjectures for Maass forms on the upper half plane, coupled with the fact that there is basically only one orbit of $O_f(\mathbb{Z})$ on $V_t(\mathbb{Z})$ for each t (see the paper of Cohen [**Coh05**] for an analysis of a similar problem). The second method is to use Ratner's Theorem about equidistribution of unipotent orbits and that these geodesic hyperbolic surfaces are orbits of an $SO_{\mathbb{R}}(2,1)$ action in $\Gamma_d \backslash SL(2,\mathbb{C})$ (see the analysis in Eskin-Oh [**EO**]).

Acknowledgements

Thanks to Jim Davis for introducing me to these questions about reciprocal geodesics, to P. Doyle for pointing out some errors in my original letter and for the references to Fricke and Klein, to E. Ghys and Z. Rudnick for directing me to the references to reciprocal geodesics appearing in other contexts, to E. Lindenstrauss and A. Venkatesh for discussions about equidistribution of closed geodesics and especially the work of Linnik, and to W. Duke and Y. Tschinkel for suggesting that I prepare this material for this volume.

References

[Cas82] J. W. S. Cassels – "Rational quadratic forms", in *Proceedings of the International Mathematical Conference, Singapore 1981 (Singapore, 1981)* (Amsterdam), North-Holland Math. Stud., vol. 74, North-Holland, 1982, p. 9–26.

[CD] F. X. Connolly & J. F. Davis – "L-theory of $\mathrm{PSL}_2(\mathbb{Z})$ and connected sums of manifolds", in preparation.

[CF89] T. W. Cusick & M. E. Flahive – *The Markoff and Lagrange spectra*, Mathematical Surveys and Monographs, vol. 30, American Mathematical Society, Providence, RI, 1989.

[Coh05] P. B. Cohen – "Hyperbolic equidistribution problems on Siegel 3-folds and Hilbert modular varieties", *Duke Math. J.* **129** (2005), no. 1, p. 87–127.

[DFI94] W. Duke, J. B. Friedlander & H. Iwaniec – "Bounds for automorphic L-functions. II", *Invent. Math.* **115** (1994), no. 2, p. 219–239.

[DRS93] W. Duke, Z. Rudnick & P. Sarnak – "Density of integer points on affine homogeneous varieties", *Duke Math. J.* **71** (1993), no. 1, p. 143–179.

[Duk88] W. Duke – "Hyperbolic distribution problems and half-integral weight Maass forms", *Invent. Math.* **92** (1988), no. 1, p. 73–90.

[Efr93] I. Efrat – "Dynamics of the continued fraction map and the spectral theory of $\mathrm{SL}(2,\mathbb{Z})$", *Invent. Math.* **114** (1993), no. 1, p. 207–218.

[ELMV] M. Einsiedler, E. Lindenstrauss, P. Michel & A. Venkatesh – "Distribution properties of periodic torus orbits on homogeneous spaces", in preparation.

[EM93] A. Eskin & C. McMullen – "Mixing, counting, and equidistribution in Lie groups", *Duke Math. J.* **71** (1993), no. 1, p. 181–209.

[EO] A. Eskin & H. Oh – "Representations of integers by an invariant polynomial and unipotent flows", preprint.

[FK] R. Fricke & F. Klein – "Theorie der Elliptischen Modulfunktionen", Vol. I and II, *Leipzig*, 1890 and 1892.

[Gau] C. Gauss – "Disquisitiones Arithmeticae".

[GS80] E. Ghys & V. Sergiescu – "Stabilité et conjugaison différentiable pour certains feuilletages", *Topology* **19** (1980), no. 2, p. 179–197.

[Hej83] D. A. Hejhal – *The Selberg trace formula for* $\mathrm{PSL}(2,\mathbb{R})$*. Vol. 2*, Lecture Notes in Mathematics, vol. 1001, Springer-Verlag, Berlin, 1983.

[HM] G. Harcos & P. Michel – "The subconvexity problem for Rankin-Selberg L-functions and equidistribution of Heegner points", preprint (2005).

[Hoo84] C. Hooley – "On the Pellian equation and the class number of indefinite binary quadratic forms", *J. Reine Angew. Math.* **353** (1984), p. 98–131.

[Ing27] A. Ingham – "Some asymptotic formulae in the theory of numbers", *J. London Math. Soc.* **2** (1927), p. 202–208.

[Iwa95] H. Iwaniec – *Introduction to the spectral theory of automorphic forms*, Biblioteca de la Revista Matemática Iberoamericana, Revista Matemática Iberoamericana, Madrid, 1995.

[JM96] D. G. James & C. Maclachlan – "Fuchsian subgroups of Bianchi groups", *Trans. Amer. Math. Soc.* **348** (1996), no. 5, p. 1989–2002.

[Kwo] S. Kwon – "On the average of class numbers", Princeton University undergraduate thesis, (2006).

[Lag80] J. C. Lagarias – "On the computational complexity of determining the solvability or unsolvability of the equation $X^2 - DY^2 = -1$", *Trans. Amer. Math. Soc.* **260** (1980), no. 2, p. 485–508.

[Lan79] R. P. Langlands – "Stable conjugacy: definitions and lemmas", *Canad. J. Math.* **31** (1979), no. 4, p. 700–725.

[LS95] W. Z. Luo & P. Sarnak – "Quantum ergodicity of eigenfunctions on $\mathrm{PSL}_2(\mathbb{Z})\backslash\mathbf{H}^2$", *Inst. Hautes Études Sci. Publ. Math.* (1995), no. 81, p. 207–237.

[Mor90] P. Morton – "On the nonexistence of abelian conditions governing solvability of the -1 Pell equation", *J. Reine Angew. Math.* **405** (1990), p. 147–155.

[MR91] C. Maclachlan & A. W. Reid – "Parametrizing Fuchsian subgroups of the Bianchi groups", *Canad. J. Math.* **43** (1991), no. 1, p. 158–181.

[Pop] A. Popa – "Central values of Rankin L-series over real quadratic fields", preprint (2005).

[PR04] L. Polterovich & Z. Rudnick – "Stable mixing for cat maps and quasi-morphisms of the modular group", *Ergodic Theory Dynam. Systems* **24** (2004), no. 2, p. 609–619.

[R3́6] L. Rédei – "Über einige Mittelwertfragen im quadratischen Zahlkörper", *Jnl. Reine Angew Math.* **174** (1936), p. 15–55.

[Sar] P. Sarnak – "Prime Geodesic Theorems", thesis, (1980), Stanford.

[Sar85] P. C. Sarnak – "Class numbers of indefinite binary quadratic forms. II", *J. Number Theory* **21** (1985), no. 3, p. 333–346.

[Sie44] C. L. Siegel – "On the theory of indefinite quadratic forms", *Ann. of Math. (2)* **45** (1944), p. 577–622.

[Ste93] P. Stevenhagen – "The number of real quadratic fields having units of negative norm", *Experiment. Math.* **2** (1993), no. 2, p. 121–136.

[Ven82] A. B. Venkov – "Spectral theory of automorphic functions", *Proc. Steklov Inst. Math.* (1982), no. 4(153), p. ix+163 pp. (1983), A translation of Trudy Mat. Inst. Steklov. **153** (1981).

[Zag82] D. Zagier – "On the number of Markoff numbers below a given bound", *Math. Comp.* **39** (1982), no. 160, p. 709–723.

Department of Mathematics, Princeton University, Princeton NJ 08544-1000
E-mail address: sarnak@math.princeton.edu

Clay Mathematics Proceedings
Volume 7, 2007

The fourth moment of Dirichlet L-functions

K. Soundararajan

Abstract. Extending a result of Heath-Brown, we prove an asymptotic formula for the fourth moment of $L(\frac12,\chi)$ where χ ranges over the primitive Dirichlet characters $\pmod q$.

1. Introduction

In [**HB81**], D.R. Heath-Brown showed that

$$\sum_{\chi \pmod q}^{*} |L(\tfrac12,\chi)|^4 = \frac{\varphi^*(q)}{2\pi^2}\prod_{p|q}\frac{(1-p^{-1})^3}{(1+p^{-1})}(\log q)^4 + O(2^{\omega(q)}q(\log q)^3). \tag{1.1}$$

Here $\sum^*$ denotes summation over primitive characters $\chi \pmod q$, $\varphi^*(q)$ denotes the number of primitive characters $\pmod q$, and $\omega(q)$ denotes the number of distinct prime factors of q. Note that $\varphi^*(q)$ is a multiplicative function given by $\varphi^*(p) = p-2$ for primes p, and $\varphi^*(p^k) = p^k(1-1/p)^2$ for $k \ge 2$ (see Lemma 1 below). Also note that when $q \equiv 2 \pmod 4$ there are no primitive characters $\pmod q$, and so below we will assume that $q \not\equiv 2 \pmod 4$. For $q \not\equiv 2 \pmod 4$ it is useful to keep in mind that the main term in (1.1) is $\asymp q(\varphi(q)/q)^6(\log q)^4$.

Heath-Brown's result represents a q-analog of Ingham's fourth moment for $\zeta(s)$:

$$\int_0^T |\zeta(\tfrac12+it)|^4 dt \sim \frac{T}{2\pi^2}(\log T)^4.$$

When $\omega(q) \le (1/\log 2-\epsilon)\log\log q$ (which holds for almost all q) the error term in (1.1) is dominated by the main term and (1.1) gives the q-analog of Ingham's result. However if q is even a little more than 'ordinarily composite', with $\omega(q) \ge (\log\log q)/\log 2$, then the error term in (1.1) dominates the main term. In this note we remedy this, and obtain an asymptotic formula valid for all large q.

Theorem. *For all large q we have*

$$\sum_{\chi \pmod q}^{*} |L(\tfrac12,\chi)|^4 = \frac{\varphi^*(q)}{2\pi^2}\prod_{p|q}\frac{(1-p^{-1})^3}{(1+p^{-1})}(\log q)^4\Big(1+O\Big(\frac{\omega(q)}{\log q}\sqrt{\frac{q}{\varphi(q)}}\Big)\Big)+O(q(\log q)^{\frac72}).$$

2000 *Mathematics Subject Classification.* Primary 11M06.

The author is partially supported by the American Institute of Mathematics and the National Science Foundation.

Since $\omega(q) \ll \log q / \log\log q$, and $q/\varphi(q) \ll \log\log q$, we see that

$$(\omega(q)/\log q)\sqrt{q/\varphi(q)} \ll 1/\sqrt{\log\log q}.$$

Thus our Theorem gives a genuine asymptotic formula for all large q.

For any character $\chi \pmod q$ (not necessarily primitive) let $\mathfrak{a} = 0$ or 1 be given by $\chi(-1) = (-1)^{\mathfrak{a}}$. For $x > 0$ we define

$$W_{\mathfrak{a}}(x) = \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} \Big(\frac{\Gamma(\frac{s+\frac12+\mathfrak{a}}{2})}{\Gamma(\frac{\frac12+\mathfrak{a}}{2})}\Big)^2 x^{-s}\frac{ds}{s}, \tag{1.2}$$

for any positive c. By moving the line of integration to $c = -\frac12 + \epsilon$ we may see that

$$W(x) = 1 + O(x^{\frac12-\epsilon}), \tag{1.3a}$$

and from the definition (1.2) we also get that

$$W(x) = O_c(x^{-c}). \tag{1.3b}$$

We define

$$A(\chi) := \sum_{a,b=1}^{\infty} \frac{\chi(a)\overline{\chi}(b)}{\sqrt{ab}} W_{\mathfrak{a}}\Big(\frac{\pi ab}{q}\Big). \tag{1.4}$$

If χ is primitive then $|L(\frac12,\chi)|^2 = 2A(\chi)$ (see Lemma 2 below). Let $Z = q/2^{\omega(q)}$ and decompose $A(\chi)$ as $B(\chi) + C(\chi)$ where

$$B(\chi) = \sum_{\substack{a,b\ge 1\\ ab\le Z}} \frac{\chi(a)\overline{\chi}(b)}{\sqrt{ab}} W_{\mathfrak{a}}\Big(\frac{\pi ab}{q}\Big),$$

and

$$C(\chi) = \sum_{\substack{a,b\ge 1\\ ab> Z}} \frac{\chi(a)\overline{\chi}(b)}{\sqrt{ab}} W_{\mathfrak{a}}\Big(\frac{\pi ab}{q}\Big).$$

Our main theorem will follow from the following two Propositions.

Proposition 1. *We have*

$$\sideset{}{^*}\sum_{\chi \pmod q} |B(\chi)|^2 = \frac{\varphi^*(q)}{8\pi^2}\prod_{p|q}\frac{(1-1/p)^3}{(1+1/p)}(\log q)^4\Big(1 + O\Big(\frac{\omega(q)}{\log q}\Big)\Big).$$

Proposition 2. *We have*

$$\sum_{\chi \pmod q} |C(\chi)|^2 \ll q\Big(\frac{\varphi(q)}{q}\Big)^5(\omega(q)\log q)^2 + q(\log q)^3.$$

Proof of the Theorem. Since $|L(\frac12,\chi)|^2 = 2A(\chi) = 2(B(\chi)+C(\chi))$ for primitive characters χ we have

$$\sideset{}{^*}\sum_{\chi \pmod q} |L(\tfrac12,\chi)|^4 = 4\sideset{}{^*}\sum_{\chi \pmod q}\Big(|B(\chi)|^2 + 2B(\chi)C(\chi) + |C(\chi)|^2\Big).$$

The first and third terms on the right hand side are handled directly by Propositions 1 and 2. By Cauchy's inequality

$$\sideset{}{^*}\sum_{\chi \pmod q} |B(\chi)C(\chi)| \le \Big(\sideset{}{^*}\sum_{\chi \pmod q}|B(\chi)|^2\Big)^{\frac12}\Big(\sum_{\chi \pmod q}|C(\chi)|^2\Big)^{\frac12},$$

and thus Propositions 1 and 2 furnish an estimate for the second term also. Combining these results gives the Theorem. □

In [**HB79**], Heath-Brown refined Ingham's fourth moment for $\zeta(s)$, and obtained an asymptotic formula with a remainder term $O(T^{\frac{7}{8}+\epsilon})$. It remains a challenging open problem to obtain an asymptotic formula for $\sum^*_{\chi \pmod q} |L(\frac12,\chi)|^4$ where the error term is $O(q^{1-\delta})$ for some positive δ.

This note arose from a conversation with Roger Heath-Brown at the Gauss-Dirichlet conference where he reminded me of this problem. It is a pleasure to thank him for this and other stimulating discussions.

2. Lemmas

LEMMA 1. *If $(r,q)=1$ then*

$$\sum^*_{\chi \pmod q} \chi(r) = \sum_{k|(q,r-1)} \varphi(k)\mu(q/k).$$

PROOF. If we write $h_r(k)=\sum^*_{\chi \pmod k}\chi(r)$ then for $(r,q)=1$ we have

$$\sum_{k|q} h_r(k) = \sum_{\chi \pmod q} \chi(r) = \begin{cases} \varphi(q) & \text{if } q \mid r-1 \\ 0 & \text{otherwise.}\end{cases}$$

The Lemma now follows by Möbius inversion. □

Note that taking $r=1$ gives the formula for $\varphi^*(q)$ given in the introduction. If we restrict attention to characters of a given sign $\mathfrak{a}$ then we have, for $(mn,q)=1$,

(2.1)
$$\sum^*_{\substack{\chi \pmod q \\ \chi(-1)=(-1)^{\mathfrak{a}}}} \chi(m)\overline{\chi}(n) = \frac12 \sum_{k|(q,|m-n|)} \varphi(k)\mu(q/k) + \frac{(-1)^{\mathfrak{a}}}{2} \sum_{k|(q,m+n)} \varphi(k)\mu(q/k).$$

LEMMA 2. *If χ is a primitive character* $\pmod q$ *with $\chi(-1)=(-1)^{\mathfrak{a}}$ then*

$$|L(\tfrac12,\chi)|^2 = 2A(\chi),$$

where $A(\chi)$ is defined in (1.4).

PROOF. We recall the functional equation (see Chapter 9 of [**Dav00**])

$$\Lambda(\tfrac12+s,\chi) = \Big(\frac{q}{\pi}\Big)^{s/2}\Gamma\Big(\frac{s+\frac12+\mathfrak{a}}{2}\Big)L(\tfrac12+s,\chi) = \frac{\tau(\chi)}{i^{\mathfrak{a}}\sqrt{q}}\Lambda(\tfrac12-s,\overline{\chi}),$$

which yields

$$\Lambda(\tfrac12+s,\chi)\Lambda(\tfrac12+s,\overline{\chi}) = \Lambda(\tfrac12-s,\chi)\Lambda(\tfrac12-s,\overline{\chi}). \tag{2.2}$$

For $c>\frac12$ we consider

$$I := \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} \frac{\Lambda(\frac12+s,\chi)\Lambda(\frac12+s,\overline{\chi})}{\Gamma(\frac{\frac12+\mathfrak{a}}{2})^2}\frac{ds}{s}.$$

We move the line of integration to $\mathrm{Re}(s)=-c$, and use the functional equation (2.2). This readily gives that $I=|L(\frac12,\chi)|^2-I$, so that $|L(\frac12,\chi)|^2=2I$. On the other hand, expanding $L(\frac12+s,\chi)L(\frac12+s,\overline{\chi})$ into its Dirichlet series and integrating termwise, we get that $I=A(\chi)$. This proves the Lemma. □

We shall require the following bounds for divisor sums. If k and ℓ are positive integers with $\ell k \ll x^{\frac{5}{4}}$ then

$$\sum_{\substack{n \le x \\ (n,k)=1}} d(n)d(\ell k \pm n) \ll x(\log x)^2 \sum_{d|\ell} d^{-1}, \tag{2.3}$$

provided that $x \le \ell k$ if the negative sign holds. This is given in (17) of Heath-Brown [**HB81**]. Secondly, we record a result of P. Shiu [**Shi80**] which gives that

$$\sum_{\substack{n \le x \\ n \equiv r \pmod k}} d(n) \ll \frac{\varphi(k)}{k^2} x \log x, \tag{2.4}$$

where $(r,k)=1$ and $x \ge k^{1+\delta}$ for some fixed $\delta > 0$.

LEMMA 3. *Let k be a positive integer, and let Z_1 and Z_2 be real numbers ≥ 2. If $Z_1 Z_2 > k^{\frac{19}{10}}$ then*

$$\sum_{\substack{Z_1 \le ab < 2Z_1 \\ Z_2 \le cd < 2Z_2 \\ (abcd,k)=1 \\ ac \equiv \pm bd \pmod k \\ ac \ne bd}} 1 \ll \frac{Z_1 Z_2}{k} (\log(Z_1 Z_2))^3.$$

If $Z_1 Z_2 \le k^{\frac{19}{10}}$ the quantity estimated above is $\ll (Z_1 Z_2)^{1+\epsilon}/k$.

PROOF. By symmetry we may just focus on the terms with $ac > bd$. Write $n = bd$ and $ac = k\ell \pm bd$. Note that $k\ell \le 2ac$ and so $1 \le \ell \le 8Z_1Z_2/k$. Moreover since $ac \ge k\ell/2$ we have that $bd \le 4Z_1Z_2/(ac) \le 8Z_1Z_2/(k\ell)$. Thus the sum we desire to estimate is

$$\ll \sum_{1 \le \ell \le 8Z_1Z_2/k} \sum_{\substack{n \le 8Z_1Z_2/(k\ell) \\ n < k\ell \pm n \\ (n,k)=1}} d(n)d(k\ell \pm n). \tag{2.5}$$

Since $d(n)d(k\ell \pm n) \ll (Z_1Z_2)^\epsilon$ the second assertion of the Lemma follows.

Now suppose that $Z_1Z_2 > k^{\frac{19}{10}}$. We distinguish the cases $k\ell \le (Z_1Z_2)^{\frac{11}{20}}$ and $k\ell > (Z_1Z_2)^{\frac{11}{20}}$. In the first case we estimate the sum over n using (2.3). Thus such terms contribute to (2.5)

$$\ll \sum_{\ell \le (Z_1Z_2)^{\frac{11}{20}}/k} \frac{Z_1Z_2}{k\ell} (\log Z_1Z_2)^2 \sum_{d|\ell} d^{-1} \ll \frac{Z_1Z_2}{k} (\log Z_1Z_2)^3.$$

Now consider the second case. Here we sum over ℓ first. Writing $m = k\ell \pm n (= ac)$ we see that such terms contribute

$$\ll \sum_{n \le 8Z_1Z_2/k} d(n) \sum_{\substack{(Z_1Z_2)^{\frac{11}{20}}/2 \le m \le 4Z_1Z_2/n \\ m \equiv \pm n \pmod k}} d(m),$$

and by (2.4) (which applies as $(Z_1Z_2)^{\frac{11}{20}} > k^{\frac{209}{200}}$) this is

$$\ll \sum_{n \le 8Z_1Z_2/k} d(n) \frac{Z_1Z_2}{kn} \log Z_1Z_2 \ll \frac{Z_1Z_2}{k} (\log Z_1Z_2)^3.$$

The proof is complete. □

The next two Lemmas are standard; we have provided brief proofs for completeness.

LEMMA 4. *Let q be a positive integer and $x \geq 2$ be a real number. Then*

$$\sum_{\substack{n \leq x \\ (n,q)=1}} \frac{1}{n} = \frac{\varphi(q)}{q}\Big(\log x + \gamma + \sum_{p|q} \frac{\log p}{p-1}\Big) + O\Big(\frac{2^{\omega(q)} \log x}{x}\Big).$$

Further $\sum_{p|q} \log p/(p-1) \ll 1 + \log \omega(q)$.

PROOF. We have

$$\sum_{\substack{n \leq x \\ (n,q)=1}} \frac{1}{n} = \sum_{d|q} \mu(d) \sum_{\substack{n \leq x \\ d \mid n}} \frac{1}{n} = \sum_{\substack{d \mid q \\ d \leq x}} \frac{\mu(d)}{d}\Big(\log \frac{x}{d} + \gamma + O\Big(\frac{d}{x}\Big)\Big)$$

$$= \sum_{d|q} \frac{\mu(d)}{d}\Big(\log \frac{x}{d} + \gamma\Big) + O\Big(\frac{2^{\omega(q)} \log x}{x}\Big).$$

Since $-\sum_{d|q}(\mu(d)/d) \log d = \varphi(q)/q \sum_{p|q}(\log p)/(p-1)$ the first statement of the Lemma follows. Since $\sum_{p|q} \log p/(p-1)$ is largest when the primes dividing q are the first $\omega(q)$ primes, the second assertion of the Lemma holds. □

LEMMA 5. *We have*

$$\sum_{\substack{n \leq q \\ (n,q)=1}} \frac{2^{\omega(n)}}{n} \ll \Big(\frac{\varphi(q)}{q}\Big)^2 (\log q)^2.$$

For $x \geq \sqrt{q}$ we have

$$\sum_{\substack{n \leq x \\ (n,q)=1}} \frac{2^{\omega(n)}}{n}\Big(\log \frac{x}{n}\Big)^2 = \frac{(\log x)^4}{12\zeta(2)} \prod_{p|q}\Big(\frac{1-1/p}{1+1/p}\Big)\Big(1 + O\Big(\frac{1+\log \omega(q)}{\log q}\Big)\Big).$$

PROOF. Consider for $\mathrm{Re}(s) > 1$

$$F(s) = \sum_{\substack{n=1 \\ (n,q)=1}}^{\infty} \frac{2^{\omega(n)}}{n} = \frac{\zeta(s)^2}{\zeta(2s)} \prod_{p|q} \frac{1-p^{-s}}{1+p^{-s}}.$$

Since

$$\sum_{\substack{n \leq q \\ (n,q)=1}} \frac{2^{\omega(n)}}{n} \leq e \sum_{\substack{n=1 \\ (n,q)=1}}^{\infty} \frac{2^{\omega(n)}}{n^{1+1/\log q}} = eF(1 + 1/\log q),$$

the first statement of the Lemma follows. To prove the second statement we note that, for $c > 0$,

$$\sum_{\substack{n \leq x \\ (n,q)=1}} \frac{2^{\omega(n)}}{n}\Big(\log \frac{x}{n}\Big)^2 = \frac{2}{2\pi i} \int_{c-i\infty}^{c+i\infty} F(1+s) \frac{x^s}{s^3} ds.$$

We move the line of integration to $c = -\frac{1}{2} + \epsilon$ and obtain that the above is

$$2 \operatorname*{Res}_{s=0} \; F(1+s) \frac{x^s}{s^3} + O(x^{-\frac{1}{2}+\epsilon} q^{\epsilon}).$$

A simple residue calculation then gives the Lemma. □

3. Proof of Proposition 1

Applying (2.1) we easily obtain that

$$\sideset{}{^*}\sum_{\chi \pmod q} |B(\chi)|^2 = M + E,$$

where
(3.1)

$$M := \frac{\varphi^*(q)}{2} \sum_{\substack{a,b,c,d\ge 1\\ ab\le Z,\, cd\le Z\\ ac=bd\\ (abcd,q)=1}} \frac{1}{\sqrt{abcd}}\Big(W_0\Big(\frac{\pi ab}{q}\Big)W_0\Big(\frac{\pi cd}{q}\Big)+W_1\Big(\frac{\pi ab}{q}\Big)W_1\Big(\frac{\pi cd}{q}\Big)\Big)$$

and

$$E = \sum_{k|q} \varphi(k)\mu^2(q/k)E(k),$$

with

$$E(k) \ll \sum_{\substack{(abcd,q)=1\\ k\,|\,(ac\pm bd)\\ ac\neq bd\\ ab,\,cd\le Z}} \frac{1}{\sqrt{abcd}}.$$

To estimate $E(k)$ we divide the terms ab, $cd \le Z$ into dyadic blocks. Consider the block $Z_1 \le ab < 2Z_1$, and $Z_2 \le cd < 2Z_2$. By Lemma 3 the contribution of this block to $E(k)$ is, if $Z_1Z_2 > k^{\frac{19}{10}}$,

$$\ll \frac{1}{\sqrt{Z_1Z_2}}\frac{Z_1Z_2}{k}(\log Z_1Z_2)^3 \ll \frac{\sqrt{Z_1Z_2}}{k}(\log q)^3,$$

and is $\ll (Z_1Z_2)^{\frac12+\epsilon}/k$ if $Z_1Z_2 \le k^{\frac{19}{10}}$. Summing over all such dyadic blocks we obtain that $E(k) \ll (Z/k)(\log q)^3 + k^{-\frac{1}{20}+\epsilon}$, and so

$$E \ll Z2^{\omega(q)}(\log q)^3 \ll q(\log q)^3.$$

We now turn to the main term (3.1). If $ac = bd$ then we may write $a = gr$, $b = gs$, $c = hs$, $d = hr$, where r and s are coprime. We put $n = rs$, and note that given n there are $2^{\omega(n)}$ ways of writing it as rs with r and s coprime. Note also that $ab = g^2rs = g^2n$, and $cd = h^2rs = h^2n$. Thus the main term (3.1) may be written as

$$M = \frac{\varphi^*(q)}{2}\sum_{\mathfrak{a}=0,1}\sum_{\substack{n\le Z\\ (n,q)=1}}\frac{2^{\omega(n)}}{n}\Big(\sum_{\substack{g\le\sqrt{Z/n}\\ (g,q)=1}}\frac{1}{g}W_{\mathfrak{a}}\Big(\frac{\pi g^2n}{q}\Big)\Big)^2.$$

By (1.3a) we have that $W_{\mathfrak{a}}(\pi g^2n/Z) = 1 + O(\sqrt{g}n^{\frac14}/q^{\frac14})$, and using this above we see that

$$M = \varphi^*(q)\sum_{\substack{n\le Z\\ (n,q)=1}}\frac{2^{\omega(n)}}{n}\Big(\sum_{\substack{g\le\sqrt{Z/n}\\ (g,q)=1}}\frac{1}{g} + O(2^{-\omega(q)/4})\Big)^2.$$

We split the terms $n \le Z$ into the cases $n \le Z_0$ and $Z_0 < n \le Z$, where we set $Z_0 = Z/9^{\omega(q)} = q/18^{\omega(q)}$. In the first case, Lemma 4 gives that the sum over g is

$(\varphi(q)/q)\log\sqrt{Z/n}+O(1+\log\omega(q))$. Thus the contribution of such terms to M is

$$\begin{aligned}&\varphi^*(q)\sum_{\substack{n\le Z_0\\(n,q)=1}}\frac{2^{\omega(n)}}{n}\Big(\frac{\varphi(q)}{2q}\log\frac{Z}{n}+O(1+\log\omega(q))\Big)^2\\ =&\varphi^*(q)\Big(\frac{\varphi(q)}{2q}\Big)^2\sum_{\substack{n\le Z_0\\(n,q)=1}}\frac{2^{\omega(n)}}{n}\Big(\Big(\log\frac{Z_0}{n}\Big)^2+O(\omega(q)\log q)\Big).\end{aligned}$$

Using Lemma 5 we conclude that the terms $n\le Z_0$ contribute to M an amount

$$\frac{\varphi^*(q)}{8\pi^2}\prod_{p|q}\frac{(1-1/p)^3}{(1+1/p)}(\log q)^4\Big(1+O\Big(\frac{\omega(q)}{\log q}\Big)\Big). \tag{3.2}$$

In the second case when $Z_0\le n\le Z$, we extend the sum over g to all $g\le 3^{\omega(q)}$ that are coprime to q, and so by Lemma 4 the sum over g is $\ll\omega(q)\varphi(q)/q$. Thus these terms contribute to M an amount

$$\ll\varphi^*(q)\Big(\omega(q)\frac{\varphi(q)}{q}\Big)^2\sum_{Z_0\le n\le Z}\frac{2^{\omega(n)}}{n}\ll\varphi^*(q)\Big(\frac{\varphi(q)}{q}\Big)^2(\omega(q))^3\log q.$$

Since $q\omega(q)/\varphi(q)\ll\log q$, combining this with (3.2) we conclude that

$$M=\frac{\varphi^*(q)}{8\pi^2}\prod_{p|q}\frac{(1-1/p)^3}{(1+1/p)}(\log q)^4\Big(1+O\Big(\frac{\omega(q)}{\log q}\Big)\Big).$$

Together with our bound for E, this proves Proposition 1.

4. Proof of Proposition 2

The orthogonality relation for characters gives that

$$\begin{aligned}\sum_{\chi\pmod q}|C(\chi)|^2&\ll\varphi(q)\sum_{\substack{(abcd,q)=1\\ac\equiv\pm bd\pmod q\\ab,cd>Z}}\frac{1}{\sqrt{abcd}}\sum_{\mathfrak{a}=0,1}\Big|W_{\mathfrak{a}}\Big(\frac{\pi ab}{q}\Big)W_{\mathfrak{a}}\Big(\frac{\pi cd}{q}\Big)\Big|\\ &\ll\varphi(q)\sum_{\substack{(abcd,q)=1\\ac\equiv\pm bd\pmod q\\ab,cd>Z}}\frac{1}{\sqrt{abcd}}\Big(1+\frac{ab}{q}\Big)^{-2}\Big(1+\frac{cd}{q}\Big)^{-2},\end{aligned}$$

using (1.3a,b). We write the last expression above as R_1+R_2, where R_1 contains the terms with $ac=bd$, and R_2 contains the rest.

We first get an estimate for R_2. We break up the terms into dyadic blocks; a typical one counts $Z_1\le ab<2Z_1$ and $Z_2\le cd<2Z_2$ (both Z_1 and Z_2 being larger than Z). The contribution of such a dyadic block is, using Lemma 3 (note that $Z_1Z_2>Z^2>q^{\frac{19}{10}}$)

$$\ll\frac{\varphi(q)}{\sqrt{Z_1Z_2}}\Big(1+\frac{Z_1}{q}\Big)^{-2}\Big(1+\frac{Z_2}{q}\Big)^{-2}\frac{Z_1Z_2}{q}(\log Z_1Z_2)^3.$$

Summing this estimate over all the dyadic blocks we obtain that

$$R_2\ll q(\log q)^3.$$

We now turn to the terms $ac = bd$ counted in R_1. As in our treatment of M, we write $a = gr$, $b = gs$, $c = hs$, $d = hr$, with $(r, s) = 1$, and group terms according to $n = rs$. We see easily that

$$R_1 \ll \varphi(q) \sum_{(n,q)=1} \frac{2^{\omega(n)}}{n} \Big(\sum_{\substack{g > \sqrt{Z/n} \\ (g,q)=1}} \frac{1}{g} \Big(1 + \frac{g^2 n}{q}\Big)^{-2} \Big)^2. \tag{4.1}$$

First consider the terms $n > q$ in (4.1). Here the sum over g gives an amount $\ll q^2/n^2$ and so the contribution of these terms to (4.1) is

$$\ll \varphi(q) \sum_{n>q} \frac{2^{\omega(n)}}{n} \frac{q^4}{n^4} \ll \varphi(q) \log q.$$

For the terms $n < q$ the sum over g in (4.1) is easily seen to be

$$\ll 1 + \sum_{\substack{\sqrt{Z/n} \le g \le \sqrt{q/n} \\ (g,q)=1}} \frac{1}{g} \ll 1 + \frac{\varphi(q)}{q} \omega(q).$$

The last estimate follows from Lemma 4 when $n < Z/9^{\omega(q)}$, while if $n > Z/9^{\omega(q)}$ we extend the sum over g to all $g \le 6^{\omega(q)}$ with $(g, q) = 1$ and then use Lemma 4. Thus the contribution of terms $n < q$ to (4.1) is, using Lemma 5,

$$\ll \varphi(q) \Big(1 + \frac{\varphi(q)}{q} \omega(q)\Big)^2 \sum_{\substack{n \le q \\ (n,q)=1}} \frac{2^{\omega(n)}}{n} \ll q \log^2 q \Big(\frac{\varphi(q)}{q}\Big)^5 \omega(q)^2.$$

Combining these bounds with our estimate for R_2 we obtain Proposition 2.

References

[Dav00] H. Davenport – *Multiplicative number theory*, third ed., Graduate Texts in Mathematics, vol. 74, Springer-Verlag, New York, 2000, Revised and with a preface by Hugh L. Montgomery.

[HB79] D. R. Heath-Brown – "The fourth power moment of the Riemann zeta function", *Proc. London Math. Soc. (3)* **38** (1979), no. 3, p. 385–422.

[HB81] ———, "The fourth power mean of Dirichlet's L-functions", *Analysis* **1** (1981), no. 1, p. 25–32.

[Shi80] P. Shiu – "A Brun-Titchmarsh theorem for multiplicative functions", *J. Reine Angew. Math.* **313** (1980), p. 161–170.

Department of Mathematics, University of Michigan, Ann Arbor, MI 48109, USA
E-mail address: ksound@math.stanford.edu, ksound@umich.edu
Current address: Department of Mathematics, Stanford University, 450 Serra Mall, Bldg. 380, Stanford, CA 94305-2125, USA

Clay Mathematics Proceedings
Volume 7, 2007

The Gauss Class-Number Problems

H. M. Stark

1. Gauss

In Articles 303 and 304 of his 1801 Disquisitiones Arithmeticae [**Gau86**], Gauss put forward several conjectures that continue to occupy us to this day. Gauss stated his conjectures in the language of binary quadratic forms (of even discriminant only, a complication that was later dispensed with). Since Dedekind's time, these conjectures have been phrased in the language of quadratic fields. This is how we will state the conjectures here, but we make some comments regarding the original versions also. Throughout this paper, $k = \mathbb{Q}(\sqrt{d})$ will be a quadratic field of discriminant d and $h(k)$ or sometimes $h(d)$ will be the class-number of k.

In Article 303, Gauss conjectures that as k runs through the complex quadratic fields (i.e., $d < 0$), $h(k) \to \infty$. He also surmises that for low class-numbers, his tables contain the complete list of fields with those class-numbers including all the one class per genus fields. This innocent addendum caused much heartache when in 1934 Heilbronn [**Hei34**] finally proved that $k(d) \to \infty$ as $d \to -\infty$ ineffectively. Thus it remained at that time impossible to even give an algorithm that would provably terminate at a predetermined time with a complete list of the complex quadratic fields of class-number one (or any other fixed class-number). By the "class-number n problem for complex quadratic fields", we mean the problem of presenting a complete list of all complex quadratic fields with class-number n. We will discuss complex quadratic fields and generalizations in Sections 3 – 5.

For real quadratic fields (i. e., $d > 0$), Gauss surmises in Article 304 that there are infinitely many one class per genus real quadratic fields. By carrying over this surmise to prime discriminants, we get the common interpretation that Gauss conjectures there are infinitely many real quadratic fields with class-number one. We call this the "class-number one problem for real quadratic fields". This is completely unproved and, to this day, it is not even known if there are infinitely many number fields (degree arbitrary) with class-number one (or even just bounded).

We will discuss two approaches each to the one class per genus problem for complex quadratic fields and the class-number one problem for real quadratic fields. Admittedly, I don't have much hope currently for the first approaches to each problem but I think the questions raised are interesting. On the other hand, I

2000 *Mathematics Subject Classification.* Primary 11R29, 11R11, Secondary 11M20.

think the second approaches to each problem will ultimately work. We discuss all these in Sections 4 – 6 below.

It is particularly appropriate that this paper appear in these proceedings. From Gauss and Dirichlet at the start to Landau, Siegel and Deuring, people connected with Göttingen have made major contributions to the questions discussed here.

2. Dirichlet

Dirichlet introduced L-functions in order to study the distribution of primes in progressions. A key fact in this study is that for every character $\chi \pmod f$, $L(1,\chi) \neq 0$. Dirichlet knew that

$$\prod_{\chi} L(s,\chi) = \sum_{n=1}^{\infty} a_n n^{-s} \,,$$

where the product is over all characters $\chi \pmod f$ and the a_n are non-negative integers with $a_1 = 1$. Thus for real $s > 1$ where everything converges, we must have

$$\prod_{\chi(\bmod f)} L(s,\chi) \geq 1 \,. \tag{2.1}$$

We now know that $L(s,\chi)$ has a first order pole at $s = 1$ when χ is the trivial character and is analytic at $s = 1$ for other characters. It follows from (2.1) that at most one of the $L(1,\chi)$ can be zero and that such a χ must be real since otherwise χ and $\bar{\chi}$ would both contribute zeros to the product and the product would be zero at $s = 1$. Echos of this difficulty that there could be an exceptional real χ still persist today in the study of zeros near $s = 1$.

Of necessity, Dirichlet developed his class-number formula in order to finish his theorem on primes in progressions. Although Kronecker symbols were still in the future, Dirichlet discovered that every primitive real character corresponds to a quadratic field (and conversely; the beginnings of class field theory!). We write χ_d to be the primitive real character which corresponds to $\mathbb{Q}(\sqrt{d})$. The part of the class-number formula which concerns us here gives a non-zero algebraic interpretation of $L(1,\chi_d)$. Dirichlet showed that

$$L(1,\chi_d) = \begin{cases} \dfrac{2\pi h(d)}{w_d\sqrt{|d|}} & \text{when } d < 0 \\[2ex] \dfrac{2h(d)\log(\varepsilon_d)}{\sqrt{d}} & \text{when } d > 0 \,. \end{cases}$$

Here when $d < 0$, $w_{-3} = 6$, $w_{-4} = 4$, $w_d = 2$ for $d < -4$, and when $d > 0$, ε_d is the fundamental unit of $\mathbb{Q}(\sqrt{d})$.

Landau [**Lan18b**] states that Remak made the remark that even without the class-number formula, from (2.1) we are able to see that with varying moduli there can be at most one primitive real character χ with $L(1,\chi) = 0$ and thus the primes in progressions theorem would hold outside of multiples of this one extraordinary modulus. To see this, we apply (2.1) with f the product of the conductors of the two characters χ of interest.

In truth, (2.1) also holds when the product over χ is restricted to χ running over all characters $(\bmod\ f)$ which are identically 1 on a given subgroup of $(\mathbb{Z}/f\mathbb{Z})^*$. This is equivalent to χ running over a subgroup of the group of all characters $(\mathrm{mod}\, f)$. This product too is the zeta function of an abelian extension of $\mathbb{Q}$, but the proof that (2.1) holds does not require such knowledge. In 1918, Landau already makes use of the product in (2.1) over just four characters: the trivial character, the two interesting real characters, and their product. The product of the four L-functions is just the zeta function of the biquadratic field containing the two interesting quadratic fields.

Landau also proves that if for some constant $c > 0$, $L(s, \chi_d) \neq 0$ for real s in the range $1 - \frac{c}{\log(|d|)} < s < 1$, then

$$L(1, \chi_d) \gg \frac{1}{\log(|d|)} \quad \text{as } |d| \to \infty \ .$$

In particular, the Gauss conjectures for complex quadratic fields become consequences of the Generalized Riemann Hypothesis.

When one looks at the two 1918 Landau papers [**Lan18b**], [**Lan18a**], one is struck by how amazingly close Landau is to Siegel's 1935 theorem [**Sie35**]. All the ingredients are in the Landau papers!

3. Complex Quadratic Fields

The original Gauss class-number one conjecture is restricted to even discriminants and is much easier. For even discriminants, 2 ramifies and yet for $d > -8$, absolute value estimates show there is no integer in k with norm 2. Thus the only even class-number one discriminants are -4 and -8. Gauss also allowed non-fundamental discriminants. These correspond to ring classes and it now becomes a homework exercise to show that the non-fundamental class-number one discriminants (even or odd) are -12, -16, -27, -28.

In 1934 Heilbronn [**Hei34**] proved the Gauss Conjecture that $k(d) \to \infty$ as $d \to -\infty$. Then also in 1934, Heilbronn and Linfoot [**HL34**] proved that besides the nine known complex quadratic fields of class-number one, there is at most one more. Heilbronn's proof followed a remarkable 1933 theorem of Deuring [**Deu33**] who proved that if there were infinitely many class-number one complex quadratic fields, then the Riemann hypothesis for $\zeta(s)$ would follow! Many authors promptly carried this over to other class-numbers. But Heilbronn realized that Deuring's method would allow one to prove the generalized Riemann hypothesis for any $L(s, \chi)$ as well and this, together with Landau's earlier result above, implies Gauss's conjecture for complex quadratic fields.

These theorems are purely analytic in the sense that there is no use made of any algebraic interpretations of any special values of any relevant functions. These theorems are also noteworthy in that they are ineffective. Three decades later, the class-number one problem was solved by Baker [**Bak66**] and Stark [**Sta67**] completely. There was also the earlier discounted method of Heegner [**Hee52**] from 1952 which at the very least could be turned into a completely valid proof of the same result. It is frequently stated that my proof and Heegner's proof are the same. The two papers end up with the same Diophantine equations, but I invite anybody to read both papers and then say they give the same proof!

As an aside, I believe that I was the modern rediscoverer of Heegner's paper, having come across it in 1963 while working on my PhD thesis. Fortunately for me, if not for mathematics, it was reaffirmed at a 1963 conference in Boulder, which

I did not attend, that Heegner was incorrect and as a result I graduated in 1964 with degree in hand. Back then, it was commonly stated that the problem with Heegner's proof was that it relied on the unproved conjecture of Weber that for $d \equiv -3 \pmod 8$ and $3 \nmid d$, the classical modular function $f(z)$ evaluated at $z = \sqrt{d}$ is an algebraic integer lying in the ring class field of $k \pmod 2$. The assertion that Heegner relied upon this conjecture in his class-number one proof turned out to be absolutely false (although he did make use of Weber's conjecture in other unrelated portions of his paper) and I believe the first outline since Heegner's paper of what is actually involved in Heegner's class-number one proof occurs in my 1967 paper [**Sta67**]. In addition to Heegner [**Hee52**] and Stark [**Sta67**]. I refer the reader to Birch [**Bir69**], Deuring [**Deu68**], and Stark [**Sta69a**], [**Sta69b**]. In particular, Birch also proves Weber's conjecture. I don't think this is the place to go further into this episode.

The Gauss class-number problem for complex quadratic fields has been generalized to CM-fields (totally complex quadratic extensions of totally real fields). Since the mid 1970's we now expect that there are only finitely many CM fields with a given class-number. This has been proved effectively for normal CM fields and conditionally under each of various additional conjectures including the Generalized Riemann Hypothesis (GRH) for number field zeta functions, Artin's conjecture on L-functions being entire, and more recently under the Modified Generalized Riemann Hypothesis (MGRH) which allows real exceptions to GRH. In particular, this latter result allows Siegel zeroes to exist and would still result in effectively sending the class-number $h(K)$ of a CM field K to ∞ as K varies! It also turns out that at least some of the implied complex exceptions to GRH that hamper an attempted proof without MGRH are very near to $s = 1$. All this was prepared for a history lecture at IAS in the Fall of 1999; this part of the lecture was delivered in the Spring of 2000. It is still unpublished, but will appear someday [**Sta**].

4. Zeros of Epstein zeta functions

From the point of view of this exposition, none of the proofs of Heegner, Baker or Stark qualify as a purely analytic proof. Harder to classify is the Goldfeld [**Gol76**], Gross-Zagier [**GZ86**] combinded effective proof of the Gauss conjecture that $h(d) \to \infty$ as $d \to -\infty$. Goldfeld showed that the existence of an explicit L-function of an elliptic curve with a triple zero at $s = 1$ would imply Gauss's conjecture and Gross-Zagier prove the existence of such an L-function by giving a meaning to the first derivative at $s = 1$ of the L-function of a CM curve. For the sake of argument, I will say that this result also is not purely analytic although there remains the chance that it could be made so.

I believe that it is highly desirable that a purely analytic proof of the class-number one result be found. This is because such a proof would have a chance of extending to other fixed class-numbers and, if we were really lucky, might even begin to effectively approach the strength of Siegel's theorem. In particular, we might at long last pick up the one class per genus complex quadratic fields.

There are two potential purely analytic approaches to the class-number one problem. Both originated from the study of Epstein zeta functions. Let

$$Q(x, y) = ax^2 + bxy + cy^2 \ ,$$

be a positive definite binary quadratic form with discriminant $d = b^2 - 4ac < 0$. We define the Epstein zeta functions

$$\zeta(s, Q) = (1/2) \sum_{m,n \neq 0,0} Q(m,n)^{-s} \ .$$

This series converges absolutely for $\sigma > 1$ and has an analytic continuation to the entire complex s-plane with a first order pole at $s = 1$ whose residue depends only on d and not on a, b, c. I will begin with a well known "folk theorem".

THEOREM 4.1. (Folk Theorem.) *Let $c > 1/4$ be a real number and set*

$$Q(x, y) = x^2 + xy + cy^2 \ ,$$

with discriminant $d = 1-4c < 0$. Then for $c > 41$, $\zeta(s, Q)$ has a zero s with $\sigma > 1$.

REMARK 4.2. This implies that for $d < -163$, $h(d) > 1$!

FOLK PROOF. Davenport and Heilbronn [**DH36**] prove the cases where c is transcendental and where c is rational, the exception being any integral d with $h(d) = 1$. But we now know that there are no class-number one fields past -163 (hence the 41), and so this covers the case of rational c. Finally, Cassels [**Cas61**] proved the case where c is an irrational algebraic number. □

There are three problems here. First, the only "proof" of this theorem uses the class-number one determination as part of the proof, thereby rendering it useless as an analytic proof of the class-number one theorem. A second difficulty is that Davenport and Heilbronn only prove the transcendental case for Hurwitz zeta functions, but their proof carries over, with slight complications. They also deal with integral quadratic forms, which would not be a problem except that they restrict themselves to fundamental discriminants. In principle, their method should go through, with more serious complications this time, for non-fundamental discriminants so long as class-number one non-fundamental discriminants are avoided (the last such is -28). The third difficulty is that this folk theorem has not actually been proved because Cassels did not prove the algebraic case! Cassels did prove the algebraic case of a similar theorem for Hurwitz zeta functions, but no one has managed to carry over his proof to Epstein zeta functions. So the challenge is clear: prove the folk theorem, but better still, FIND A PURELY ANALYTIC PROOF OF THE FOLK THEOREM. As a warmup problem, but one which I still have no idea how to prove, let alone purely analytically, one could deal with

$$Q(x, y) = x^2 + cy^2 \quad \text{with} \quad c > 7 \ .$$

Once such a theorem is proved, the next step would be to generalize it to the sum of h Epstein zeta functions of the same discriminant, but with real coefficients. At the moment, I don't even have any approach to the case of the one Epstein zeta function of the folk theorem. In particular, an attempt to track a particular zero of $\zeta(s, Q)$ as c grows seems likely to end on the line $\sigma = 1/2$ and stay there.

5. Zero Spacing of Zeta Functions of Complex Quadratic Fields

The other purely analytic approach seems to me to be more hopeful. In his 1933 and 1935 papers, Deuring [**Deu33**], [**Deu35**], found a very useful expansion of an Epstein zeta function with

$$Q(x, y) = ax^2 + bxy + cy^2, \ d = b^2 - 4ac < 0$$

in the case that $|d|/a^2$ is large. We can easily see where the two main terms come from. We have

$$\zeta(s,Q) = \sum_{m=1}^{\infty}(am^2)^{-s} + \sum_{n=1}^{\infty}\sum_{m}(am^2+bmn+cn^2)^{-s} \ . \tag{5.1}$$

We approximate the inner sum on the right by the integral,

$$\int_{-\infty}^{\infty}(at^2+bnt+cn^2)^{-s}dt = a^{-s}\left(\frac{\sqrt{|d|}}{2a}n\right)^{1-2s}\int_{-\infty}^{\infty}(u^2+1)^{-s}du \ .$$

The integral on the right evaluates to

$$\int_{-\infty}^{\infty}(u^2+1)^{-s}du = \frac{\sqrt{\pi}\Gamma(s-1/2)}{\Gamma(s)} \ .$$

This gives the approximation,

$$\zeta(s,Q) = a^{-s}\zeta(2s) + a^{s-1}\left(\frac{\sqrt{|d|}}{2}\right)^{1-2s}\frac{\sqrt{\pi}\Gamma(s-1/2)}{\Gamma(s)}\zeta(2s-1) + R(s)$$

where $R(s)$ is the error made in approximating the sum by the integral. Equivalently, with

$$\xi(s) = \pi^{-s/2}\Gamma(\frac{s}{2})\zeta(s) \quad \text{and} \quad \tilde{R}(s) = \left(\frac{\sqrt{|d|}}{2\pi}\right)^{s}\Gamma(s)R(s) \ ,$$

we have

(5.2)

$$\begin{aligned}\left(\frac{\sqrt{|d|}}{2\pi}\right)^{s}\Gamma(s)\zeta(s,Q) &= \left(\frac{\sqrt{|d|}}{2}\right)^{s}\xi(2s)a^{-s} + \left(\frac{\sqrt{|d|}}{2}\right)^{1-s}\xi(2s-1)a^{s-1} + \tilde{R}(s) \\ &= \left(\frac{\sqrt{|d|}}{2}\right)^{s}\xi(2s)a^{-s} + \left(\frac{\sqrt{|d|}}{2}\right)^{1-s}\xi(2-2s)a^{s-1} + \tilde{R}(s) \,.\end{aligned}$$

The main terms interchange on the right when s is replaced by $1-s$. We are entitled to suspect that we have stumbled upon the functional equation for $\zeta(s,Q)$; this is indeed the truth and can be derived from this expansion if one uses the Poisson summation formula on the sum on m in (5.1). The Poisson summation formula leads to the same main terms and an expansion of $\tilde{R}(s)$ in K-Bessel functions in a form where $K_{s-1/2}$ appears and is invariant under $s \mapsto 1-s$. Deuring used the Euler MacLaurin summation formula to estimate $R(s)$. On $\sigma = 1/2$, the two main terms have the same absolute value and as t increases, the arguments of the two main terms spin in opposite directions in a manner which is practically linear over short ranges in t. Deuring realized in [**Deu35**] that this leads to the zeros of $\zeta(s,Q)$ lying practically in arithmetic progressions in t.

From Stirling's formula, when

$$s = \frac{1}{2} + it \ ,$$

we have

(5.3)
$$\arg\left[\left(\frac{\sqrt{|d|}}{2}\right)^s \xi(2s)\right] = \arg\left[\left(\frac{\sqrt{|d|}}{2\pi}\right)^s \Gamma(s)\zeta(2s)\right]$$
$$= t\log\left(\frac{\sqrt{|d|}}{2\pi}\right) + t\log(t) - t + \arg[\zeta(1+2it)] + O(\frac{1}{t}).$$

If t goes from t_0 to $t_0+\varepsilon$, where ε is suitably small, then to a first approximation, the right side grows by

$$\varepsilon\log\left(\frac{\sqrt{|d|}}{2\pi}t\right) + O(\varepsilon)\,.$$

In particular, the right side grows by π when ε is approximately

(5.4)
$$\frac{\pi}{\log(t\sqrt{|d|})}\quad .$$

For our particular Q, we find that the two main terms have the same absolute values on $\sigma = 1/2$ and the sum of the two main terms has zeros almost precisely in arithmetic progressions over short ranges of t. As a result, with $a = 1$, if one can estimate $\tilde{R}(1/2+it)$ as small enough, we find that $\zeta(s,Q)$ also has zeros almost precisely in arithmetic progressions over short ranges of t. The methods of Deuring allowed such estimates out to t about $\sqrt{|d|}$, but more recent work takes t out to high powers of $|d|$ and even further. The number in (5.4) is the average spacing of the zeros of $\zeta_k(s)$. One consequence is that if we can get t out to even small powers of $|d|$, we cannot have a class-number one field if $\zeta(1/2+it)$ has zeros significantly closer than the average spacing at this height. And if we can get t out to high powers of $|d|$, then we can't have a class-number one field if $\zeta(1/2+it)$ has zeros closer than 1/2 the average spacing.

For fields of higher class numbers,

$$\zeta_k(s) = \sum_Q \zeta(s,Q)$$

where the sum is over the reduced quadratic forms of discriminant d. We write each $Q(x,y)$ as

$$Q(x,y) = ax^2 + bxy + cy^2 \quad \text{with} \quad d = b^2 - 4ac < 0 \text{ and } a > 0$$

if $b \le a < (|d|/4)^{1/2}$, then Q is reduced; if $a > (|d|/3)^{1/2}$, then Q is not reduced. In the intermediate range $(|d|/4)^{1/2} \le a \le (|d|/3)^{1/2}$, Q may or may not be reduced, but Q is within one or two reduction steps of being reduced and the corresponding reduced form has an a of about the same size. Our expansion of $\zeta_k(s)$ then takes the shape,

(5.5)
$$\left(\frac{\sqrt{|d|}}{2\pi}\right)^s \Gamma(s)\zeta_k(s) = \left(\frac{\sqrt{|d|}}{2}\right)^s \xi(2s)\sum_Q a^{-s} + \left(\frac{\sqrt{|d|}}{2}\right)^{1-s} \xi(2-2s)\sum_Q a^{s-1}$$
$$+ \tilde{R}_k(s)\ .$$

The sum $\sum_{Q} a^{-s}$ is somewhat troublesome for class-numbers up towards $|d|^{1/2-\varepsilon}$, but for a one class per genus field, we can take

$$\prod_{p||d|}(1+p^{-s}) \tag{5.6}$$

as a very good approximation to $\sum_{Q} a^{-s}$. When the arguments all line up correctly, the product (5.6) can cause difficulties in deducing a zero spacing result, but this only happens rarely. On average, we still end up with the approximate arithmetic progressions and again, the higher we can do this the more we can hope that close zeros of $\zeta(s)$ will provide the desired contradiction.

With the expansion (5.2) and Rouché's theorem, Deuring [**Deu35**] proved that when $|d|/a^2$ is large, except for two real zeros, one near $s = 1$ and its reflection near $s = 0$, all zeros of a single $\zeta(s, Q)$ up to height roughly $(|d|/a^2)^{1/2}$ are simple and on the line $\sigma = 1/2$. I rediscovered this result complete with the application of Rouché's theorem, when working on my PhD thesis in 1963. I spent a fruitless year then trying to prove that $\zeta(s)$ has occasional close zeros, with no luck whatsoever before using the expansion (5.2) and numerical values of zeros of $\zeta(s)$ to push the hypothetical tenth class number one discriminant out to 10^{10^7}. Proving that $\zeta(s)$ has close zeros has been one of my favorite problems for 43 years and it would appear that everyone since has been fixated on this as well. However, it is not necessary to get close zeros. For instance, suppose that one could simply show that between T and $2T$ there are pairs of zeros of $\zeta(s)$ whose distance is within 1% of the average spacing for $\zeta(s)$. This would provide an analytic solution of the class-number one problem and likely lead to a solution of the one class per genus question also. One simply chooses a height t as a suitable power of d so that the average spacing of zeros of $\zeta(s)$ is not an integral multiple of the average spacing of zeros of $\zeta(s, Q)$. Other variations are possible as well. This certainly has to be explored.

6. Real Quadratic Fields

Here again, because he allows non-fundamental discriminants, the original Gauss version of his class-number one conjecture was proved long ago by using a carefully constructed family of orders in a fixed real quadratic field of class-number one [**Dic66**]!

I have already in the commentaries to Heilbronn's collected works sketched a beginning potential approach to getting small class-numbers of real quadratic fields by finding Euclidean rings of S-integers in quadratic fields. This was motivated by a suggestion of Heilbronn [**Hei51**] that a certain explicit family of quartic fields may contain infinitely many Euclidean fields. In truth I am dubious about the Euclidean S-integer approach getting more than infinitely many S-integer Euclidean rings with small $|S|$ (and at the moment, I don't see how to even approach that much either).

But there is another approach to class-number one real quadratic fields which I believe will eventually succeed. The Cohen-Lenstra heuristics [**CL84**] predict that the probability a_p of a real quadratic field having class number divisible by an odd prime p is

$$a_p = 1 - \prod_{j=2}^{\infty}(1 - p^{-j}) \ .$$

They then predict that for real quadratic fields k the probability of the odd part of the class group being the identity is

$$\prod_{p \geq 3}(1 - a_p) = .7544598... \tag{6.1}$$

In particular for prime discriminants where there is no two part of the class group, this should be the probability that the $h(k) = 1$ for prime discriminant fields.

Since the product in (6.1) is convergent, the sum of the a_p is convergent as well. This means that to estimate the number of fields with discriminant up to x such that the odd part of the class group is one, we can do inclusion-exclusion up to some point and then just exclude fields with $p|h(k)$ for primes past that point. The inclusion-exclusion part would complicate life since we would require lower bounds on densities of fields being put back in. However, the a_p are so small that

$$\sum_{p \geq 3} a_p = .265802... < 1 \ .$$

This suggests that it might be possible to take the total number of quadratic fields of prime discriminant up to x, say, and subtract the number of fields with class-number divisible by 3 up to x and then subtract the number of fields with class-number divisible by 5 up to $x, \ldots$, and still have a positive result at the end. What makes this interesting is that all we would need to make this work is an upper bound on the number of quadratic fields with class-number divisible by p. Since upper bound density estimates are often easier to come by than lower bounds, there is a chance this approach could succeed. If successful, we would not come up with the Cohen-Lenstra predicted density, but we would get a positive lower estimate of the density which at best would be .734197... Of course, one would need some sort of error term in an upper estimate of number of real quadratic fields of discriminant less than x whose class-numbers are divisible by p. And if we wanted, say, narrow class-number one rather than class-number a power of 2, we would have to restrict our quadratic field discriminants to being prime.

In turn, from class-field theory, we would like an estimate of the number of fields of degree p and certain types of Galois groups. Again, since a good upper bound is all that is needed, we could likely relax the conditions that the degree p fields have to satisfy for larger p. The closer we get to counting just the number of fields of degree p with prime power (for example, a prime to the $(p-1)/2$ power) discriminants, without worrying about what the Galois group is, the more possible it is that such an estimate could ultimately be derived.

References

[Bak66] A. Baker – “Linear forms in the logarithms of algebraic numbers”, *Mathematika* **13** (1966), p. 204–216.

[Bir69] B. J. Birch – “Weber's class invariants”, *Mathematika* **16** (1969), p. 283–294.

[Cas61] J. W. S. Cassels – “Footnote to a note of Davenport and Heilbronn”, *J. London Math. Soc.* **36** (1961), p. 177–184.

[CL84] H. Cohen & H. W. Lenstra, Jr. – "Heuristics on class groups of number fields", in *Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983)*, Lecture Notes in Math., vol. 1068, Springer, Berlin, 1984, p. 33–62.

[Deu33] M. Deuring – "Imaginäre quadratische Zahlkörper mit der Klassenzahl 1", *Math. Z.* **37** (1933), no. 1, p. 405–415.

[Deu35] M. Deuring – "Zeta Funktionen Quadratischer Formen", *J. Reine Angew. Math.* (1935), p. 226–252.

[Deu68] M. Deuring – "Imaginäre quadratische Zahlkörper mit der Klassenzahl Eins", *Invent. Math.* **5** (1968), p. 169–179.

[DH36] H. Davenport & H. Heilbronn – "On the zeros of certain Dirichlet series I, II", *J. London Math. Soc.* **11** (1936), p. 181–185 and 307–312.

[Dic66] L. E. Dickson – *History of the theory of numbers. Vol. III: Quadratic and higher forms.*, Chelsea Publishing Co., New York, 1966.

[Gau86] C. F. Gauss – *Disquisitiones arithmeticae*, Springer-Verlag, New York, 1986.

[Gol76] D. M. Goldfeld – "The class number of quadratic fields and the conjectures of Birch and Swinnerton-Dyer", *Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4)* **3** (1976), no. 4, p. 624–663.

[GZ86] B. H. Gross & D. B. Zagier – "Heegner points and derivatives of L-series", *Invent. Math.* **84** (1986), no. 2, p. 225–320.

[Hee52] K. Heegner – "Diophantische Analysis und Modulfunktionen", *Math. Z.* **56** (1952), p. 227–253.

[Hei34] H. Heilbronn – "On the class-number in imaginary quadratic fields", *Quart. J. Math. Oxford Ser.* **5** (1934), p. 150–160.

[Hei51] ———, "On Euclid's algorithm in cyclic fields", *Canad. J. Math.* **3** (1951), p. 257–268.

[HL34] H. Heilbronn & E. H. Linfoot – "On the imaginary quadratic corpora of class-number one", *Quart. J. Math. Oxford Ser.* **5** (1934), p. 293–301.

[Lan18a] E. Landau – "Über die Klassenzahl imaginärer quadratischer Zahlkörper", *Göttinger Nachrichten* (1918), p. 285–295.

[Lan18b] ———, "Über imaginäre quadratische Zahlkörper mit gleicher Klassenzahl", *Göttinger Nachrichten* (1918), p. 278–284.

[Sie35] C. L. Siegel – "Über die Klassenzahl quadratischer Zahlkörper", *Acta Arith.* **1** (1935), p. 83–86.

[Sta] H. M. Stark – "Class-numbers of CM-fields and Siegel zeros", to be published.

[Sta67] ———, "A complete determination of the complex quadratic fields of class-number one", *Michigan Math. J.* **14** (1967), p. 1–27.

[Sta69a] ———, "On the "gap" in a theorem of Heegner", *J. Number Theory* **1** (1969), p. 16–27.

[Sta69b] ———, "The role of modular functions in a class-number problem", *J. Number Theory* **1** (1969), p. 252–260.

Current address: Department of Mathematics - 0112 UCSD La Jolla, CA 92093
E-mail address: stark@math.ucsd.edu

Articles in this volume are based on talks given at the Gauss–Dirichlet Conference held in Göttingen on June 20–24, 2005. The conference commemorated the 150th anniversary of the death of C.-F. Gauss and the 200th anniversary of the birth of J.-L. Dirichlet.

The volume begins with a definitive summary of the life and work of Dirichlet and continues with thirteen papers by leading experts on research topics of current interest in number theory that were directly influenced by Gauss and Dirichlet. Among the topics are the distribution of primes (long arithmetic progressions of primes and small gaps between primes), class groups of binary quadratic forms, various aspects of the theory of L-functions, the theory of modular forms, and the study of rational and integral solutions to polynomial equations in several variables.

ISBN 978-0-8218-4307-9

9 780821 843079

CMIP/7

www.ams.org
www.claymath.org