Diss. ETH No. 12278

Cyclotomy of Rings & Primality Testing

A dissertation submitted to the
SWISS FEDERAL INSTITUTE OF TECHNOLOGY
ZURICH

for the degree of
Doctor of Mathematics

presented by
PREDA MIHĂILESCU
Dipl. Math. ETH
born May 23d, 1955
citizen of Zürich

accepted on the recommendation of
Prof. E. Engeler, examiner
Prof. M. Bronstein, co-examiner
Prof. H.W. Lenstra Jr., co-examiner

1998

To my grandfather Vintila I who once opened my eyes in wondering in the dark forests of the Carpathians. And to all friendly faces in this World, who helped along the way to keep the wondering going.

Chanson du professeur

Elle est à toi cette chanson
Toi l'professeur qui sans façon
As ouvert ma petite thèse
Quand mon espoir manquait de braise

Tous les gens bien intentionnés
Riaient de me voir travailler ...
ailluers!

Ce n'était rien qu'un clair regard,
Mais il m'avait chauffé le cœur
Et dans mon âme il brille encore
A la manière d'un grand soleil.

Toi l'professeur quand tu mourras
Quand le crocq'mort t'emportera
Qu'il te conduise à travers ciel
Au Père Éternel!

Georges Brassens (approximately)

Zusammenfassung

Die Kreisteilung über Ringe ist die Theorie der $s-$ten zyklotomischen Erweiterungen der Ringe $(\mathbb{Z}/s \cdot \mathbb{Z})$ mit positiv ganzzahligen n und s. Solche Erweiterungen existieren nicht für allen Paaren (n, s) und geben – falls sie *existieren* – wertvolle Auskunft über die möglichen Teilern von n. Die zyklotomischen Erweiterungen wurden von Lenstra eingeführt, um ein gemeinsames theoretisches Verständnis für die meisten bekannten Primheitsbeweismethoden zu geben; sie bilden die Grundlage aller aktuell bekannten Primheitsbeweisalgorithmen, mit Ausnahme der auf elliptischen Kurven basierenden. Kreisteilungsprimheitsbeweise wurden von H. W. Lenstra Jr. vorgeschlagen und von seinen Studenten W. Bosma and M. van der Hulst implementiert. Sie sind in der Praxis relativ effizient, asymptotisch aber nicht polynomial.

In dieser Thesis entwickeln wir eine vollständige Theorie der zyklotomischen Erweiterungen und Untererweiterungen von Ringen aus der Perspektive der Zerfällung des Kreisteilungspolynoms. Dieser Zugang zeigt neue, wichtige Kennwerte dieser Erweiterungen – wie z.B. den *Sättigungsindex* – auf und führt auch zu einigen praktischen Zusatzergebnissen.

1. Ein neuer Algorithmus zur Zerlegung des Kreiteilungspolynoms, das praktisch und asymptotisch besser ist als die zur Zeit bekannten und weitgehend auf dem klassischen Programm der Auflösung der Gleichungen durch Radikale basiert.
2. Es führt zu einigen zusätzlichen Algorithmen für Faktorisierung und Wurzelziehen über galois Felder, die auf der verallgemeinerten Riemannschen Hypothese (ERH) basieren und eine minimale Anzahl von Zufallsbits verwenden.

Diese Dissertation hat einen betont dualen Charakter: der theoretische Teil wurde jenseits der unmittelbaren Anwendungszwecke verfolgt, während dem der praktische Teil eine Vielzahl von zum Bereich der berechenbaren Algebra und Zahlentheorie gehöhrenden Teilproblemen angeht und verbessert löst. Dieser duale Zugang führte unter anderen zu folgenden Resultaten:

3. Vom theoretischen Standpunkt her werden neue geschlossen Formeln für Gauss und Jacobi Summen mit Primzahlpotenz – Führern sowohl über Felder wie auch über $(\mathbb{Z}/n \cdot \mathbb{Z})$ Ringe hergeleitet.
4. Die Berechnung von Jacobi Summen wurde vom Gesichtspunkt der Gitterreduktion (Lattice reduction) angegangen, mit dem Ergebnis einer effizienten Berechnungsmethode, die jedoch im Kontext von Zyklotomie Primheitsbeweisen nicht polynomial ist. Eine weitere, algebraische Methode wird vorgeschlagen, die mit einfachen Mitteln grosse Berechnungen ermöglicht.
5. Es wurde gezeigt, sowohl in der Theorie wie auch in der Implementation, dass der Toom-Cook Algorithmus zur Multiplikation von Polynomen über galois Feldern von kleinem Grad und grosser Charakteristik am besten geeignet ist – praktisch ist diese Methode einer FFT Methode für $d = O(\sqrt{\log(p)})$ vorzuziehen; dabei ist d der Erweiterungsgrad und p die Körpercharakteristik.

6. Die deterministische Variante der Zyklotomie – Primheitsbeweise ist von der ERH unabhängig; obwohl es die gleiche Asymptotik wie die häufiger implementierte probabilistische Variante hat, wurde es lange als für realistischen Implementationen ungeeignet betrachtet. Dies ist auf die Verwendung von Erweiterungen von nicht polynomialen Grad zurückzuführen. Wir zeigen, dass der Algorithmus in viel kleineren – insbesondere, polynomialen – Erweiterungen durchgeführt werden kann und somit praktisch mit der konzeptuell einfacheren, probabilistischen Variante von der Effizienz her vergleichbar ist.

7. Zum Abschluss gelang noch eine Verbesserung der letzten nicht polynomialen Phase des Tests, und zwar unter Verwendung eines neuartigen elliptischen Kurven Vortests. Dieser Erfolg könnte vieliecht die Bahn öffnen für bislang nicht untersuchten Kombinationsmöglichkeiten von Zyklotomie und elliptischen Kurven...

Die in dieser Thesis beschriebenen Algorithmen wurden in der objektorientierten Library LiDIA schliesslich implementiert. Sie verwenden dabei die von Victor Shoup entwickelte Arithmetik. Obwohl noch nicht alle im theoretischen Teil ausgearbeiteten arithmetischen Verbesserungen implementiert wurden, ist das Zeitverhalten bereits erfreulich: Wenn man die relative Komplexität im Verhältnis zu einem Rabin-Miller Test betrachtet – ein guter, maschinenunabhängiger Indikator – so wurde dieser in Vergleich zur [BovdH] Implementation um einen Durchschnittsfaktor 8 verbessert; die letzte Implementation hatte einen Verbesserungsfaktor von etwa 2 in bezug auf die aller erste von [CoLe]. Kurz vor dem Abschluss wurden zwei neue allgemeine Primheitsbeweis – Rekorde mit dieser Implementation geschlagen. Der Beweis der ersten 10000 – bit langen Pseudoprimzahl $N = 2^{10000} + 177$ gelang innert 5 3/4 Tagen auf einer DEC Alpha 500; dies ist die grösste mit einem allgemeinem Beweis – Algorithmus bewiesene Primzahl. Sie übertrifft den letzten mit elliptischen Kurven erreichten Rekord mit 36%. Die Performanz ist etwa 50 mal höher.

Abstract

Cyclotomy of rings is the theory of $s-$th cyclotomic extensions of rings $(\mathbb{Z}/n \cdot \mathbb{Z})$, with both s and n positive integers. Such extensions do not exist for all pairs (n, s), and when they do, they provide valuable information about the possible factors of n. Introduced by Lenstra in [Le1] for the purpose of giving a better general setting for a large variety of primality proving algorithms, cyclotomic extensions are the background of all currently known primality proving algorithms, except for the elliptic curve based ones. Cyclotomy proving of primality was proposed by H. W. Lenstra Jr. and first implemented by his students W. Bosma and M. van der Hulst. They are very performant in practice, asymptotically, though, superpolynomial.

In this thesis we make a complete theory of cyclotomic extensions and subextensions of rings, from the perspective of the factorization of the cyclotomic polynomial. Beside giving a more complete and detailed theory of the topic and revealing new key parameters like the *saturation index* of an extension, this approach has several practical advantages:

1. It leads to a new algorithm for the factorization of cyclotomic polynomimals over a galois field, which is both practically and asymptotically more efficient then currently known algorithms, and is deterministic under the ERH.

2. It leads to several additional combined algorithms for factoring and root finding over galois fields, which have a minimal use of randomness, while being deterministic only under the assumption of the ERH.

The thesis has a pronounced dual character: the theoretical part is studied far beyond the immediate applications for primality testing, while the practical part attacks different computational subproblems, which belong to the general scope of computational algebra and number theory. This dual approach led to some unexpected novelties:

3. From the theoretical point of view, new formulae for Gauss and Jacobi-Sums of prime power conductor have been computed both over classical (galois and characteristic 0) fields, and over the finite $(\mathbb{Z}/n \cdot \mathbb{Z})$ rings.

4. The computation of Jacobi-Sums has been approached from the point of view of lattice reduction, thus revealing a performant method, which is however not polynomial in the context of cyclotomy primality proving. A further, galois field based method is developed in order to allow large computations.

5. The fact has been proved, in theory and in practice, that the Toom-Cook algorithm for polynomial multiplication over galois fields is best among all fast convolution algorithms, in the case when the characteristic p is large as compared to the extension degree d – in fact the advantage was proved to hold for $d = O(\sqrt{\log(p)})$.

6. The deterministic variant of cyclotomy primality proving ([Le1]) does not relay upon ERH; while being asymptotically equivalent to the probabilistic version, it was long believed to be practically prohibitive, due to very large degrees of extensions in which it was needed to operate. We show that the algorithm can be

performed in moderate sized extensions, thus being also in practice comparable to the conceptually easier probabilistic version. The deteministic main stage is in fact only $\log\log(N)$ times slower than the probabilistic one.

7. Last but not least, we give a special elliptic curve pseudoprime test, which leads to an important reduction of the final, superpolynomial stage of the cyclotomy primality proof. This is a first success in attempting to combine elliptic curve and cyclotomy primality proving.

The algorithms described in this thesis have been programmed using the object oriented LiDIA package ([LiDIA]). Allthough not all possible arithmetic improvements studied in the theoretical part have yet been implemented in the program, it already has a very satisfactory behavior: comparing the relative complexity to one Rabin-Miller test – which is a good machine independent ratio – it shows out that the performance of our implementation is faster by a factor of 8 (roughly) then the average performance of the [BovdH] one; their improvement with respect to previous implementations was of about 2. Shortly before submitting the thesis for printing, some new records in general primality proving have been achieved with this implementation. First, the Mersenne factor $MC7673 = (2^{7673}-1)/(184153\cdot 13918823)$, a number with 2298 decimal digits, was proved prime in 29 hours on a DEC Alpha 500. This was the last unproved pseudoprime in the range $2000-4000$ digits, from the Mersenne factor list computed by E.Mayer. Shortly after that, $N = 2^{10000}+177$, the first 10000 bit prime was proved on the same machine in 5 3/4 days. This outranges the last record proved with elliptic curves by a factor of 36% in length and about 50 in speed.

Acknowledgment

I got acquainted with the domain of primality testing due to Profs. V. Strassen and E. Specker's seminar on algorithmics. I thank them for the lively, fascinating way of leading the two hours on Tuesdays. They encouraged me to write this thesis and seek external help from Prof. H. W. Lenstra Jr.. It was due to his generous acceptance to survey the development of the thesis as a referee under non standard conditions that this work could come into existence. His careful reading and focused hints and criticisms were a ferment that stimulated the structuring of my ideas into the final shape of this thesis. To him my profound recognition. I only met W. Bosma and M. van der Hulst once, at the very begining of my research. However their thesis on the same subject, which was finished in 1990, long before mine, has been for several years a major means for orientation in this scarcely researched field. If the present thesis brought the subject of cyclotomy a small step further than it was left by theirs, this fact was definitely made easier by the existence of their work. It is, unsurprisingly, the most frequently cited paper of my thesis.

I thank Prof. E. Engeler for his friendly and informal way of assuming the leadership of this doctorate. Prof. M. Bronstein gave his strong support to the finalization of this thesis and, among others, stimulated the implementation of the algorithm. I am grateful for his attentive involvement in all aspects of the finalization of my work and the energetic impulses he gave for its fulfillment. Dr. H. Thomas had with his poetic views on programming an inspiring impact upon the structure of the implementation.

I am thankful to Dr. Clifford Williamson for his careful reading of a preliminary version of the thesis and to him, Dr. T. Mittelholzer and A. Stadler for stimulating discussions. I thank my colleagues at $\mathbf{r}^3$ Security Engineering for the fruitful atmosphere which was the background of the last year of work on this thesis. During summer and fall 1996 I had intensive disucssions with D. Muster about elliptic curve tests, in a cryptographic context. It is at that time that we came to consider dual elliptic pseudoprimes. Without his stubborn wish to prove more, very likely would I not have succeeded to prove the little that could be proven for the CIDE algorithm. My recognition to him for his motivating enthusiasm and perseverence !

To the numerous friends - I could hardly list them all here - who encouraged my research during all these years, a heart full of thanks.

The political striving for liberty and the changes in Eastern Europe - and especially in Romania, my country of birth - during the last decade involved much of my energies and activities. This gave the material of this thesis the time to ripen in the background. The happiness that something did happen and the sadness for the questionable results have, of course, no addressee at this point. But I am grateful to all above mentioned, for their patience with my shift in priorities during a long period of time.

Dr. Thiery Gautier was a good companion during the implementation time and the frequent discussions we had, helped me come over many a dead lock of the kind that happen while programming. I thank him for his patience while looking at C++ problems together. A future parallel implementation of cyclotomy is planed with him, consequence also of these initial collaboration.

In the very last days of testing, Paul Leyland provided me some large test examples that had been prepared in long work by E. Mayer. This helped spread the word about this implementation and provide the right measure for my tests. Thanks to my internet helpers for their stimulating interest.

Last but not least, I am grateful to Dr. T. Roos who introduced me to the art of using LaTeX. Thanks go also to the family Grossu-Betrix under whose mountain roof the first and the last version of this thesis were conceived.

Contents

Eins, zwei, drei,
Polizei,
Vier, fünf, sechs,
Alte Hex ...

Children's song

Chapter 1

Introduction

1.1 Development of Primality Testing Methods

This work was motivated by the development which took place in the last decade, in the field today called "primality proving". It is dedicated both to the practical aspect of primality proving and the theoretical foundation of the proving techniques using "cyclotomy".

The topic of primality proving is, given a positive odd integer $n \neq 1$, to give an answer to the question "is n a prime?". The answer may be "yes" or "no", and must be backed up by a proof of the statement.

The simplest way to provide an answer is trying to divide n by all integers $1 < m \leq \sqrt{n}$ – with all the primes in the same interval, if their list is known. By doing this, one may find a divisor m_0 of n, in which case the equality $n = m_0 \cdot \frac{n}{m_0}$ is a proof of n not being prime – i.e., being *composite*. Note that any composite number has a factor $m \leq \sqrt{n}$ – indeed, since it has at least two factors: $n = m \cdot m'$ and assuming $m \leq m'$, it follows that $m^2 \leq m \cdot m' = n$. Thus, if the process of trial division does not yield any divisor, n must be prime. The proof is in this case the negative result of the process itself. It is note worth that the compositeness proof may be reduced to a simple equality, whereas the primality proof may not be reduced to any subset of the sequence of operations which led to the *conclusion* that n is prime. The situation is typical for the difference between compositeness and primality proofs.

Primes belonging to the oldest objects of study of mathematics, along with the above described intuitively naive approach, one may find the most astonishing answers to the primality question. It is for instance possible to prove that the set of prime numbers is equal to the set of positive values of certain multivariate polynomials $f(x_1, x_2, \ldots, x_k) \in \mathbb{Z}[X_1, X_2, \ldots, X_k]$ ([JSWW], [Ma]). A proof for the primality of n may thus theoretically be provided by a set of values $(u_i)_{i=1,2,\ldots,k}$, such that

$$n = f(u_1, u_2, \ldots u_k).$$

But even if this set was provided – finding one is the hardest task! – verifying the above equation is more time - exhaustive than the naive trial division test, due to the size of the polynomial values involved. We see that along with the abstract request for the validity of a proof, measurable time becomes an important condition for a good primality proof.

Methods for providing fast primality proofs for very special numbers n were known for the last three centuries. In these cases the proofs are *polynomial* in the number of bits of the binary representation of n, or, equivalently, in $\log(n)$. These methods where summarized by E. Lucas, a high school teacher at the Lycée Saint Louis in Paris, in the last century ([Lu]). They involve recursive sequences that bear his name.

Lucas sequences are sequences $(u_m)_{m\in\mathbb{N}}$ defined by a recurrence formula of the shape:

$$u_{m+1} \quad = \quad Pu_m - Qu_{m-1}, \quad \text{for given integers } P \text{ and } Q, \text{ and } m \geq 1. \tag{1.1}$$

The tests developed by Lucas were studied during a whole century until the early 80-es. They bear today the name of Lucas-Lehmer tests, honoring thus the important ulterior contributions of D.H.Lehmer – [Lu], [Pe]. A good overview of Lucas-Lehmer tests can be found in [WiJu] and they are discussed in more detail in Appendix C. Further modern applications of Lucas sequences for primality testing are found in [AdS], [BLS], [We], [WiZa]. Primality proofs using general Lucas-Lehmer tests amount to finding bases $\alpha_q \in \mathbf{R}$, where $\mathbf{R}$ is $(\mathbb{Z}/n\cdot\mathbb{Z})$ or some small extension of degree k, F is a completely factored part of $n^k - 1$ and q goes through all the prime factors of F. The bases α_q must satisfy the following test:

$$\alpha_q^{n^k-1} \quad = \quad 1 \quad \text{and} \tag{1.2}$$

$$\alpha_q^{(n^k-1)/q} - 1 \quad \in \quad \mathbf{R}^* \tag{1.3}$$

The Lucas-Lehmer tests share following properties:

a1) they are *fast* – being polynomial in the length of the input n.

b1) they need a "sufficiently large" – typically $O(\sqrt{n})$ – factored part of $n-1$ or n^2-1 or more generally of $\Phi_k(n)$, where Φ_k is the $k-$th cyclotomic polynomial and k is some small index. In known examples of Lucas-Lehmer tests [WiJu], the value of k is $1, 2, 3, 4, 6$ or 8. In particular, they are *conditional* and apply only to test numbers n, for which the necessary factored part can be gained either due to a special shape of n or to a successful factoring of $\Phi_k(n)$.

c1) they give a *primality proof* for the numbers n declared primes and they also prove compositeness.

d1) most Lucas-Lehmer tests are not deterministic, since there is no explicit law for choosing the parameters P and Q – except for few cases.

In the cases $k = 3$, for each known prime factor p of $\Phi_k(n)$ a sequence $u_m = u_m(P, Q)$ is sought randomly, so that:

$$u_{\Phi_k(n)}(P, Q) \quad = \quad 0 \bmod n \ \text{ but } \ u_{\Phi_k(n)/p}(P, Q) \ \neq \ 0 \bmod n. \tag{1.4}$$

The cases $k > 3$ are slightly different and shall be mentioned in Appendix C. Sequences verifying (1.4) are "good sequences" for the probabilistic Lucas-Lehmer tests; other sequences are rejected, since they provide no information for the primality proof. Quadratic reciprocity allows deterministic efficient tests for most numbers of the shape

$$n = m \cdot 2^h - 1, \quad \text{with } m \text{ an integer such that } m < n, \tag{1.5}$$

in the sense that "good" parameters P and Q can be a priorily chosen in dependence of m, so that the test can be proved to provide the required information on n [Lu]. Most notorious in this direction is the Lucas test for Mersenne numbers (see Appendix C), with which the largest known primes have been found.

In [Mi] we used the explicit cubic reciprocity laws of Jacobi and obtained similar results for numbers

$$n = m \cdot 2^h \cdot 3^l, \quad \text{with } m \text{ an integer such that } m < n. \tag{1.6}$$

The Lucas-Lehmer tests could not give a satisfying answer to the natural request of having *fast* tests that can be applied to *any* test number n.

A new approach was proved to be possible by using the "little theorem of Fermat", which states:

Theorem 1.6 (Fermat) *Let p be a prime. Then for all a with $(a, p) = 1$,*

$$a^{p-1} = 1 \ mod \ p. \tag{1.7}$$

If n is a number to be tested for primality, and a is coprime to n, then the equation (1.7) and the definition of the Jacobi symbol $(a \backslash n)$ lead to a necessary condition for n being a prime, which is of practical significance:

$$a^{(n-1)/2} = (a \backslash n) \bmod n \tag{1.8}$$

The number a involved in this condition is called a base; if (1.8) does not hold, a is called a witness (for n being composite). The time used for testing if (1.8) holds for a given base is polynomial in the length of n – while the trial division algorithm is exponential; this shows why (1.8) is relevant for the question whether n is prime or not.

Of course, the relations (1.9), on which the Lucas-Lehmer tests are based, are acquainted to the "little Fermat", of which in fact they are a generalization. The breakthrough was made by Solovay and Strassen, of course, at a cost. The problem they had to deal with is that, given a base a, (1.8) also holds for certain non primes n; for the Carmichael numbers, which are composite numbers, (1.8) even holds for all a with $(a, n) = 1$. In their paper they introduced notions of statistics and probabilities in the decision question, whether n is prime or composite. They propose to choose k bases a_k randomly and test for each one, if (1.8) holds. If for a given a_j, (1.8) is not fulfilled, n is composite and a proof is given by the equation

$$a_j^{(n-1)/2} \neq (a_j \backslash n) \bmod n.$$

A primality *proof* is not provided, unless (1.8) is tested for *all* possible bases – or for all primes $p < n$. It was the contribution of [SoSt] to prove, that the probability that a fixed n is non prime while (1.8) holds for k randomly chosen bases a decreases exponentially with k, and is in fact $< (1/2)^k$. The concept of "probable prime" was born. Their method was improved by Rabin in [Ra] who considered the sequence

$$\{a^{m2^l} \bmod n \ : \ 0 \leq l \leq k\}$$

where a is some base with $(a, n) = 1$ and $n - 1 = m \cdot 2^k$ with odd m and $h = \min\{l \geq 0 \ : \ a^{m2^l} \bmod n = 1\}$. With these prerequisites, Rabin replaced (1.8) by following condition:

$$a^{m2^{h-1}} \quad = \quad -1 \bmod n \ \text{ or } \ h = 0. \tag{1.9}$$

Rabin proved that the probability $p(k, n)$ that a number n passing the test (1.9) for k independently chosen bases a is composite satisfies $p(k, n) < (1/4)^k$. Recent research ([DLP]) has brought proofs for much tighter bounds on $p(k, n)$, which also depend upon the size of n. Both algorithms of Solovay-Strassen and of Miller-Rabin have the following in common:

a2) they are *fast* – being polynomial in the length of the input n.

b2) they apply to *any* test number n.

c2) they are probabilistic, in the sense that k random bases a are drawn – k is a free parameter – and one of the conditions (1.8) or (1.9) is tested for each of these bases.

d2) they prove compositeness, but they do not prove primality. In fact, a number declared composite by one of the tests (1.8) or (1.9) does not verify Fermat's theorem and is thus not a prime. However, a number declared prime after k tests, might still be composite.

There is an obvious complementarity between the two types of tests discussed above, since the second apply to all test numbers, but do not give a primality proof, while the first provide the primality proof but set requirements to n, which make them only applicable to special cases.

The new approach to "proof" introduced by the "probabilistic" primality tests is a pragmatic one. To the extent in which it is practically relevant to know that a number n is prime, one may be satisfied to know that it is highly improbable that n will not behave as one – the lack of a complete proof may in that case be considered as *practically* irrelevant. Due to the development of public key cryptography, it *became* practically important to find prime numbers and Rabin-Miller tests are currently the most popular for finding "primes for practical use". Numbers that were not proven composite by several such tests – also called "compositeness tests" – are denoted by "(Rabin-Miller) pseudo primes". The term of pseudo prime had been itself used for decades before [SoSt], but it was the contribution of these two authors to give a statistical measure for this notion. Involved evaluations of the probability bounds for the event that a number is composite given the fact that it passes k Rabin-Miller tests and arguments like "it is more probable that the result of a computer calculation [for finding a Rabin-Miller pseudo prime] go wrong due to the influence of some – highly improbable – cosmic ray than that the number declared prime was indeed composite" (Rabin) contribute to the general acceptance of the use of pseudo primes for cryptographic purposes.

In 1982, Quisquater developed in an internal research report of the Phillips Laboratories a simple and practical method for generating primes ([CQ]). Unlike Rabin-Miller, the method provides also a primality proof. On the other hand, while it is possible, with a compositeness test, to pick a random number and make a probable statement about its primality, the Quisquater method will not generate *any* prime. In fact the author did not address the question, whether this property of his algorithm may or may not be used for cryptographical attacks. Between 1989 and 1995 Maurer enriched Quisquater's approach in order to address exactly this question; he produced a series of papers repeating and refining the same basic idea and algorithm ([Ma1], [Ma2], etc.). His purpose was to produce provable primes which have a distribution as close as possible to the one of the primes in the series of natural integers. The purpose is reached using several empirical statements and at the cost of efficiency, compared to the Rabin Miller test. In 1994, we gave ([Mi1]) a simple prime generation algorithm – similar to the one of [CQ] – which is more efficient than Rabin-Miller and provides provable primes. We were able to prove that the distribution of the primes produced by this algorithm converges to the distribution of all the primes in the natural integers. The proof uses the information entropy measure and is also not free of unproved conjectures. In fact, it relays on a classical conjecture of Hardy and Littlewood concerning the distribution of k - tuples of primes in arithmetic progressions. Modulo this conjecture, the uncertainty about the primeness of "practical purpose primes" may thus be dropped, since *provable* primes may be generated faster than pseudo primes and their distribution is cryptographically secure. The common idea to all three above mentioned algorithms for generating provable primes is to recursively produce numbers n which satisfy the requirements for a Lucas-Lehmer primality test. Although the practical relevance of pseudo primes has thus vanished, it is very probable that they will still be in use for a long time, due to their wide popularity at the early times of public key cryptography and their application in most software packages for this purpose.

While [SoSt] opened the way for a practically satisfactory answer to the question whether n is prime or not, the problem of a consistent primality proof for *any* n remained open. The only efficient primality proofs were provided by Lucas-Lehmer tests, which are conditional tests. The gap was filled in 1981 by the publication of the algorithm of Adleman, Rumely and Pomerance [ARP]. The algorithm used Jacobi-Sums and has the following properties:

a3) it is *fast* – being *super*-polynomial in the length of the input n. Precisely, if $f(n) = \log\log\log(n)$, there is an effectively computable constant c, so that the runtime is upper bounded by $(\log n)^{c \cdot f(n)}$.

b3) it provides primality proofs and there is no restriction to the test numbers n it can be applied to.

c3) it has two versions: one is probabilistic, in the sense that random bits are used in order to calculate certain primitive roots of unity; this version is faster and was implemented on computers. It has a certain, negligible but non – vanishing probability of ending without a decision whether the test number is prime or composite. It does however provide a proof of the decision whenever it ends. The second version is deterministic being of high theoretical interest, but more intricate for implementations. The runtime of both versions is bounded like in a3).

In the same year, Lenstra gave in [Le1] a simplified version of the [ARP] algorithm, which used also Gauss-Sums, thus putting the use of higher reciprocity laws in evidence. This version was revised and implemented on computers [CoLe], and bears the name of Jacobi-Sum test. The same paper gives a simplified description of the deterministic test, which is more elegant than the one in [ARP], yet as hard to implement.

The way the Jacobi-Sum test generalizes tests like [SoSt] and [Ra] is summarized in the following statements. We describe the basic ideas, which may slightly be changed for more efficient implementations:

(i) it works in ring extensions $(\mathbb{Z}/n \cdot \mathbb{Z})[\zeta]$, where ζ is some primitive root of unity of prime power order, rather than in $(\mathbb{Z}/n \cdot \mathbb{Z})$.

(ii) the role of the random bases a in (1.8) and (1.9) is taken by elements $\alpha \in (\mathbb{Z}/n \cdot \mathbb{Z})[\zeta]$, which are products of Jacobi-Sums and are chosen in a deterministic way by the algorithm. If p^k is the order of the primitive root ζ, the information provided by the test which the bases α have to pass is:

$$\alpha^{(n^{(p-1)p^{k-1}}-1)/p^k} \in <\zeta> \text{ in } (\mathbb{Z}/n \cdot \mathbb{Z})[\zeta]. \tag{1.10}$$

The notation $< x >$ stands for the cyclic group generated by the variable x and will be very frequently used in this thesis. We refer to the information content of the test, since there are more efficient implementations of relations revealing the same information. The similarity to the Solovay-Strassen test appears when replacing respectively " mod n" by " mod $n \cdot \mathbb{Z}[\zeta]$", a by α, the exponent $(n-1)/2$ by

$$\frac{n^{(p-1)p^{k-1}} - 1}{p^k}$$

and "$= \pm 1$" by "$\in <\zeta>$".

The choice of the elements α makes the fundamental difference from the first type of tests and allows a primality proof. Jacobi-Sums are used for proving higher reciprocity laws, and the choice of α in (1.10) is connected to this proof. A square free parameter $s > \sqrt{n}$ is initially chosen, so that s splits into primes $q < (\log n)^{cf(n)}$, and the exponent T of the multiplicative group $(Z/s \cdot Z)^*$ is also such that $T < (\log n)^{c \cdot f(n)}$; the existence of a parameter s is the consequence of a theorem of Prachar, Odlyzko and Pomerance ([CoLe] and section 6). The set of bases to be tested is

$$A = \{\alpha_{p,q} \ : \ p^k \parallel T, q | s\}$$

$\log_3(n)$	n
2	10^{702}
3	$10^{229\cdot 10^6}$
4	$10^{223\cdot 10^{21}}$

Table 1.1: *Growth of* $\log_3(n)$

where $p^k \parallel T$ means $p|t$ and $(p^{k+1}, T) = p^k$; $p|t$ is the common notation for "p divides t". It can be shown, that if n passes the tests (1.10) for all the bases in A, then:

$$r \in \; < n \bmod s > \quad \forall\, r|n, \tag{1.11}$$

where $< n \bmod s >$ is the multiplicative subgroup generated by $n \bmod s$.

The implicit use of higher reciprocity laws suggest some deeper relation between the Jacobi-Sum and the Lucas-Lehmer tests; remember, quadratic reciprocity is used by the later ones for finding bases that provide a primality proof. While somewhat hidden in the original setting of Jacobi-Sum tests, the connection is strong and natural and was revealed by the *cyclotomy* tests. Since these are a main subject of this dissertation, we shall treat their evolution and properties in more detail in the following section.

The Jacobi-Sum tests and their later development in cyclotomy tests had given satisfying answers to almost all problems involving primality proving. In its deterministic variant, the test provides a proof of primality or compositeness for any test input n. Furthermore, it does this in a practically efficient time. The exponent $\log_3(n) = \log\log\log(n)$ in the upper bound for the running time of these algorithms is – for all conceivable implementations – a small constant. Its growth is reflected by table 1.1:

For $n \approx 10^{10000}$ which is currently a proud target for primality testing, $\log_3(n) \approx 2.3$. Using Karatsuba multiplication for long integers and fast convolutions for the arithmetic in galois extensions, we estimate the complexity of our algorithm in this area of magnitude of about $O(\log^{4.5}(n))$. But the theoretical, not the practical, standpoint is relevant for these tests, given the fact that the practical problem is solved more efficiently. Despite of the slow growth of the exponent, the cyclotomy tests are thus *not* polynomial.

In 1986 a new approach to primality testing rose by the use of elliptic curves for this purpose. First Goldwasser and Kilian [GoKi] showed that it was possible to use elliptic curves in order to find primality proofs in polynomial time. An elliptic curve modulo n is a group structure

$$E_n(a, b) \subset \{(\mathbb{Z}/n\cdot\mathbb{Z}) \times (\mathbb{Z}/n\cdot\mathbb{Z}) \cup \{\mathcal{O}\}\},$$

with parameters $a, b \in (\mathbb{Z}/n\cdot\mathbb{Z})$ and with an addition rule that we shall denote simply by "+". The group elements are called "points" and the element $\mathcal{O}$ is the "point at infinity" (see for instance [Me] for a precise and geometrically intuitive definition of the group structure). For prime n, the useful thing about elliptic curves is that while a, b vary, the size of the group is bounded in a small interval around n. In this case, by a theorem of Hasse,

$$(\sqrt{n} - 1)^2 \le \sharp E_n(a, b) \le (\sqrt{n} + 1)^2.$$

This fact may be used for primality proofs much in the same way as Lucas-Lehmer tests used generalizations of the "little Fermat": Find a curve such that

$$\sharp E_n(a, b) = FR, \qquad F > (\sqrt[4]{n} + 1)^2,$$

such that F is completely factored. Then find a point $P \in E_n(a, b)$ – the analog of bases for Lucas-Lehmer tests – whose order is a multiple of F. With this, $F, E_n(a, b)$ are a prime certificate for n. The main contribution of Goldwasser and Kilian was to prove that it is possible to find a curve verifying the strict constraint $\sharp E_n(a, b) = 2p$, with p prime, within a polynomial amount of curve trials. It is thus the abundance of elliptic curves which makes it possible to achieve for random n what can only be done for special test numbers in the case of Lucas-Lehmer tests: a factorization of the group order.

The elliptic curve algorithm of Goldwasser and Kilian has following properties:

a4) it is polynomial in the length of the input n.

b4) it is probabilistic in the sense that it draws random curves and random points on those curves. "Good bases", resp. "good curves and points" are necessary for the Lucas-Lehmer, resp. elliptic curve tests in order to provide a primality proof.

c4) it is recursive in the sense that the order of a "good elliptic curve" must be divisible by some "big prime". The fact that such a factor is indeed a prime is proved by a recursive call of the algorithm, and the primes to be certified during recursion decrease exponentially, eventually reaching a size for which the deterministic primality test in [ARP] and [Le1] becomes polynomial in the size of the initial input.

d4) it provides a primality proof. If a certain unproved conjecture is true, every prime can be certified by this algorithm. Without use of unproved conjectures, Goldwasser and Kilian prove that a certificate can be found for a fraction of at least $1 - O(2^{-n/(\log\log n)})$ of the inputs of length $\log n$.

Note that the recursion in c4) may also be continued until the size of the primes to be proved becomes itself polynomial in the size of the input and an exhaustive trial division may be performed. The computation of $\sharp E_n(a, b)$ is a hard core of the procedure and uses an algorithm of Schoof ([Sch]). This algorithm, while being polynomial, is very slow (asymptotically $\log(n)^9$, in Schoof's initial paper).

The elliptic curve algorithm was improved by Atkin by avoiding the use of Schoof's algorithm. He used complex multiplication (see e.g. [Cox]) in order to generate elliptic curves with orders that may be quickly evaluated. In order to do this, the choice of elliptic curves is restricted to such ones which have complex multiplication in imaginary quadratic fields with polynomially bounded class number. These curves are rather sparse and it is not obvious if the Goldwasser - Kilian proof for the ending of the algorithm still holds for the Atkin improvement. The Atkin variant was implemented together with Morain [AtMo] and was successful in performing the first primality proof of an integer with more than 1000 digits with a general primality proving algorithm, in 1989. The test lasted at that time about 9 months using old SUN3 workstations.

Bosma used Atkin's approach of complex multiplication for some elliptic curve based tests which take advantage of known factors of $n^k - 1$, for $k = 4$ and 6 ([Bo]).

Considering the "theoretical goal of primality proving" to be a polynomial algorithm which is deterministic in the sense that it does not use random trials, the elliptic curve test still has two drawbacks:

A. It cannot be proved to end in all cases, without use of unproved conjectures.

B. It requires random trials.

In 1987, Adleman and Huang [AH] wrote the first of an announced series of articles, in which they try to eliminate A. Their approach differs from [GoKi], in that they use hyperelliptic curves of genus 2 and the unproved conjecture of this latter is replaced by a weaker, proved proposition on repartition of primes in intervals. Thus the algorithm of [AH] holds for all inputs without restriction. As [GoKi], the algorithm of Adleman and Huang uses recursive primality proving. The tradeoff to not relaying upon unproved conjectures consists in the fact that the recursion "goes the wrong way": the primes to be proved grow! They show that this recursion stops with some prime which can be proved using [GoKi].

As for today, the "theoretical goal of primality proving" was not reached and although pretty closely touched by the two main streams – cyclotomy and elliptic curves – it may as well be unreachable. Or the last steps are the hardest.

It is an aim of this dissertation to explore the limits of the cyclotomy test, reduce and sharpen the formulation of unsolved problems which are on the way for reaching this goal.

The theoretical exploring of elliptic curves is even less advanced. Even more, as mentioned above, it took a shift from theory to practice by the Atkin method and this brought additional unsolved theoretical questions as price for the practical improvements. On the other hand, despite of these improvements, the polynomial elliptic curve algorithm is still much slower in practice than the cyclotomy test. So complex and intricate is the game between asymptotics and implementation!

The improvements of Atkin have the great value of bringing more of the rich properties of elliptic curves at action in the domain of primality proving. It is not evident if these have already shown all their potential. The simple question of combining information from several independent tests was solved by cyclotomy. For elliptic curves, it would mean to combine informations on n, gathered from tests on different curves. This question was not solved – in fact we are not aware if it has been asked so far. It might be a prerequisite for combining cyclotomy and elliptic curve tests – or may even be a way in itself, for reaching the "theoretical goal of primality proving".

1.2 The Cyclotomy Test

While the connection to the Rabin-Miller test was already vaguely pointed out in [ARP], there was no link to Lucas-Lehmer tests in the initial version of the Jacobi-Sum test. In [Le1] section 8, Lenstra addressed this question and indicated a direction of research. In [Le2] he introduced the concept of cyclotomic extensions of rings $(\mathbb{Z}/n \cdot \mathbb{Z})$ and used it for giving the theoretical background for combining the Jacobi-Sum and Lucas-Lehmer tests. An $s-$th cyclotomic extension of $(\mathbb{Z}/n \cdot \mathbb{Z})$ – one can think of s for instance as being the parameter defined above – is basically a galois extension containing a primitive $s-$th root of unity ζ_s upon which the galois group acts as if n were a prime. The existence of an $s-$th cyclotomic extension of $(\mathbb{Z}/n \cdot \mathbb{Z})$ is a property of n mod s and it has (1.11) as a consequence. This gives the link to Jacobi-Sum tests. Actually, p^k-th cyclotomic extensions can be used in (1.10) for replacing the complex root of unity ξ by a root ζ_{p^k} which lays generally in an extension of $(\mathbb{Z}/n{\cdot}\mathbb{Z})$ of lower degree than $(\mathbb{Z}/n{\cdot}\mathbb{Z})[\zeta]$, so that the test (1.10) can be performed more efficiently. But also Lucas-Lehmer tests can be generalized to cyclotomic extensions, whereas the recursive sequences (1.1) are replaced by elements of the extension, which are subjected to test (1.10). Recursive sequences are linked to elements of extensions by their characteristic polynomial. The theorem of Lenstra which opened the way to combining Jacobi-Sum and Lucas-Lehmer tests is the following:

Theorem 1.12 *Let $s \in \mathbb{Z}_{>0}$. Let $\mathbf{A}$ be a ring containing $(\mathbb{Z}/n{\cdot}\mathbb{Z})$ as a subring. Suppose that there exists $\alpha \in \mathbf{A}$ satisfying the following conditions:*

$$\begin{aligned} \alpha^s &= 1, \\ \alpha^{s/q} - 1 &\in \mathbf{A}^*, \text{ for every } i \text{ prime } q|s, \\ \Psi_\alpha(X) = \prod_{i=0}^{t-1} (X - \alpha^{n^i}) &\in (\mathbb{Z}/n \cdot \mathbb{Z})[X], \text{ for some } t \in \mathbb{Z}_{>0} \end{aligned} \tag{1.13}$$

Then every divisor r of n is congruent to a power of n modulo s.

Bosma and Van der Hulst developed in their dissertation [BovdH] a combined Jacobi-Sum and Lucas-Lehmer test – which they named *cyclotomy test* – using the above theorem and the concept of *cyclotomic extensions* introduced in [Le2]. Their thesis was developed at the same time with the present one – while being completed before. It contains a theoretical part which develops the ideas from [Le2] in depth and from the perspective of an implementation. It uses the algorithm [AdLe] for constructing cyclotomic extensions, which is more efficient than the initial idea of factoring cyclotomic polynomials with the Berlekamp algorithm, which had been suggested in [Le2]. It also develops a new method for combining several Jacobi-Sum tests in one single computation. The practical part describes in intricate detail the aspects of the implementation of the cyclotomy test. Their experiments showed that cyclotomy tests performed best in the range of implementations of the early 90-es, although being asymptotically more complex then the elliptic curve test implemented by Morain ([Mo]). Meanwhile, the cyclotomy test has not been maintained while the elliptic curve test has been continuously improved and distributed on the internet by F.Morain ([ECPP]). It has become thus the tool for a series of continuously increasing primality records, among which : 1065 digits (1989), over 1126 and 1226 digits (1990) and 1505 digits in 1992 and 2196 digits this fall ([MM]), together with E.Mayer.

Our current implementation uses the LiDIA ([LiDIA]) arithmetic library . It brought a new improvement in performance of about a factor 8 in the machine independent ratio between the run – times of one cyclotomy test and one Rabin-Miller test, as compared to the [BovdH] implementation of cyclotomy. It is now possible to test a *titanic* prime of 1000 decimals in about one hour on a DEC Alpha 500. Before the completion of this thesis a new record for general primality proving was established with this implementation.

1.3 About this Dissertation

This dissertation was motivated by previous work made on special Lucas-Lehmer tests ([Mi]) and the perspectives opened by theorem (1.12). It was made possible by Prof. Hendrik Lenstra Jr. who generously accepted to act as referee under nonstandard conditions.

1.3.1 General Presentation

The idea of our approach to cyclotomy is simple and conceptually different from the one of [BovdH]. With n, s and T like in section 1.1, equation (1.11) holds if the $s-$th cyclotomic polynomial $\Phi_s(x)$ splits in factors of degree T over $(\mathbb{Z}/n \cdot \mathbb{Z})$. So factoring $\Phi_s(x)$ or building an $s-$th cyclotomic extension – which is equivalent, as we show in section 3.2 – is the central problem of primality testing using cyclotomy. Except for a minor improvement, of theoretical interest, this approach does not lead to a modification of the main steps of a cyclotomy test, as described in [BovdH] and [CoLe]. Its interest is however both of theoretical and of practical nature. Theoretically it brings the common roots of Jacobi-Sum and Lucas-Lehmer tests into light, by showing that both can be regarded as methods for factoring the cyclotomic polynomial. At the same time it shows that the Jacobi-Sum test as conceived before ([CoLe], [BovdH]) provided slightly redundant information, thus requiring more tests of (1.10) then actually necessary. This interesting improvement has no impact in terms of efficiency. Our approach has also a practical byproduct, since it offers a new algorithm for factoring the cyclotomic polynomial over finite fields (and rings) by using Jacobi-Sums. In most cases, this algorithm is more efficient then the known algorithm for this purpose ([Hu1]).

We also give the design of an implementation of the cyclotomy test in which we improve upon the [BovdH] implementation in each major step of the algorithm. The improvements are not asymptotical, but help enhance the efficiency of the implementation by a factor of 10 – using a various bag of tricks that may be denoted as "skill of computation". A current implementation which is presented in Chapter 6 does not yet cover all the aspects described in the design.

The purpose of this dissertation is cyclotomy in itself and its applications to primality testing. It has thus a double goal: on the one hand treat cyclotomy of rings as a self contained mathematical topic and develop their theory beyond immediate application perspectives. This despite of the throughout plausible question, whether cyclotomy of rings may ever receive a mathematical use outside the realm of primality testing. On the other hand, we explore the limits of the cyclotomy approach to primality proving. This leads to manifold punctual improvements to the previous work of Bosma and Van der Hulst but also to a proof of the limits of asymptotic improvement that may be expected.

It is a consequence of this perspective, that new results are interleaved with repetitions of classical results on cyclotomy, Gauss and Jacobi-Sums, and with known results from the small literature covering cyclotomy of rings ([Le2], [BovdH]). The material is self-contained and should be accessible without prior knowledge of the field. We treat the ingredients of cyclotomy as theoretically independent subjects and develop their properties beyond the scope of primality testing. This leads to some new results, such as formulae for Gauss-Sums for characters with prime power conductors, an algorithm for computing Jacobi-Sums by using lattice reduction and some detailed results on cyclotomic extensions of rings and their sub extensions.

It was also our aim to clarify the historical continuity of primality testing using cyclotomy. An apparent hiatus had been suggested by the publication of [ARP], given the use of an apparatus that did not generalize – at a first glance – the classical apparatus of Lucas-Lehmer tests. This gap had been sensibly reduced by theorem (1.12), [Le2] and [BovdH]. We achieve the aim of putting the connection of Jacobi-Sum and Lucas-Lehmer tests in evidence, by showing that the Jacobi-Sum and the Lucas-Lehmer tests are different means for the same purpose of factoring cyclotomic polynomials. We dedicate for historical reasons an Appendix for generalizing the Lucas sequences in order to express the modern Lucas-Lehmer tests in terms of recurrent sequences. This may be interesting in the context of a certain rebirth of interest in generalizations of classical Lucas-Lehmer tests, stemming out of the field of the symbolic computation ([Bb]). We also develop, in an other Appendix, the implementation theory for the deterministic test and show that it can be dynamically interleaved with the random one and performed in much smaller extensions than described in [Le1]. Of course , this is a consequence of our applied perspective, the treatment in [Le1] being of exclusive theoretical nature. While treating the same subject, we expect to provide in this thesis comparably many original results and improvements - both of theoretical and practical nature - with respect to [BovdH], as that dissertation brought with respect to anterior papers by Lenstra.

1.3.2 Contents

Cyclotomic extensions of rings are the *structures* used for the cyclotomy test. The *objects* used in this context are cyclotomic polynomials, primitive roots of unity, Gauss-Sums and Periods and Jacobi-Sums. The *possibility of constructing* a cyclotomic extension is the premise of a primality proof based on (1.11). The constructive perspective is developed in the first 3 chapters. Chapter 2 is dedicated to the objects and tools of cyclotomy, chapter 3 to the structures and chapter 4 to their construction. *Primality testing criteria are the byproduct of the algorithms for constructing cyclotomic extensions.* In the first two subsections of chapter 2, we define the concept of primitive roots of unity over rings and develop all the the properties of Gauss-Sums and Periods and Jacobi-Sums which shall subsequently be used in the construction of extensions. The context are finite rings ($\mathbb{Z}/n\cdot\mathbb{Z}$). This topics were already treated in this context by Lenstra ([Le1]) and Bosma ([BovdH]). In section 2.3 we make a theoretical excursion to Gauss and Jacobi-Sums of characters with prime power conductors. This topic is irrelevant for primality testing, but was not found to be treated in the larger literature of the field either (Number Theory Index). We develop some closed formulae for these Sums both over fields and rings. In section 2.4 we consider multiple Jacobi-Sums, which occur in the definition of the set A of bases $\alpha_{p,q}$ subject to test (1.10) in the Jacobi-Sum test. Computing the multiple Jacobi-Sums $\alpha_{p,q}$ by direct summation leads to following restriction of the size of primes q that build up s:

$$q \quad < \quad (\log n)^{cf(n)} \tag{1.14}$$

We show that the lattice reduction algorithm can be used for the calculation of $\alpha_{p,q}$ in a time $O(p^p \log q)$ and give an explicit algorithm, which drops the restriction on the size of q. This gives a partial answer to a question raised by Lenstra in [Le1]. Indeed, lattice reduction allows using *any* known factors of $n^T - 1$, while the time for computing the multiple Jacobi-Sums $\alpha_{p,q}$ stays bounded by $(\log n)^{cf(n)}$, for any $q < n^T - 1$. For "initial primes" (see [ARP]) verifying

$$p = O\Big(\frac{\log\log n}{\log\log\log n}\Big),$$

the computing time for $\alpha_{p,q}$ is even polynomial. However, in order to guarantee $s > \sqrt{n}$, initial primes up to $O(\log\log n)$ are needed. Using this method of computation in the cyclotomy test allows the use of generalized Lucas-Lehmer tests in their original scope of taking advantage of large factored parts of $\Phi_{t'}(n)$, where t' is any divisor of t. We propose also a galois field based method for computing Gauss Periods, Sums and Jacobi-Sums; this method is not more efficient than the previous, but it allows performing large computations by bounding the required memory space. Further developments using this method may be possible.

Chapter 3 is dedicated to the structures used in cyclotomy testing. The paragraph section 3.1 treats cyclotomic fields, their intermediate fields and bases for the integers thereof. We also introduce the Artin map and the Artin symbol in this context and establish the relation to Frobenius automorphisms of finite fields. The galois group of finite fields being cyclic, these fields can be regarded as factor rings of intermediate cyclotomic fields taken modulo a rational prime. This gives the motivation for a method of constructing cyclotomic extensions, which is generalizing a case treated in [AdLe].

In section 3.2, we introduce cyclotomic extensions and prove a list of equivalent properties thereof. These properties, which have not been explicitly proved or stated in the previous literature concerning cyclotomy of rings, help understanding the constructive approach as means for deducing primality conditions. Only few of these properties are directly used for primality proving. Their totality gives a simple insight in the richness of implications of the definition of a cyclotomic extension. We also point out to a simplification of the Jacobi-Sum test which consists in the fact that not all multiplicative characters modulo s, but only the ones mapping n to 1 are needed for this test.

We introduce the concept of *saturated* cyclotomic extensions, which have the property that if an $s-$th cyclotomic extension is saturated, then $s'-$th cyclotomic extensions exist and can be explicitly constructed for all s' built up from primes dividing s. The term of saturated extensions is used to explain the cases in which the random Jacobi-Sum test fails.

In section 3.3 we treat intermediate extensions of cyclotomic extensions of rings. This topic, which was not dealt with explicitly before, also covers some interesting results concerning combination of cyclotomic extensions. It brings new insights in the connections between Jacobi-Sum and Lucas-Lehmer tests.

In chapter 4 we treat the problem of building cyclotomic extensions. We distinguish two ways of posing the problem: one may be interested in building an extension of given *order*, which defines implicitly also the degree; or one may be interested in merely defining the *degree* of the extension, finding thus a suitable order which produces an extension of the given degree. The later case is treated using the Lucas-Lehmer approach in section 4.1. For the first scenario, the Jacobi-Sum approach is suited; it is developed in section 4.2.

The Jacobi-Sum approach requires taking roots for computing Lagrange Resolvents (Gauss-Sums). This step is probabilistic and it may fail, if used in a primality test context, thus revealing that the test number was composite. However, if the Gauss-Sums can be successfully computed, the construction of a cyclotomic extension can proceed by a sequence of deterministic steps. This means that the existence of such an extension is settled by the computation of the Gauss-Sums. The constructive approach reveals thus that the Jacobi-Sum test is exactly the initial part of the construction of a cyclotomic extension using Jacobi-Sums, which may fail if the test number is composite.

In section 4.3 we develop conditions for existence of cyclotomic extensions from the two different construction algorithms. We also show how to test several such conditions simultaneously, using *amalgams*. A similar procedure is proposed in [BovdH], described as "combining tests". It appears however, that the way amalgams are built differs. In section 4.4, we state the Jacobi-Sum method for factoring cyclotomic polynomials over finite fields, which is an algorithm of interest beyond the scope of primality testing. Among others, it may find applications in the field of BCH codes ([Bl2], [VO]). We conclude the chapter by showing in section 4.5 that this algorithm is of interest also in a setting in which random bits economy is important. In fact, the expected number of random bits required for building cyclotomic extensions - or factoring cyclotomic polynomials - using the Jacobi-Sum method is inferior to the amount required by the Lucas-Lehmer method, proposed in [Hu1].

In chapter 5, we give the design of an (ongoing) implementation of the cyclotomy test. We distinguish the following main steps in the implementation of a cyclotomy test for a prime candidate n:

(i) establishing the parameters s and T.

(ii) building working cyclotomic extensions. .

(iii) computing Jacobi-Sums – or mapping them to the cyclotomic extensions, using look up tables.

(iv) performing tests consisting of exponentiations in the working extensions.

(v) performing the final trial division test (1.11).

Steps (iv) and (v) are the most time consuming ones in the test. Due to the intricately detailed description of sub algorithms in [BovdH], it is difficult to ascertain singling out correctly the choices made by the authors for the above five steps in their implementation. Despite of this doubt, it is probable that our design is more efficient - by considerable factors - in all the main steps.

The single sections of chapter 5 describe the implementation of the main steps. Section 5.3 is dedicated to arithmetic in cyclotomic extensions. There we give an overview of the available algorithms for fast convolutions, show how to combine them with the Montgomery algorithm ([Mg]) for modular division and give some choice criteria in dependence of the size of the test candidates and the degrees of the working extensions. We make the simple, but apparently novel remark, that algorithms as the Toom Cook convolution, which have limitations when used for fast integer multiplications([Kn]), are ideally suited for multiplication of polynomials over finite fields (or rings) with large characteristics, and thus for multiplications in cyclotomic extensions. In section 5.5, we make several improvements for the performance of the final trial division stage. In chapter 6 we describe our implementation in C++ and give average timings, compare to the results of previous implementations and document the first tests on primes larger than 1500 digits, that we have made. Two primality proving records have been established: the proof of the 2298 digit pseudoprime factor $MC7673$ of the Mersenne number $m = 2^{7673} - 1$ and the first 10000 binary digit pseudoprime: the number $2^{10000} + 117$ has been proved prime and is thus the currently largest prime proved with an all purpose proving algorithm. The proof of Mersenne factors, revealed that our implementation is about 50 times faster than elliptic curves one, on a similar machine ([May]). After publishing these results on the number theory list, requests for proving primes arising in different researches came in: it is likely than this program will gain in popularity, as the tool for proving primes in the internet.

In chapter 7 we treat the asymptotic behavior of the cyclotomy test. The conclusion of this chapter is a negative one, since it shows that the use of additional factors of $n^T - 1$ in the Lucas-Lehmer test can not reduce the size of T to a polynomial one with current known factorization methods. Bosma and van der Hulst were also aware of this fact.

The size of T has a direct impact on the run time of the algorithm in the computation of Jacobi-Sums and in the final test (1.11). Even if that step can be reduced to polynomial time by using specialized lattice reduction methods - which we did not succeed to develop -, only producing the remainders $n^k \bmod s$ in (1.11) requires T operations, thus super polynomial time. Reducing the final step to polynomial time is thus only doable, if one can produce a subset of these remainders which are "small", without having to compute the whole set. In section 5.5.1 we give a formal statement of this open problem, of combinatorial nature.

The last chapter gives a new algorithm in which we combine cyclotomy with an initializing elliptic curve test of a new kind. The elliptic curve test gives information allowing to reduce the parameter s of the test to $s = O(\sqrt[4]{n})$. This might only be a first knock at the door of new elliptic curve and cyclotomy combinations.

In Appendix A, we present the deterministic test from an implementational perspective, while following the ideas from [Le1]. As mentioned above, some practical advantages may result from this perspective.

In Appendix B, we reproduce the paper [Mi1] which gives an answer to the problem of constructing provable primes for cryptographical purposes. Appendix C is dedicated to "classical flavored" Lucas-Lehmer tests. We make a general theory of recurrent sequences and their periodicities modulo integers, which are used for primality testing. We then review some old results, among others the Lucas test for Mersenne numbers. The main result of the appendix is a generalization of Lucas sequences, which allows formulating the cyclotomy Lucas-Lehmer test in terms of recurrence relations. We also give a general test for numbers of the shape $mF \pm 1$ with $m < F$ and F completely factored with explicit methods for choosing the bases required for testing (1.3).

1.3.3 A guide to the reader

Regarding mathematics as an art of using shadow and light, we consider that the virtues and faults of this thesis are not isomorphic to the set of repetitions of known results versus the novelties. The light stops made along the thesis respond alternately to theoretical, practical or aesthetical needs. We add the following brief guide to the reader as a nontechnical survey of the connections between the various theoretical and practical chapters. Inevitably, this section overlaps the preceding one. It is intended for the reader willing to make a choice of the parts of the thesis he wants to look into in more detail. The main theme of this thesis is to develop the theoretical background of the cyclotomy of rings and to apply it to an algorithm for primality proving. The sections 2.1 and 2.2 give a brief introduction to the concepts of primitive roots of unity, Gauss-Sums and Periods and Jacobi-Sums, when working over finite rings. They can be read in diagonal by the reader familiar with the papers of the domain - [Le1], [CoLe], [BovdH].

Chapter 3 is dedicated to cyclotomy. The first section reviews the cyclotomy of fields, the orders of integers in these fields and their bases and the Artin map. It is classical knowledge, with some personal new proofs, which were chosen due to their better fitting in the general setting. The second section introduces the central concept of *cyclotomic extension* and proves a large variety of properties of these extensions, which go beyond what was proved in the above mentioned papers. Cyclotomic extensions of order s of the ring $(\mathbb{Z}/n \cdot \mathbb{Z})$ are the generalization of $s-$th cyclotomic extensions of prime galois fields $\mathbb{F}_p$ to the case of non necessarily prime characteristic. The existence of these extensions is not granted in general; it depends on special relations between n and s. The level of uncertainty about cyclotomic extensions is caught in the concept of *saturated extensions*, introduced in section 3.2; saturated $s-$th extensions have the property that their existence guarantees existence of $s'-$th extensions for *any* s' built up from the primes dividing s. The picture of cyclotomic extensions is completed in section 3.3 by analyzing also the sub extensions of cyclotomic extensions, which are images of abelian fields. This gives a simple tool for understanding the combination of Jacobi-Sum and Lucas-Lehmer tests.

Chapter 4 is concerned with the duality between constructing cyclotomic extensions and factoring cyclotomic polynomials, on the one hand, and primality proving on the other hand. In the first two sections, a method for finding roots of unity is introduced together with two approaches for building cyclotomic extensions, respectively factoring cyclotomic polynomials. We call these approaches the Lucas-Lehmer and the Jacobi-Sum approach. There is a duality between "horizontality" and "verticality" which traverses the topic of cyclotomic extensions. It is caught in the concepts of "push" and "pop" characters, which we introduce in section 3.2. The horizontal aspect refers to abelian extensions which are mapped into the base ring $(\mathbb{Z}/n \cdot \mathbb{Z})$ - are thus "flattened"; it is exploited by the Jacobi-Sum approach to building cyclotomic extensions. The vertical aspect corresponds to abelian extensions whose degree is conserved by the mapping from the complex field into extensions of $(\mathbb{Z}/n\cdot\mathbb{Z})$. It is exploited by the Lucas-Lehmer approach. The section 4.3 uses the constructive algorithms of the first two sections of the chapter for deducing pseudo prime tests which are the core of the cyclotomic primality proving method. The information provided by these tests can be combined for proving the existence of certain cyclotomic extensions. The existence of these extensions itself reduces the number of possible divisors of the test number n to a small – unfortunately super polynomial – set of modular residues.

Chapter 5 is exclusively of practical nature. It provides the backbone of an implementation of the cyclotomy test together with a bag of algorithmic tricks allowing to improve the efficiency of the implementation with respect to the one in [BovdH]. We thus show that the Toom-Cook algorithm is particularly practical for multiplications in small extensions of fields or rings with large characteristic. This approach is homogeneous and more efficient than the choice of extension - specific algorithms given in the addendum to [CoLe]. In this way we give the answer to a question raised by Prof. H. Cohen at a "Tuesday seminary" on algorithmics, at the Zürich University. The practical choice for the working extensions in which pseudo prime tests will be performed has an important impact upon the overall performance of the algorithm. The selection between different possible choices is made under consideration of the arithmetic algorithms that will be used for working in these extensions. The final trial division stage tends asymptotically to dominate the cyclotomy test; we show that, by making repeated use of the Chinese Remainder Theorem the multiplications required by these stage may be reduced to a polynomial set and *only* a super polynomial amount of long integer additions is necessary. The implementation theory is followed by a brief chapter describing a practical implementation of the algorithms and comparing times and algorithms.

Chapter 7 treats the asymptotic aspects of the algorithm. It proves a negative result, which is that the super polynomial aspect of the algorithm cannot be reduced by the combination of Lucas-Lehmer and Jacobi-Sum approaches, even if factoring methods would dramatically improve in the future.

Like a longer mountain walk, this thesis has several sight seeing stops allowing a brief look into topics which are at most loosely connected with the main subject. In section 2.3 we deduce some novel, interesting and *totally useless formulae* for Gauss and Jacobi-Sums of prime power conductor over fields and also over rings where the galois action of the two characters of the sums differ. In section 2.4 we consider the problem of computing Jacobi-Sums - which, along with the final trial division, is a simple but super polynomial stage of the cyclotomy test. Following a question raised by Lenstra in [Le1] regarding the possibility of using the arithmetic properties of the Stickelberger element ([La1]) for the efficient computation of Jacobi-Sums, we develop the use of lattice reduction for this purpose. This makes it possible to compute Jacobi-Sums in time polynomial in the *conductor* of the sums - which permits using considerably larger conductors then before. The algorithm is however still super polynomial for the larger character orders which are required by the test.

The concept of intermediate cyclotomic extensions developed in section 3.3 brings to light the fact that the set of pseudo prime tests performed both in the classic Jacobi-Sum test as described in [ARP] and [CoLe] as well as in the cyclotomy test of [BovdH] is slightly redundant. Using equivalence conditions for the existence of combined cyclotomic extensions, we establish the exact size of this set. The difference, of course, is practically negligible. The equivalence conditions of section 3.2 have the advantage of pointing out the exact limitations of the cyclotomy approach. The duality between primality proving and factoring cyclotomic polynomials is materialized in proposing a new algorithm for factoring cyclotomic polynomials over finite fields in section 4.4. This algorithm combines the use of the Lucas-Lehmer approach which was common for former algorithms ([AdLe]) – to the one using Jacobi-Sums and is more efficient due to the later. In section 4.5 we treat the slightly exotic topic of the economy of random bits used for constructing working extensions. A motivation for this question came from the necessity of comparing in a measurable way random algorithms like the elliptic curve test – which make extensive use of randomized trials and the random cyclotomy test. The latter only uses random trials for building working extensions. We show that these trials can also be reduced to a minimum by using the Jacobi-Sum factoring method for cyclotomic polynomials. A more formal motivation for this topic may be found in a paper of Bach: [Ba1].

The last chapter introduces a totally new approach for combining elliptic curve and cyclotomy tests. It results in the reduction of the parameter s to $O(\log \sqrt[4]{n})$, thus bellow the results of [Le4]. Appendix A describes the implementation theory and algorithms for the deterministic variant of the test. Appendix B is a reprint of a paper concerning the generation of provable primes for cryptographic purposes. In this paper, we showed that provable primes may be generated more efficiently than pseudo primes. This is done without loss of cryptographic security in spite of the biased distributions of the primes produced.

The thesis concludes with Appendix C by making a step back to classical Lucas-Lehmer tests. We treat the classical tests from the perspective of the cyclotomy test, while keeping their specific methods – namely recursive sequences. In particular, we define generalized Lucas - Lehmer sequences of arbitrary order. These sequences permit to formulate the cyclotomy test in terms of recurrent sequences.

HORA is a traditional solar dance.
It is danced by men and women of
a village in a large circle. A
man or a woman at the center
splits the circle and chooses a partner ...

Dictionary

Chapter 2

Gauss Periods and Sums; Jacobi-Sums

The central question of cyclotomy of finite rings $(\mathbb{Z}/n \cdot \mathbb{Z})$ is the one of splitting the cyclotomic polynomial $\Phi_s(x)$ over $(\mathbb{Z}/n \cdot \mathbb{Z})$. Thus, the notion of primitive root of unity plays an important role. Since the splitting may not be unique, some care is necessary for defining the notion of primitive root of unity itself. We do this in §2.1.

The polynomial $\Phi_s(x)$ is cyclic and thus, when solving the equation $\Phi_s(x) = 0$, Lagrange Resolvents may used. The special resolvents arising in this case are called Gauss-Sums. The invariants associated with the Lagrange Resolvents are the Jacobi-Sums. Gauss and Jacobi-Sums are rich in properties, which are treated generally over fields ([La1]) and need to be reformulated in the context of the cyclotomy of rings ([Le2], [BovdH]). We develop these properties in §2.2.

In §2.3 we treat, for the sake of completeness, the Gauss and Jacobi-Sums of characters of prime power conductors. This leads to new, closed formulae, both over fields and rings.

Jacobi-Sums are simple objects, obtained by summing up roots of unity over a summation domain defined by their conductor. When the conductor is large, however, these sums become cumbersome. In §2.4 we give a new algorithm for computing Jacobi-Sums. The algorithm uses lattice reduction ([LLL], [Ka]) and is polynomial in the logarithm of the conductor. Throughout this thesis, *ring* will denote a commutative ring with 1.

2.1 Roots of unity and p-adic numbers

We start with some definitions.

Definition 2.1 *Let* $\mathbf{A}$ *be a ring. Let* $k > 1$ *be an integer such that* $k \cdot 1 \in \mathbf{A}^*$*, with* $\mathbf{A}^*$ *the group of the units in* $\mathbf{A}$*; we shall call an element* $\zeta \in A$ *a* $k-$th primitive root of unity *if* $\Phi_k(\zeta) = 0$*, where* Φ_k *is the* $k-$th *cyclotomic polynomial.*

Note that for $\mathbf{A}$ some algebraic closure of the ring $\mathbb{Z}$ of rational integers, the $k-$th complex roots of unity satisfy (2.1). Furthermore, if ζ' is a complex $k-$th primitive root of unity, there is a ring homomorphism $\nu : \mathbb{Z}[\zeta'] \to \mathbf{A}$, defined by $\nu(\zeta') = \zeta$.

Since $\prod_{i=1}^{k} (1-\zeta^i) \;=\; k$, we have

$$\nu\left(\prod_{i=1}^{k} (1-\zeta'^i)\right) \;=\; \prod_{i=1}^{k} (1-\zeta^i) \;=\; k \cdot 1 \;\in\; \mathbf{A}^*$$

Consequently $(1-\zeta^i) \in \mathbf{A}^*$ and $\nu(1-\zeta'^k) = 1-\zeta^k = 0$. Thus $\zeta \in \mathbf{A}^*$ and it generates a cyclic group with order dividing k; since $(1-\zeta^i) \in \mathbf{A}^*$ for $i < k$, the order is precisely k. If $k = h \cdot l$, then $\Phi_l(\zeta'^h) = 0$, and $\nu(\Phi_l(\zeta'^h)) = \Phi_l(\zeta^h) = 0$ and $l \cdot 1 \in \mathbf{A}^*$; ζ^h is thus a primitive $l-$th root of unity. We have proved:

Lemma 2.2 *Let $\mathbf{A}$ be a ring. Let $k > 1$ be an integer such that $k \cdot 1 \in \mathbf{A}^*$ and $\zeta \in A$ a* $k-$th primitive root of unity *defined as above. Then:*

(i) $\zeta \in \mathbf{A}^*$ *and it generates a cyclic group* $< \zeta >$ *of order* k.

(ii) $(1-\zeta^i) \in \mathbf{A}^*$ *for* $i = 1, 2, \ldots, k-1$.

(iii) if $k = h \cdot l$, *then* ζ^h *is a primitive* $l-$th *root of unity.*

Note that $< \zeta >$ does not in general contain all the zeroes of $\Phi_k(x)$ in $\mathbf{A}$, since the factorization of $\Phi_k(x)$ may not be unique in $\mathbf{A}$. The condition $\zeta^k = 1$ and $\zeta^d \neq 1$ for all divisors $d|k, 1 < d < k$ (which is (i) of the preceding Lemma) does not define in general primitive $k-$th roots of unity in $\mathbf{A}$ either, since there are rings $\mathbf{A}$ and elements $\zeta \in \mathbf{A}^*$ such that (i) is satisfied but (ii) is not. The situation is made clear by the following example, which shows that primitive roots of unity are in general not closed under multiplication.

Example 2.3 *If* $\mathbf{R} = (\mathbb{Z}/21 \cdot \mathbb{Z})$ *and* $\mathbf{A} = \mathbf{R}[x]/(\Phi_5(x))$, *let ξ be the image of x in $\mathbf{A}$ and $\zeta = 15 + 7 \cdot \xi$, so that $\zeta \cong \xi$ mod 3 and $\zeta \cong 1$ mod 7. By the Chinese remainder theorem, ζ satisfies (i) with $k = 5$, but $(1-\zeta) \notin \mathbf{A}^*$. Also $\Phi_5(\xi) = 12$. Note that $\zeta = \xi^3 \cdot (15 \cdot \xi^2 + 7 \cdot \xi^3)$: while both factors are primitive, as can be seen by a simple computation, the product is not.*

One can, however, prove by using the definition of cyclotomic polynomials, the following:

Lemma 2.4 *Let $\mathbf{A}$ be a ring with 1. Let $k > 1$ be an integer such that $k \cdot 1 \in \mathbf{A}^*$ and $\zeta \in \mathbf{A}$ be such that*

(i') $\zeta \in \mathbf{A}^*$ *and it generates a cyclic group* $< \zeta >$ *of order* k.

(ii') $(1-\zeta^{k/p}) \in \mathbf{A}^*$ *for all primes* $p|k$.

Then ζ is a $k-$th primitive root of unity. Furthermore, if $k = h \cdot l$, then ζ^h is a primitive $l-$th root of unity.

Proof If $g(x) = x^k - 1$, then $g(\zeta) = \Phi_k(\zeta) \cdot v$, where v is a product of units in $\mathbf{A}$ (this is a consequence of (ii') and the Möbius - formula for Φ_k). Since $g(\zeta) = 0$ by (i'), it follows that $\Phi_k(\zeta) = 0$ and ζ is a $k-$th primitive root of unity. The second assertion is a consequence of Lemma 2.2. □

Primitive roots of unity ζ have the property:

$$S \;=\; \sum_{x \in <\zeta>} x \;=\; 0. \tag{2.5}$$

This follows from $\zeta \cdot S = S$ and $(1 - \zeta)$ being a unit in $\mathbf{A}$. Note again that (2.5) is not true, if ζ satisfies (i') but not (ii') of Lemma (2.4). Suppose there is an $m \in \mathbb{N}_{>0}$ such that $m \cdot \mathbf{A} \;=\; \{0\}$ and let $n > 1$ be a positive integer with the property that

$$n \;=\; \min\{m \in \mathbb{N}_{>0} \;:\; m \cdot \mathbf{A} = \{0\}\}. \tag{2.6}$$

In this case n is called the minimal annihilator of $\mathbf{A}$. The ring $\mathbf{R} = (\mathbb{Z}/q^v \cdot \mathbb{Z})$ is a *local ring* and for all integers $d > 0$ there is exactly one galois extension $\mathbf{R}(q, v, d)$ of $(\mathbb{Z}/q^v \cdot \mathbb{Z})$ which is called a *galois ring* of degree d over $(\mathbb{Z}/q^v \cdot \mathbb{Z})$. For a proof, let f, g be irreducible polynomials of degree d over $(\mathbb{Z}/q^v \cdot \mathbb{Z})$; by Hensel's lemma, their images $f_0 = f \bmod q$ and $g_0 = g \bmod q$ in $\mathbb{F}_q$ are also irreducible and there is a field isomorphism $\sigma : \mathbb{F}_q[x]/(f_0(x)) \to \mathbb{F}_q[x]/(g_0(x))$. If ξ, ζ are the images of x in the two fields, respectively, let $p(x) \in \mathbb{F}_q[x]$ be the monic polynomial of degree $\deg(p) \leq d$ such that $\sigma(\xi) = p(\zeta)$; then $f_0(p(\zeta)) = 0 \mod g_0(x)$, or

$$f_0(p(x)) - h(x)\; g_0(x) = 0 \tag{2.7}$$

for some polynomial $h(x) \in \mathbb{F}_q[x]$ of degree $\deg(h) \leq d(d-1)$. the proof follows, if we can lift the polynomials $p(x)$ and $h(x)$ to $(\mathbb{Z}/q^v \cdot \mathbb{Z})$. Using the Hensel lemma ([Zip], Proposition 124, page 272), this is the case, if the Jacobian of the equation (2.7), considered as a nonlinear system in the unknown coefficients of $p(x)$ and $h(x)$ does not vanish over $\mathbb{F}_q$. In fact, after some algebraic manipulations, the Jacobian turns out to equal the resultant $\mathcal{R}(g_0(x), f_0'(p(x)))$ of the polynomial $g_0(x)$ and the derivative of f_0 at $p(x)$. Since $g_0(x)$ is irreducible and $f_0(x)$ separable, the two polynomials have no common factor, the resultant is nonzero and so is the Jacobian.

If $q^{v(q)} \parallel n$ are the prime powers dividing n and $\mathbf{A}_q$ is given by $\mathbf{A}_q = \mathbf{A}/(q^{v(q)} \cdot \mathbf{A})$, if $n \neq q^{v(q)}$ and $\mathbf{A}_q = \mathbf{A}$ otherwise, then the Chinese remainder theorem [La2], p.11 shows that $\mathbf{A} \;=\; \prod_{q|n} \; \mathbf{A}_q$. Furthermore, if $\mathbf{A}_q$ is an algebraic extension of $(\mathbb{Z}/q^v \cdot \mathbb{Z})$, then it is a direct sum of galois rings. We now show that localization is an efficient method for the use of primitive roots of unity, since in a galois ring, all roots of unity are primitive.

Lemma 2.8 *Let q be a prime, $\mathbf{A} = \mathbf{R}(q, v, d)$ be the galois ring of degree d containing $(\mathbb{Z}/q^v \cdot \mathbb{Z})$ for some $v > 1$ and let $\alpha \in \mathbf{A}$ generate a cyclic group of index k, with $(k, q) \;=\; 1$. Then α is a primitive $k-$th root of unity.*

Proof Let $t = \mathrm{ord}_{\varphi(k)}(q)$. It is a simple consequence of Hensel's lemma, that $\Phi_k(x)$ splits over $(\mathbb{Z}/q^v \cdot \mathbb{Z})$ in $\varphi(k)/t$ irreducible polynomials of degree t. The primitive $k-$th roots of unity over $(\mathbb{Z}/q^v \cdot \mathbb{Z})$ are thus elements of the galois ring of degree t. By the hypothesis, there is a map $\sigma : \mathbb{Z}[\zeta_k] \rightarrow \mathbf{A}$ defined by $\sigma\ \zeta_k = \alpha$. This map can be continued by reduction modulo q to a map $\sigma_0 : \mathbb{Z}[\zeta_k] \rightarrow \mathbb{F}_{q^t}$. Since $\sigma_0(\mathbb{Z}[\zeta_k])$ is an extension of degree t, it follows by comparing degrees, that $t|d$ and finally, $\mathbf{A} = \mathbf{R}(q, v, d)$ is an extension of degree d/t of $\sigma(\mathbb{Z}[\zeta_k]) = \mathbf{R}(q, v, d)$. In particular, α is a primitive root of unity, being an element of the subring $\sigma(\mathbb{Z}[\zeta_k])$. □

It is now obvious that an algebraic extension $\mathbf{A}$ of $(\mathbb{Z}/n \cdot \mathbb{Z})$ can be written as direct sum of galois rings and the $k-$th roots of unity in these extensions will be direct sums of primitive $k-$th roots of unity, in the single galois rings.

It will be useful to recall some elementary facts about p-adic numbers. A p-adic integer is a sequence $(a_i)_{i\in\mathbb{N}}$ with $a_i \in (\mathbb{Z}/p^i \cdot \mathbb{Z})$ and $a_{i+1} = a_i \bmod p^i$. The set of p-adic integers forms a ring $\mathbb{Z}_p$ which contains $\mathbb{Z}$ as a subring - $\mathbb{Z}$ corresponding to the subring of p-adic integers represented by sequences $\mathbf{a} = (a_i)_{i\in\mathbb{N}}$ with $a_i = z \bmod p^i$, z being the rational integer to be represented. There is also a unique representation of p-adic integers of the form:

$$\mathbf{a} = \sum_{m\in\mathbb{N}} a_m \cdot p^m, \quad \text{with } 0 \leq a_m < p. \tag{2.9}$$

The sum in (2.9) can be regarded either as a formal power series or as a series converging under the p-adic metric. The following properties of $\mathbb{Z}_p$ are commonly used:

$$\mathbb{Z}_p/(p^m \cdot \mathbb{Z}_p) \cong \mathbb{Z}/(p^m \cdot \mathbb{Z}). \tag{2.10}$$

The units in $\mathbb{Z}_p$ are $\mathbb{Z}_p^* = \mathbb{Z}_p - p \cdot \mathbb{Z}_p$ and have the following properties([Se]):

$$\mathbb{Z}_p^* \cong ((\mathbb{Z}/(p-1) \cdot \mathbb{Z})) \times (1 + p \cdot \mathbb{Z}_p), \qquad \text{for } p > 2. \tag{2.11}$$

$$\mathbb{Z}_2^* = \{-1, 1\} \times (1 + 4 \cdot \mathbb{Z}_2) = <\mathbf{5}> \cup \{-<\mathbf{5}>\}. \tag{2.12}$$

$$\forall\, \mathbf{a} \in \mathbb{Z}_p, \quad \exists m \geq 0 \ \text{ and } u \in \mathbb{Z}_p^* \text{ such that } \mathbf{a} = p^m u. \tag{2.13}$$

We write $v_p(\mathbf{a}) = m$; v_p is called the p-adic *valuation*. We shall be particularly interested in the multiplicative group generated by p-adic units. We have :

Lemma 2.14 *(i)* $\mathbf{a}^{\mathbb{Z}_p} = 1 + p^m \cdot \mathbb{Z}_p$, *for* $p \geq 2$, *if* $m = v_p(\mathbf{a} - 1) \geq 1$.

(ii) $\mathbf{a}^{\mathbb{Z}_2} = 1 + 2^m \cdot \mathbb{Z}_2$, *if* $m = v_2(\mathbf{a} - 1) \geq 2$.

(iii) $\mathbf{a}^{\mathbb{Z}_p} = (1 + p^\mu \cdot \mathbb{Z}_p) \times <\mathbf{a} \bmod p^\mu>$,
if $v_p(\mathbf{a} - 1) = 0$, $t = \mathrm{ord}_p(\mathbf{a})$ *and* $\mu = v_p(\mathbf{a}^t - 1)$.

(iv) $\mathbf{a}^{\mathbb{Z}_2} = (1 + 2^m \cdot \mathbb{Z}_2) \cup (\mathbf{a} + 2^m \cdot \mathbb{Z}_2)$, *if* $v_2(\mathbf{a} - 1) = 1$ *and* $v_2(\mathbf{a} + 1) = m$.

Proof Let $p \geq 3$, $v_p(\mathbf{a}-1) = m \geq 1$ and $\mathbf{b} \in 1 + p^m \cdot \mathbb{Z}_p$, $n > m$. It is easy to check that $\mathbf{a}$ has order p^{n-m} in the group $\mathbb{Z}_p/(p^n \cdot \mathbb{Z}_p)$, and consequently generates all the elements $\mathbf{x} \in \mathbb{Z}_p/(p^n \cdot \mathbb{Z}_p)$ with $v_p(\mathbf{x}-1) \geq m$. Let $l = l(n-m)$ be such that $\mathbf{a}^l = \mathbf{b}_n \bmod p^n \cdot \mathbb{Z}_p$. Then $\mathbf{a}^{l\cdot(n-m+1)} = \mathbf{b}_{n+1} \bmod p^{n+1} \cdot \mathbb{Z}_p = \mathbf{b}_n \bmod p^n \cdot \mathbb{Z}_p$ and since $\mathbf{a}$ has order p^{n-m} in $\mathbb{Z}_p/(p^m \cdot \mathbb{Z}_p)$, it follows that $l(n-m+1) = l(n-m) \bmod p^{n-m} \cdot \mathbb{Z}_p$.

This shows that there is a p-adic number $\mathbf{l} \in \mathbb{Z}_p$ such that $\mathbf{a}^{\mathbf{l}} = \mathbf{b}$, which is (i). Assertion (iii) follows by putting $\alpha = \mathbf{a}^t$, where $t = \mathrm{ord}_p(\mathbf{a})$ and applying (i) to α. The anomalies for the case $p = 2$ are a consequence of $(\mathbb{Z}/2^k \cdot \mathbb{Z})^*$ not being a cyclic group for $k \geq 2$; (ii) can be proved by a similar reasoning as (i), while (iv) follows from $\mathbf{a}^2 = 1 \bmod 2^{m+1}$ and (ii). □

As a general rule, we have :

$$\begin{aligned} v_p(\mathbf{a}^p - 1) &= 1 + v_p(\mathbf{a}-1), \\ & \quad \text{for } v_p(\mathbf{a}-1) \geq 1,\ p \geq 3 \text{ and for } v_p(\mathbf{a}-1) \geq 2,\ p = 2. \\ v_2(\mathbf{a}^2 - 1) &= v_2(\mathbf{a}-1) + v_2(\mathbf{a}+1),\ \text{ if } v_2(\mathbf{a}-1) = 1, p = 2. \end{aligned} \tag{2.15}$$

2.2 General properties of Gauss and Jacobi-Sums

Let $m > 1$ be an integer and let $\lambda(m)$ be the exponent of $(\mathbb{Z}/m \cdot \mathbb{Z})^*$, where λ is the Carmichael function. In this section, $u = \lambda(m)$ and f will be some divisor of u. Let $\mathbf{A}$ be a ring and suppose that $m \cdot 1$ and $u \cdot 1 \in \mathbf{A}^*$ and $\mathbf{A}$ contains two primitive roots of unity ζ and ξ of respective orders u and m. A multiplicative character $\chi : (\mathbb{Z}/m \cdot \mathbb{Z})^* \to <\zeta>$ is a multiplicative group homomorphism $(\mathbb{Z}/m \cdot \mathbb{Z})^* \to <\zeta>$. We denote by $(\mathbb{Z}/m \cdot \mathbb{Z})^\perp$ the set of multiplicative characters defined on $(\mathbb{Z}/m \cdot \mathbb{Z})^*$; $(\mathbb{Z}/m \cdot \mathbb{Z})^\perp$ is a multiplicative group and the order of χ is the cardinality of $Im(\chi)$. We shall also denote characters $\chi \in (\mathbb{Z}/m \cdot \mathbb{Z})^\perp$ by characters modulo m.

Let $\chi \in (\mathbb{Z}/m \cdot \mathbb{Z})^\perp$ and d be a divisor of m. If there is a character

$$\chi' : (\mathbb{Z}/(m/d) \cdot \mathbb{Z})^* \to <\zeta>$$

such that

$$\chi(x) = \chi'(x \mod (m/d)) \text{ for all } x \in (\mathbb{Z}/m \cdot \mathbb{Z})^*,$$

then χ is said to be *induced* by χ'.

A character $\chi : (\mathbb{Z}/m \cdot \mathbb{Z})^* \to <\zeta>$ is called *primitive* if it is induced by no character different from itself; in this case, m is called the *conductor* of χ. Each character χ is induced by a unique primitive character χ' and the conductor of χ is defined to be equal to the conductor of the primitive character it is induced by. In particular, the principal character $\mathbf{1} : \{1\} \to <1>$ is primitive and has conductor 1.

If $\chi \in (\mathbb{Z}/m \cdot \mathbb{Z})^\perp$, the *Gauss-Sum* of χ with respect to x is the element of $\mathbf{A}$ given by:

$$\tau(\chi) = \sum_{x \in (\mathbb{Z}/m \cdot \mathbb{Z})^*} \chi(x) \cdot \xi^x. \tag{2.16}$$

The Gauss-Sum depends upon the choice of an element in $< \xi >$ according to:

$$\tau_a(\chi) \;=\; \sum_{x\in(\mathbb{Z}/m\cdot\mathbb{Z})^*} \chi(x)\cdot\xi^{a\cdot x} \;=\; \chi^{-1}(a)\cdot\tau(\chi), \qquad \forall\, a\in(\mathbb{Z}/m\cdot\mathbb{Z})^*. \tag{2.17}$$

If $\nu \in (\mathbb{Z}/m\cdot\mathbb{Z})^*$ and $H(\nu) = (\mathbb{Z}/m\cdot\mathbb{Z})^* \;/\; < \nu \bmod m >$ and h is a coset in $H(\nu)$, then the $h-$th *Gauss Period* with respect to ν is defined by:

$$\eta_h(\xi,\nu) \;=\; \sum_{\mu\in h} \xi^{\mu}, \qquad \forall\, h\in H(\nu). \tag{2.18}$$

Let $H(\nu)^{\perp} = \{\chi \in (\mathbb{Z}/m\cdot\mathbb{Z})^{\perp} \mid \chi(\nu) = 1\}$. $H(\nu)^{\perp}$ is dual to $H(\nu)$ in the sense that characters $\chi \in H(\nu)^{\perp}$ operate on cosets $h \in H(\nu)$. Gauss-Sums and Gauss Periods are connected by:

$$\tau(\chi) = \sum_{h\in H(\nu)} \chi(h)\cdot\eta_h(\xi,\nu) \tag{2.19}$$

and

$$\mid H(\nu)\mid \;\cdot\; \eta_h(\xi,\nu) \;=\; \sum_{\chi\in H(\nu)^{\perp}} \chi^{-1}(h)\cdot\tau(\chi), \qquad \forall\, h\in H(\nu). \tag{2.20}$$

Equation (2.19) follows by using $\chi(\nu) = 1$ and regrouping the summation order in (2.16). The equality (2.20) is a consequence of following:

Lemma 2.21 *If G is a subgroup of $(\mathbb{Z}/m\cdot\mathbb{Z})^{\perp}$ and $x \in (\mathbb{Z}/m\cdot\mathbb{Z})^*$, then*

$$s(x) \;=\; \sum_{\chi\in G} \chi(x) \;=\; \begin{cases} 0, & \textit{if} \quad \exists\chi\in G \textit{ with } \chi(x)\neq 1, \\ \mid G\mid, & \textit{otherwise.} \end{cases} \tag{2.22}$$

Proof If $\chi(x) = 1$ for all $\chi \in G$, the statement is trivial. Otherwise, let $\chi_0 \in G$ be such that $\chi_0(x) \neq 1$ and thus the root of unity $\chi_0(x)$ has order 2 by (2.2) (iii). By multiplication of $s(x)$ with $\chi_0(x)$ we get: $\chi_0(x)\cdot s(x) = \sum_{\chi\in G} \chi_0(x)\cdot\chi(x)$; since G is a group, the last sum is equal to $s(x)$ and consequently $s(x)\cdot(\chi_0(x)-1) = 0$ and $s(x) = 0$, since $(\chi_0(x) - 1)$ is a unit in $\mathbf{A}$, by (2.2) (ii). □

If $\chi, \chi' \in (\mathbb{Z}/m\cdot\mathbb{Z})^{\perp}$ are primitive, the *Jacobi-Sum* $j(\chi,\chi')$ is defined by:

$$j(\chi,\chi') \;=\; \sum_{x,(1-x)\in(\mathbb{Z}/m\cdot\mathbb{Z})^*} \chi(x)\cdot\chi'(1-x). \tag{2.23}$$

Gauss and Jacobi-Sums factor with respect to the ideals $(p^{v(p)}\cdot(\mathbb{Z}/m\cdot\mathbb{Z}))$ of $(\mathbb{Z}/m\cdot\mathbb{Z})$, where $p^{v(p)} \parallel m$, as shown by:

Lemma 2.24 *Let $\chi \in (\mathbb{Z}/m\cdot\mathbb{Z})^{\perp}$ and $m = \prod_{p|m} p^{v(p)}$. Then there are characters $\chi_p \in (\mathbb{Z}/p^{v(p)}\cdot\mathbb{Z})^{\perp}$ and Gauss-Sums $\tau_p(\chi_p)$ such that:*

$$\tau(\chi) \;=\; \prod_{p|m} \tau_p(\chi_p). \tag{2.25}$$

If $\chi',\ \chi'' \in (\mathbb{Z}/m\cdot\mathbb{Z})^{\perp}$, then there are characters $\chi'_p,\ \chi''_p \in (\mathbb{Z}/p^{v(p)}\cdot\mathbb{Z})^{\perp}$ and Jacobi-Sums $j_p(\chi'_p, \chi''_p)$ such that:

$$j(\chi', \chi'') \;=\; \prod_{p|m} j_p(\chi'_p, \chi''_p). \tag{2.26}$$

Proof By the Chinese remainder theorem, there is a multiplicative isomorphism

$$\varphi \;:\; (\mathbb{Z}/m\cdot\mathbb{Z}) \;\rightarrow\; G = \prod_{p|m} (\mathbb{Z}/p^{v(p)}\cdot\mathbb{Z}). \tag{2.27}$$

Every $x_p \in (\mathbb{Z}/p^{v(p)}\cdot\mathbb{Z})$ can be lifted to an element $l_p(x_p) \in (\mathbb{Z}/m\cdot\mathbb{Z})$ such that $l_p(x_p) = x_p \bmod p^{v(p)}$ and $l_p(x_p) \bmod q^{v(q)} = 1$ for all primes $q \mid m,\ q \neq p$. Let further $\{e_p\}$ be a base for G, such that $e_p = 1 \bmod p^{v(p)}$ and $e_p = 0 \bmod q^{v(q)}$ for all primes $q \mid m,\ q \neq p$. Consequently, $x = \sum_{p|m} e_p \cdot (x \bmod p^{v(p)})$, where $(x \bmod p^{v(p)})$ is regarded as an element of $(\mathbb{Z}/m\cdot\mathbb{Z})$, with value less than $p^{v(p)}$. If the characters χ_p are defined by $\chi_p(x) = \chi(l_p(x)),\ \forall\, x \in (\mathbb{Z}/p^{v(p)}\cdot\mathbb{Z})^*$, then χ splits according to:

$$\chi(x) = \prod_{p|m} \chi_p(x \bmod p^{v(p)}),\ \forall x\, \in (\mathbb{Z}/m\cdot\mathbb{Z})^*.$$

Using the shorthand $x_p = (x \bmod p^{v(p)})$, the Gauss-Sum splits accordingly:

$$\tau(\chi) \;=\; \sum_{x\in(\mathbb{Z}/m\cdot\mathbb{Z})^*} \chi(x)\cdot\xi^x \;=\; \sum_{x\in G}\prod_{p|m} \chi_p(x_p)\cdot\xi^{\mathbf{x}\cdot\mathbf{e}}$$

where $\mathbf{e} = (e_p)_{p|m}$ and $\mathbf{x}\cdot\mathbf{e} = \sum_{p|m} x_p\cdot e_p$. After changing the order of summation, we get:

$$\tau(\chi) \;=\; \sum_{x\in(\mathbb{Z}/m\cdot\mathbb{Z})^*} \left(\prod_{p|m} \chi_p(x_p)\cdot\xi^{x_p\cdot e_p}\right) \;=\; \prod_{p|m}\left(\sum_{x_p} \chi_p(x_p)\cdot\xi^{x_p\cdot e_p}\right) \;=\; \prod_{p|m}\tau_p(\chi_p).$$

Note that the $p^{v(p)}-$th roots of unity used in the definition of $\tau_p(\chi_p)$ are ξ^{e_p}. The proof of (2.26) is similar. □

We state two formulae, which are known for prime characters of prime conductors. Their proof will be given in §2.3, where we let the conductor be built up from prime powers. If χ is a primitive character, the absolute value of its Gauss-Sum is determined by:

$$\tau(\chi)\cdot\tau(\chi^{-1}) \;=\; \chi(-1)\cdot m. \tag{2.28}$$

Gauss and Jacobi-Sums are connected by:

$$j(\chi, \chi')\cdot\tau(\chi\cdot\chi') \;=\; \tau(\chi)\cdot\tau(\chi'), \qquad \text{if } \chi,\ \chi' \text{ and } \chi\cdot\chi' \text{ are primitive.} \tag{2.29}$$

If χ is a character of conductor q and order p^k, the above relation yields a simple formula for computing the field invariants $\tau(\chi)^\nu/\tau(\chi^\nu),\ \nu = 2,\ldots,p^k-1$. Let the *multiple Jacobi-Sums* J_ν be defined by:

$$\begin{aligned} J_1 &= 1 \\ J_{\nu+1} &= J_\nu\cdot j(\chi,\chi^\nu), \qquad \text{for } \nu = 1,2,\ldots,p^k-2 \\ J_{p^k} &= \chi(-1)\cdot q\cdot J_{p^k-1} \end{aligned} \tag{2.30}$$

It is easy to verify by induction that:

$$J_\nu \;=\; \frac{\tau(\chi)^\nu}{\tau(\chi^\nu)}, \qquad \text{for } \nu = 1, 2, \ldots, p^k, \text{ where } \tau(\chi^{p^k}) = 1. \tag{2.31}$$

The Chinese Remainder Theorem can be used for expressing the Gauss-Sum of a character χ as a product of Gauss-Sums of characters of prime power orders.

Lemma 2.32 *Let χ be a primitive character of conductor m and order $f = h \cdot k$ with $(h, k) = 1$. Then there are two characters χ_i $(i = 1, 2)$ of conductor m and orders h and k respectively, such that:*

$$\tau(\chi) \;=\; \tau(\chi_1) \cdot \tau(\chi_2) \cdot j(\chi_1, \chi_2)^{-1}.$$

Proof Let s and t be such that $s \cdot h + t \cdot k = 1$ and define $\chi_1 = \chi^{t \cdot k}$ and $\chi_2 = \chi^{s \cdot h}$, so that $\chi_1 \cdot \chi_2 = \chi$. The assertion of the lemma is a consequence of (2.29). □

If m is a prime power, $\nu \in (\mathbb{Z}/m \cdot \mathbb{Z})^*$ and t and f are such that $t = \mathrm{ord}_q(\nu)$ and $f = \varphi(m)/t$, then $H(\nu) = (\mathbb{Z}/m \cdot \mathbb{Z})^* \; / \; < \nu \bmod q >$ is a cyclic group isomorphic to $\{g^{t \cdot i} \mid i = 1, 2, \ldots, f\}$, where g is a generator of $(\mathbb{Z}/m \cdot \mathbb{Z})^*$. With ξ a primitive $m-$th root of unity, the relations (2.18) – (2.20) can be rewritten explicitly as:

$$\eta_j(\xi, \nu) \;=\; \sum_{i=1}^{t} \xi^{g^{t \cdot j} \cdot \nu^i} \text{ for } j = 1, 2, \ldots, f. \tag{2.33}$$

$$\tau(\chi) \;=\; \sum_{j=1}^{f} \eta_j(\xi, \nu) \cdot \chi(g^{t \cdot j}), \quad \forall\, \chi \in H(\nu)^\perp. \tag{2.34}$$

$$f \cdot \eta_j(\xi, \nu) \;=\; \sum_{j=1}^{f} \chi^{-1}(g^{t \cdot j}) \cdot \tau(\chi^i) \quad \text{for } j = 1, 2, \ldots, f. \tag{2.35}$$

It follows from (2.35), that the Gauss-Sums $\tau(\chi), \chi \in H(\nu)^\perp$ are *Lagrange resolvents* for the Gauss Periods $\eta_j(\xi, \nu)$. In this context, one can interpret (2.19) as a generalization of Lagrange resolvents to abelian extensions. We shall see in the next chapter, that Gauss Periods generate intermediate extensions in cyclotomic fields. The Gauss-Sums can be used to calculate the periods and thus to generate intermediate cyclotomic fields. We now consider the case when $\mathbf{A}$ is a finite field of characteristic r. Let again $m = p^k$ be a prime power, χ a primitive character of conductor m and order f; $\zeta, \xi \in \mathbf{A}$ are primitive roots of unity, with respective orders f and m. We investigate the action of the automorphism $x \to x^r$ of $\mathbf{A}$ upon $\tau(\chi)$:

$$\tau(\chi)^r \;=\; \sum_x \left(\chi(x) \cdot \xi^x\right)^r \;=\; \sum_x \chi^r(x) \cdot \xi^{r \cdot x}.$$

By using (2.17) we have:

$$\tau(\chi)^r \;=\; \chi^{-r}(r) \cdot \tau(\chi^r). \tag{2.36}$$

By iteration of (2.36), we get:

$$\tau(\chi)^{r^k} = \chi^{-k\cdot r^k}(r)\cdot\tau(\chi^{r^k}), \text{ for } k\geq 1\ , \tag{2.37}$$

and if $r^t = 1 \bmod f$,

$$\tau(\chi)^{r^t-1} = \chi^{-t}(r). \tag{2.38}$$

The relations (2.36) and (2.38) are central in primality testing. It will be important to have efficient computing methods for powers of Gauss-Sums and for Jacobi-Sums, if they are to be used in practical algorithms.

2.3 Characters of prime power order

Lemma (2.24) allows us to proceed with the study of Gauss and Jacobi-Sums considering characters of a prime power conductor. We shall put in this section $m = p^k$, where p is a prime. A character $\chi\in(\mathbb{Z}/m\cdot\mathbb{Z})^{\perp}$ is primitive iff $p^{k-1}\mid \mathrm{ord}(\chi)$, for odd p and $k>1$ and iff $2^{k-2}\mid\mathrm{ord}(\chi)$, for $p=2$ and $k>2$. If χ is primitive, its absolute value is given by (2.28). Otherwise,

$$\tau(\chi) = \mu(m) \quad \text{with } \mu \text{ the Möbius function.} \tag{2.39}$$

The formulae (2.28), (2.29) and (2.39) are commonly known for $k=1$. We shall now prove them for $k>1$:

Theorem 2.40 *Let $m = p^k$, with $k>1$ be a prime power, χ,χ' be two characters of conductor m, such that χ, χ' and $\chi\cdot\chi'$ are primitive. Then*

$$\tau(\chi) = \mu(m) \quad \textit{and,} \tag{2.41}$$

$$j(\chi,\chi')\cdot\tau(\chi\cdot\chi') = \tau(\chi)\cdot\tau(\chi') \tag{2.42}$$

Proof Let $k>1$, p be odd and χ not primitive – thus $\chi^{\varphi(m/p)}(x)=1$, $\forall x\in(\mathbb{Z}/m\cdot\mathbb{Z})^{\perp}$. If g is a generator of $(\mathbb{Z}/m\cdot\mathbb{Z})^{\perp}$, then the cyclic group generated by $g^{\varphi(m/p)}$ is:

$$< g^{\varphi(m/p)} > = \{1+m\cdot p^{k-1}\mid m\in(\mathbb{Z}/p\cdot\mathbb{Z})^*\}.$$

Using this remark, we split the summation of the Gauss-Sum and get:

$$\begin{aligned}\tau(\chi) &= \sum_{\lambda\in(\mathbb{Z}/p^{k-1}\cdot\mathbb{Z})^*}\xi^{\lambda}\cdot\Big(\sum_{\mu=1}^{p}\chi(\lambda\cdot(1+\mu\cdot p^{k-1}))\cdot\xi^{\lambda\cdot\mu\cdot p^{k-1}}\Big)\\ &= \sum_{\lambda}\chi(\lambda)\cdot\xi^{\lambda}\cdot\Big(\sum_{\mu=1}^{p}\chi(1+\mu\cdot p^{k-1})\cdot\xi^{\lambda\cdot\mu\cdot p^{k-1}}\Big)\end{aligned}$$

Since $\chi(1+\mu\cdot p^{k-1})=1$, the inner sum vanishes as a consequence of (2.5), which proves (2.39). If χ is primitive, then (2.28) follows by using (2.21). We shall now prove (2.29), which establishes the connection between Gauss and Jacobi-Sums:

$$j(\chi,\chi')\cdot\tau(\chi\cdot\chi') = \tau(\chi)\cdot\tau(\chi'), \quad \text{if } \chi,\chi' \text{ and } \chi\cdot\chi' \text{ are primitive.}$$

This formula is also well known for $k = 1$ and follows after some computation involving (2.22), if $k > 1$. Indeed, let p be any prime and $M = (\mathbb{Z}/m \cdot \mathbb{Z})$. Then

$$M_k = \{1 + a \cdot p^{k-1} \ : \ a \in ((m/p) \cdot M)^*\}$$

is a subgroup of M^* generated by $1 + p^{k-1}$. We use in this proof, for simplicity, the convention $\chi(x) = 0$ when $(x, m) > 1$ and χ is any primitive character in $(\mathbb{Z}/m \cdot \mathbb{Z})^{\perp}$.

$$\tau(\chi) \cdot \tau(\chi') \ = \ \sum_{x,y \in M^*} \xi^{x+y} \cdot \chi(x) \cdot \chi'(x) \ = \ \sum_{c \in M} \xi^c \ \cdot \ \Big(\sum_{x \in M^*} \chi(x) \cdot \chi'(c - x) \Big).$$

Put $s(c) = \sum_{x \in M^*} \chi(x) \cdot \chi'(c - x)$. If $c \in M^*$, one can substitute $x = c \cdot y$ with $y \in M^*$ and thus

$$\begin{aligned}
\tau(\chi) \cdot \tau(\chi') &= \sum_{c \in M^*} \xi^c \cdot s(c) + \sum_{c \notin M^*} \xi^c \cdot s(c) \\
&= \sum_{c \in M^*} \xi^c \cdot \Big(\sum_{y \in M^*} \chi(c) \cdot \chi'(c) \cdot \chi(y) \cdot \chi'(1 - y) \Big) \ + \ \sum_{c \notin M^*} \xi^c \cdot s(c) \\
&= \tau(\chi \cdot \chi') \cdot \jmath(\chi, \chi') \ + \ \sum_{c \notin M^*} \xi^c \cdot s(c).
\end{aligned}$$

We want to prove, that the second sum vanishes. If $Q = M/p^{k-1} \cdot M$, then

$$M_0 = M - M^* = \{x \in M \mid x = p \cdot y, y \in Q\}$$

and

$$\begin{aligned}
\sum_{c \notin M^*} \xi^c \cdot s(c) &= \sum_{a \in Q} \xi^{a \cdot p} \ \cdot \ \Big(\sum_{x \in M^*} \chi(x) \cdot \chi'(a \cdot p - x) \Big) \\
&= \sum_{x \in M^*} \chi(x) \cdot \chi'(x) \ \cdot \ \Big(\sum_{a \in Q} \xi^{a \cdot p} \cdot \chi'(x^{-1} \cdot a \cdot p - 1) \Big) \\
&= \sum_{x \in M^*} \chi(x) \cdot \chi'(x) \ \cdot \ \Big(\sum_{b \in Q} \xi^{b \cdot x \cdot p} \cdot \chi'(b \cdot p - 1) \Big), \qquad \text{where } b = a \cdot x^{-1}.
\end{aligned}$$

Let $v(x) = \sum_{b \in Q} \xi^{b \cdot x \cdot p} \cdot \chi'(b \cdot p - 1)$. Evidently, $v(x) = v(x')$ if $x = x' \bmod p^{k-1}$. We can group:

$$\sum_{c \notin M^*} \xi^c \cdot s(c) \ = \ \sum_{x \in Q^*} v(x) \cdot \Big(\sum_{a \in \{0, \ldots, p-1\}} \chi \cdot \chi'(a \cdot p^{k-1} + 1) \Big).$$

Since $\chi \cdot \chi'$ is a primitive character, the inner sum is

$$\sum_{a \in \{0, \ldots, p-1\}} \chi \cdot \chi'(a \cdot p^{k-1} + 1) \ = \ \sum_{x \in M_k} \chi \cdot \chi'(x)$$

and it vanishes by (2.5). For $p = k = 2$, there is only one primitive character χ with conductor $m = 4$ and $\chi \cdot \chi$ is not primitive, so the premises of (2.29) do not hold. This finishes our proof of (2.29). $\square$

We shall deduce subsequently some formulae for Gauss-Sums for characters of prime-power conductor. Suppose χ is primitive of conductor p^k, with p prime and $k > 1$. Let ζ_{p^k} and ζ_{p-1} be primitive p^k-th and $(p-1)-$th roots of unity in $\mathbf{A}$, respectively; by (2.2), $\zeta_{p^i} = \zeta_{p^k}^{p^{k-i}}$ for $i = 1, 2, \ldots, k-1$ are also primitive of order p^i. We shall require first that

$$\mathrm{Im}(\chi^{p-1}) \subset < \zeta_{p^k} > . \tag{2.43}$$

and derive a closed formula for Gauss-Sums under this assumption. Subsequently, we will drop this condition and generalize the formulae found.

We let first p be an odd prime and χ a primitive character of conductor $p^k, k > 1$. Let $[k/2] = l$, such that $k = 2 \cdot l$ or $k = 2 \cdot l + 1$. The group $G_l = \{1 + p^l \cdot a \mid a \in (\mathbb{Z}/p^{k-l} \cdot \mathbb{Z})\}$ is a cyclic subgroup of $(\mathbb{Z}/p^k \cdot \mathbb{Z})^*$ and, as a consequence of (2.43), there is a $v \in (\mathbb{Z}/p^{k-l} \cdot \mathbb{Z})^*$ such that

$$\chi(1 + v \cdot p^l) \cdot \zeta_{p^{k-l}} \; = \; 1 \tag{2.44}$$

This follows from the fact that χ is primitive and $\zeta_{p^{k-l}} \in \mathrm{Im}_{\chi}(G_l)$. Let now $u = v^{-1} \bmod p^l$. We regard u as a rational integer, $1 \leq u < p^l$ and obtain thus a unique embedding in $(\mathbb{Z}/p^k \cdot \mathbb{Z})^*$. Suppose first that $k = 2 \cdot l$. Then

$$\tau(\chi) \; = \sum_{t \in (\mathbb{Z}/p^l \cdot \mathbb{Z})^*} \Big(\sum_{\lambda=0}^{p^l-1} \chi(t + \lambda \cdot p^l) \cdot \xi_{p^k}^{t+\lambda \cdot p^l} \Big).$$

Since t is a unit, the inner sum is

$$s(t) \; = \; \sum_{\lambda=0}^{p^l-1} \chi(t + \lambda \cdot p^l) \cdot \xi_{p^k}^{t+\lambda \cdot p^l} \; = \; \chi(t) \cdot \zeta_{p^k}^t \cdot \Big(\sum_{\lambda=0}^{p^l-1} \chi(1 + \lambda \cdot t^{-1} \cdot p^l) \cdot \xi_{p^{k-l}}^{\lambda} \Big).$$

Note that

$$(1 + t^{-1} \cdot p^l)^{\lambda} \; = \; 1 + \lambda \cdot t^{-1} \cdot p^l + \binom{\lambda}{2} \cdot t^{-2} \cdot p^{2 \cdot l} + \ldots \; = \; 1 + \lambda \cdot t^{-1} \cdot p^l \bmod p^{2 \cdot l}$$

Hence

$$s(t) \; = \; \chi(t) \cdot \zeta_{p^k}^t \cdot \left[\sum_{\lambda=0}^{p^l-1} \Big(\chi(1 + \lambda \cdot t^{-1} \cdot p^l) \cdot \xi_{p^{k-l}} \Big)^{\lambda} \right]$$

and $\chi(1 + \lambda \cdot t^{-1} \cdot p^l) \cdot \xi_{p^{k-l}}$ is a primitive root of unity. It satisfies (2.5), by (2.43) - note that the weaker condition

$$\mathrm{Im}(\chi^{(p-1) \cdot p^{l-1}}) \subset < \zeta_{p^{k-l}} > \tag{2.45}$$

would also be sufficient. Thus $s(t) = \delta_l(t)$, where

$$\delta_l(t) \; = \; \begin{cases} 0 & t \neq u \bmod p^l \\ p^l & t = u \bmod p^l \end{cases} \tag{2.46}$$

and finally

$$\begin{array}{rcll} \tau(\chi) & = & \chi(u)\cdot\zeta_{p^k}^{u}\cdot p^l & \text{for } k=2\cdot l \text{ and } u \text{ with } 1\le u<p^l \\ \chi(1+v\cdot p^l)\cdot\zeta_{p^{k-l}} & = & 1, \quad \text{and} & \\ u & = & v^{-1} \bmod p^l & \end{array} \tag{2.47}$$

Let now $k=2\cdot l+1$; we again split the Gauss-Sum $\tau(\chi)$:

$$\begin{aligned} \tau(\chi) &= \sum_{t\in(\mathbb{Z}/p^{l+1}\cdot\mathbb{Z})^*} \Big(\sum_{\lambda=0}^{p^l-1} \chi(t+\lambda\cdot p^{l+1})\cdot\xi_{p^k}^{t+\lambda\cdot p^{l+1}}\Big) \\ &= \sum_{t\in(\mathbb{Z}/p^{l+1}\cdot\mathbb{Z})^*} \chi(t)\cdot\zeta_{p^k}^{t}\cdot\Big(\sum_{\lambda=0}^{p^l-1} \chi(1+\lambda\cdot t^{-1}\cdot p^{l+1})\cdot\xi_{p^{k-(l+1)}}^{\lambda}\Big) \end{aligned}$$

Once again, $(1+t^{-1}\cdot p^{l+1})^\lambda = 1+\lambda\cdot t^{-1}\cdot p^{l+1} \bmod p^{2\cdot l+1}$, so the inner sum vanishes unless $t=u \bmod p^l$. In this case, however, there are p values of $t\in(\mathbb{Z}/p^{l+1}\cdot\mathbb{Z})^*$ verifying this condition; consequently:

$$\tau(\chi) = \sum_{\lambda=0}^{p^l-1} \chi(u+\lambda\cdot p^l)\cdot\xi_{p^k}^{u+\lambda\cdot p^l} = \chi(u)\cdot\xi_{p^k}^{u}\cdot\Big(\sum_{\lambda=0}^{p^l-1} \chi(1+u^{-1}\cdot\lambda\cdot p^{l+1})\cdot\xi_{p^l}^{\lambda}\Big)$$

By definition of u, there is a $w\in\{0,1,\ldots,p-1\}$ such that $v=ui^{-1}+w\cdot p^l$ (w is the coefficient v_l in the p-adic expansion (2.9) of v). With this notation,

$$(1+v\cdot p^l)^{1-w\cdot u'\cdot p^l} = (1+u^{-1}\cdot p^l) \bmod p^{2\cdot l+1},$$

where $u'\cdot v=1$ and thus $u'=u \bmod p$. Furthermore,

$$(1+u^{-1}\cdot p^l)^{\lambda-v\cdot\binom{\lambda}{2}\cdot p^l} = (1+u^{-1}\cdot p^l) \bmod p^{2\cdot l+1}.$$

Combining the last two relations, we have:

$$(1+\lambda\cdot u^{-1}\cdot p^l) = (1+\lambda\cdot v\cdot p^l)^{(\lambda-v\cdot\binom{\lambda}{2}\cdot p^l)\cdot(1-w\cdot u'\cdot p^l)} \bmod p^{2\cdot l+1}$$

and

$$\begin{aligned} \chi(1+\lambda\cdot u^{-1}\cdot p^l)\cdot\zeta_{p^{l+1}}^{\lambda} &= \zeta_{p^{l+1}}^{\lambda}\cdot\chi(1+\lambda\cdot v\cdot p^l)^{\lambda-p^l\cdot(\lambda\cdot u'\cdot w+v\cdot\binom{\lambda}{2})} \\ &= (\chi(1+v\cdot p^l)\cdot\zeta_{p^{l+1}})^{\lambda}\cdot\Big(\chi(1+\lambda\cdot v\cdot p^l)^{-p^l\cdot(\lambda\cdot u'\cdot w+u'\cdot\binom{\lambda}{2})}\Big) \\ &= \zeta_p^{\lambda\cdot u'\cdot w+u'\cdot\binom{\lambda}{2}}. \end{aligned}$$

With the definition

$$\theta_p(\chi) = \sum_{\lambda=0}^{p-1} \zeta_p^{\lambda\cdot u'\cdot w+u'\cdot\binom{\lambda}{2}}, \tag{2.48}$$

we have:

$$\tau(\chi) \;=\; \chi(u)\cdot\zeta_{p^k}^{u}\cdot p^l\cdot\theta_p(\chi) \tag{2.49}$$

where $k = 2\cdot l + 1$, and u, v, w and χ are connected by

$0 < v < p^{l+1}$, $\chi(1+v\cdot p^l)\cdot\zeta_{p^{l+1}} = 1$, $u = v^{-1} \bmod p^l$ and $w = \dfrac{v - (v \bmod p^l)}{p^l}$.

One can check that

$$\theta_p(\chi)\cdot\theta_p(\chi^{-1}) \;=\; p \tag{2.50}$$

in agreement with (2.28) and (2.39).

Let now $p = 2$ and $k > 3$. By (2.12) $(\mathbb{Z}/2^k\cdot\mathbb{Z}) = <5> \times \{-1,1\}$. Unlike the case of odd primes, a primitive character of conductor 2^k is thus given by two values: $\chi(-1)$ and $\chi(5)$; the cycle of 5 has index $2^k - 2$. Let $k = 2\cdot l$, $l > 1$ and χ be a primitive character of conductor 2^k, ζ_{2^k} be a primitive 2^k-th root of unity in $\mathbf{A}$ and $\mathrm{Im}(\chi^{2^l}) \subset <\zeta_{2^k}>$; by (2.2), $\zeta_{2^i} = \zeta_{2^k}^{2^{k-i}}$, $i = 1,2,\ldots,k-1$, are also primitive of order 2^i. We use again the technique of splitting the summation domain for calculating a Gauss-Sum. It can be shown by induction, that $5^{2^{l-2}} = 1 + (2^{l-1}-1)\cdot 2^l \bmod 2^{2\cdot l}$. Thus $5^{t\cdot 2^{l-2}} = 1 + t\cdot(2^{l-1}-1)\cdot 2^l \bmod 2^{2\cdot l}$ for $t \in (\mathbb{Z}/2^l\cdot\mathbb{Z})$. With these prerequisites,

$$\begin{aligned}
\tau(\chi) \;&=\; \sum_{t=0}^{2^{l-2}-1}\Big(\sum_{\lambda=0}^{2^l-1}\chi(5)^{t+\lambda\cdot 2^{l-2}}\cdot\xi_{2^k}^{5^{t+\lambda\cdot 2^{l-2}}}\Big)\\
&\quad+\sum_{t=0}^{2^{l-2}-1}\Big(\sum_{\lambda=0}^{2^l-1}\chi(-5)^{t+\lambda\cdot 2^{l-2}}\cdot\xi_{2^k}^{-5^{t+\lambda\cdot 2^{l-2}}}\Big)\\
&=\; \sum_{t=0}^{2^{l-2}-1}\chi(5)^t\cdot\zeta_{2^k}^{5^t}\cdot\Big(\sum_{\lambda=0}^{2^l-1}(\chi(5)^{2^{l-2}}\cdot\xi_{2^l}^{5^t})^\lambda\Big)\\
&\quad+\sum_{t=0}^{2^{l-2}-1}\chi(-5)^t\cdot\zeta_{2^k}^{5^t}\cdot\Big(\sum_{\lambda=0}^{2^l-1}(\chi(-5)^{2^{l-2}}\cdot\xi_{2^l}^{-5^t})^\lambda\Big)
\end{aligned}$$

Let $\omega_+ = \chi(5)^{2^{l-2}}\cdot\xi_{2^l}^{-5^t}$; the first inner sum vanishes unless $\omega_+ = 1$. Similarly, the second inner sum vanishes, unless $\omega_- = \chi(-5)^{2^{l-2}}\cdot\xi_{2^l}^{-5^t} = 1$. Since $\omega_+\cdot\omega_- = \chi(5)^{2^{l-1}} \neq 1$, it follows that ω_+ and ω_- cannot be simultaneously equal to the unit and there is a unique $u \in (\mathbb{Z}/2^l\cdot\mathbb{Z})^*$ with $\chi(5)^{2^{l-2}}\cdot\xi_{2^l}^{-u} = -1$, such that:

$$\tau(\chi) = 2^l\cdot\chi(u)\cdot\zeta_{2^k}^{u}\ ,\ \text{for } k = 2\cdot l,\ l > 1 \text{ and } \chi(u)\cdot\zeta_{2^k}^{u} = \chi(u\cdot 5^{2^{l-2}})\cdot\zeta_{2^k}^{u\cdot 5^{2^{l-2}}} \tag{2.51}$$

We shall give the result for $k = 2\cdot l+1$ without entering into details of the proof, which uses the same techniques as in the previous cases. We let

$$\theta_2(\chi) \;=\; \Big(1+\chi(1+u'\cdot 2^{l-2})\Big)\cdot\zeta_{2^k}^{2^{l-2}}$$

and v be such that $\chi(5)^{2^{l-2}} \cdot \xi_{2^{l+1}}^{-v} = \zeta_4^{-1}$; it follows that $v = u + 2^{l-1} \bmod 2^l$. Some substitutions similar to the one used for deducing $\theta_p(\chi)$ for odd p lead to following formula:

$$\theta_2(\chi) = 1 + \zeta_4^{-u} \tag{2.52}$$

in accordance with (2.39).

$$\begin{aligned} \tau(\chi) &= 2^l \cdot \chi(u) \cdot \zeta_{2^k}^u \cdot \theta_2(\chi), \quad \text{for } k = 2 \cdot l + 1, l > 1 \text{ and} \qquad (2.53) \\ \chi(u) \cdot \zeta_{2^k}^u &= \chi(u \cdot 5^{2^{l-1}}) \cdot \zeta_{2^k}^{u \cdot 5^{2^{l-1}}}. \end{aligned}$$

We have proved:

Theorem 2.52 *Let χ be a character of prime power conductor p^k and $l = [k/2], l > 0$ for odd p and $l > 1$ for $p = 2$. Let ζ_{p^k} be a p^k-*th *primitive root of unity in* $\mathbf{A}$ *such that*

$$\mathrm{Im}(\chi^{(p-1)\cdot p^{l-1}}) \subset < \zeta_{p^{k-l}} > , \textit{ with } \zeta_{p^{k-l}} = \zeta_{p^k}^{p^l}. \tag{2.55}$$

and $\tau(\chi)$ the Gauss-Sum of χ with respect to ζ_{p^k}. Let u be defined by $0 < u < p^l$, and

(a) $\chi(u + p^l) \cdot \zeta_{p^{k-l}} = \chi(u)$ *, for odd p .*

(b) $\chi(u) \cdot \zeta_{2^k}^u = \chi(u \cdot 5^{2^{l-2}}) \cdot \zeta_{2^k}^{u \cdot 5^{2^{l-2}}}$*, for $p = 2$,*

and $\theta_p(\chi)$ is given by (2.48) for odd p and by (2.52) for $p = 2$. Then

$$\tau(\chi) = \begin{cases} \chi(u) \cdot \zeta_{p^k}^u \cdot p^l & \textit{for } k \textit{ even} \\ \\ \chi(u) \cdot \theta_p(\chi) \cdot \zeta_{p^k}^u \cdot p^l, & \textit{for } k \textit{ odd} \end{cases} \tag{2.56}$$

We saw that (2.56) holds if (2.55) holds. This is the case for instance in (2.43). In primality testing however, one assumes that the roots used for building Gauss-Sums and the images of the character χ are independent. We shall give two approaches for a variant of (2.56), when (2.55) does not hold. We illustrate this approaches for the case when p is odd and $k = 2 \cdot l$. In this case,

$$\omega_t = \chi(1 + t^{-1} \cdot p^l) \cdot \zeta_{p^l} \tag{2.57}$$

is in general not a primitive root of unity. The first approach uses the splitting of the minimal annihilator of $\mathbf{A}$ into prime factors, which allows working in rings where all roots of unity are primitive, according to (2.8); the second approach uses the difference between the galois actions on ζ and ξ. If we put

$$s_0(t) = \sum_{\lambda=0}^{p^l-1} \left(\chi(1 + t^{-1} \cdot p^l) \cdot \xi_{p^l}\right)^\lambda = \frac{s(t)}{\chi(t) \cdot \zeta_{p^k}^t}, \tag{2.58}$$

following relation holds without restriction upon χ :

$$\sum_{t\in(\mathbb{Z}/p^l\cdot\mathbb{Z})^*} s_0(t) \;=\; p^l.$$

as can be easily seen after some habitual reorderings of the summation. In the first approach we shall use the rings $\mathbf{A}_q$ introduced for the lemma (2.8). By this definition, the image of $\tau(\chi)$ in $\mathbf{A}_q$, is $\pi_q(\tau(\chi)) = \pi_q(\chi(u_q)\cdot\zeta_{p^k}^{u_q})\cdot p^l$, for some unique u_q such that $\pi_q(\omega_{u_q}) = 1$. We can thus use the Chinese remainder theorem after calculating the Gauss-Sum $\tau(\chi)$ in the rings $\mathbf{A}_q$. It follows in particular, that $p^l \mid \tau(\chi)$ and

$$\tau(\chi) = p^l\cdot v(\chi,\zeta_{p^l}) \quad \text{for some } v(\chi,\zeta_{p^l})\in\mathbf{A}^*. \tag{2.59}$$

Note that u_q depends upon q, so that the unit in (2.59) cannot be evaluated without knowledge of the factors of n. On the other hand, if the Gauss-Sum $\tau(\chi)$ is computed in the context of primality testing, where n is to be tested, then either the test $(1-\omega_t,n)=1$ is passed for all $t\in(\mathbb{Z}/p^l\cdot\mathbb{Z})^*$, in which case ω_t are all primitive and $\tau(\chi)$ can be computed according to (2.47). Otherwise, a factor of n is found, which stops a primality testing procedure.

We now give a second approach, which does not make use of factors of the minimal annihilator n – and does not use the existence of a finite minimal annihilator. Let ζ be a primitive $p^{2\cdot l-1}$–th root of unity in $\mathbf{A}$ such that $\mathrm{Im}(\chi^{p-1})\subset<\zeta>$ and let $\vartheta=\zeta^{p^{l-1}}$. Let ξ be a primitive $p^{2\cdot l}$–th root of unity in $\mathbf{A}$ and $\eta=\xi^{p^l}$. Let $\mathbf{A}_0=\{z\in\mathbb{Z}\mid z\times 1\in\mathbf{A}\}$ and $\mathbf{A}_1=\mathbf{A}_0[\zeta]$, $\mathbf{B}=\mathbf{A}_1[x]/(\Phi_{p^l}(x))$. Since $(\Phi_{p^l}(x))$ splits completely over $\mathbf{A}_1$, the Chinese remainder theorem yields

$$\mathbf{B} \;=\; \prod_{i\in(\mathbb{Z}/p^l\cdot\mathbb{Z})^*\ \mathbf{A}_1} \tag{2.60}$$

where $\pi_i(x)=\vartheta^i$, π_i being the projection of x in the i–th copy of $\mathbf{A}_1$. Obviously, $\mathbf{A}_1[\eta]$ maps injectively in $\mathbf{B}$. Let I be the subset of $(\mathbb{Z}/p^l\cdot\mathbb{Z})^*$ such that $\mathbf{A}_1[\eta]$ maps bijectively to $\mathbf{A}_2=\prod_{i\in I}\mathbf{A}_1$. Let finally $\mathbf{A}'=\mathbf{A}_2[\zeta]=\mathbf{A}_2[x]/((x^{p^l}-\eta))$, so that we have the tower of rings $\mathbf{A}\supset\mathbf{A}'\supset\mathbf{A}_2\supset\mathbf{A}_1$. The Gauss-Sum is defined as an element of $\mathbf{A}'$ by $\tau(\chi)=\sum_{t\in(\mathbb{Z}/p^{2\cdot l}\cdot\mathbb{Z})^*}\chi(t)\cdot\xi^t$. The splitting $\mathbf{A}_2=\prod_{i\in I}\mathbf{A}_1$ of $\mathbf{A}_2$ induces a splitting $\mathbf{A}'=\prod_{i\in I}\mathbf{A}'_1$ of $\mathbf{A}'$, where $\mathbf{A}'_1=\mathbf{A}_1[x]/((x^{p^l}-\vartheta))$, and we let π'_i be the extension of π_i to $\mathbf{A}'_1$. If ζ' is the image of ζ in $\mathbf{A}'_1$, then $\pi'_i(x)=\zeta'^i$. For determining $\pi'_i(s(t))$, with $s(t)$ defined in (2.58), we come to considering $\pi(\omega_t)=\chi(1+t^{-1}\cdot p^l)\cdot\pi_i(\xi)=\chi(1+t^{-1}\cdot p^l)\cdot\zeta'_i$. If u is such that $\pi'_1(\omega_u)=1$, then $\pi_1(\omega_{u\cdot i^{-1}})=1$. Combining with (2.48) we get:

$$\pi'_i(\tau(\chi)) \;=\; \chi(u)\cdot\zeta'^u\cdot\chi(i^{-1}\cdot p^l). \tag{2.61}$$

Let $\{\mathbf{e}_i\mid i\in I\}$ be a basis for $\mathbf{A}'$ as an $\mathbf{A}'_1$ - module, such that $\mathbf{e}_i=0 \bmod (x-\vartheta^j)$ for $i\neq j$ and $\mathbf{e}_i=1 \bmod (x-\vartheta^i)$. Then we have the closed formula:

$$\tau(\chi) \;=\; \chi(u)\cdot\zeta^u\cdot p^l\cdot\sum_{i\in I}\chi(i^{-1})\cdot\mathbf{e}_i. \tag{2.62}$$

If $g(x)=\prod_{i\in I}(x-\vartheta^i)$ is the minimal polynomial of η over $\mathbf{A}_1$ and

$$g_i(x)=\prod_{j\in I,j\neq i}(x-\vartheta^j),$$

then $\mathbf{e}_i = g_i(\eta)/g'(\vartheta^i)$, where $g'(x)$ is the algebraic derivative of $g(x)$ and the sum $\tau(\chi)$ may also be written as follows:

$$\tau(\chi) \quad = \quad \chi(u) \cdot \zeta^u \cdot p^l \cdot \sum_{i \in I} \chi(i^{-1}) \cdot g_i(\eta)/g'(\vartheta^i). \tag{2.63}$$

In fact, $g_i(x) = 0 \bmod (x - \vartheta^j)$ for $j \neq i$ by definition, and $g_i(\vartheta^i) = g'(\vartheta^i)$, leading to the norming factor in the denominator. Furthermore, since η is the image of x in $\mathbf{A}_2$, $\mathbf{e}_i = g_i(\eta)/g'(\vartheta^i)$. In particular, if $I = \{1\}$, one recovers (2.49). Note that the inner sum is an element of $\mathbf{A}_2$, which explains the fact the base $\mathbf{e}_i$ needed not be taken for $\mathbf{A}$', but rather for its subring $\mathbf{A}_2$, where the sums $s(t)$ are annihilated. We shall see in the next chapter, that I is the galois group of $\mathbf{A}_2$ over $\mathbf{A}_1$; we thus deduced a formula for the general case of a ring $\mathbf{A}_2$ which contains two primitive p^l-th roots of unity, whose galois groups do not act identically. The group I measures the difference of the actions of the galois groups of ϑ and η over $\mathbf{A}_0$. Obviously the same technique can be used for odd k and for $p = 2$. This leads to following generalization of theorem (2.52):

Theorem 2.62 *Let χ be a character of prime power conductor p^k and $l = [k/2], l > 0$ for odd p and $l > 1$ for $p = 2$. Let ζ be a primitive $p^{k-1}-$th root of unity in $\mathbf{A}$ such that $\mathrm{Im}(\chi^{p-1}) \subset < \zeta >$ and let $\vartheta = \zeta^{p^{k-l}}$. Let ξ be a primitive p^k-th root of unity in $\mathbf{A}$, $\eta = \xi^{p^{k-l}}$ and $\tau(\chi)$ be the Gauss-Sum of χ with respect to ξ. Let the tower of rings $\mathbf{A} \supset \mathbf{A}' \supset \mathbf{A}_2 \supset \mathbf{A}_1$ and $\mathbf{A}_1'$ be defined as above, π_i be the projection from $\mathbf{A}_2$ into the $i-$th copy of $\mathbf{A}_1$ and ζ' be the image of ζ in $\mathbf{A}_1'$. Let u be defined by $0 < u < p^l$, and*

(a) $\pi_1(\chi(u + p^l) \cdot \zeta_{p^{k-l}}) \; = \; \pi_1(\chi(u))$, *for odd p,*

(b) $\pi_1(\chi(u) \cdot \zeta_{2^k}^u) \; = \; \pi_1(\chi(u \cdot 5^{2^{l-2}}) \cdot \zeta_{2^k}^{u \cdot 5^{2^{l-2}}})$, *for $p = 2$,*

and $\theta_p(\chi)$ be defined by (2.49) for odd p and by (2.53) for $p = 2$. If $g(x) = \prod_{i \in I} (x - \vartheta^i)$ is the minimal polynomial of η over $\mathbf{A}_1$ and $g_i(x) = \prod_{j \in I, j \neq i} (x - \vartheta^i)$, and, for all $i \in I$, $\pi_i(\theta(\chi))$ is given by:

$$\begin{aligned} \pi_i(\theta_p(\chi)) &= \sum_{\lambda=0}^{p-1} (\vartheta^{i \cdot p^l})^{\lambda \cdot u' \cdot w + u' \cdot \binom{\lambda}{2}}, \quad \textit{for } p \textit{ odd },\\ \pi_i(\theta_2(\chi)) &= 1 + \vartheta^{-u \cdot i \cdot 2^l}, \quad \textit{for } p = 2, \end{aligned} \tag{2.65}$$

with u' and w defined by (2.49), then

$$\tau(\chi) \quad = \quad \begin{cases} \chi(u) \cdot \zeta'^u \cdot p^l \cdot \prod_{i \in I} \chi^{-1}(i) \cdot g_i(\eta)/g'(\vartheta^i), & \textit{for } k \textit{ even} \\ \\ \chi(u) \cdot \zeta'^u \cdot p^l \cdot \prod_{i \in I} \chi^{-1}(i) \cdot \pi_i(\theta_p(\chi)) \cdot g_i(\eta)/g'(\vartheta^i), & \textit{for } k \textit{ odd} \end{cases} \tag{2.66}$$

This finishes our deduction of formulae for Gauss-Sums of characters with prime power conductors. For this class of characters, the Jacobi-Sums are not simpler then Gauss-Sums in the sense that they do not give rise to smaller extensions. They can be computed by solving (2.29) with respect to the Jacobi-Sum. If χ and χ' are two characters of conductor p^k, (2.55) holds and if $u(\chi)$ and $u(\chi')$ are defined like in theorem (2.50), then

$$u(\chi \cdot \chi') = u(\chi) + u(\chi') \tag{2.67}$$

Finally, with $u = u(\chi)$ and $u' = u(\chi')$, we have:

$$\begin{aligned} j(\chi, \chi') &= \frac{\chi(u) \cdot \chi'(u')}{(\chi \cdot \chi')(u + u')}\, p^l && \text{for } k \text{ even} \\ j(\chi, \chi') &= \frac{\chi(u) \cdot \chi'(u') \cdot \theta_p(\chi) \cdot \theta_p(\chi')}{\theta_p(\chi \cdot \chi') \cdot (\chi \cdot \chi')(u + u')}\, p^l && \text{for } k \text{ odd} \end{aligned} \tag{2.68}$$

2.4 Fast computation methods for Jacobi-Sums: Lattice reduction

Jacobi-Sums $\chi : (\mathbb{Z}/q \cdot \mathbb{Z}) \to < \zeta_{p^k}$, with primes p and q and their associated invariants defined by (2.32) play a central role in practical primality testing. We shall look closer in this section to relations existing between these invariants and formulate a new algorithm for computing them.

We let now χ be a character of prime conductor q. Let p be a prime dividing $u = q - 1$, with $v_p(u) = k$, thus $p^{v(p)} \parallel u$. We consider two complex primitive roots of unity ζ and ξ, of respective order $p^{v(p)}$ and q and let $\mathbf{A} = \mathbb{Z}[\zeta, \xi]$ and $\mathbf{R} = \mathbb{Z}[\zeta]$.

Let $G = \{\sigma_x \ : \ x \in (\mathbb{Z}/p^k \cdot \mathbb{Z})^*\}$ be the automorphism group of $\mathbf{R}$ over $\mathbb{Z}$, with σ_x sending ζ to ζ^x. The group ring $\mathbb{Z}[G]$ is a free $\mathbb{Z}$ - module with base G. The action of $\mathbb{Z}[G]$ upon $\mathbf{R}$ is written exponentially ([CoLe]) and given by:

$$\begin{aligned} \alpha^{\sigma_x} &= \sigma_x(\alpha) \quad \forall \alpha \in \mathbf{A}, \forall x \in (\mathbb{Z}/p^k \cdot \mathbb{Z})^*. \\ (\alpha \cdot \beta)^\nu &= (\alpha)^\nu \cdot (\beta)^\nu, \quad \forall \alpha, \beta \in \mathbf{A}, \forall \nu \in \mathbb{Z}[G]. \\ \alpha^{\mu+\nu} &= (\alpha)^\mu \cdot (\alpha)^\nu, \quad \forall\, \alpha \in \mathbf{A}, \forall\, \mu, \nu \in \mathbb{Z}[G]. \end{aligned} \tag{2.69}$$

Note that $\alpha = \alpha^1 = \alpha^{\sigma_1}$. Furthermore,

$$\sigma_{x \cdot y} = \sigma_x \cdot \sigma_y, \quad \forall\, x, y \in (\mathbb{Z}/p^k \cdot \mathbb{Z})^*, \tag{2.70}$$

which makes $\mathbb{Z}[G]$ into a $\mathbb{Z}$ - algebra.

If g generates $(\mathbb{Z}/p^k \cdot \mathbb{Z})^*$, there is a map $\gamma : \mathbb{Z}[G] \to \mathbb{Z}[\zeta]$ given by $\gamma(\sigma_g) = \zeta$ and $\gamma(\sigma_1) = 1$ with $\mathrm{Kern}(\gamma) = \{\nu \in \mathbb{Z}[G] \ : \ \mathbf{R}^\nu \neq \mathbf{R}\}$. This suggests:

$$\sigma_1 \cdot g^x - \sigma_{g^x} = (g \cdot \sigma_1 - \sigma_g) \cdot \sum_{i=0}^{x-1} g^i \cdot \sigma_{g^i}, \quad \forall\, g^x \in (\mathbb{Z}/p^k \cdot \mathbb{Z})^*. \tag{2.71}$$

The identity follows by straightforward computation in $\mathbb{Z}[G]$ and will be used further in following shape:

Lemma 2.70 *If g generates $(\mathbb{Z}/p^k\cdot\mathbb{Z})^*$, then for any $y \in (\mathbb{Z}/p^k\cdot\mathbb{Z})^*$ there is an $x \in \{0,1,\ldots,\varphi(p^k)-1\}$ and an integer λ such that:*

$$\sigma_1\cdot y - \sigma_y \;=\; (g\cdot\sigma_1-\sigma_g)\cdot\mu - \lambda\cdot p^k \quad \textit{where} \;\; \mu \;=\; \sum_{i=0}^{x-1} g^i\cdot\sigma_{g^i} \in \mathbb{Z}[G]. \tag{2.73}$$

Let $G' = \{\theta_x \mid x(\mathbb{Z}/m\cdot\mathbb{Z})^*\}$ be the group of automorphisms of $\mathbf{A}$ over $\mathbb{Z}$, with θ_x sending ξ to ξ^x and $\theta_x(\zeta)=\zeta$; we shall let σ_x act upon ξ by $\sigma_x(\xi)=\xi$. Let χ be a character of conductor q and order p^k and $\tau(\chi)$ be the Gauss-Sum of χ with respect to ξ. Let $h \in (\mathbb{Z}/p^k\cdot\mathbb{Z})^*$ and $\alpha_h = \tau(\chi)^h/\tau(\chi^h) = \tau(\chi)^{h-\sigma_h}$. Then

$$\theta_x(\alpha_h) \;=\; \frac{(\chi^{-1}(x)\cdot\tau(\chi))^h}{\chi^{-h}(x)\cdot\tau(\chi^h)} \;=\; \tau(\chi)^{h-\sigma_h} \;=\; \alpha_h.$$

Thus α_h is invariant under G' and lays in $\mathbf{R}$. These invariants are actually the *multiple Jacobi-Sums* defined in (2.30). As suggested by (2.36), we shall be interested in primality testing, to compute objects of the type $\tau(\chi)^{n-\sigma_n}$, where n is some "large" integer to be tested for primality, verifying: $(n, q\cdot u)=1$. We need the numbers α_h as well as $\alpha_0 = \tau(\chi)^{p^k} = \chi(-1)\cdot q\cdot\alpha_{-1}$ (by (2.30)). First note that:

$$\alpha_h \;=\; \frac{\tau(\chi)^h}{\tau(\chi^h)} \;=\; \prod_{i=1}^{h-1} j(\chi,\chi^i), \quad \forall\, h \in (\mathbb{Z}/p^k\cdot\mathbb{Z})^*,\;\; h>1. \tag{2.74}$$

Indeed, for this range of h, the premises of (2.29) are satisfied by $j(\chi,\chi^i)$ and (2.74) follows by induction on h. Let P be a set of primes. It can be shown by straightforward computation in $\mathbb{Z}[G]$, that if α_h is known for all $h \in P\cap(\mathbb{Z}/p^k\cdot\mathbb{Z})^*$, then α_l can be determined up to a power of α_0 for all l in the subgroup of $(\mathbb{Z}/p^k\cdot\mathbb{Z})^*$ generated by P (see [BovdH], II, 8.12). In particular, if P contains a generator g of $(\mathbb{Z}/p^k\cdot\mathbb{Z})^*$, the set $\{\alpha_h \mid h \in (\mathbb{Z}/p^k\cdot\mathbb{Z})^*\}$ can be determined up to a power of α_0. We have thus following system of equations:

$$\begin{aligned} &\alpha_0^{l_h}\cdot\alpha_h = \alpha_g^{\mu_h}, && \forall\, h \in (\mathbb{Z}/p^k\cdot\mathbb{Z})^* \\ &\alpha_0^{l_0} = \chi(-1)\cdot q\cdot\alpha_g^{\mu_1}, && \text{where } l_0 = l_{-1}+1. \end{aligned} \tag{2.75}$$

For "small" p and q, one can compute α_g using (2.74) and some reductions like in [BovdH] and then attempt to eliminate α_0 in (2.75) by integer Gauss elimination in $\mathbb{Z}[G]$. Typically, we want to compute $\tau(\chi)^{n-\sigma_n} = \alpha_0^a\cdot\alpha_b$, with $n = a\cdot p^k + b,\ 0\le b<p^k$. If elimination fails, combining the equations for α_0 and α_b in (2.75), one can compute $\tau(\chi)^{t(n-\sigma_n)}$, where $t=[l_0,l_b]$ is the least common multiple of l_0 and l_b.

We show now, that there is an algorithm for computing

$$\{\alpha_h \;:\; h \in (\mathbb{Z}/p^k\cdot\mathbb{Z})^* \cup 0\},$$

which is asymptotically more efficient then direct summation whenever

$$p^k \;=\; o(\log q/\log\log q). \tag{2.76}$$

In such cases, elimination can be avoided by applying this algorithm twice, for α_0 and α_b. Since the conductor q of χ is prime, by (2.28) and (2.29), α_b are algebraic integers factoring into ideals of $\mathbf{R}$ laying over q. Let $a \in (\mathbb{Z}/q\cdot\mathbb{Z})^*$ be such that:

$$\begin{aligned} a^{p^k} &= 1 \bmod q \\ a^{p^k} &\neq 1 \bmod q^2 \\ (a^{p^{k-1}}-1, q) &= 1 \end{aligned} \tag{2.77}$$

and define the ideal $\varrho \in \mathbf{R}$ by:

$$\varrho = (a-\zeta, q) \tag{2.78}$$

It is easy to verify, that $\mathbf{N}(\varrho) = q$ and thus ϱ is a prime lying above q. Let g be a generator of $(\mathbb{Z}/q\cdot\mathbb{Z})^*$ and $\chi_a \in (\mathbb{Z}/q\cdot\mathbb{Z})^{\perp}$ be defined by:

$$\begin{aligned} g^{-(q-1)/p^k} &= a \bmod q \\ \chi_a(g) &= \zeta \end{aligned} \tag{2.79}$$

The character χ_a thus generates the cycle of characters of conductor q and order dividing p^k. For $b \in (\mathbb{Z}/q\cdot\mathbb{Z})^*$, the element $\Theta(b) \in \mathbb{Z}[G]$ (Stickelberger) is defined by:

$$\Theta(b) = \sum_{x \in (\mathbb{Z}/p^k\cdot\mathbb{Z})^*} [bx/p^k]\sigma_x^{-1} \tag{2.80}$$

With this notation, we can state the following basic result from the theory of cyclotomic fields ([La2]):

$$(\alpha_b) = \varrho^{\Theta(b)}, \quad \text{where } \alpha_b = \tau(\chi)^{b-\sigma_b}, \tag{2.81}$$

the equality being between principal ideals. Using (2.78) and (2.29), the principal ideal (α_b) can be presented by the generators $\gamma = (a-\zeta)^{\Theta(b)}$ and $\delta = q^{b-1}$. This follows from $\gamma, \delta \in (\alpha_b)$ and $(\mathbf{N}(\gamma), \mathbf{N}(\delta)) = \mathbf{N}(\alpha_b)$. Note that γ is a product of Jacobi-Sums of characters with prime conductors $l \mid (a^{p^k}-1)$.

Let $d = \varphi(p^k)$ and consider $\mathbf{R}$ embedded in a d-dimensional real vector space $\mathbf{V}$ generated by $\{\zeta^i \mid i \in (\mathbb{Z}/p^k\cdot\mathbb{Z})\}$; we shall denote this set of generators a *superbase*, since it is not linearly independent. It actually allows the choice of p^k-1 independent parameters. Let ι be the map $\mathbf{R} \to \mathbf{V}$, and v_i be the images of ζ^i in $\mathbf{V}$ $(i = 0, 1, \ldots, p^k-1)$ and let the metric of $\mathbf{V}$ be induced by ([Le3]):

$$\mathbf{N}^2(x) = \frac{\sum_{\sigma\in G} \sigma(x)\sigma^{-1}(x)}{d} \tag{2.82}$$

Let

$$\mathbf{v} = \sum_{i=0}^{p^k-1} \mathbf{v}_i a_i \quad \text{and} \quad \mathbf{w} = \sum_{i=0}^{p^k-1} \mathbf{v}_i b_i$$

be two vectors in $\mathbf{V}$ (we do not care for the moment about making this representation unique). It follows by straight forward computation, that:

$$\begin{aligned}\mathbf{N}(\mathbf{v}) &= \sum_{i=0}^{p^{k-1}} a_i^2 - \Big(\sum_{i=0}^{p^{k-1}} \sum_{j=1}^{p-1} a_{i+j\cdot p^{k-1}}\Big) \;/\; (p-1) \\ &= \Big(\sum_{i=j \bmod p^{k-1}} (a_i - a_j)^2\Big) \;/\; (p-1) \end{aligned} \tag{2.83}$$

and

$$\begin{aligned}(\mathbf{v}, \mathbf{w}) &= \sum_{i=0}^{p^{k-1}} a_i b_i - \Big(\sum_{i=0}^{p^{k-1}} a_i \sum_{j=1}^{p-1} b_{i+j\cdot p^{k-1}}\Big) \;/\; (p-1) \\ &= \Big(\sum_{i=j \bmod p^{k-1}} (a_i - a_j)(b_i - b_j)\Big) \;/\; (p-1). \end{aligned} \tag{2.84}$$

In particular,

$$\mathbf{N}^2(\mathbf{v}_i) = 1, \quad \text{for } i = 0, 1, \ldots, p^k - 1. \tag{2.85}$$

and

$$(\mathbf{v}_i, \mathbf{v}_j) = \begin{cases} 0 & \text{if } i \neq j \bmod p^{k-1} \\ \dfrac{-1}{p-1} & \text{if } i = j \bmod p^{k-1} \end{cases} \tag{2.86}$$

It follows from (2.83), that for any $\mathbf{v} \neq 0$, $\mathbf{N}^2(\mathbf{v}) \geq 1$, with equality for $\mathbf{v} = \mathbf{v}_i$. If $k = 1$, the superbase vectors point to the vertices of a regular (d-dimensional) superpyramid. If $k > 1$, they point to the vertices of p^{k-1} such pyramids which are disposed in reciprocally orthogonal $(p-1)$-dimensional subspaces. The indices of the superbase - vectors disposed in the same pyramid are congruent mod p^{k-1}. We consider the lattice L generated by the image of α_b in $\mathbf{V}$:

$$L = \{\iota\Big(\sum_{i=0}^{p^{k-1}} a_i \cdot \alpha_b \cdot \zeta^i\Big) \;:\; a_i \in \mathbb{Z}\}.$$

If $\beta \in (\alpha_b)$, then $\beta = \nu \cdot \alpha_b$ for a $\nu \in \mathbf{R}$. By (2.29),

$$\sigma(\alpha_b) \cdot \sigma^{-1}(\alpha_b) = q^{b-1}, \;\; \forall \sigma \in G$$

and thus $\mathbf{N}^2(\alpha_b) = q^{b-1} = \mathbf{N}(\delta)$. Furthermore,

$$\mathbf{N}^2(\beta) = \frac{\sum_{\sigma \in G} \; \sigma(\nu\alpha_b)\sigma^{-1}(\nu\alpha_b)}{d} = \mathbf{N}^2(\alpha_b)\mathbf{N}^2(\nu).$$

This shows that $\iota(\varepsilon \cdot \alpha_b)$ are the shortest vectors in the lattice L, where $\varepsilon \in < -\zeta >$, and they all have length $q^{(b-1)/2}$. The shortest vector in a d-dimensional lattice can be found in time

$$\max\{O(d^d), pol(inputlength)\} \quad \text{[Ka]}.$$

This proves the assertion (2.76). We can state an algorithm for fast computation of multiple Jacobi-Sums:

Algorithm I *(* Computation of multiple Jacobi-Sums up to a root of unity. *)*

Let p, q be primes with $p^k \mid (q-1), k > 0$ and $1 < b < q-1$

(i) Find $a \in \mathbb{Z}$, $(a, q) = 1$ satisfying (2.77) and define ϱ by (2.78)

(ii) Compute $\gamma = (a - \zeta)^{\Theta(b)} \bmod q^{b-1}$ as element of $\mathbf{R}/(q^{b-1} \cdot \mathbf{R})$, where $\Theta(b)$ is given by (2.80).

(iii) Find $\alpha \in \mathbb{Z}[\zeta]$, a generator of the principal ideal (γ, q^{b-1}) by using lattice reduction.

Then $\alpha = \varepsilon \cdot \alpha_b$ for some $\varepsilon \in < -\zeta >$.

Remark 2.85

(i) Algorithm I is polynomial in $(p^p \cdot \log q)$, the largest amount of work being involved in step (iii).

(ii) Although this algorithm does not compute the exact value α_b, it is sufficient for the practical tests of this work.

(iii) The algorithm can be adapted to computation of Jacobi-Sums $j(\chi^i, \chi^j)$, with $i \cdot j \cdot (i+j) \neq 0 \bmod p^k$. This can be done by replacing $\Theta(b)$ by an adequate element of the group ring.

While lattice reduction offers an algorithm for computing Jacobi-Sums which is in many cases superior to the naive approach, it fails in the concrete setting of cyclotomy primality testing from being polynomial in the input of the test. A new algorithm, based only on algebraic properties of Gauss and Jacobi-Sums had to be designed. The computation of Jacobi-Sums was implemented with a naive approach in our program, using full character tables. This approach leads into a dead end for test above roughly 4000 digits, since the size of required tables cannot be allocated (on our DEC Alpha). Looking for means of circumventing this impass without further restriction in the conductor size, we considered an algebraic approach using images of Jacobi-Sums in finite fields and chinese remainder theorem. The primary goal of freeing the size restriction on the Jacobi-Sum may be reached by this approach. It is not clear before completion of the thesis, if there is not more to it – especially, if one cannot achieve some sensible run time improvements. The topic will thus stay under research. We present in the next section the algebraic approach with its developed and tested aspects, as well as some idea that may be useful for further research. The development will require some of the facts developed in the next chapter, so chapter 3 may be read first.

2.5 Fast computation methods for Jacobi-Sums: The algebraic approach

We shall show in this section how to compute the minimal polynomial of Gauss Periods using the images in finite fields. Given these minimal polynomials, the task of computing both simple and multiple Jacobi-Sums is a simple task which shall be explained at the end of the section. The method is slower than naive computation of Jacobi-Sums. It can be however implemented such that the same core computation yield *all* the Gauss Periods – and implicitly, all Jacobi-Sums – which are requested for one given conductor q.

2.5.1 Computing Gauss Periods

Let q be a prime, $G \subset (\mathbb{Z}/q \cdot \mathbb{Z})^*$ a subgroup of the galois group Gal $(\mathbb{C}_q/\mathbb{Q})$ and $H = (\mathbb{Z}/q \cdot \mathbb{Z})^*/G$, such that $G \cap H = \{1\}$. Define $f = \sharp G$ and $h = \frac{q-1}{f} = \sharp H$. If $\xi \in \mathbb{C}_q$ is a $q-$th primitive root of unity, the Gauss Periods we want to compute are

$$\{\eta_\tau = \sum_{\sigma \in H} \sigma(\tau(\xi)) : \tau \in G\}.$$

We assume q is large. Naive computation in $\mathbb{C}_q$ is thus not possible, since, as mentioned above, it would require too large table for the given machine memory. Our simplest method consists in mapping $\mathbb{C}_q$ to a prime galois field $\mathbb{F}_r$, with $r = 1 \mod q$. The choice of r is such that $r > B$, for a bound which depends whether the ultimate goal is computing Gauss Periods or Jacobi-Sums.

By the definition of r, $\exists\ \zeta \in \mathbb{F}_r$ with $\zeta \neq 1$ and $\zeta^q = 1$: i.e., ζ is a primitive $q-$th root of unity. If $\nu : \mathbb{C}_q \longrightarrow \mathbb{F}_r$ is the natural map given by $\nu(\xi) = \zeta$, the images $\nu(\eta_\tau)$ can thus be computed by a long succession of multiplications in $\mathbb{F}_r$.

We aim to compute the minimal polynomial $m(x) \in \mathbb{Z}[x]$ of Gauss Periods over the ring of the rational integers - by the obvious multiplication of monomials:

$$\nu(m(x)) = \prod_{\tau \in G} (x - \nu(\eta_\tau)).$$

For this purpose, either r will be chosen larger than an upper bound B for the coefficients of $m(x)$, or several r will be used, after which the Chinese remainder theorem may be applied for finding the true value of $m(x)$.

We finally have to evaluate the bound B. Since

$$|\sum_{\sigma \in H} \zeta^\sigma| \leq \sum_{\sigma \in H} |\zeta^\sigma| = h,$$

a safe upper bound for the $k-$th coefficient of $m(x)$ will be $B_k = \binom{f}{k}\ h^k \leq (2h)^k$ and thus $B = (2h)^f$ is a safe absolute bound for *all* the coefficients of $m(x)$. Naturally, better bounds should be available. For instance, using theorem 8.8.12 of [BaS], one can show that $|\eta| \leq \frac{8}{f}\sqrt{q}\log(q)|$, thus yielding a safe bound $B' = \left(\frac{8h}{f}\right)^{f/2} = O\left(\frac{8q}{f^2}\right)^{f/2}$.

We shall now treat the problem of retrieving simple and multiple Jacobi-Sums from the Gauss Periods.

2.5.2 Simple and Multiple Jacobi-Sums

In order to construct Jacobi-Sums, the same algorithm used above can lead to the values of $\nu(\eta)$ in a finite field $\mathbb{F}_r$. Note that the only difference is the size of the characteristic r of $\mathbb{K}$: since the coefficients of Jacobi-Sums have upper bounds $< q$, the characteristic will be moderate too, which is a computational advantage.

Let q be like above and χ a character of conductor q and order $f, \rho \in \mathbb{C}$ a primitive $f-$th root of unity. Let $\mathbb{K}$ thus be as defined in the previous section and denote by ν the image in $\mathbb{K}$ of a Gauss Period of conductor q and order f. Assume that r is chosen such that $\Phi_f(x)$ is irreducible modulo r, so that ρ may be identified to an element over $\mathbb{F}_r$. Let $\mathbb{L}$ be a field containing $\mathbb{F}_r$ and ρ. Then the Gauss-Sums are

$$\tau(\chi^k) = \sum_{i=0}^{f-1} \rho^{ki}\nu(\tau^i(\eta)), \tag{2.88}$$

where τ generates the group G.

Once the Gauss-Sums computed, the Jacobi-Sums follow by their definition (2.29). For simple Jacobi-Sums, one uses

$$j(\chi^a, \chi^b) = \frac{\tau(\chi^a)\tau(\chi^b)}{\tau(\chi^{a+b})} = \chi(-1)^{a+b}\frac{\tau(\chi^a)\tau(\chi^b)\tau(\chi^{-(a+b)})}{q}, \tag{2.89}$$

for multiple Jacobi-Sums,

$$J_k(\chi) = \frac{\tau(\chi)^k}{\tau(\chi^k)} = \chi(-1)^k\frac{\tau(\chi)^k \cdot \tau(\chi^{-k})}{q}. \tag{2.90}$$

Note that by (2.89), each calculation of Jacobi-Sum involves 2 multiplications in $\mathbb{L}$.

In cyclotomy primality proving, we deal with conductors q such that $q-1$ is highly composite and splits in a product of powers of small primes:

$$q - 1 = \prod_k p_k^{v_k}.$$

We are interested in virtually all Jacobi-Sums of characters with conductor q and order $l|p_k^{v_k}$. Since all the respective Gauss Periods may be computed in the same field $\mathbb{F}_r$, much of the work may be done in common. Let $L = \{l|p_k^{v_k} : p_k^{v_k}||(q-1)\}$, $G_l \subset (\mathbb{Z}/q\cdot\mathbb{Z})^*$ be the subgroup of order l in $(\mathbb{Z}/q\cdot\mathbb{Z})^*$ and

$$\Theta = \{\eta_{\tau_l} : \tau_l \in G_l, l \in L\}.$$

The set Θ may be generated by computing sequentially all powers $\zeta^h \in \mathbb{F}_r : h \in (\mathbb{Z}/q-1 \cdot \mathbb{Z})$ and adding then to the due elements $\eta_{\tau_l} \in \Theta$. The computation of Jacobi-Sums proceeds as above.

We can state following:

Algorithm Ia *(* Computation of Jacobi-Sums *)*

Let q be a prime and $f > 1$ with $f \mid (q-1)$ and $1 < b < q-1$

1. Find a prime r such that:

   (i) $r > q$
   (ii) $r = 1 \mod q$.
   (iii) The polynomial $\Phi_f(x)$ is irreducible modulo r.

2. Let ζ, ρ be primitive $q-$th and $f-$th roots of unity over $\mathbb{F}_r$ – their degrees being, by the definition of r equal to 1 and $\varphi(f)$, respectively. Let $\mathbb{L} = \mathbb{K}[\rho]$.

3. Compute all Gauss Periods η_τ of conductor q and order f in $\mathbb{F}_r$.

4. Compute the Gauss-Sums in $\mathbb{L}$.

5. Compute the Jacobi by multiplication of Gauss-Sums (2.89). in $\mathbb{L}$, using (2.90)

The work for a fast method of computation of Jacobi-Sums is on going. Some results concerning the map form $\mathbb{C}_q(\xi)$ to general galois fields, which have not yielded yet improvements of the calculation method have been skipped in this presentation. So far, the algebraic approach has succeeded in solving the space limitation for computing Jacobi-Sums. The time problem is open.

Vedi cara, e difficile spiegare,
e difficile capire,
sè non hai capito già ...

Guccini

Chapter 3

Cyclotomic extensions of fields and rings

In primality testing we face the paradoxical situation of working over rings $(\mathbb{Z}/n \cdot \mathbb{Z})$, using ring properties in order to prove that n was actually prime and $(\mathbb{Z}/n \cdot \mathbb{Z})$ a field. Since this obviously cannot be assumed from the beginning, we shall need to develop some concepts concerning cyclotomic extensions of $(\mathbb{Z}/n \cdot \mathbb{Z})$.

We are also interested in the complex cyclotomic extensions of $\mathbb{Q}$ and especially in their orders of integers and Artin maps. In §3.1 we shall review classical results from this domain. Some of the proofs are new and were preferred either for their simplicity or for the use of techniques which can also be applied over rings. The topics of this section may found, for instance in, [Ono], [Lo], [IR].

In §3.2 we define cyclotomic extensions of rings $(\mathbb{Z}/n \cdot \mathbb{Z})$. We use the term

and definition introduced by Lenstra in [Le2], since we are interested in the problem of constructing these structures as extensions of rings, in which primality proofs can be performed. The term "cyclotomic constellation", which stresses the fact that cyclotomic extensions of $(\mathbb{Z}/n \cdot \mathbb{Z})$ of order s exist only for certain pairs (n, s) - "constellations" - was used instead of "extension" in [BovdH]. We prove a long list of equivalent properties of cyclotomic extensions. With these, we establish, among others, the relation between:

(i) existence of an $s-$th cyclotomic extension of $(\mathbb{Z}/n \cdot \mathbb{Z})$.

(ii) the property (1.11), which is relevant for primality testing.

(iii) factoring of the cyclotomic polynomial.

(iv) special properties of Gauss-Sums.

(v) properties of mappings of the integer orders of cyclotomic extensions of $\mathbb{Q}$ into cyclotomic extensions of $(\mathbb{Z}/n \cdot \mathbb{Z})$.

We also give a new, efficient formula for the Lucas - Lehmer method of finding roots of unity and building extensions. In the last section we treat separately the topic of intermediate extensions of cyclotomic extensions of rings. This gives rise to interesting necessary and sufficient conditions for combining known cyclotomic extensions. This can be applied when building working extensions or when combining Lucas - Lehmer and Jacobi-Sum tests.

3.1 Cyclotomic fields and the Artin map

Let $m > 2$ be an integer and $\zeta_m \in \mathbb{C}$ be a primitive $m-$th root of unity; let $\mathbb{C}_m = \mathbb{Q}[\zeta_m]$ be the $m-$th cyclotomic field; m is the order of $\mathbb{C}_m$ and $\varphi(m) = [\mathbb{C}_m : \mathbb{Q}]$ is the degree of $\mathbb{C}_m$. The galois group Gal $(\mathbb{C}_m/\mathbb{Q})$ is isomorphic to $(\mathbb{Z}/m \cdot \mathbb{Z})^*$. If a is coprime to m and σ_a is the automorphism of $\mathbb{C}_m$ with $\sigma_a(\zeta_m) = \zeta_m^a$, then the map $\alpha : a \rightarrow \sigma_a$ is a group isomorphism between $(\mathbb{Z}/m \cdot \mathbb{Z})^*$ and Gal $(\mathbb{C}_m/\mathbb{Q})$. Let $H \subset (\mathbb{Z}/m \cdot \mathbb{Z})^*$ be a subgroup, $G = (\mathbb{Z}/m \cdot \mathbb{Z})^*/H$ and $\mathbb{L} = \mathbb{C}_m^H$. Let $H^{\perp} = \{\chi \in (\mathbb{Z}/m \cdot \mathbb{Z})^{\perp} \ : \ \chi(x) = 1, \forall\, x \in H\}$; $H^{\perp}$ is called the *annihilator* of H. We have following diagram:

$$\begin{array}{ccccc}
\mathbb{Q} & \rule[0.5ex]{2cm}{0.4pt} & \mathbb{L} & \rule[0.5ex]{2cm}{0.4pt} & \mathbb{C}_m \\
| & & | & & | \\
\{e\} & \rule[0.5ex]{2cm}{0.4pt} & G & \rule[0.5ex]{2cm}{0.4pt} & (\mathbb{Z}/m \cdot \mathbb{Z})^* \\
| & & | & & | \\
(\mathbb{Z}/m \cdot \mathbb{Z})^* & \rule[0.5ex]{2cm}{0.4pt} & H & \rule[0.5ex]{2cm}{0.4pt} & \{e\} \\
| & & | & & | \\
(\mathbb{Z}/m \cdot \mathbb{Z})^{\perp} & \rule[0.5ex]{2cm}{0.4pt} & H^{\perp} & \rule[0.5ex]{2cm}{0.4pt} & \{\mathbf{1}\}
\end{array} \tag{3.1}$$

The first line presents inclusions of fields, the second, the corresponding galois groups. The third contains the automorphisms under which the fields in the first line are invariant and the last line shows the annihilators of the groups in the third line. We shall not explicitly use this diagram in the subsequent proofs, but it will be very useful as a background situation map, whenever we deal with intermediate fields, galois- and character groups.

Fact 3.2 (see [Lo], p.88) *If $m = p^k$ is a prime power, then p is the only prime which is ramified in $\mathbb{C}_{p^k}$; p is in fact totally ramified and $(\pi) = p^{\varphi(p^k)}$ with $\pi = (1 - \zeta_{p^k})$. The order of the integers in $\mathbb{C}_{p^k}$ is $\mathbf{A}_{p^k} = \mathbb{Z}[\zeta_{p^k}]$. The discriminant of $\mathbb{C}_{p^k}$ is:*

$$d(\mathbb{C}_{p^k}) \quad = \quad (-1)^t \ (pk - k - 1)p^{p^{k-1}}, \tag{3.3}$$

where $t = \frac{p-1}{2}$ for odd p and $t = 2^{k-1}$ for $p = 2$.

Definition 3.4 *If $\mathbb{K}$ is a field and $\mathbb{F}, \mathbb{L}$ are extensions, $\mathbb{F}$ and $\mathbb{L}$ are linearly disjoint over $\mathbb{K}$, if any finite set of elements in $\mathbb{F}$ which is linearly independent over $\mathbb{K}$ is also linearly independent over $\mathbb{L}$.*

Fact 3.5 *It can be shown ([Lo], pp.90-92), that if $\mathbb{F}$ and $\mathbb{L}$ are linearly disjoint over $\mathbb{Q}$, and their discriminants are coprime: $(d(\mathbb{F}), d(\mathbb{L})) = 1$, then $O(\mathbb{F} \cdot \mathbb{L}) = O(\mathbb{F}) \cdot O(\mathbb{L})$*

where $O(.)$ is the ring of integers of a field. Also, $d(\mathbb{F}\cdot\mathbb{L}) = d(\mathbb{F})^{[\mathbb{L}:\mathbb{Q}]}\cdot d(\mathbb{L})^{[\mathbb{F}:\mathbb{Q}]}$. For $(m,m')=1$, the cyclotomic fields $\mathbb{C}_m$ and $\mathbb{C}_{m'}$ are linearly disjoint; their discriminants are coprime - as follows from fact (3.2), by induction on the number of primes dividing m and m'. For the ring of integers $O(\mathbb{C}_m)$ it follows that $O(\mathbb{C}_m)=\mathbb{Z}[\zeta_m]$. Furthermore, if $\mathbb{K}_m$ and $\mathbb{K}_{m'}$ are subfields of $\mathbb{C}_m$ and $\mathbb{C}_{m'}$ respectively, then $\mathbb{K}_m$ and $\mathbb{K}'_m$ are a fortiori linearly disjoint.

We want to find bases for the intermediate fields of a cyclotomic extension and for the integers in those fields. Due to (3.5), we can concentrate on cyclotomic extensions of prime power order p^k.

Fact 3.6 *If $p=2$ and $k>2$, the galois group Gal $(\mathbb{C}_{2^k}/Q)=(\mathbb{Z}/2^k\cdot\mathbb{Z})^*$ is not cyclic and has three subgroups of index 2. These are $G_1=(\mathbb{Z}/2^{k-1}\cdot\mathbb{Z})^*$, $G_2=<5>$ and $G_3=<-5>$ to which correspond the factor groups $H_1=<-1>$, $H_2=<5^{2^{k-3}}>$, $H_3=<-5^{2^{k-3}}>$ and the subfields $\mathbb{L}_1=\mathbb{C}_{2^{k-1}}$, $\mathbb{L}_2=\mathbb{Q}[\eta_k]$ and $\mathbb{L}_3=\mathbb{Q}[\eta'_k]$, where $\eta_k=\zeta_{2^k}+\zeta_{2^k}^{-1}$ and $\eta'_k=\zeta_{2^k}-\zeta_{2^k}^{-1}$. Note that the extensions $\mathbb{L}_2$ and $\mathbb{L}_3$ are cyclic. Furthermore, $\eta_k^2=\eta_{k-1}+2$ and $\eta_k'^2=\eta'_{k-1}-2$, so that $\mathbb{Q}[\eta_k]\supset\mathbb{Q}[\eta_{k-1}]$ and $\mathbb{Q}[\eta'_k]\supset\mathbb{Q}[\eta'_{k-1}]$. This settles the question of bases for $p=2$. As for the integer bases, they are given by (3.2) for the case of $\mathbb{L}_1$. As for $\mathbb{L}_2$, the trace $\mathbf{Tr}(\mathbb{Q}[\eta_k]/\mathbb{Q}[\eta_{k-1}])(\eta_k)=0$, so $\{1,\eta_k\}$ is a base for the integers of $\mathbb{Q}[\eta_k]$ over $\mathbb{Q}[\eta_{k-1}]$. By induction also, if $\mathbf{A}_{k-1}$ is a base for the integers in $\mathbb{Q}[\eta_{k-1}]$ and μ generates Gal $(\mathbb{Q}[\eta_k]/\mathbb{Q})$, then the set*

$$\mathbf{A}_k \;=\; \mathbf{A}_{k-1}\;\cup\;\{\mu^i(\eta_k)\;:\;i=0,1,...,2^k-1\}$$

is a base for the integers of $\mathbb{Q}[\eta_k]$. The situation is analogous for $\mathbb{L}_3$.

Let now p be an odd prime and consider first the case $k=1$.

Definition 3.7 *Let $\mathbb{K}$ be a field over $\mathbb{L}$ and suppose $\mathbb{K}$ has a base $[\alpha_i]$ over $\mathbb{L}$ made up of conjugate elements. Then $[\alpha_i]$ is called a normal base. If the integers $O(\mathbb{K})$ have a base $[\beta_i]$ over $\mathbb{L}$, which is made up of conjugate elements, then $[\beta_i]$ is called a normal integer base. Obviously, a normal integer base is a normal base.*

Lemma 3.8 *Let $\mathbb{K}$ be a field over $\mathbb{L}$. If $\mathbb{K}$ has a normal integer base $[\beta_i]$ over $\mathbb{L}$, then every intermediate field $\mathbb{K}\supset\mathbb{F}\supset\mathbb{L}$ has a normal integer base over $\mathbb{L}$.*

Proof Let $G=$ Gal $(\mathbb{K}/\mathbb{L})\supset H=$ Gal $(\mathbb{F}/\mathbb{L})$. Let α be an integer in $\mathbb{F}$; α can be expressed in terms of the base $[\beta_i]$; this base is normal and can be indexed by the automorphisms in G:

$$\alpha \;=\; \sum_{\sigma\in G} c_\sigma\cdot\beta_\sigma,\quad \text{where } c_\sigma\in O(\mathbb{L}) \tag{3.9}$$

Let $\tau\in G/H$; then $\tau\alpha=\alpha$, hence

$$\alpha \;=\; \sum_{\sigma\in G} c_\sigma\cdot\beta_\sigma \;=\; \sum_{\sigma\in G} c_{\sigma\tau^{-1}}\cdot\beta_\sigma.$$

Consequently $c_\sigma=c_{\sigma\tau^{-1}}$ for all $\tau\in G/H$. Let $\eta_\theta=\sum_{\tau\in G/H}\beta_{\sigma\tau}$ where $\eta\in H$ and σ is some representative of the coset $\theta\cdot H$ in G. By the above, $[\eta\theta\;:\;\theta\in H]$ is a normal integer base of $\mathbb{F}$ over $\mathbb{L}$. □

3.1.1 Integers in the cyclotomic field $\mathbb{C}_{p^k}$

By (3.2), $O(\mathbb{C}_p) = \mathbb{Z}[\zeta_p]$. Since $\sum_{i=1}^{p-1} \zeta_p^i = -1$, $\{\zeta_p^i \ : \ i \in (\mathbb{Z}/p\cdot\mathbb{Z})^*\}$ is a normal integer base for $\mathbb{C}_p$. Let H be a subgroup of $(\mathbb{Z}/p\cdot\mathbb{Z})^*$, $G = (\mathbb{Z}/p\cdot\mathbb{Z})^*/H$ and $\mathbb{L} = \mathbb{C}_p^G$. By the above lemma, $[\eta^\theta \ : \ \theta \in H]$ is a normal integer base for $\mathbb{L}$, where $\eta = \mathbf{Tr}(\mathbb{C}_p/\mathbb{L})(\zeta_p)$. This settles the case for k=1. Let now $k > 1$. Since $\sum_{i\in(\mathbb{Z}/p^k\cdot\mathbb{Z})^*} \zeta_{p^k}^i = 0$, ζ_{p^k} does not generate a normal base for $\mathbb{C}_{p^k}$. In the theory of abelian extensions, a subfield $\mathbb{L}$ of $\mathbb{C}_m$ is told to have *conductor* m, if $\mathbb{L} \subset \mathbb{C}_{m'}$ for no $m'|m$, $m' \neq m$. If $\mathbb{L}$ has conductor p^k and H is the subgroup of Gal $(\mathbb{C}_{p^k}/\mathbb{Q})$ such that $\mathbb{L} = \mathbb{C}_{p^k}^H$, then the annihilator $H^\perp$ of H is made up of primitive characters of conductor p^k [Lo]. Following theorem gives a base for $\mathbb{L}$.

Theorem 3.10 *Let $\mathbb{L}$ be a field of conductor p^k and $\eta = \mathbf{Tr}(\mathbb{C}_{p^k}/\mathbb{L})(\zeta_{p^k})$. Then $\mathbb{L} = \mathbb{Q}[\eta]$, i.e. η generates the field $\mathbb{L}$.*

Proof This theorem is usually proved in literature by using Gauss-Sums. We shall give here a proof which only uses the cyclic galois group of $\mathbb{L}$.

Since $\eta \neq 0$ ($\mathbb{L}$ has conductor p^k) the field $\mathbb{L}' = \mathbb{Q}[\eta] \neq 0$. Let $G =$ Gal $(\mathbb{L}/\mathbb{Q})$ and $H =$ Gal $(\mathbb{C}_{p^k}/\mathbb{Q})/$ Gal $(\mathbb{L}/\mathbb{Q})$. The minimal polynomial of η over $\mathbb{Q}$ is cyclic and thus $\mathbb{L}'$ is a galois extension and has a base of conjugates $\{\tau\eta \ : \ \tau \in G\}$ of η over $\mathbb{Q}$ and $L' \subset \mathbb{L}$. Let $\sigma_h = \sigma_h(\zeta_{p^k}^\sigma \ : \ \sigma \in H)$ be the elementary symmetric polynomials, $t = \#H$ and $s_h = \sum_{\sigma\in H} \zeta_{p^k}^{h\sigma}$ be the sums of $h-$th powers of ζ_{p^k} over $\mathbb{L}'$ $(h = 1, 2, \ldots, t)$. Obviously, $s_h = \eta^{\tau(h)}$ for some $\tau(h) \in H$, so $s_h \in \mathbb{L}'$. The Newton formulæ([Ku], pp 341-342) establish the connection between s_i and σ_j:

$$\begin{aligned} s_h - s_{h-1}\cdot\sigma_1 + \ldots + (-1)^{h-1}s_1\cdot\sigma_{h-1} + (-1)^h h\sigma_h &= 0 \ \text{ for } h \leq t \\ s_h - s_{h-1}\cdot\sigma_1 + \ldots + (-1)^t s_{h-t}\sigma_t &= 0 \ \text{ for } h > t \end{aligned} \tag{3.11}$$

Since $\mathbb{L}$ has conductor p^k and $t \mid (p-1) < p$, (3.11) yields a regular linear system in the unknowns $\sigma_h, (h = 1, 2, \ldots, t)$ and thus $\sigma_h \in \mathbb{L}'$ and ζ_{p^k} has a minimal polynomial of degree t over $\mathbb{L}'$. But $[\mathbb{C}_{p^k} : L'] \leq t = [\mathbb{C}_{p^k} : \mathbb{L}]$; this shows that $\mathbb{L}' = \mathbb{L} = \mathbb{Q}[\eta]$. $\square$

We consider now the problem of finding a base for the integers in subfields of cyclotomic fields. Let from now on to the end of this section, p be odd and $k > 1$, $\mathbb{C}_{p^k}$ be the p^k-th cyclotomic field, g be a generator of $(\mathbb{Z}/p^k\cdot\mathbb{Z})^*$ and σ be the automorphism of $\mathbb{C}_{p^k}$ with $\sigma(\zeta_{p^k}) = \zeta_{p^k}^g$; thus σ generates Gal $(\mathbb{C}_{p^k}/\mathbb{Q})$. We shall also consider the subfields $\mathbb{C}_{p^h}$ generated by $\zeta_{p^h} = \zeta_{p^k}^{p^{k-h}}$. The automorphism σ induces automorphisms of $\mathbb{C}_{p^h}$, which generate the corresponding galois groups. We shall denote these induced automorphisms also by σ and regard them as actions of σ in $\mathbb{C}_{p^h}$. If $l|(p-1)$, we shall denote by $\mathbb{L}_{h,l}$ the fields of conductor p^h with $[\mathbb{L}_{h,l} : \mathbb{Q}] = p^{h-1}\cdot l$; we shall write $\mathbb{L}_h$ for $\mathbb{L}_{h,1}$, the subfield of $\mathbb{C}_{p^h}$ of degree p^{h-1}. In particular, $\mathbb{L}_1 = \mathbb{Q}$. We put $\eta_{h,l} = \mathbf{Tr}(\mathbb{C}_{p^h}/\mathbb{L}_{h,l})(\zeta_{p^h})$ and $\eta_h = \eta_{h,1}$; in particular, $\eta_1 = -1$. Let $\tau = \sigma^{p^{k-1}}$ and

$\theta = \sigma^{p-1}$, so that $< \tau > \times < \theta > =$ Gal $(\mathbb{C}_{p^k}/\mathbb{Q})$ and $\mathbb{L}_k = \mathbb{C}_{p^k}^{<\tau>}$. Using the same symbol for the automorphisms induced by τ in the subfields of $\mathbb{C}_{p^k}$, we also have $\mathbb{L}_h = \mathbb{C}_{p^h}^{<\tau>}$, for $1 \le h \le k$.

We know by (3.2), that the ring of integers in $\mathbb{C}_{p^h}$ is $\mathbf{A}_{p^h} = \mathbb{Z}[\zeta_{p^h}]$. Let $B_h = \{\zeta_{p^h}^i \ : \ i = 0, 1, \ldots, \varphi(p^h) - 1\}$ be the standard base of $\mathbf{A}_{p^h}$; then $B_{h+1} \supset B_h$ and we put $B_h^0 = \{\zeta_{p^h}^i \ : \ i = 0, 1, \ldots, \varphi(p^h) - 1; (i, p) = 1\} = B_h - B_{h-1}$. We shall denote by $[X]$ the $\mathbb{Z}$-lattice generated by a set X. We seek a set $\mathbb{C}_h^0$ such that:

$$\begin{aligned} (i) \qquad \tau(C_h^0) &= C_h^0 \\ (ii) \qquad [C_h^0] &= [B_h^0] \end{aligned} \tag{3.12}$$

Condition (ii) allows to replace the base B_h by $\bigcup_{l=1}^h C_l^0$, (i) makes C_h^0 closed under the action of τ and allows to take traces from C_{p^h} to $\mathbb{L}_h$. This shows that the sets C_h^0 can be used for finding integer bases in the fields $\mathbb{L}_{h,l}$.

For $h = 1$, $B_1 = \{\zeta_p^i \ : \ i \in (\mathbb{Z}/p \cdot \mathbb{Z})^*\} = C_1$. Let us fix h, $1 < h \le k$.

Lemma 3.13 *Let $A_{h,i}$ $(i = 1, 2, \ldots, p)$ be the subsets of $(\mathbb{Z}/p^{h-1} \cdot \mathbb{Z})$ with*

$$A_{h,i} = \{(i-1) \cdot p^{h-2} + l \ : \ l \in (\mathbb{Z}/p^{h-2} \cdot \mathbb{Z})\}.$$

Define $C_h^0 = \{\tau^i(\theta^j(\zeta_{p^h})) \ : \ i \in (\mathbb{Z}/(p-1) \cdot \mathbb{Z}), \ j \in \bigcup_{l=1}^{p-1} A_{h,l}\}$. Then C_h^0 satisfies (3.12).

Proof The first assertion follows directly from the definition. For the second, we need following two facts:

$$\begin{aligned} (a) \qquad & < g^{(p-1)p^{h-2}} \bmod p^h > = \{(1 + p^{h-1} \cdot (\mathbb{Z}/p \cdot \mathbb{Z})) \bmod p^h\} \\ (b) \qquad & \sum_{i=0}^{p-1} \zeta_{p^h}^{a+ip^{h-1}} = 0, \quad \text{for all } a \text{ with } (a,p) = 1 \end{aligned} \tag{3.14}$$

(b) is a consequence of $\sum_{i=0}^{p-1} \zeta_p^i = 0$, (a) establishes the identity between two definitions of the cyclic subgroup of order p in $(\mathbb{Z}/p^h \cdot \mathbb{Z})^*$; let G_h be this group and $Z_h = \{\zeta_{p^h}^j \ : \ j \in (\mathbb{Z}/p^h \cdot \mathbb{Z})^*/G_h\}$. If we define $E = (\mathbb{Z}/(p-1) \cdot p^{h-2} \cdot \mathbb{Z})$, then

$$Z_h = \{\sigma^j(\zeta_{p^h}) \ : \ j \in E\}.$$

Since $p-1$ and p^h are coprime, we can apply the Chinese remainder theorem to E and find

$$Z_h = \{\tau^i(\theta^j(\zeta_{p^h})) \ : \ i \in (\mathbb{Z}/(p-1) \cdot \mathbb{Z}), j \in (\mathbb{Z}/p^{h-2} \cdot \mathbb{Z})\}.$$

By definition of Z_h, it follows that for all $a \in (\mathbb{Z}/p^h \cdot \mathbb{Z})^*$, there is exactly one $c = c(a) \in G_h$, such that $\zeta_{p^h}^{ca} \in Z_h$. If we identify $A_{h,p}$ to $(\mathbb{Z}/p^{h-2} \cdot \mathbb{Z})$ in the definition of Z_h, we conclude that

$$\forall \ a \in (\mathbb{Z}/p^h \cdot \mathbb{Z})^* \quad \exists! \ c = c(a) \in G_h, \quad \text{such that} \quad \zeta_{p^h}^{ca} \notin C_h^0 \tag{3.15}$$

Since c is unique, it follows from (3.14)(b), that $\zeta_{p^h}^{ca} \in [C_h^0]$. Consequently we have

$$[C_h^0] \;=\; [B_h^0] \;=\; \left[\{\zeta_{p^h}^a \;:\; a \in (\mathbb{Z}/p^h \cdot \mathbb{Z})^*\}\right]$$

□

Remark 3.16 *Note that any $p-1$ sets $A_{h,i}$ could be allowed in the definition of C_h^0, as it can be easily seen from the proof of the lemma. This implies that for any $a \in (\mathbb{Z}/p^h \cdot \mathbb{Z})^*$, there is a set C_h^0 verifying (3.12) and which contains $\zeta_{p^h}^a$.*

Theorem 3.17 *Let $D_h^0 = \{\theta^j(\eta_h) \;:\; j \in \bigcup_{l=1}^{p-1} A_{h,l}\}$, for $h > 1$, $D_1^0 = \{1\}$. Define $D_h = \bigcup_{i=1}^{h} D_i^0$. Then D_h is a base for the integers in $\mathbb{L}_h$.*

Proof The proof goes like in Lemma (3.8), using the fact that C_h^0 is closed under the action of τ and the definition of D_h^0, which verifies $D_h^0 = (C_h^0)^{<\tau>}$. □

Theorem 3.18 *Let $l|(p-1)$ and $D_{h,l}^0 = \{\theta^j(\eta_{h,l}) \;:\; j \in \bigcup_{l=1}^{p-1} A_{h,l}\}$, for $h > 1$. Let $E_{h,l}^0 = \bigcup_{j=1}^{l} \tau^j(D_{h,l}^0)$ for $h > 1$ and $E_{1,l}^0 = \{\tau^j(\eta_{1,l}) \;:\; j = 1, 2, \ldots, l\}$. Define $E_{h,l} = \bigcup_{h=1}^{k} E_{h,l}^0$. Then $E_{h,l}$ is a base for the integers in $\mathbb{L}_{h,l}$.*

Proof The proof follows easily from the established facts. □

It is also interesting to consider the relative bases. For avoiding notational explosion, we shall illustrate this only for the extensions $\mathbb{L}_h/\mathbb{L}_{h-1}$.

Theorem 3.19 *Let ν generate the galois group $Gal\ (\mathbb{L}_k/\mathbb{L}_{k-1})$ for $k > 2$. Then $\mathbb{F}_k = \{1\} \cup \{\nu^j(\eta_k) \;:\; j = 1, 2, \ldots, p-1\}$ is a base for the integers in $\mathbb{L}_k/\mathbb{L}_{k-1}$.*

Proof The statement follows from the definition of D_k by factoring

$$\text{Gal}\ (\mathbb{L}_k/\mathbb{Q})\ /\ \text{Gal}\ (\mathbb{L}_{k-1}/\mathbb{Q}).$$

We have $\nu = \theta^{p^{k-2}}$ in the previous notation. □

Note that none of the integer bases found for odd p and $k > 1$ are normal. This explains the relatively involved deductions. We give now a lemma concerning the integers in an abelian field taken modulo a rational integer. This proposition will be used in the context of galois extensions of rings, which we introduce in the next paragraph.

Theorem 3.20 *Let $\mathbb{L} = \mathbb{Q}[\eta]$ be an abelian field of conductor m and $n > 1$ be such that $(m, n) = 1$. Then*

$$\eta \not\equiv \sigma(\eta)\ mod\ n \cdot O(\mathbb{L}), \qquad \forall\ \sigma \in\ Gal\ (\mathbb{L}/\mathbb{Q}) \tag{3.21}$$

Proof We use reduction ad absurdum. If (3.21) does not hold, there is a subgroup G of Gal $(\mathbb{L}/\mathbb{Q})$, such that $\eta = \sigma(\eta) \bmod n \cdot O(\mathbb{L})$, $\forall\, \sigma \in G$. Let u be the exponent of G and $\chi \in (\mathbb{Z}/m \cdot \mathbb{Z})^{\perp}$ a multiplicative character which does not vanish on G. We build the Gauss-Sum of χ in the ring $(O(\mathbb{L})/n \cdot O(\mathbb{L})) \otimes_Z \mathbb{Z}[\zeta_u]$, where ζ_u is a primitive $u-$th root of unity. It is easy to check that $\tau(\chi) = 0$ which is a contradiction to (2.29) and $(m, n) = 1$. This proves (3.21). □

Note that $d(\eta)$ is a multiple of the field discriminant $d(\mathbb{L})$, so it may contain factors coprime to m. If $p|d(\eta)$ and $(p, m) = 1$, the theorem (3.20) states that

$$\eta \neq \sigma(\eta) \bmod p \cdot O(\mathbb{L}).$$

However, the ideal $(\eta - \sigma(\eta), p) \neq O(\mathbb{L})$ in this case.

3.1.2 The Artin map

We shall now consider some facts on the Artin Symbol and Map. Except for theorem (3.29), these facts can be found, in a different notation in [Ono].

Definition 3.22 *Let $m > 2$ be an integer and $\mathbb{C}_m$, the $m-$th cyclotomic field, $\mathbb{C}_m \supset \mathbb{L}$. Let q be a prime with $(q, m) = 1$ and $\mathbf{q}$ a prime ideal laying above q in $\mathbb{L}$. The Artin Symbol ψ_q is the element of Gal $(\mathbb{L}/\mathbb{Q})$ with:*

$$\psi_q(\alpha) \;=\; \alpha^q \textit{ mod } \mathbf{q} \quad \forall\, \alpha \in O(\mathbb{L}) \tag{3.23}$$

If s is a natural number, $(s, m) = 1$ and $s = \prod_{q|s} q^{v(q)}$, the Artin symbol ψ_s is defined by multiplicativity from (3.23):

$$\psi_s \;=\; \prod_{q|s} \psi_q^{v(q)} \tag{3.24}$$

Note that ψ_s depends upon the field $\mathbb{L}$.

Lemma 3.25 *Let q be a prime, $(q, m) = 1$ and $\mathbb{L} \subset \mathbb{C}_m$. Then $\psi_q(\mathbb{L})$ is the restriction to $\mathbb{L}$ of $\psi_q(\mathbb{C}_m)$. Furthermore, $\psi_q(\mathbb{C}_m)(\zeta_m) = \zeta_m^q$.*

Proof Let $\mathbf{q}'$ be a prime laying above $\mathbf{q}$ in $\mathbb{C}_m$, $G =$ Gal $(\mathbb{L}/\mathbb{Q})$, $H = (\mathbb{Z}/m{\cdot}\mathbb{Z})^*/G$ and ν the natural projection $(\mathbb{Z}/m \cdot \mathbb{Z})^* \to G$. We shall write $\psi'_q = \psi_q(\mathbb{C}_m)$ and $\psi_q = \psi_q(\mathbb{L})$. Let $\alpha \in O(\mathbb{L})$. By definition, $\psi'_q(\alpha) = \alpha^q \bmod \mathbf{q}' = \alpha^q \bmod \mathbf{q}$. By taking the restriction to $\mathbb{L}$, it follows that $\psi_q = \nu(\psi'_q)$. Suppose $\psi'_q(\zeta_m) = \zeta_m^a$. Then

$$\left(\psi'_q(\zeta_m) = \zeta_m^a = \zeta_m^q\right) \bmod \mathbf{q}' \tag{3.26}$$

Thus $\zeta_m^q \cdot (1 - \zeta_m^{a-q}) = 0 \bmod \mathbf{q}'$ and since ζ_m^q is a unit, $(1 - \zeta_m^{a-q}) \in \mathbf{q}'$. Suppose $\eta = \zeta_m^{a-q} \neq 1$. Then η is a primitive $m'-$th root of unity for some $m'|m$, $m' \neq 1$. Consequently, $(N(1-\eta), q) = (m, q) = 1$, which is a contradiction to $(1 - \zeta_m^{a-q}) \in \mathbf{q}'$. So $\zeta_m^{a-q} = 1$ and $\psi'_q(\zeta_m) = \zeta_m^q$. □

Corollary 3.27 *The Artin symbol $\psi_s(\mathbb{L})$ is the restriction to $\mathbb{L}$ of the automorphism of $\mathbb{C}_m$ with $\zeta_m \to \zeta_m^s$.*

Proof From (3.25) and multiplicativity of the Artin symbol. $\square$

Definition 3.28 *The map $\psi : \mathbb{N}_m = \{s \in \mathbb{N} \ : \ (s,m) = 1\} \to \ Gal\,(\mathbb{L}/\mathbb{Q})$ is a surjective homomorphism. It is called the Artin Map of $\mathbb{L}$.*

We shall now investigate the situation when taking cyclotomic fields modulo a prime r not dividing m.

Theorem 3.29 *Let the situation be like in Lemma (3.25), $\mathbb{L}$ have the conductor m, q be odd and $\eta = \mathbf{Tr}(\mathbb{C}_m/\mathbb{L})(\zeta_m)$, $\psi_q = \psi_q(\mathbb{L})$. Then $\mathbb{F} = O(\mathbb{L})/\mathbf{q}$ is a field of characteristic q, $Gal\,(\mathbb{F}/\mathbb{F}_q) \cong < q >_{\mathbb{L}}$, where $< q >_{\mathbb{L}}$ is the image of $< q \bmod m >$ under the natural map of $(\mathbb{Z}/m\cdot\mathbb{Z})^*$ onto $Gal\,(\mathbb{L}/\mathbb{Q})$ and $[\mathbb{F} : \mathbb{F}_q] = t \,|\, \# < q \bmod m >$. The Frobenius automorphism generating $Gal\,(\mathbb{F}/\mathbb{F}_q)$ is $\theta_q = \psi_q \bmod \mathbf{q}$. Furthermore, $O(\mathbb{L})/(q\cdot O(\mathbb{L}))$ is a $((\mathbb{Z}/q\cdot\mathbb{Z}))$-algebra. If $H = \ Gal\,(\mathbb{L}/\mathbb{Q})/ < q >_{\mathbb{L}}$, then*

$$O(\mathbb{L})/(q\cdot O(\mathbb{L})) \ = \ (\mathbb{Z}/q\cdot\mathbb{Z})[\eta] \ = \ \prod_{h\in H} \mathbb{F}. \tag{3.30}$$

In particular, if $Gal\,(\mathbb{L}/\mathbb{Q}) =< q \bmod m >$, the Artin map $\psi_q = \psi_q(\mathbb{L})$ generates the galois group of $\mathbb{L}$, and $(\mathbb{Z}/q\cdot\mathbb{Z})[\eta] = \ \mathbb{F}$ is a field.

Proof By definition of ψ_q, $\psi_q(\alpha) = \alpha^q \bmod \mathbf{q}$, $\forall\ \alpha \in O(\mathbb{L})$, thus

$$\theta_q(\alpha \bmod \mathbf{q}) \ = \ (\alpha \bmod \mathbf{q})^q,$$

which settles the first statement. By (3.21) with $p = n, (d(\eta), q) = 1$, so

$$O(\mathbb{L})/(qO(\mathbb{L})) \ = \ (\mathbb{Z}/q\cdot\mathbb{Z})[\eta].$$

Let $f(x)$ be the minimal polynomial of η over $\mathbb{Z}$ and $\Psi_h(x) = \prod_{\tau\in h}\ (x - \eta \bmod q)$ for $h \in H$. Then $\Psi_h(x) \in (\mathbb{Z}/q\cdot\mathbb{Z})[x]$ and $f(x) = \prod_{h\in H} \Psi_h(x) \bmod q$. The second part of (3.30) follows from $\mathbb{F}_q \cong (\mathbb{Z}/q\cdot\mathbb{Z})[x]/(\Psi_h(x))$. The final special case is obvious; it has some useful consequences for constructing cyclotomic fields ([AdLe]). $\square$

3.2 Cyclotomic extensions of rings

We shall follow the line of [[Le2], §2, §4] keeping the generality to the minimum needed for our purposes and giving at places definitions which are closer to our testing concerns. Through this paragraph, n will be an odd positive integer and $\mathcal{N} = (\mathbb{Z}/n\cdot\mathbb{Z})$.

Definition 3.31 *If G is a group, a ring $\mathbf{R} \supset \mathcal{N}$ is called galois extension of $\mathcal{N}$ with group G, if, given $t = \#G$, there are t elements $z_1, z_2, \ldots, z_t \in \mathbf{R}$ such that:*

(i) $\mathbf{R} = \prod_{i=1}^{t} \mathcal{N} z_i$ *and the map $\mathcal{N} \to R$ is injective*

(ii) $\det(\sigma(z_i))_{\sigma \in G} \in \mathcal{N}^*$

Note that (ii) implies that the z_i must be independent.

Examples 3.32

(a) If $\mathbf{R}_i$ is galois over $\mathcal{N}$ with group G_i, for $i = 1, 2$ then $\mathbf{R}_1 \otimes_{\mathcal{N}} \mathbf{R}_2$ is galois over $\mathcal{N}$ with group $G_1 \times G_2$.

(b) if n is a prime, $\mathcal{N}$ is a galois field $\mathbb{K}$ and a galois extension $\mathbf{R}$ of $\mathbb{K}$ in the sense of field theory is a galois extension of $\mathcal{N}$ in the sense of (3.31).

(c) let s be a positive integer with $(n, s) = 1$ and ζ_s a primitive $s-$th root of unity in $\mathbb{C}$. The ring $\mathbf{R} = \mathbb{Z}[\zeta_s]/(n \cdot \mathbb{Z}[\zeta_s])$ is galois over $\mathcal{N}$ with group $G = (\mathbb{Z}/s \cdot \mathbb{Z})^*$. The element ($x$ mod s) acts upon $\mathbf{R}$ by raising ζ_s to the power x.

Indeed, put $z_i = \zeta_s^i$, for $i \in (\mathbb{Z}/s \cdot \mathbb{Z})^*$; (i) of (3.31) is easily checked and (ii) follows by properties of Vandermonde determinants and the identity

$$\prod_{i=1}^{s-1} (1 - \zeta_s^i) = s \in \mathcal{N}^*.$$

(d) consider example (c) with n a prime and $\mathcal{N}$ a galois field. If

$$H = (\mathbb{Z}/s \cdot \mathbb{Z})^* / < n \text{ mod } s >$$

and $t = \# < n$ mod $s >$ then

$$\mathbf{R} \;=\; \mathbb{Z}[\zeta_s]/(n\mathbb{Z}[\zeta_s]) \;\cong\; \prod_{\rho \in H} \mathbb{F}_{p^t} \tag{3.33}$$

by a known theorem of algebraic number theory [H.Cohn]. We shall investigate integers n that lead to the decomposition (3.33) of the ring $\mathbb{Z}[\zeta_s]/(n\mathbb{Z}[\zeta_s])$.

We let throughout this paragraph s be a positive integer, $t = \# < n \bmod s >$ and suppose $(n, st) = 1$. We denote as usual the $s-$th cyclotomic polynomial by Φ_s.

Definition 3.34 ([Le2], (4.1)) *An $s-$th cyclotomic extension of $\mathcal{N}$ is an $\mathcal{N}$-algebra $\mathbf{R}$ together with an automorphism σ of $\mathbf{R}$ and an element $\zeta \in \mathbf{R}$ such that:*

(i) $\mathbf{R}$ is galois over $\mathcal{N}$ with group generated by σ.

(ii) $\Phi_s(\zeta) = 0$ *and* $\sigma\zeta = \zeta^n$.

(iii) $\sigma^t = id_{\mathbf{R}}$.

s is the order and t is the degree of the extension $\mathbf{R}$.

Cyclotomic extensions do not exist for every pair (n, s) – the existence of an $n-$th cyclotomic extension of $\mathcal{N}$ can be regarded as a property of n. This fact can be used for primality testing.

In the next theorems we shall prove some properties equivalent to (3.34), which can alternatively be used for primality testing.

Theorem 3.35 *Let* $\mathbf{A}$ *be the ring of integers in* $\mathbb{L}_n = \mathbb{Q}[\xi_s]^{<n \bmod s>}$ *and* $\Psi_0(x) = \prod_{i=1}^{t-1} (x - \xi_s^{n^i}) \in \mathbf{A}[x]$*,* ξ_s *being a primitive* $s-$th *root of unity in* $\mathbb{C}$.

The following statements are equivalent:

(I) an $s-$th *cyclotomic extension of* $\mathcal{N}$ *exists*

(II) $r|n \longrightarrow r \in < n \bmod s >$ *("divisor property")*

(III) there is a surjective ring homomorphism $\tau_0 : \mathbf{A} \to \mathcal{N}$ *("squeezing automorphism")*

Proof Assume (I) holds and let $(\mathbf{R}, \sigma, \zeta)$ be an $s-$th cyclotomic extension of $\mathcal{N}$. Put $\Psi(x) = \prod_{i=1}^{t} (x - \sigma^i(\zeta)) \in \mathcal{N}[x]$. Let $\tau : \mathbb{Z}[\xi_s] \to \mathbf{R}$ be defined by $\tau(\xi_s) = \zeta$. The restriction τ_0 of τ to $\mathbf{A}$ is given by:

(a) $\tau_0(a_i) = b_i$, where a_i, b_i are the coefficients of Ψ_0 and Ψ, respectively.

(b) $\tau_0(p(a_1, a_2, \ldots, a_t)) = p(b_1, b_2, \ldots, b_t) \bmod n$, p being any polynomial in $\mathbb{Z}[x_1, \ldots, x_t]$.

The coefficients of $\Psi_0(x)$ are the elementary symmetric functions, invariant under $< n \bmod s >$; they generate $\mathbf{A}$ by (3.11). The map τ_0 is by definition a homomorphism and it follows from (a) and (b) that it maps $\mathbf{A}$ into $\mathcal{N}$. It is surjective, since $\tau_0(\mathbb{Z}) = \mathcal{N}$. Thus $(I) \to (III)$.

Suppose (III) holds and let $\Psi(x) = \tau_0(\Psi_0(x))$. Put $\mathbf{R} = \mathcal{N}[x]/(\Psi(x))$ and $\zeta = x + (\Psi(x)) \in \mathbf{R}$. Then $\Psi(\zeta) = 0$. By definition of Ψ, $\Psi(x)|\Phi_s(x) \bmod n$ and consequently $\Phi_s(\zeta) = 0$. By lifting τ_0 to a homomorphism $\tau : \mathbb{Z}[\xi_s] \to \mathbf{R}$ with $\zeta = \tau_0(\xi_s)$, we deduce $\Psi(x) = \prod_{i=1}^{t} (x - \zeta^{n^i})$. Any element $x \in \mathbf{R}$ which is invariant under the substitutions $\zeta \to \zeta^{n^i}$, $i = 1, 2, \ldots, t$, is a symmetric polynomial in $E = \{\zeta^{n^i} : i = 1, 2, \ldots, t\}$ and is thus a polynomial in the coefficients of $\Psi(x)$, consequently belonging to $\mathcal{N}$. This shows that there is an automorphism σ of $\mathbf{R}$ with $\sigma\zeta = \zeta^n$ and $\sigma^t = \mathrm{id}_{\mathbf{R}}$; finally, $(\mathbf{R}, \sigma, \zeta)$ is an $s-$th cyclotomic extension of $\mathcal{N}$ and $(III) \to (I)$. Furthermore, if $r|n$ is a prime and $\mathcal{M}$ is a maximal ideal of $\mathbf{R}$ containing r, $\mathbb{K} = \mathbf{R}/\mathcal{M}$ and ν the projection $\mathbf{R} \to \mathbb{K}$, let $\alpha = \nu(\zeta)$. Then

$$\Psi_r(x) \;=\; \nu(\Psi(x)) \;=\; \prod_{i=1}^{t} (x - \alpha^{n^i}) \;\in\; \mathbb{F}_r[x],$$

since $\nu(\mathcal{N}) = \mathbb{F}_r$.

The polynomial Ψ_r has as roots α together with its conjugates over $\mathbb{F}_r$, which are the images of α under the Frobenius automorphisms of $\mathbb{F}_r[\alpha]$. In particular $\alpha^r = \alpha^{n^k}$ for some $k \in \{1, 2, \ldots, t\}$ and $\alpha^{n^k - r} = 1$. Since $\Psi_r(x) | \Phi_s(x)$, α is a primitive $s-$th root of unity and $r = n^k \bmod s$ or $r \in < n \bmod s >$. The property (II) for non prime $r|n$ follows by multiplicativity and $(III) \to (II)$.

Assume now that (II) holds and let $r|n$ be such that $r^k \| n$. The splitting of $\Phi_s(x)$, over $\mathbb{F}_r$ together with Hensel's lemma imply that there is a polynomial

$$\Psi_r(x) \;\in\; ((\mathbb{Z}/r^k \cdot \mathbb{Z}))[x]$$

together with a map $\tau_r : \mathbf{A} \to (\mathbb{Z}/r^k \cdot \mathbb{Z})$, such that $\tau_r(\Psi_0(x)) = \Psi_r(x)$. Let $\Psi(x) \in \mathcal{N}[x]$ be defined by the Chinese Remainder Theorem such that:

$$\Psi(x) \;=\; \Psi_r(x) \bmod r^k, \quad \forall\, r \text{ prime},\ r^k \| n \ \text{ and } \ \tau_0 = \prod_{r|n} \tau_r.$$

By definition of Ψ and τ_0, (III) is fulfilled and $(II) \to (III)$. □

The interest of cyclotomic extensions for primality testing is obviously given by statement (II). This statement is also used in the well-known Adleman test. We shall prove some more equivalent statements to $(I) - (III)$, which can be used for practical testing.

Theorem 3.36 *Following statements are equivalent to (I) - (III):*

(IV) there is a polynomial $\Psi(x) \in \mathcal{N}[x]$ of degree t with:

> *(i)* $\Psi(x) \,|\, \Phi_s(x)$
>
> *(ii) if $\zeta = x + (\Psi(x)) \in \mathcal{N}[x]/(\Psi(x))$, then $\Psi(\zeta^{n^i}) = 0$, for $i = 1, 2, \ldots, t$*
> *"proper factoring of the cyclotomic polynomial"*

(V) $H(r)^{\perp} \supset H(n)^{\perp}$ (defined in §2.2) and $\forall\, r|n$ "divisor annihilators"

Proof If (III) holds, then the polynomial $\Psi(x)$ in (IV) can be defined by $\Psi(x) = \tau_0(\Psi_0(x))$ and (IV) follows. Conversely if $\Psi(x) \in \mathcal{N}[x]$ has property (IV), let $\mathbf{R} = \mathcal{N}[x]/(\Psi(x))$ and $\zeta = x + (\Psi(x))$. Let $\tau : \mathbb{Z}[\xi_s] \to \mathbf{R}$ be defined by $\tau(\xi_s) = \zeta$. This map is well defined, since $\Phi_s(\zeta) = 0$; furthermore, (ii) implies that $\tau(\Psi_0) = \Psi$ and $(IV) \to (III)$ follows.

The implication $(II) \to (V)$ is trivial since $r \in < n \bmod s >$ implies $\chi(r) = \chi(n^k) = 1$, $\forall\, \chi \in H(n)^{\perp}$, where k is such that $r = n^k \bmod s$. Suppose that (V) holds and there is a $r|n$ with $r \notin < n \bmod s >$. A character $\chi \in H(n)^\perp$ is given by its values on $H(n)$, where $H(n) = (\mathbb{Z}/s\cdot\mathbb{Z})^*/ < n \bmod s >$. If ρ is the image of r in $H(n)$, then $\rho \neq 1$ and there is a $\chi \in H(n)^\perp$ with $\chi(\rho) \neq 1$, in contradiction to (V). Hence $(V) \rightarrow (II)$. $\square$

Note that (V) is a slight restriction of the condition used in the Adleman test:

$$\chi(r) = \chi(n^k) \qquad \forall\, r|n \text{ and } \forall\, \chi \in (\mathbb{Z}/s\cdot\mathbb{Z})^\perp. \tag{3.37}$$

The next theorem settles the connection between characters and their Gauss sums on one hand and degrees of sub extensions of cyclotomic extensions, on the other hand.

Theorem 3.38 *Let ξ_t be a complex primitive $t-$th root of unity,*

$$H(n) = (\mathbb{Z}/s\cdot\mathbb{Z})^*/ < n \text{ mod } s >$$

and $(\mathbf{R}, \sigma, \zeta)$ a $t-$th cyclotomic extension of $\mathcal{N}$. Then the following condition is equivalent to (I) - (V):

(VI) $\chi \in H(n)^\perp \iff \exists$ *a homomorphism* $\vartheta : \mathbb{Z}[\xi_t, \tau(\chi)] \rightarrow \mathbf{R}$.

(VII) If $G \subseteq (\mathbb{Z}/s\cdot\mathbb{Z})^*$ is a group and $\eta_G = \xi_s^G$, then $< n \text{ mod } s > \subseteq G \iff$ $\exists$ a homomorphism $\varsigma : O(\mathbb{Q}[\eta_G]) \rightarrow \mathcal{N}$.

Furthermore, if an $s-$th cyclotomic extension $(\mathbf{S}, \sigma_s, \zeta_s)$ of $\mathcal{N}$ exists, we write $\mathbf{B}_G = O(\mathbb{Q}[\xi_s]^G)$ for all subgroups $G \subseteq (\mathbb{Z}/s\cdot\mathbb{Z})^*$ and $\nu : \mathbb{Z}[\xi_s] \rightarrow \mathbf{S}$ is the natural projection of $\mathbb{Z}[\xi_s]$ into $\mathbf{S}$ then

(i) $\mathbf{S} = \mathcal{N}[\zeta_s]$

(ii) For all distinct groups $H, H' \supseteq G, \nu(\mathbf{B}_H) \neq \nu(\mathbf{B}'_H) \iff G \supset H(n)$

Proof We first prove (VI) $\iff$ (VII). Note that

$$\tau(\chi^k) \;=\; \frac{J_k(\chi)}{(\tau(\chi))^k} \;\in\; \mathbb{Z}[\xi_t, \tau(\chi)],\; \forall\, k \in (2, \dots, t).$$

Consequently, $\chi \in H(n)^\perp \iff \eta^{<n \bmod s>} \in \mathbb{Z}[\xi_t, \tau(\chi)]$. Let ϑ be the natural lifting of ς to $\mathbb{Z}[\xi_t, \tau(\chi)]$. The equivalence follows now easily. Suppose (VII) holds; η_G is mapped by ς into $\mathcal{N}$ iff $< n \bmod s > \subseteq G$, so $\tau(\chi)$ is mapped by ϑ into $\mathcal{N}$ iff χ annihilates $< n \bmod s >$, thus $\chi \in H(n)^\perp$. If (VI) holds, η_G is mapped by ϑ into $\mathbf{R}$ iff $< n \bmod s > \subseteq G$, thus (VII) holds. We shall prove (III) $\Longrightarrow$ (VII). If (III) holds, a map $\tau_0 : O(\mathbb{Q}[\eta_G]) \rightarrow \mathcal{N}$ exists for all groups $G \supseteq < n \bmod s >$. Suppose conversely, that $\varsigma : O(\mathbb{Q}[\eta_G]) \rightarrow \mathcal{N}$ is a ring homomorphism and let $r \mid n$ be a prime. Then $\varsigma_r = \varsigma \bmod r$ is a map of $O(\mathbb{Q}[\eta_G])$ into the prime field $\mathbb{F}_r$, thus $< r \bmod s > \subseteq G$. The implication $< n \bmod s > \subseteq G$ follows now by multiplicativity.

We now prove (VI) $\Longrightarrow$ (V). Let $r \mid n$ be prime and $\mathbb{F}$ be the minimal field of characteristic r which contains a $t-$th root of unit ω_t. Let $\chi \in H(n)^\perp$ and $\vartheta_r = \nu \circ \vartheta$, where ν is the projection from $\mathbf{R}$ to $\mathbb{F}$. Since $\mathbb{F}$ is a cyclotomic extension, from the implication that we proved, follows that $\chi \in H(r)^\perp$ iff ϑ exists; but by (VI) this is the case iff $\chi \in H(n)^\perp$. Thus $\chi(r) = 1$ for $\chi \in H(n)^\perp$; this proves (V).

We now prove the third part of the theorem. Since $\mathbf{S}$ is galois as cyclotomic extension, $\mathcal{N}[\zeta_s] \subset \mathbf{S}$; the other inclusion follows from $\sigma_s^t = Id_{\mathbf{S}}$ by comparing ranks. This proves (i). For $G = H(n)$, the map $\nu_{H(n)}$, which is the restriction of ν to $H(n)$, is rank conserving. If H, H' are distinct groups containing $H(n)$, then it follows that the ranks of $\nu_{H(n)}(\mathbf{B}_H)$ and $\nu_{H(n)}(\mathbf{B}_{H'})$ are different, being respectively equal to $\varphi(s)/\#H$ and $\varphi(s)/\#H'$. This shows that $H(n)$ has the property in (ii). Suppose that $G \not\supset H(n)$ has this property. Let $G^\perp = G \cap H(n)$. Then $\nu(\mathbf{B}_G) = \nu(\mathbf{B}_{G^\perp})$, in contradiction to the assumption. This proves (ii). $\square$

Remark 3.39 *The statement (VI) shows that the characters χ of conductor s, such that the image of $\tau(\chi)$ lays in $\mathcal{N}[\zeta_t]$ are exactly $H(n)^\perp$. For this reason we shall call these characters* **push** *characters. We shall also denote the characters $\chi \in (\mathbb{Z}/s\cdot\mathbb{Z})^\perp - H(n)^\perp$ by* **pop** *characters. If χ is a pop character and l is the order of the primitive root $\chi(n)$ ($l > 1$ by definition) then $\mathbf{R}[\tau(\chi)]$ has degree l over $\mathbf{R}$ since $\tau(\chi)^l \in \mathbf{R}$ by (2.30). By extending the homomorphism ϑ defined above, it follows that the same holds for the degree of the algebra $\mathbf{R}[\tau(\chi)]$ over $\mathbf{R}$. It follows that:*

$$[\mathbf{R}[\tau(\chi)] : \mathbf{R}] \;=\; \mathrm{ord}(\chi(n)) \qquad \forall\, \chi \in (\mathbb{Z}/s \cdot \mathbb{Z})^\perp, \tag{3.40}$$

where $\mathrm{ord}(\chi(n))$ is the order of $\chi(n)$ in $< \zeta_t >$.

We shall now investigate the connection between cyclotomic extensions of $\mathcal{N}$ and the Artin symbol.

Theorem 3.41 *The following statement is equivalent to (I) – (VII):*

(VIII) $\psi_r = \psi_n^i, \quad \forall\, r|n$, *for some* $i = i(r),\ 1 \le i \le t.$

Proof Suppose $(I) - (VII)$ hold. Then statement $(VIII)$ is a consequence of (V). Conversely, $(VIII)$ implies (II) by the isomorphism of the cyclic groups $< \psi_n >$ and $< n \bmod s >$. $\square$

Following theorem is useful for constructing cyclotomic extensions, as well as for generalized Lucas-Lehmer tests:

Theorem 3.42 *Let $\mathbb{L}$ be a field of conductor s, with $Gal\,(\mathbb{L}/\mathbb{Q}) = < n \bmod s >$ and $[\mathbb{L} : \mathbb{Q}] = t$. Suppose that*

$$\exists\, \alpha \in O(\mathbb{L}) \quad \textit{such that} \quad \psi_n(\alpha) = \alpha^n \ \textit{mod}\ n \cdot O(\mathbb{L}). \tag{3.43}$$

For $q|s$, *let* $(n^t-1)/q = \sum_{i=0}^{t-1} c_i(q)\cdot n^i$. *Let* $\mathbf{R} = O(\mathbb{L})/n\cdot O(\mathbb{L})$ *and suppose*

$$(\beta(q)-1)\in \mathbf{R}^*, \quad \textit{where} \quad \beta(q) \;=\; \prod_{i=0}^{t-1} (\psi_n^i(\alpha^{c_i(q)})) \textit{ mod } n\cdot O(\mathbb{L}). \tag{3.44}$$

Let $\beta = \prod_{q|s}\beta(q)$ *mod* $n\cdot O(\mathbb{L})$ *and* σ *be the automorphism induced by* ψ_n *in* $\mathbf{R}$. *Then* $(\mathbf{R},\sigma,\beta)$ *is an* $s-$th *cyclotomic extension of* $\mathcal{N}$.

Proof By Lemma (2.4), β is a primitive $s-$th root of unity in $\mathbf{R}$. If

$$\Psi(x) \;=\; \prod_{i=0}^{t-1} (x-\sigma(\beta)),$$

then $\Psi(x)\in\mathcal{N}[x]$ since ψ_n generates Gal $(\mathbb{L}/\mathbb{Q})$. The statement follows from (IV). $\square$

Remark 3.45 *In practical applications of (3.42),* $n \gg q$. *We show that there is a simple expansion of the shape* $(n^t-1)/q = \sum_{i=0}^{t-1} c_i(q)\cdot n^i$. *Let* $n = a\cdot q + b$, *with* $0\le b<q$. *Then*

$$(n^t-1)/q \;=\; ((n^t-b^t)+(b^t-1))/q \;=\; (b^t-1)/q + a\cdot\sum_{i=0}^{t-1} n^{t-i-1}\cdot b^i.$$

This leads to the equation:

$$(n^t-1)/q \;=\; \sum_{i=0}^{t-1} c_i(q)\cdot n^i, \qquad \textit{with } c_0(q) = (b^t-1)/q \tag{3.46}$$
$$\textit{and } c_i(q) = a\cdot b^i,\ \textit{for } i = 1,\ldots,t-1.$$

Note that $c_i(q)$ *are not necessarily* $< n$, *but* $c_i(q)/n$ *is at most a small number. The regular shape of the coefficients is however very useful for the simultaneous computation of an* α^n *and* $\alpha^{c_i(q)}$. *Suppose that the cost for the application of one automorphism* ψ_n *is* $c\cdot$ *(multiplication in* $\mathbf{R}$*) – if no fast polynomial multiplication methods are used,* $c=1$. *The time needed for the evaluation of* $\beta(q)$ *using (3.44) is bounded by*

$$2\cdot(t-1)(\log q + c + 1) + \log n.$$

This method of evaluation is thus for $t > (\log q)/\log(n/q^2\cdot 4^{c+1})$ *more efficient than defining* $\beta(q) = \alpha^{(n^t-1)/q}$, *and performing the direct exponentiation.*

We shall give now a condition for existence of an $s-$th cyclotomic extension of $\mathcal{N}$, given coprime s_1 and s_2 with $s = s_1\cdot s_2$ and such that s_i-th cyclotomic extensions of $\mathcal{N}$ are known to exist for $i=1,2$.

Theorem 3.47 (**"combining extensions"**) *Let* s_1 *and* s_2 *be coprime such that* $s = s_1\cdot s_2$ *and suppose* s_i-th *cyclotomic extensions of* $\mathcal{N}$ *are known to exist for* $i=1,2$. *For* χ *a character modulo* s, *let* $\chi = (\chi_1,\chi_2)$ *be the splitting of* χ *according to* s_1 *and* s_2 *(as defined in Lemma (2.24)). Then following condition is equivalent to* **(I) - (VIII)**

(IX) $\forall\, r|n, \chi \in H(n)^{\perp}$ *with* $\chi_1(n) \neq 1$, $\chi(r) = 1$ *holds. "condition for combining extensions"*

Proof The implication $(IX) \to (V)$ follows from the fact that for each $\chi \in H(n)^{\perp}$, either $\chi_1(n) = \chi_2(n) = 1$, in which case $\chi(r) = 1$ by hypothesis or $\chi_1(n) = \chi_2(n)^{-1} \neq 1$ and the condition X requires thus $\chi(r) = 1$, $\forall\, \chi \in H(n)^{\perp}$. The implication $(V) \to (X)$ is trivial. □

Note that if $\chi_1(n) \neq 1$, from $\chi \in H(n)^{\perp}$ follows $\chi_1(n) = \chi_2^{-1}(n)$, and the order of the root of unity $\chi_1(n)$ is a divisor of (t_1, t_2), since the orders of χ_i are divisors of $t_i = \mathrm{ord}_{s_i}(n)$, $i = 1, 2$.

Corollary 3.48 *If* n, s_1, s_2, t_1, t_2 *are as above and* $(t_1, t_2) = 1$, *then an* $s-$th *cyclotomic extension of* $\mathcal{N}$ *exists.*

This theorem gives a practical approach to combining cyclotomic extensions, which are proved to exist by different or similar methods. This is the object of [[Le2], (6.9)].

This completes the sequence of equivalent statements defining an $s-$th cyclotomic extension of $\mathcal{N}$. Note that (IX) is an exception in this sequence, since it cannot be used as definition, unless prime power extensions are first defined by an induction hypothesis. We shall now investigate explicitly the case when s is not square free and give following:

Definition 3.49 *Let* $(\mathbf{R}, \sigma, \zeta)$ *be a* p^k-th *cyclotomic extension of* $\mathcal{N}$, *for a certain prime power* $p^k, k \geq 1$. *If* k *is such that:*

$$k \geq k_s(p) \quad = \quad \begin{cases} \max_h \{2^h \mid (n^2-1)\} & \text{if } p = 2 \text{ and } n = -1 \bmod 4 \\ \\ \mathrm{ord}_p(n) & \text{otherwise} \end{cases} \tag{3.50}$$

Then the ring $\mathbf{R}$ *is called* **saturated** *and* k_s *is called the* **saturation exponent**. *If* $k < k_s$, $\mathbf{R}$ *is* **subsaturated**.

Note that using the term "saturated p^h-th extension", one implicitly asserts $h \geq k_s(p)$. This implicit assertion is compact and will be used repeatedly in the rest of this thesis. We shall also use the expression *saturated* $p-$th cyclotomic extension in order to denote an extension which not only contains a $p-$th root but also a saturated $p^{k_s}-$th primitive root of unity. Saturated extensions are characterized by following property:

Theorem 3.51 *If* $(\mathbf{R}, \sigma, \zeta)$ *is a saturated* $p^{k_s}-$th *extension and* $h > k_s$ *then a* p^h-th *extension of* $\mathcal{N}$ *exists.*

Proof Consider $h > k_s$, $\mathbf{R}(h) = \mathbf{R}[x]/(x^{p^{(h-k_s)}} - \zeta)$ and let $\zeta(h)$ be the image of x in $\mathbf{R}(h)$. It is easy to establish by comparing ranks, that $(\mathbf{R}(h), \sigma(h), \zeta(h))$ is an p^h-th cyclotomic extension – where $\sigma(h)$ is the extension of σ to $\mathbf{R}(h)$. □

We shall use for commodity, the term of *complete extension* for the union of all saturated extension of orders p^h:

Definition 3.52 *suppose a saturated* p^k-th *extension* $(\mathbf{R}, \sigma, \zeta)$ *of* $\mathcal{N}$ *exists and let:*

$$(\mathbf{R}_\infty\ (p), \sigma_\infty\ (p), \zeta_\infty\ (p)) \quad = \quad \bigcup_{h=k_s}^{\infty} (\mathbf{R}(h), \sigma(h), \zeta(h)). \tag{3.53}$$

$\mathbf{R}_\infty$ *is called complete* $p-$th *extension and its existence is granted by the premises and the preceding theorem.*

The definition of saturation is generalized to non prime orders s *as follows. Let* $(\mathbf{R}, \sigma, \zeta)$ *be an* $s-$th *cyclotomic extension of* $\mathcal{N}$ *and suppose that* $p^{k_s} \mid s, \forall$ *primes* $p \mid s$, *where* k_s *is the saturation exponent of* p. *Then* $\mathbf{R}$ *is a* saturated $s-$th *extension.*

Remark 3.54 *Theorem (3.51) motivates the denomination of "saturated". The existence of a saturated extension implies existence of any extension of degree built up of the primes dividing* s. *This is not the case for non saturated extensions as can be seen from following example.*

Example 3.55 *Let* $n = 91 = 7 \cdot 13$. *Then (II) implies that a third cyclotomic extension of* n *exists, since* $r \in < n \bmod 3 >$ *for all* $r|n$. *However, this extension is not saturated, since* $n = 1 \bmod 9$. *A saturated extension does in fact not exist, since* $r \notin < n \bmod 9 >$ *for all* $r|n$.

The proving of existence of cyclotomic extensions is thus focussed to proving existence of saturated extensions. The existence of saturated extensions has also implications for the properties of primes r dividing n [CoLe]:

Lemma 3.56 *Suppose* p *is a prime with* $(p, n) = 1$, *for which saturated* $p-$th *cyclotomic extensions of* $\mathcal{N}$ *exist. Then for any* $r|n$ *there is a* p*-adic integer* $l_p(r)$ *and, for* $p > 2$, *a number*
$u_p(r) \in (\mathbb{Z}/(p-1) \cdot \mathbb{Z})$, *such that:*

$$\begin{aligned} r &= n^{u_p(r)} \bmod p \quad \text{and} \\ r^{p-1} &= (n^{p-1})^{l_p(r)} \in \{1 + p \cdot \mathbb{Z}_p\} \quad \text{if} \quad p > 2, \\ r &= n^{l_p(r)} \in \{1 + 2 \cdot \mathbb{Z}_2\} \quad \text{if} \quad p = 2. \end{aligned} \tag{3.57}$$

Proof Using theorem (3.35), the hypothesis implies that $r \in < n \bmod p^k >$ for all $k \geq 1$ which implies (3.57). □

Finally, from properties of saturated extensions we deduce following lemma, which has consequences for the practical implementation of primality tests:

Lemma 3.58 *Suppose the integers* t, s, n *are such that:*

1. *A saturated* $t-$th *extension* $(\mathbf{R}, \sigma, \zeta)$ *of* $\mathcal{N}$ *exists.*

2. *The number s is square free, $t = \sharp < n \bmod s >$ and there is an $s-$*th *cyclotomic extension in* $\mathbf{R}$.

*Then there is an $2 \cdot s \cdot t-$*th *extension* $(\mathbf{R}, \sigma, \alpha)$ *of degree t.*

Proof By theorem 3.51 and the fact that the $s-$th extension contains $\mathbf{R}$, a $t'-$th extension exists for all t' that are built up from primes dividing t. We only have thus to prove that the degree of an $2 \cdot s \cdot t-$th extension is t. Let $p|t$ be an odd prime. then $v_p(n^t - 1) \geq v_p(s) + v_p(t)$; similarly, $v_2(n^t - 1) \geq v_2(s) + v_2(t) + 1$. Both facts are a consequence of lemma 2.14 and s being square free. It follows that $2 \cdot s \cdot t | n^t - 1$, which completes the proof. □

3.3 Artin map and intermediate cyclotomic extensions

We defined cyclotomic extensions as galois extensions of rings into which the integers of a cyclotomic field of characteristic 0 are mapped homomorphically. Using the Artin symbol, which generates the galois group of cyclotomic extensions, we shall investigate now the structure of intermediate extensions as maps of intermediate fields. The galois structure is maintained and the galois group is generated by the Artin map.

The investigation of intermediate extensions is interesting in itself; it also helps understanding the composition of cyclotomic extensions occurring in primality proofs using cyclotomy.

Let n be a positive odd integer, $m > 0$ with $(m, n) = 1$, $t = \mathrm{ord}_m(n)$ and $\mathbb{Q}_m$, the $m-$th cyclotomic field. If $\psi_n = \psi_n(\mathbb{Q}_m)$ is the Artin symbol defined by (3.24), we shall use the same notation for the restriction of ψ_n to subfields of $\mathbb{Q}_m$. Let

$$H = (\mathbb{Z}/m \cdot \mathbb{Z})^* / < n \bmod m > ,$$

and $\mathbb{L} = \mathbb{Q}_m^H$ be the abelian field which has $G =< n \bmod m >$ as galois group; let $\mathbb{H}$ be the subfield of $\mathbb{Q}_m$ with galois group H. By analogy to (3.39), we shall call $\mathbb{L}$ the *maximal pop field* of $\mathbb{Q}_m$ and $\mathbb{H}$ the *maximal push field* of $\mathbb{Q}_m$, both *with respect* to n.

Theorem 3.59 *Suppose that an $m-$*th *cyclotomic extension $(\mathbf{R}, \zeta, \sigma)$ of $\mathcal{N}$ exists. Let $\mathbb{K} = \mathbb{Q}_m^{H'}$ be a subfield with galois group $G' = (\mathbb{Z}/m \cdot \mathbb{Z})^*/H'$, $\mathbb{K}^\top = \mathbb{K} \cap \mathbb{L}$ and $\mathbb{K}^\perp = \mathbb{K} \cap \mathbb{H}$. Then there is a map*

$$\nu : O(\mathbb{Q}_m) \to \mathbf{R} \quad \textit{with} \quad \sigma\nu = \nu\psi_n. \tag{3.60}$$

*Furthermore, $\mathcal{R} = \nu(O(\mathbb{K}))$ is a galois extension and $\nu(O(\mathbb{K})) = \nu(O(\mathbb{K}))$. We define $\eta = \mathbf{Tr}(\mathbb{Q}_m/\mathbb{K})(\xi_m)$ and $\iota = \mathbf{Tr}(\mathbb{Q}_m/\mathbb{K}^\top)(\xi_m)$, where ξ_m is a complex $m-$*th *root of unity. Then $\mathcal{R} = \mathcal{N}[\nu(\iota)]$ – using the convention that $\mathcal{N}[x] = \mathcal{N}$ for $x \in \mathcal{N}$. The galois group of $\mathcal{N}[\nu(\iota)]$ is generated by σ, where the same symbol is used for the restriction of σ to $\mathcal{R}$. Finally $\nu(\eta) = \nu(\iota)$ and in particular, if $\mathbb{K} = \mathbb{Q}$, then $\nu(\eta) \in \mathcal{N}$.*

Proof Let ν be defined by $\nu(z) = z \bmod n$ for $z \in \mathbb{Z}$ and $\nu(\xi_m) = \zeta$. It follows from (3.41), that ν is surjective and $\sigma\nu = \nu\psi_n$ is a consequence of the definition of the two automorphisms σ and ψ_n.

Let $\mathcal{R} = O(\mathbb{K})/(n \cdot O(\mathbb{K}))$. Since $\iota \in O(\mathbb{K})$, $\mathcal{R} \supset \mathcal{N}[\nu(\iota)]$; the other inclusion follows from $\mathbb{Z}[\iota] \supset \det(\iota) \cdot O(\mathbb{K})$ and $\det(\iota)$ being a unit $\bmod n$, by (3.21). It is also a consequence of (3.21), that $\{1, \iota, \ldots, \iota^{k-1}\}$ is a base for $\mathcal{R}$, where $k = [\mathbb{K} : \mathbb{Q}]$. We have thus $\mathcal{R} = \mathcal{N}[\iota \bmod n]$. By the same argument, $O(\mathbb{K})/(n \cdot O(\mathbb{K})) = \mathcal{N}[\eta \bmod n]$. The map σ acts by restriction on both $\mathcal{N}[\iota \bmod n]$ and $\mathcal{N}[\eta \bmod n]$ and it generates by definition of $\mathbb{K}$ the same group in $O(\mathbb{K})$ as it does in $O(\mathbb{K})$. It follows by a counting argument, that $O(\mathbb{K})/(n \cdot O(\mathbb{K})) = O(\mathbb{K})/(n \cdot O(\mathbb{K}))$. Finally, $\eta \bmod n = \nu(\eta)$, by taking traces in the definition of ν. The same holds for ι. □

Definition 3.61 *Let $\mathbf{R} = \mathcal{N}[\alpha]$ be a galois algebra over $\mathcal{N}$, with $(\det(\alpha), n) = 1$ and galois group G. Suppose there is an integer m with $(m, n) = 1$ and an $m-$th cyclotomic extension $(\mathcal{R}, \sigma, \zeta)$ of $\mathcal{N}$, such that $\mathcal{R} \supset \mathbf{R}$ and $< \sigma > \supset G$. Then the algebra $\mathbf{R}$ is called an* **abelian extension of $\mathcal{N}$** *with respect to m.*

Note that $(\det(\alpha), n) = 1$ is a consequence of the definition (3.30) of a galois extension. By (3.59), abelian extensions of rings are images of the integers in abelian fields under extensions of the modulo map, defined like ν in (3.60). The integer m with respect to which $\mathbf{R}$ is abelian is by no means unique - this is the difference between abelian extensions of rings and the ones of fields. If n is prime, all galois extensions are abelian in the sense defined above and the degree of the extension defines it uniquely, by a basic theorem of algebraic number theory. We shall investigate in the next proposition the role of the order of the cyclotomic extension containing an abelian extension, when n is not prime.

Lemma 3.62 *If $\mathbf{R}$ is an abelian extension with respect to m and $(\mathcal{R}, \sigma, \zeta)$ is an $m-$th cyclotomic extension of $\mathcal{N}$, then there is a unique $\mu(m)|m$, such that the minimal sub extensions of $\mathcal{R}$ containing $\mathbf{R}$ has order $\mu(m)$.*

Proof Under the assumptions of the lemma, there is a $k > 0$, such that $G = < \sigma^k >$. For $m'|m$, the galois groups $< \sigma(m') >$ of the $m'-$th cyclotomic sub extensions containing $\mathbf{R}$ form a descending chain. We can define

$$\begin{aligned} \mu(m) \quad = \quad \min\{m'|m \ : \ & (\mathcal{R}(m'), \sigma(m'), \zeta(m')) \text{ is a } m'\text{−th} \\ & \text{sub extensions and } < \sigma(m') > \supset G\}, \end{aligned}$$

the minimal extension of $\mathbf{R}$ included in $\mathbf{r}$. □

Definition 3.63 *The* **chain-conductor** *of an abelian extension $\mathbf{R} = \mathcal{N}[\alpha]$ with respect to m is the order $\mu(m)$ of the minimal cyclotomic extension defined by lemma (3.62).*

Theorem (3.47) can be rephrased using abelian extensions:

Theorem 3.64 *Let* $\mathbf{R} = \mathcal{N}[\alpha]$ *be an abelian extension with group* G *and* μ, μ' *two coprime chain conductors of* $\mathbf{R}$*,* $(\mathcal{R}, \sigma, \zeta)$ *and* $(\mathcal{R}', \sigma', \zeta')$ *the respective extensions. If* $\mathbf{R} = \mathcal{R} \cap \mathcal{R}'$*, then the composite of* $\mathcal{R}$ *and* $\mathcal{R}'$ *is an* $\mu \cdot \mu'-$th *cyclotomic extension.*

Proof The restrictions of σ and σ' act identically on $\mathcal{R} \cap \mathcal{R}'$ and they generate the galois group G. The claim follows from (3.47). □

Theorem (3.64) shows that given $(\mathcal{R}, \sigma, \zeta)$ and $(\mathcal{R}', \sigma', \zeta')$, two cyclotomic extensions of coprime orders μ, μ', an $\mu \cdot \mu'-$th cyclotomic extension exists, provided the intersection $\mathbf{R} = \mathcal{R} \cap \mathcal{R}'$ is abelian with group $\sigma \cap \sigma'$. With the same $\mathcal{R}$ and $\mathcal{R}'$, we show now conversely, that a $\mu \cdot \mu'-$th cyclotomic extension exists if $\mathcal{R}$ and $\mathcal{R}'$ are embedded in a common abelian extension:

Theorem 3.65 *Let* $(\mathcal{R}, \sigma, \zeta)$ *and* $(\mathcal{R}', \sigma', \zeta')$ *and* μ, μ' *be as above and suppose there is a cyclotomic extension* $(\mathbf{S}, \sigma_0, \zeta_0)$*, such that* σ*,* σ' *are the restrictions of* σ_0 *to* $\mathcal{R}$ *and* $\mathcal{R}'$*, respectively. Then a* $\mu \cdot \mu'-$th *cyclotomic extension exists.*

Proof Put $\mathbf{R} = \mathcal{R} \cdot \mathcal{R}'$, $\zeta_0 = \zeta \cdot \zeta'$ and let σ_0' be the restriction of σ_0 to $\mathbf{R}$. It follows from (3.47) that $(\mathbf{R}, \sigma_0', \zeta_0')$ is a $\mu \cdot \mu'-$th cyclotomic extension. □

We saw in (V) of theorem (3.36) that an $m-$th cyclotomic extension of $\mathcal{N}$ exists, if:

$$\chi(r) = 1 \ \ \forall \ \chi \in H(n)^{\perp} \text{ and } \forall \, r | n.$$

We called the characters in $H(n)^{\perp}$ "push characters" since condition (V) proves that their Gauss Periods can be embedded in $\mathcal{N}$, without leading to proper ring extensions. We use the notion of abelian extensions for explaining the significance of the "pop characters". This will lead to the possibility of combining Lucas-Lehmer and Jacobi-Sum tests.

Theorem 3.66 *Let* $(\mathbf{S}, \tau, \zeta)$ *be a* $k-$th *cyclotomic extension of* $\mathcal{N}$ *with degree* t *and* m_1, m_2 *coprime positive integers,* $u_i = \mathrm{ord}_{m_i}(n), i = 1, 2$*, such that:*

(i) $(t \cdot m_1 \cdot m_2 \cdot u_1 \cdot u_2, n) = 1$ *and* $\mathit{lcm}\ (u_1, u_2) | t$.

(ii) $(\mathcal{R}_2, \sigma_2, \zeta_2)$ *is an* m_2-th *cyclotomic extension embedded in* $\mathbf{S}$.

(iii) $\chi(r) = 1 \ \ \forall \, \chi \in H(n)^{\perp}$ *and* $\forall \, r | n$*, where*

$$H(n)^{\perp} \ = \ \{\chi : (\mathbb{Z}/m_1 \cdot \mathbb{Z}) \to \mathbf{S} \ : \ \chi(n) = 1\}$$

(iv) $\chi(r) = \chi(n)^{i(r)} \ \ \forall \, \chi \in G(n)^{\perp}$ *and* $\forall \, r | n$*, where*

$$G(n)^{\perp} \ = \ \{\chi : (\mathbb{Z}/m_1 \cdot \mathbb{Z}) \to \mathbf{S} \ : \ \mathrm{ord}(\chi(n)) | u_2\}$$

Then an $m_1 \cdot m_2-$th *cyclotomic extension of* $\mathcal{N}$ *exists.*

Proof Conditions (i) and (ii) are obvious. Condition (iii) shows the existence of an m_1−th extension $(\mathcal{R}_1, \sigma_1, \zeta_1)$. Condition (iv) finally uses pop characters and implies the existence of an abelian sub extensions $\mathbf{R}_1$ of $\mathcal{R}$ with group $G(n)$, which is embedded in $\mathbf{S}$. The definition of $G(n)$ shows that $\mathbf{R} = \mathcal{R}_1 \cap \mathcal{R}_2$ and we are in the situation of theorem (3.64). □

Obviously, (ii) refers to an extension constructed by the Lucas-Lehmer method, (iii) to one constructed by Jacobi-Sums. These two methods of constructing cyclotomic extensions will be considered in detail in the next chapter. Since $G(n)^{\perp} \supset H(n)^{\perp}$, (iv) implies (iii); we separated the two conditions in order to underline the role of the pop characters in (iv). Jacobi-Sum tests as implemented in [CoLe] and [BovdH] used (3.37), i.e. the whole character group $(\mathbb{Z}/m \cdot \mathbb{Z})^{\perp}$, with images in an accordingly chosen extension, in the case of [BovdH], which combines the Jacobi-Sum test to Lucas-Lehmer tests. This explains why the latter never mentions conditions for combining the two tests: they are fulfilled by the choice of the character group in the Jacobi-Sum test. Theorem (3.66) shows that this choice is (slightly) *redundant*. This observation is more of theoretical interest and has but negligible influences on the implementation.

... but something is happening
and you don't know what it is –
do you, Mr. Jones ?

Bob Dylan, Highway 61

Chapter 4

A constructive approach for the Jacobi-Sum test

We defined in the last chapter cyclotomic extensions of $\mathcal{N}$ and proved properties of Gauss and Jacobi-Sums in the second chapter. We shall turn our attention now to the question how to build a $q-$th cyclotomic extension.

The Lucas-Lehmer approach consists in seeking a $q-$th primitive root of unity by trial and error in extension of adequate degree. In §4.1 we show how to choose the extensions where the roots can be found and the conditions that must be verified.

In the Jacobi-Sum approach, the coefficients of the factors of $\Phi_q(x)$ over $\mathcal{N}$ are computed directly, by solving cyclic equations. This method has the advantage of working in extensions of lower degree then the Lucas - Lehmer approach, being thus more efficient, although more complex in its concepts. It is treated in §4.2. In §4.3 we show how to combine both approaches for giving conditions of *existence* of an $s-$th cyclotomic extension. These conditions are used for primality proving. Two explicit pseudoprime tests are stated, which can be combined with (3.35) in order to provide primality proofs. In §4.4 we state a new algorithm for factoring cyclotomic polynomials over finite fields and rings, which is based on Jacobi-Sums. In the last section we show that this approach is also efficient in a setting in which the *number of random bits* required by an algorithm is important.

4.1 Constructing cyclotomic extensions of given degree – the Lucas-Lehmer approach

The problem of constructing cyclotomic extensions of given degree can be reduced to the case of prime power degrees p^k, due to theorems (3.42) and (3.64). Furthermore, theorem (3.29) suggests where to look for extensions of degree p^k. We resume this in following:

Lemma 4.1 *Suppose m is an integer such that:*

(i) there is a primitive character of conductor m and order p^k.

(ii) $n^{\varphi(m)/p} \neq 1 \bmod m$.

Let s be such that $\mathrm{ord}_s(n) = p^k$ and $(\mathbf{R}, \sigma, \zeta)$ be an $s-$th cyclotomic extension. Then $\mathbf{R}$ is isomorphic to $O(\mathbb{L})/(n \cdot O(\mathbb{L}))$, where $\mathbb{L}$ is the cyclic field of conductor m and degree p^k over $\mathbb{Q}$.

Proof Conditions (i) and (ii) imply that $Gal(\mathbb{L}/\mathbb{Q}) = <\psi_n>$ and the statement follows from theorem (3.40). □

Note that this lemma does not produce a cyclotomic extension, nor does it prove its existence. It gives however indications about the rings in which cyclotomic extensions may be defined. We give in next lemma a list of the different cyclic fields of degree p^k over $\mathbb{Q}$; see also [BovdH] for a similar result.

Lemma 4.2 *Let $\mathbb{L}$ be a cyclic field of conductor m and degree p^k over $\mathbb{Q}$. Then one of the following holds:*

(i) m is prime and $p^k \parallel (m-1)$.

(ii) p is odd and $m = p^{k+1}$.

(iii) $p = 2$, $k \geq 2$ and $m = 2^{k+2}$. In this case $\mathbb{L}$ is one of the two subfields $\mathbb{L}_2$ and $\mathbb{L}_3$ of $\mathbb{C}_{2^{k+2}}$ defined in (3.6).

(iv) $p = 2$ and $k = 1$. Then either $m = 4$ and $\mathbb{L} = \mathbb{Q}[i]$ or $m = 8$ and $\mathbb{L}$ is one of the subfields $\mathbb{L}_2$ and $\mathbb{L}_3$ of $\mathbb{C}_8$.

Proof For p odd, it follows from the definitions of the conductor of a field, that $p^k \parallel \varphi(m)$, which settles (i) and (ii). The cases (iii) and (iv) follow from (3.6). □

If $\mathbb{L}$ is a field of degree p^k defined by Lemma (4.1), an $s-$th cyclotomic extension can be constructed by using theorem (3.42). This is the Lucas - Lehmer approach to constructing cyclotomic extensions. It is obvious that, when the degree of extensions is of importance and the order irrelevant, a minimal s will be chosen. The extensions constructed by the Lucas - Lehmer method are *saturated*. This approach is used in [AdLe] for constructing galois fields.

4.2 Constructing cyclotomic extensions of given order

Before describing the Jacobi-Sum method for constructing cyclotomic extensions we will have to consider the problem of taking roots in these extensions. We shall show that, provided some working saturated extensions, there is a constructive, deterministic algorithm for taking roots over $\mathcal{N}$. Suppose thus that $(\mathbf{R}, \sigma, \zeta)$ is a saturated p-th cyclotomic extension, in which we want to find some p^l-th root of an element $\alpha \in \mathbf{R}$ – provided such roots exist; l is a positive integer with $1 \leq l \leq v_p(n^{p-1} - 1)$. Let t be the degree of $\mathbf{R}$ and $N = n^t - 1$. Let α be such that

$$\alpha^{N/p^l} = 1 \tag{4.3}$$

We wish to find a solution in $\mathbf{R}$ to the equation $x^{p^l} = \alpha$; (4.3) guarantees that a solution exists. With this notation we shall prove:

Theorem 4.4 *Let $\alpha \in \mathbf{R}$, with $(\mathbf{R}, \sigma, \zeta)$ a saturated p-th cyclotomic extension, such that (4.3) is satisfied. Then there is a polynomial deterministic algorithm for finding a root β of the equation $x^{p^l} = \alpha$.*

Proof Let $k = v_p(N)$ and u be given by $N = u \cdot p^k$, so that $(u, p) = 1$; since $\mathbf{R}$ is saturated, $\zeta \in \mathbf{R}$ is a p^k-th root of unity. Such a root can be found for instance by using the Lucas-Lehmer approach described in the previous section. If α is a p^l-th power in $\mathbf{R}$, then

$$\alpha^u = \zeta^{\nu \cdot p^l} \qquad \text{with } \nu \in (\mathbb{Z}/p^{k-l} \cdot \mathbb{Z}). \tag{4.5}$$

Note that $\nu \bmod p^i$ $(i = 1, 2, \ldots, k - l)$ can be successively computed by comparing $\alpha^{u \cdot p^{k-i-l}}$ to powers of $\zeta^{p^{k-i}}$. Given ν, one can define a solution to $x^{p^l} = \alpha$ in the following way. Let u' be such that $u \cdot u' = -1 \bmod p^k$ and $e = (1 + u \cdot u')/p^l$. Then $\beta = \alpha^e \cdot \zeta^{-u' \cdot \nu}$ is such that $\beta^{p^l} = \alpha$, which can be proved by a straightforward computation. Similar algorithms are described in [AMM] and [Hu2] for the case when $\mathbf{R}$ is a galois field and have been used in practice for several decades in computational algebra. □

The case $p = 2$ deserves additional attention, since in this case both $v_2(n - 1)$ and $v_2(n + 1)$ influence the existence of a saturated extension. We shall show now that in 3 out of 4 cases such an extension can be constructed deterministically. If

$$v = v_2(n - 1) > 2,$$

a saturated extension can be constructed by the Lucas - Lehmer method: no simple deterministic approach is possible (we do not consider adapting the elliptic curves root taking algorithm of Schoof [Sh] in this category). If $v = 2$, an extension can be constructed using the fact that for $\forall a, \alpha \in (\mathbb{Z}/a \cdot \mathbb{Z})^*$, either α or $-\alpha$ is a quadratic non-residue mod a. Thus $x^{\frac{n-1}{2}} = -1 \bmod a$ for $x = \alpha$ or $x = -\alpha$, and the Lucas - Lehmer method can be applied. If $v = 1$, the value of $v_2(n+1)$ has to be considered. This case is singular, being the only case in which the existence of a saturated $p-$th extension of $\mathcal{N}$ (which is $\mathcal{N}$ itself) does not imply the existence of saturated p^k-th extensions for $k > 1$ (3.5). This is why the definition of saturation differs for $p = 2$ from the odd primes. We show

how to build saturated 2^k-th extensions, or prove that none exists for $k > 1$. Suppose that $v_2(n-1) = 1$, then $n = -1 \bmod 4$, let $\mathcal{N}[i] = \mathbb{Z}[i]/(n \cdot \mathbb{Z}[i])$ with $i = \sqrt{-1}$, and define $\sigma(i) = i^n = -i$. Then $\sigma^2 = Id$ and $(\mathcal{N}[i], \sigma, i)$ is a 4-th cyclotomic extension of $\mathcal{N}$. Suppose :

$$2^{(n-1)/2} = \begin{cases} -1 \bmod n, & \text{if } n = 3 \bmod 8; \\ \\ 1 \bmod n, & \text{if } n = 7 \bmod 8. \end{cases} \tag{4.6}$$

and let $\sqrt{2} \in \mathcal{N}[i]$ be given by

$$\sqrt{2} = \begin{cases} i \cdot (-2)^{(n+1)/4} \bmod n, & \text{if } n = 3 \bmod 8; \\ \\ 2^{(n+1)/4} \bmod n, & \text{if } n = 7 \bmod 8. \end{cases} \tag{4.7}$$

and $\omega = (1+i)/\sqrt{2} \in \mathcal{N}[i]$. Then $\omega^2 = i$ and $\omega^8 = 1$. Since $n^2 = 1 \bmod 8$, $\sigma^2(\omega) = \omega^{n^2} = \omega^{8k+1} = \omega$ and $(\mathcal{N}[i], \sigma, \omega)$ is an $8-$th cyclotomic extension of $\mathcal{N}$, where $\sigma\omega = \omega^n$. If (4.6) does not hold, than n is not prime. For determining if $\mathcal{N}[i]$ is saturated, we consider $h = v_2(n^2-1) = v_2(n+1)+1$. The extension $\mathcal{N}[i]$ is saturated iff it contains a 2^h-th root of unity. We show how to construct such a root of unity. If $h = 3$, put $\zeta = \omega$ and stop. Otherwise, construct the following sequence:

$$\begin{aligned} \alpha_3 = \omega &= a_3 + i \cdot b_3; \\ \alpha_j &= a_j + i \cdot b_j, \qquad j = 4, 5, \ldots, h. \end{aligned}$$

where a_j and b_j are given by:

$$2 \cdot a_j^2 - 1 = a_{j-1} \tag{4.8}$$

$$2 \cdot a_j b_j = b_{j-1} \tag{4.9}$$

Since $a_3^2 + b_3^2 = 1$ and from

$$4 \cdot a_j^2(a_j^2 + b_j^2 - 1) = a_{j-1}^2 + b_{j-1}^2 - 1 \tag{4.10}$$

it follows by induction that $a_j^2 + b_j^2 = 1$. The identity (4.10) is obtained by squaring (4.8) and (4.9) and adding up. For $v_2(n-1) = 1$, equation (4.8) has the solution

$$a_j = \left(\frac{a_{j-1}+1}{2}\right)^{\frac{n+1}{2}}$$

If for a certain j, this solution is incorrect, no saturated 2^h-th extension of $\mathcal{N}$ exists – in particular, n is composite. Otherwise, put $\zeta = \alpha_h$; a simple verification shows that $\alpha_j^2 = \alpha_{j-1}$ and α_j is a 2^j-th root of unity. If n is prime, (4.8) necessarily has the above solution in $\mathcal{N}$. We have:

Lemma 4.11 *If $v_2(n-1) = 1$ and (4.6) holds, a 2^k-th cyclotomic extension of $\mathcal{N}$ exists and can be constructed by the above method for all $k \geq 2$.*

Taking roots is a step in the Jacobi-Sum approach for constructing cyclotomic extensions, which we shall describe in next section. It will follow from the results in this section, that if appropriate working saturated extensions are constructed and (4.3) holds, for values of α that will be precised in the next section, the construction proceeds deterministically.

4.2.1 The Jacobi-Sum approach

We wish to construct a q - th cyclotomic extension of $\mathcal{N}$, where q is an odd prime and $(n, q) = 1$, by splitting the q-th cyclotomic polynomial $\Phi_q(x)$ over $\mathcal{N}$. A probabilistic method for doing this is the Lucas-Lehmer method described in the previous paragraph ([CoLe]). The method we show here introduces the techniques used in the Jacobi-Sum test in a constructive context. If a q-th cyclotomic extension of $\mathcal{N}$ exists, our algorithm will produce such an extension, otherwise it produces a proof of n being composite. Let $t = \mathrm{ord}_q(n)$ and $f = (q-1)/t$. If $f = 1$ then $\mathbb{K} = \mathcal{N}[x]/(\Phi_q(x))$ is a $q-$th cyclotomic extension of $\mathcal{N}$ and we are done. Otherwise, $\Phi_q(x)$ splits in f irreducible factors of degree t mod n, and constructing a cyclotomic extension is equivalent to finding one of these irreducible factors. Let $\mathbb{L}$ be the subfield of $\mathbb{C}_q$ of degree f, ξ be a complex primitive q-th root of unity, $\eta = \mathbf{Tr}_{\mathbb{C}_q/\mathbb{L}}(\xi)$ and $\mathbf{A}$ be the ring of integers in $\mathbb{L}$, which has a normal base generated by η, according to (3.8). The root of unity ξ being an integer over $\mathbb{Q}$ is a fortiori an integer over $\mathbb{L}$. It follows that the coefficients of the minimal polynomial of ξ over $\mathbb{L}$ may be written as

$$\sigma_i = \sum_{j=1}^{f} c_{ij} \cdot \tau^j(\eta), \tag{4.12}$$

for fixed rational integers c_{ij}, where τ generates the galois group of $\mathbb{L}$ over $\mathbb{Q}$. We define by analogy to the preceding chapters,

$$H(n) = < n \bmod q > \quad \text{and} \quad H(n)^{\perp} = \{\chi \in (\mathbb{Z}/q \cdot \mathbb{Z})^{\perp} : \chi(n) = 1\}.$$

Assuming a q-th cyclotomic extension of $\mathcal{N}$ exists, statements (**I**) – (**IX**) of Chapter 3 hold. Let $(\mathbf{R}, \sigma, \zeta)$ be such a - yet unknown - extension and the Gauss Periods $\eta_h = \eta_h(n, \zeta)$ be defined by (2.20), for $h \in H(n)$. By (3.37), there is a map $\lambda_0 : \mathbf{A} \to \mathcal{N}$. If we can show how to build λ_0, the coefficients of the irreducible factors of $\Phi_q(x)$ over $\mathcal{N}$ are $\lambda_0(\sigma_i) = \lambda_0\left(\sum_{j=1}^{f} c_{ij} \cdot \tau^j(\eta)\right)$. Note that the coefficients c_{ij} do not depend upon n and can thus be tabulated. We have thus reduced the problem to mapping the Gauss Periods; we now show how to compute $\eta_h, h \in H(n)^{\perp}$. For this we assume, that for each $p \mid f$, saturated $p-$th cyclotomic extensions are known, such that a $p^{i(p)}-$th extension $(\mathbf{R}_p, \sigma_p, \zeta_p)$ can be found, with $i(p) = v_p(f)$. Let g be a generator of $(\mathbb{Z}/q \cdot \mathbb{Z})^*$. We define the characters χ_p by $\chi_p(g) = \zeta_p$ so that the set $\{\chi_p : \ p \mid f\}$ generates $H(n)^{\perp}$. Put $\alpha_p = J_{p^i}(\chi_p)$; according to (2.30), $\alpha_p = \tau(\chi_p)^{p^i}$. If we write $d(p)$ for the degree of the extension $\mathbf{R}_p$ then, by (2.38),

$$\alpha_p^{\frac{n^{d(p)}-1}{p^i}} = \chi_p^{d(p)}(n) = 1$$

must hold, ($\chi_p(n) = 1$ by choice of χ_p). Since $\mathbf{R}_p$ is by definition saturated, an element $\beta_p \in \mathbf{R}_p$ with $\beta_p^{p^i} = \alpha_p$ can be found using theorem (4.4). Since $\tau(\chi)^{p^i} = \alpha_p$ there is a p^i-th root of unity $\zeta' = \zeta^a$ such that $\beta_p = \zeta^a \cdot \tau(\chi)$. By (2.17) and (2.30), there is a number $a_p \in (\mathbb{Z}/p^i \cdot \mathbb{Z})$ such that

$$\begin{aligned} \beta_p &= \chi_p^{-1}(g^{a_p}) \cdot \tau(\chi) && \text{and} \\ \chi_p^{-k}(g^{a_p}) \cdot \tau(\chi_p^k) &= J_k(\chi_p)/\beta_p^k && \text{for} \quad k = 2, 3, \ldots, p^i - 1 \ . \end{aligned}$$

Let $a \in (\mathbb{Z}/f \cdot \mathbb{Z})$ be such that $a = a_p \bmod p^i$. Lemma (2.32) can be used for computing $\chi^{-1}(g^a) \cdot \tau(\chi), \quad \forall \chi \in H(n)^{\perp}$. According to (2.17), $\tau_g^a(\chi) = \chi^{-1}(g^a) \cdot \tau(\chi)$; one can compute the Gauss Periods $\{\eta_h(n, \zeta^{g^a}) : h \in H(n)\}$ using (2.35). By replacing finally ζ by ζ^{g^a}, the coefficients of $\Psi_{g^a}(x) = \sum_{i=1}^{t} (x - \zeta^{n^i \cdot g^a}) \bmod n$ can be calculated using (4.12). This completes the construction of a $q-$th cyclotomic extension. Note that the procedure succeeds if saturated $p-$th (working) extensions are known and (4.3) holds with $\tau(\chi)^{p^i(p)} = \alpha, \ \forall p \mid f$. Under this premises, the procedure is deterministic, as a consequence of (4.4) and has the advantage of yielding an efficient method for splitting the cyclotomic polynomial modulo n. It has the interesting particularity of not using $q-$th power non residues. However this is not relevant, since $p-$th power non residues for $p \mid f$ are necessary. If $v_q(n^t - 1) = 1$, the extension produced by the procedure above is saturated.

If $k = v_q(n^t - 1) > 1$ and α is a q^k-th root, found by trial and error and such that $\Psi(\alpha) = 0$, then an irreducible factor of $\Phi_{q^k}(x)$ is of the shape: $\Psi_{q^k}(x) = \alpha^t \cdot \Psi_q(x/\alpha)$. Methods for splitting the cyclotomic polynomial over galois fields are treated in a series of recent papers, including [Sho], [AdLe], [Hu1]. We shall discuss in §4.4 our method in the perspective of these papers. We consider now the case of an extension of order m, where m is an odd, square free positive integer with $(n, m) = 1$. Let again $t = \mathrm{ord}_m(n)$ and $f = \varphi(m)/t$; if an m-th cyclotomic extension of $\mathcal{N}$ exists, $\Phi_m(x)$ splits in f irreducible factors of degree t over $\mathcal{N}$. The arguments used for deducing (4.12) still hold in this case, with $\mathbb{L}$ the subfield of $\mathbb{C}_m$ with index f, $\eta = \mathbf{Tr}_{\mathbb{C}_m/\mathbb{L}}(\xi)$ and $\mathbf{A}$ being the ring of integers in $\mathbb{L}$ - which still has a normal base generated by η. It follows that $\Phi_m(x)$ can be factored, as soon as $\tau(\chi)$ has been computed for a set of generators of $H_m(n)^{\perp} = \{\chi \in (\mathbb{Z}/m \cdot \mathbb{Z})^{\perp} : \chi(n) = 1\}$. The method is analogous to the case discussed above ($m = q$, prime), so we shall not insist upon the details.

In the next paragraph, we shall use the Jacobi method for constructing cyclotomic extensions, in order to give criteria for proving the existence of such extensions. It is obvious that such a proof exists as soon as the above procedure for constructing cyclotomic extensions *can be completed deterministically*; this is the case, when the necessary intermediate saturated extensions $(\mathbf{R}_p, \sigma_p, \zeta_p)$ are proved to exist for all $p \mid f$ and condition (4.3) is verified for all Gauss-Sums involved. It is indeed this very condition that will give rise to the pseudoprime tests we shall deduce in the following section. In the deduction of these criteria, we shall give also details about the way of determining the generators of $H_m(n)^{\perp}$.

4.3 Proving existence of cyclotomic extensions

4.3.1 The Jacobi-Sum method

Several of the results proved in this paragraph are adaptations of propositions in [CoLe] to the more general setting of cyclotomic extensions.

Lemma 4.13 *Let q be a prime, $p^k \parallel (q-1)$ a prime power, $(\mathbf{R}, \sigma, \zeta)$ a p^k-th cyclotomic extension and p and q be both coprime to n. Let $\chi : (\mathbb{Z}/q \cdot \mathbb{Z}) \to < \zeta_p >$ be a* *multiplicative character and* $\alpha, \beta \in \mathbf{R}$ *be given by:*

$$\begin{aligned} \alpha &= J_{p^k}(\chi) \qquad \textit{and} \\ \beta &= J_\nu(\chi), \qquad \textit{where } \nu = n \textit{ mod } p^k. \end{aligned} \tag{4.14}$$

Let $l = [n/p^k]$ *and suppose that*

$$\alpha^l \cdot \beta = \eta^{-n} \qquad \textit{holds for some } \eta \in < \ \zeta_p \ >. \tag{4.15}$$

Then $\eta = \chi(n)$ *and* $\chi(r) = \chi(n)^{l_p(r)}$, $\forall r \mid n$, *with* $l_p(r)$ *defined by (3.57).*

Proof Let $\mathbf{A} \supset \mathbf{R}$ contain a q-th cyclotomic extension $(\mathbf{R}', \sigma', \zeta_q)$ and $\tau(\chi) \in \mathbf{A}$ be the Gauss-Sum induced by χ. By the definition of α, β and l, (4.15) is equivalent to

$$\tau(\chi)^n = \eta^{-n} \cdot \sigma(\tau(\chi)). \tag{4.16}$$

By raising (4.16) to the power n repeatedly, we have :

$$\tau(\chi)^{n^i} = \eta^{-i \cdot n^i} \cdot \sigma^i(\tau(\chi)) \qquad \forall i \geq 1 \tag{4.17}$$

and with $i = p^k \cdot (p-1)$ and $N = n^i$,

$$\tau(\chi)^{N-1} = 1. \tag{4.18}$$

If $r \mid n$ is a prime, by (2.36)

$$\tau(\chi)^r = \chi(r)^{-r} \cdot (\tau(\chi^r)) \bmod r \cdot \mathbf{A}. \tag{4.19}$$

Let $m \in \mathbb{N}$ be such that $m = l_p(r) \bmod p^k$ and $m = u_p(r) \bmod (p-1)$, with $u_p(r)$ and $l_p(r)$ defined by (3.57), so that $\sigma^m(\chi) = \chi^r$ and

$$v_p(r - n^m) = v_p(n^m \cdot (r/n^m - 1)) \geq v_p(N-1) \tag{4.20}$$

We let $i = m$ in (4.17), use $\sigma^m(\tau(\chi)) = \tau(\chi^r)$ and divide by (4.19). This is allowed, since $\tau(\chi) \mid q$ by (2.29) and $(q, n) = 1$.

$$\tau(\chi)^{n^m - r} = (\chi(r) \cdot \eta^{-m})^r \bmod r \cdot \mathbf{A}. \tag{4.21}$$

Raising this congruence to the power u, where u is the largest divisor of $(N-1)$ which is coprime to p, and using (4.18) and (4.20) we get :

$$1 = (\chi(r) \cdot \eta^{-m})^{r \cdot u} \bmod r \cdot \mathbf{A}. \tag{4.22}$$

By Lemma (4.23) below, and using $(r \cdot u, p) = 1$ we conclude that

$$\chi(r) = \eta^m = \eta^{l_p(r)} \quad \forall r \mid n, \ r \ \text{ prime.}$$

This holds by multiplicativity for all $r \mid n$ and in particular, since

$$l_p(n) = 1, \chi(n) = \eta.$$

□

Lemma 4.23 *If $\rho \in <\zeta_p>$ satisfies $\rho = 1 \ mod \ r \cdot \mathbf{A}$, then $\rho = 1$.*

Proof We have $\prod_{i=1}^{p^k-1} (1-\zeta_p^i) = p^k$. If $\rho \neq 1$, then there is a $\lambda \in \mathbf{R}$ with $\lambda\cdot(1-\rho) = p^k$; taking this equality $\mod r \cdot \mathbf{A}$ and using $\rho = 1 \mod r \cdot \mathbf{A}$ we get $p^k = 0 \bmod r \cdot \mathbf{A}$, which is a contradiction to $(p, n) = 1$. □

Corollary 4.24 *If (4.15) is verified for a set G_q of generators of $H_q(n)$, then a q-th cyclotomic extension of $\mathcal{N}$ exists.*

This shows that (4.15) can be used for testing existence of cyclotomic extensions. We shall now give a generalization of (4.13) allowing us to perform several tests (4.15) in one step. We describe the idea of this generalization: suppose χ_i $(i = 1, 2, \ldots, k)$ are a collection of characters of coprime orders (the conductors need not be different) and η some primitive root of unity of order dividing the product of the orders of the χ's. Then the Chinese Remainder Theorem allows one to use the information from one test (4.15) performed on the product of the $\tau(\chi_i)$ as if (4.15) had been tested k times, for each single Gauss-Sum. The proof is similar to (4.13) with a more involved notation. We shall call a collection of characters to be tested simultaneously an *amalgam* .

Theorem 4.25 *Let $f = \prod_{i=1}^{j} p_i^{k_i}$ with p_i primes, $f' = \prod_{i=1}^{j} p_i$, $t = \# < n \ mod \ f' >$ and $(\mathbf{R}, \sigma, \zeta)$ an f-th cyclotomic extension of $\mathcal{N}$, $\zeta_i = \zeta^{f/{p_i}^{k_i}}, i = 1, 2, \ldots, j$; thus, ζ_i are primitive roots of order ${p_i}^{k_i}$. Let $\chi_i : (\mathbb{Z}/q_i \cdot \mathbb{Z}) \to <\zeta_i>$ be characters of order ${p_i}^{k_i}$ and conductor q_i, with q_i not necessarily different primes. For $i = 1, 2, \ldots, j$, let:*

$$\begin{aligned} \alpha_i &= J_{{p_i}^{k_i}}(\chi_i) \qquad \text{and} \\ \beta_i &= J_{\nu_i}(\chi_i), \qquad \text{where } \nu_i = n \ mod \ {p_i}^{k_i}. \end{aligned} \tag{4.25}$$

Let $n = f \cdot l + \nu$ with $0 \leq \nu < f$ and $\nu = {p_i}^{k_i} \cdot \lambda_i + \nu_i$, $0 \leq \nu_i < {p_i}^{k_i}$, $i = 1, 2, \ldots, j$. Define α and β by

$$\begin{aligned} \alpha &= \prod_{i=1}^{j} \alpha_i^{f/{p_i}^{k_i}} \in \mathbf{R} \qquad \text{and} \\ \beta &= \prod_{i=1}^{j} \alpha_i^{\lambda_i} \cdot \beta_i \in \mathbf{R} \end{aligned} \tag{4.26}$$

Suppose there is an $\eta \in <\zeta_f>$ such that

$$\alpha^l \cdot \beta = \eta^{-n} \tag{4.27}$$

Then $\chi_i(r) = \chi_i(n)^{l_p(r)} \quad \forall r \mid n$ and $i = 1, 2, \ldots, j$. Furthermore $\eta = \prod_{i=1}^{j} \chi_i(n)$.

Proof Let $\mathbf{A} \supset \mathbf{R}$ contain primitive q_i-th roots of unity ξ_i. If $\tau(\chi_i) \in \mathbf{A}$ are the Gauss-Sums induced by χ_i, then by definition of α and β, (4.27) implies :

$$\prod_i \tau(\chi_i)^n = \eta_i^{-n} \cdot \prod \tau(\sigma(\chi_i)). \tag{4.28}$$

Using the Chinese remainder theorem, one can find $\eta_i \in <\zeta_i>$ such that $\eta = \prod_i \eta_i$; this is possible since the p_i are pairwise distinct and $\# <\eta> \mid \prod_i {p_i}^{k_i} = f$. By raising (4.28) repeatedly to the $n-$th power we get:

$$\prod_i \tau(\chi_i)^{n^h} = \prod_i \eta_i^{-h \cdot n^h} \cdot \sigma^h(\tau(\chi_i)). \qquad \forall h \geq 1. \tag{4.29}$$

We have $\sigma^{tf} = \mathrm{Id}$ and letting $h = tf$ in (4.29), $\eta_i^{tf} = 1$, thus :

$$\prod_i \tau(\chi_i)^{n^{tf}-1} = 1. \tag{4.30}$$

Let r be a prime dividing n. From the definition (3.57) of $u_p(r)$ and the Chinese Remainder Theorem there is a $u(r) \in (\mathbb{Z}/t \cdot \mathbb{Z})$ such that:

$$r^{u(r)} = n \bmod f'. \tag{4.31}$$

Let m be an integer defined by the Chinese Remainder Theorem, such that :

$$\begin{aligned} m &= l_{p_i}(r) \bmod {p_i}^{k_i} \qquad \text{and} \\ m &= u(r) \bmod t. \end{aligned} \tag{4.32}$$

Then $(r/n^m) \in n^{tf \cdot \mathbb{Z}_{p_i}}$ and

$$v_{p_i}(r - n^m) \geq v_{p_i}(n^{tf} - 1), \tag{4.33}$$
$$\sigma^m(\chi_i) = \chi_i^r. \tag{4.34}$$

From (2.37) we have

$$\prod_i \tau(\chi_i)^r = \prod_i \chi_i(r)^{-r} \cdot \tau(\chi_i^r) \mod r \cdot \mathbf{A}, \tag{4.35}$$

and putting $h = m$ in (4.29),

$$\begin{aligned} \prod_i \tau(\chi_i)^{n^m} &= \prod_i \eta_i^{-m \cdot n^m} \cdot \tau(\sigma^m(\chi_i)) \mod r \cdot \mathbf{A} \\ &= \prod_i \eta_i^{-m \cdot n^m} \cdot \tau(\chi_i^r) \mod r \cdot \mathbf{A}. \end{aligned} \tag{4.36}$$

Dividing the last two equations, which is allowed since $(q_i, n) = 1$, we get:

$$\prod_i \tau(\chi_i)^{n^m - r} = \prod_i \left(\frac{\chi_i(r)}{\eta_i^m}\right)^r \mod r \cdot \mathbf{A}. \tag{4.37}$$

Let u be the largest divisor of $(n^{tf} - 1)$ with $(u, f) = 1$. By (4.33), $(n^{tf} - 1) \mid u \cdot (n^m - r)$ and after raising (4.37) to the $u-$th power and using (4.30):

$$\prod_i \left(\frac{\chi_i(r)}{\eta_i^m}\right)^{ru} = 1 \mod r \cdot \mathbf{A}. \tag{4.38}$$

Since $(ru, f) = 1$ and using lemma (4.23) - with p^k replaced by f, we get $\prod_i \left(\frac{\chi_i(r)}{\eta_i^m}\right) = 1$. This product of roots of unity of coprime order can only be 1 if all factors are 1 and thus:

$$\chi_i(r) = \eta_i^m.$$

The rest of the statement follows by multiplicativity and using $l_{p_i}(n) = 1$. $\square$

4.3.2 Generating Characters

We still have to show how to find a set of generators of $H_m(n)^\perp$. If $m = q$ is a prime, $(\mathbb{Z}/q\cdot\mathbb{Z})^\perp$ is cyclic and $H_m(n)^\perp$ is generated by

$$G_q = \{\chi_p : \chi_p \text{ has order } p^k \parallel (q-1) \ \text{ and } \ \chi_p(n) = 1\}.$$

Let m be an odd positive integer, $(m,n) = 1$ and $m_1 > m_2$ be coprime, so that $m_1 \cdot m_2 = m$. Using (2.32) we can reduce our search to characters of prime power orders p^k, with $p^k \mid t$. We suppose that the groups $H_{m_i}(n)^\perp$ have known sets of generators G_{m_i} for $i = 1,2$. Let $t_i = \# < \sigma_i > = \ \mathrm{ord}_{m_i}(n)$ for $i = 1,2$ and $f = (t_1, t_2)$. If $f = 1$, then $G_m = G_{m_1} \cup G_{m_2}$ by the corollary (3.48). If $f > 1$, let $p \mid f$ with $k = v_p(f)$. Since $p^k \parallel (t_1,t_2)$ there are two primes $q_i \mid m_i$ with $v_p(\mathrm{ord}_{q_i}(n)) = v_p(t_i) \geq k$ with equality for at least one $i \in \{1,2\}$. Consider $(\mathbf{R}, \sigma, \zeta)$, a p^h-th cyclotomic extension with $h \geq v_p(q_i - 1)$, $i = 1,2$ and $\chi_{p,i} : (\mathbb{Z}/q_i\cdot\mathbb{Z}) \to <\zeta>$ such that

$$\chi_{p,1}(n) \ = \ \chi_{p,2}(n)^{-1} \ = \ \zeta^{p^{h-k}}. \tag{4.39}$$

Let $\chi_p = (\chi_{p,1}, \chi_{p,2})$ be the character of conductor $q_1 \cdot q_2$ defined by Lemma (2.24). By definition : $\chi_p(n) = \chi_{p,1}(n) \cdot \chi_{p,2}(n) = 1$, so $\chi_p \in H_m(n)^\perp$.

For $\chi \in (\mathbb{Z}/m\cdot\mathbb{Z})^\perp$ we let (χ_1, χ_2) be the decomposition in characters $\chi_i \in (\mathbb{Z}/m_i\cdot\mathbb{Z})^\perp$ cf. lemma (2.24). With this we define:

$$D(n)^\perp = \{\chi \in (\mathbb{Z}/m\cdot\mathbb{Z})^\perp : \chi_1(n) = \chi_2(n)^{-1} \neq 1\}.$$

Obviously $\chi_p \in D(n)^\perp$. Let $\chi \in D(n)^\perp$. From $\mathrm{ord}(\chi_i(n)) \mid t_i$ and $\mathrm{ord}(\chi_1(n)) = \mathrm{ord}(\chi_2(n))$ follows $\mathrm{ord}(\chi_i(n)) \mid (t_1, t_2) = f$. We define further

$$G_i = \{\chi \in G_{m_i} : (\mathrm{ord}(\chi), f) = 1\}$$

and

$$G_D = \{\chi_p \in D(n)^\perp : p \mid f \text{ and (4.39) holds}\}$$

and G_3 is the set of components $\chi_{p,i}$ of the characters $\chi_p \in G_D$. It is easy to verify that $G_m = G_1 \cup G_2 \cup G_3$. We have thus a recursive method for building a set of generators of minimal order of $H_m(n)^\perp$.

Corollary: If X is a set of amalgams, such that each character $\chi \in G_m$ is contained in an amalgam, and if (4.27) holds for all the amalgams in X, an m-th cyclotomic extension of $\mathcal{N}$ exists.

4.3.3 The Lucas-Lehmer approach

We show how to use theorem (3.42) for proving existence of cyclotomic extensions. Suppose $s \mid n^t - 1$ for some t, $s = \prod_{i=1}^{l} q_i$, for some prime powers q_i and rgS, σ, ζ is some cyclotomic extension of degree t. Let $(\mathbf{S}_i, \sigma_i, \zeta_i)$ be sub extensions of degree $k_i = \mathrm{ord}_{q_i}(n)$ of $\mathbf{S}$. Put $(n^{k_i} - 1)/q_i = \sum_{j=0}^{t-1} c_j(q_i) \cdot n^j$. Furthermore, suppose $\alpha_i \in \mathbf{S}_i$ is such that

(i) $\alpha_i^n = \sigma_i(\alpha_i)$

(ii) $(\beta_i - 1) \in \mathbf{S}_i^*$, with $\beta_i = \prod_{j=0}^{k_i-1} \sigma_i^j(\alpha^{c_j(q_i)})$

If (i) and (ii) hold for $i = 1, 2, \ldots, l$, then $(\mathbf{S}, \sigma, \beta)$, with $\beta = \prod_{i=1}^{l} \beta_i$ is an $s-$th cyclotomic extension of $\mathcal{N}$, as a consequence of (3.42) and (4.1).

4.3.4 The combined cyclotomic approach

The two approaches for construction can be combined and used for a criterion for existence of cyclotomic extensions, which is the main stage of a primality proof. The steps for such a proof are the following:

(i) Choose parameters for Jacobi-Sum and Lucas-Lehmer tests as follows: Let m, m' be coprime such that: $s = m \cdot m'$, $u = \mathrm{ord}_m(n)$, $u' = \mathrm{ord}_{m'}(n)$, $t =$ lcm (u, u') and $s \cdot t > \sqrt{n}$. By the theorem of Odlyzko and Prachar ([ARP]), t can be chosen such that $t = O\left(\log(n)^{\log\log\log n}\right)$

(ii) Construct a working $t-$th cyclotomic extension $(\mathbf{S}, \tau, \xi)$ of $\mathcal{N}$. This step is probabilistic and may break without yielding any information on n. This happens however most rarely. We shall treat in Appendix A (the deterministic test) the way of circumventing these event.

(iii) Prove the existence of an $m'-$th cyclotomic extension of $\mathcal{N}$ using the Lucas - Lehmer approach described above.

(iv) Let $C_n = G(n)^{\perp} \cup H(n)^{\perp}$, with $G(n)^{\perp}$ and $H(n)^{\perp}$ defined in (3.66). Let G_s be a set of characters generating C_n, as in §4.3.2. Build a minimal set of amalgams X, such that $\{\chi \in A \mid A \in X\} = G_s$, where A is an amalgam of characters out of X. Prove that (4.27) holds for each amalgam in X.

If all these steps can be performed without stopping with an implicit proof that n is composite, than an $n-$th cyclotomic extension of $\mathcal{N}$ exists as a consequence of (3.66), (4.25) and §4.3.3.

4.4 Factoring the cyclotomic polynomial

The constructive methods for finding cyclotomic extensions can also be used for factoring the cyclotomic polynomial. The Lucas - Lehmer approach was proposed, as mentioned above, in [AdLe]. The Jacobi-Sum approach was never proposed beyond the scope of testing primality.

We show here that it can be used for a factoring algorithm which has new, interesting properties. We consider the factoring of the $q-$th cyclotomic polynomial $\Phi_q(x)$ over $\mathcal{N}$, where q is a prime. We let as usual $t = \mathrm{ord}_q(n)$ and $f = (q-1)/t$. We keep the more general setting of cyclotomic extensions, since algorithms in the classical setting over galois fields $\mathbb{F}_p$ follow as special cases. First let us observe that the Lucas-Lehmer and Jacobi-Sum approach complete each other in the context of factoring too. The first operates in extensions of degree t, the latter one in extensions of prime power degrees dividing f. It is therefore sensible, that the Lucas-Lehmer method should be used for small t, whereas for small f - which is the more frequent case - the Jacobi-Sum method should be preferred. It is not clear which is the break-even point, but it lays lower than $f = \sqrt{q}$, due to the possibility of the second method of using small partial extensions. This means that the Lucas - Lehmer approach, which is used in the literature ([Hu1], [Ro]), is advantageous in the case when Φ_q splits in many polynomials of low degree, whereas in the - more frequent - case when the irreducible factors are not numerous, the Jacobi-Sum approach is preferable.

We explain now the idea of our algorithm for factoring the cyclotomic Al polynomial using Jacobi-Sums. Let q, f, t be defined as above and consider that a cyclotomic extension $(\mathbf{R}, \sigma, \zeta)$ of $\mathcal{N}$ containing $f-$th primitive roots of unity ζ_f exists; furthermore, let ξ_f, ξ_q be $f-$th, respectively $q-$th primitive roots of unity over $\mathbb{C}$. For all prime powers $p^k \parallel f$, $\zeta_p = \zeta_f^{f/p^k}$ is a p^k-th primitive root of unity in $\mathbf{R}$ and ξ_p is defined by analogy. Let $\mathbb{Q} \supset \mathbb{L} \supset \mathbb{C}_q$, with $\mathbb{L}$ being the field of index f in $\mathbb{C}_q$. By §3.1.1, the ring of integers $O(\mathbb{L}) = \mathbf{Z}[\eta]$, where $\eta = \mathbf{Tr}(\mathbb{C}_q/\mathbb{L})(\xi_q)$. If τ is generating Gal $(\mathbb{C}_q/\mathbb{L})$ (the group is cyclic), then the coefficients of an irreducible factor $\Psi(x) \mid \Phi_q(x), \Psi(x) \in \mathbb{L}[x]$ are $\sigma_j(\xi) = \sum_{1 \leq i_1 < i_2 < \ldots < i_j \leq t} \xi^{\tau^{i_1} + \tau^{i_2} + \ldots + \tau^{i_j}}, j = 1, 2, \ldots, t$. They are thus integers in $\mathbb{L}$ and can be expressed as linear combinations over the normal base $(\eta^{\tau}, \eta^{\tau^2}, \ldots, \eta^{\tau^t})$. The linear combination can be computed over $\mathbb{L}$, e.g. using symbolic computation or by straight forward arithmetic operations. One can thus compute a matrix $\mathbf{A}$ with integer entries, such that $\sigma = \mathbf{A}\eta$, with $\sigma = (\sigma_1, \sigma_2, \ldots, \sigma_t)$ and $\eta = (\eta^{\tau}, \eta^{\tau^2}, \ldots, \eta^{\tau^t})$. The purpose of our algorithm is to construct the image η' of η in $\mathcal{N}$. It is a consequence of $\mathbf{R}$ being a $q-$th cyclotomic extension of $\mathcal{N}$, that this image exists and it can be computed using Jacobi-Sums. The relation $\sigma = \mathbf{A}\eta$ is invariant under the canonical map $\mathbb{L} \to \mathcal{N}$ and the coefficients of an irreducible factor $\Psi(x) \mid \Phi_q(x), \Psi \in \mathcal{N}[x]$ are thus found.

Algorithm II *(* Factoring the Cyclotomic Polynomial *)*

1.) For all prime powers $p^k \parallel f$, let $\chi_p : (\mathbb{Z}/q \cdot \mathbb{Z})^* \to < \zeta_p >$ be characters of order p^k and conductor q and β_p be the p^k-th root of $\alpha_p = \tau(\chi)^{p^k}$, where $\alpha_p = J_{p^k}(\chi_p)((2.30))$ and the root is found using the theorem (4.4).

2.) Use the definition of Jacobi-Sums for computing $\tau(\chi_f)$ as follows: if $p, p' \mid f$ are two primes, then $\tau(\chi_p \chi_{p'}) = \beta_p \beta_{p'} / j(\chi_p, \chi_{p'})$. Proceed by induction on $p \mid f$. Note that the $q-$th root ζ_q used in the resulting $\tau(\chi_f)$ is fixed by the values β_p chosen as roots of α_p in step 1. In fact, the equation $x^{p^k} = \alpha_p$ allows the set of roots $\{\tau_a(\chi_p) \mid a \in H\}$, where H is the subgroup with p^k elements of $(\mathbb{Z}/q \cdot \mathbb{Z})^*$.

3.) Compute $\tau(\chi_f^i), i = 1, 2, \ldots, f-1$, using the multiple Jacobi-Sums $\tau(\chi_f^i) = (\tau(\chi_f))^i / J_i(\chi)$.

4.) Solve the linear system: $\tau(\chi_f^i) = \sum_k \zeta_f^{ki} \eta_k'$ (Lagrange resolvents).

5.) Find the integer matrix $\mathbf{A}$ with $\sigma = \mathbf{A}\eta$ by some symbolic computations over $\mathbb{L}$.

6.) Let $\sigma' = \mathbf{A}\eta'$.

7.) Put $\Psi(x) = x^t + \sum_{i=1}^t (-1)^i \sigma_i' x^{t-i}$.

As mentioned before, the proof of existence of $q-$th cyclotomic extensions stops after proving that all α_p have a p^k-th root in $\mathcal{N}$. We see from the algorithm that from that point on, factoring $\Phi_q(x)$ over $\mathcal{N}$ proceeds deterministically, i.e. a constructive proof of existence of a $q-$th cyclotomic extension of $\mathcal{N}$ may be given.

The operation count is as follows: In step 1., for each $p^k \parallel f$ an exponentiation in an extension of degree $\mathrm{ord}_{p^k}(n)$ is requested, thus $o_1(q,n) = O(\sum_{p^k \parallel f} \mathrm{ord}_{p^k}^2(n)(\log(n))^3)$. Step 2. requires a multiplication in a sub extensions of degree $\mathrm{ord}_{p^k}(n)$ for each $p^k \parallel f$, thus $o_2(q,n) = O(\sum_{p^k \parallel f} \mathrm{ord}_{p^k}^2(n)(\log(n))^2)$. In step 3, f divisions are performed in the same extension, thus $o_3(q,n) = O(f \cdot \mathrm{ord}_{p^k}^3(n)(\log(n))^2)$. Steps 4. and 5. require only shifts, additions and subtractions and finally step 6. requires $o_6(q,n) = t^2$ long by short integer multiplications. The overall operation count is

$$o(q,n) = O\Big((\log(n)^3) \sum_{p^k \parallel f} \mathrm{ord}_{p^k}^2(n)\Big) + O\Big((\log(n)^2)\ (f \cdot \mathrm{ord}_{p^k}^3(n) + \sum_{p^k \parallel f} \mathrm{ord}_{p^k}^2(n)\Big) + O(t^2 \log n).$$

Since this algorithm can be used for any scale of magnitude for both n and q, any of the three terms may become dominant. Note that for prime n, this is an algorithm for factoring over galois fields. Factoring over galois extensions of rings is a simple exercise of generalizing this algorithm.

The subject of factoring cyclotomic polynomials was addressed in [Hu1], [Ro]. The complexity of factoring the $q-$th cyclotomic polynomial over a finite field $\mathbb{F}_r$ depends upon $\log(r)$ and q. In the cited papers the complexity is $O(\log(r)^3 \cdot q^2)$, and is in most of the cases, for the reasons mentioned above, higher then the operation count when using the Jacobi-Sum approach at least by a factor q.

4.5 Random Bit Economy

We saw that the Jacobi-Sum method leads to more efficient factoring of the cyclotomic polynomial. Like in the Lucas-Lehmer case, this process requires taking roots in some extensions, which is done by trial and error, thus choosing random elements. It is sometimes argued ([Ba1]) that random bits themselves have to be produced by some algorithms, which can be expensive if one uses generators like the BBS ([BBS]) algorithm.

We shall show in this section that random bits can also be saved when using the Jacobi-Sum approach.

Consider the task of building saturated $q-$th extensions of $\mathcal{N}$ for all primes $q \leq B$, for a given bound B. Using the Lucas - Lehmer method, for all primes q in the given range, one chooses a cyclotomic field $\mathbb{L}$ with $d = [\mathbb{L} : \mathbb{Q}] = \mathrm{ord}_q(n)$ and a random element $\alpha \in O(\mathbb{L}/nO(\mathbb{L}))$, such that:

$$\alpha^{(n^d-1)/q} \neq 1$$

The probability that a random element α satisfies this relation is $p(n, q) = 1 - 1/q$, the uncertainty about α is $H_q(\alpha) = d\log(n)$. The expected number of random bits required for finding an $n-$th root by the Lucas-Lehmer method is thus:

$$\begin{aligned} H_q(L) &= d\log(n)(1 + 1/q + 1/q^2 + \ldots) \\ &= \frac{q}{q-1} d\log(n) \qquad (4.40) \\ &= qc(q)\log(n), \quad \text{where } c(q) = \frac{1}{\mathrm{ord}_q(n)}. \end{aligned}$$

The expected number of random bits required for building all the extensions in the given range is

$$H(L) = \sum_q H_q(L) = \sum_{1<q<B; q\text{prime}} qc(q)\log(n). \tag{4.41}$$

One can take a recursive approach: start by building a saturated 2-nd extension as described in §4.2. This requires no random bits, unless $n = 1 \bmod 8$, i.e. an expected number of $H_2(J) = \log(n)/4$ bits. Consider that saturated extensions have been built for all primes $2 < q < B_0$ with $2 < B_0 < B$. If the saturation degree $k_s(q) = v_q(n^{q-1}) = 1$, then a saturated $q-$th extension of $\mathcal{N}$ can be built deterministically by using the Jacobi-Sum method. The probability that this holds is $p'(q, n) = 1 - 1/q$ and increases with q. Otherwise, on must recur to the Lucas - Lehmer method for finding a primitive $q^{k_s(q)}-$th root of unity, by using thus $H_q(L)$ random bits. It follows that the number of random bits required in average by the recursive method is:

$$H_q(R) = \begin{cases} \log(n)/4, & \text{if } q = 2; \\ \\ H_q(L)/q, & \text{if } q > 2. \end{cases}$$

The total number of random bits required by the recursive method is thus:

$$H(R) = \sum_q H_q(R) = \log(n)\left(\frac{1}{4} + \sum_{2<q<B; q\text{prime}} c(q)\right). \tag{4.42}$$

The average of $qc(q)$ was considered also by Bosma [BovdH], without achieving an exact formula. It is not difficult to prove though, that $\frac{\varphi(q-1)}{q-1} \leq qc(q) \leq 1$. If one assumes for simplicity, that $c(q) = c, \forall q < B$, where c is some constant, for instance, the average of q, one has some raw estimates for the values of H:

$$H(X) = \begin{cases} c\log(n)\sum_{q<B} q \approx c\log(n)\frac{B^2}{\log(b)}, & \text{if } X = L; \\ \\ c\log(n)B, & \text{if } X = R. \end{cases}$$

The factor $\frac{B}{\log(B)}$ is thus an estimate of the economy of random bits when using the recursive method with Jacobi-Sum factoring. We now give a second approach, which completely avoids the Lucas - Lehmer construction. We shall need instead following assumptions:

(A) One can find a quadratic non residue $\alpha_0 \in \mathcal{N}$ in polynomial time.

(B) For all primes $q < B$ with $v_q(n^{q-1} - 1) > 1$, one can find a prime $r = r(q)$ with

$$r = 1 \mod q \quad \text{and} \quad n^{(r-1)/q} \neq 1 \mod r$$

in polynomial time.

It is known (see for instance [Ba2]) that (A) follows from the extended Riemann hypothesis. It is shown in [CoLe], that (B) is also a consequence of the extended Riemann conjecture. Assuming the above two conditions, the construction of saturated extensions proceeds as follows:

1. If $N \neq 1 \mod 8$, construct a saturated 2-nd extension like in lemma (4.11).
2. If $N = 1 \mod 8$, check $a_0 = \alpha_0^{(n-1)/2} = -1 \mod n$. If true, $(\mathcal{N}, \sigma, \alpha_0^{(n-1)/k_s})$ is a saturated 2-nd extension.
3. Suppose $q < B$ is a prime such that $k_s = v_q(n^{q-1} - 1) > 1$, saturated $p-$th extensions have been built recursively for all primes $p < q$, and the cyclotomic polynomial $\Phi_q(x)$ has been factored using the Jacobi-Sum method: suppose $\Psi_q(x)$ is an irreducible factor of $\Phi_q(x)$ in $\mathcal{N}[x]$. Let $\alpha_q = (\tau(\chi))^q$ for a character χ of conductor $r(q)$ and image in $\mathbf{R} = \mathcal{N}[x]/(\Psi_q(x))$. Check $\alpha_q^{(n^{\mathrm{ord}_q(n)}-1)} = 1$ and $\alpha_q^{(n^{\mathrm{ord}_q(n)}-1)/q} \neq 1$ in $\mathbf{R}$. If true, $\mathbf{R}, \sigma, \alpha_q^{(n^{\mathrm{ord}_q(n)}-1)/q^{k_s}}$ is a saturated $q-$th extension.

As can be seen in step [3.], the Lucas-Lehmer construction can be avoided as soon as a prime r verifying condition (B) is known.

"Are you ready ?"
"Ready we are !"
"Let us go !"

Horia to his troups,
when starting the peasant war,
which put and end, 1777, to peasant
servitude in the Austrian Empire.

Chapter 5

Algorithm for primality testing

The theoretical material built up in the preceding chapters can be used for the implementation of a primality test using cyclotomy. An implementation of the algorithm was performed on a SUN platform, based on the PARI arithmetic package. This implementation (see Chapter 6) proves the consistency of the algorithm. However, the very general features of the PARI library have a negative impact upon its efficiency. An own development of the core arithmetic, which will translate the algorithmic improvement in actual efficiency, is under work.

Since the only existing implementation of a test combining Lucas-Lehmer and Jacobi-Sum methods is [BovdH], we shall often refer to this thesis in this chapter. Differently from van der Hulst and Bosma, we shall refrain from making optimality claims. The reasons for the sceptical attitude towards optimality proofs is the fact that these contain assumptions about the implementation techniques. The assumptions may be explicit or implicit. However, slight changes of these techniques may result in the invalidation of the optimality proof. As an illustration of this statement, one can consider fast multiplication algorithms like Toom-Cook or the fast Fourier method [Kn]: their asymptotic advantages are well known but the opinions about the - machine dependent - complexity of the multiplications which start requiring such methods differ. As a matter of fact, polynomial modular multiplication using the Toom-Cook method ([Kn]) is an important factor of efficiency in the implementation of a cyclotomy test. Its use involves a negligible overhead; the complexity of one exponentiation in a cyclotomic extension using Toom-Cook and (3.49) depends only linearly upon the extension degree, whereas with naive exponentiation - as assumed in [BovdH] - the dependence is cubic. This and several other remarks modify the premises used by Bosma and van der Hulst in their optimization analysis and it is likely that they result in a shift in favor of the Lucas - Lehmer test.

Thus, we consider that it to be the overall complexity of the algorithm which requires a thorough analysis. This is the subject of Chapter 7. It will be proved that this complexity is dominated by the final trial division step and the evaluation of Jacobi-Sums. However, for practical computation, the central stage of the algorithm, which involves pseudoprime tests in cyclotomic extensions, is time consuming and requires attention. It is possible that using new computing techniques - e.g. a high degree of parallelism - may also modify the premises on which we made our implementation decisions. The structure of the algorithm is in fact ideal for parallel implementations, so that it will be the practical machine architecture which defines the final optimality properties of an implementation. We do not treat parallelism explicitly in this chapter.

We shall give an overview of the main stages of this test. Primality testing using cyclotomy consists of the following: Given an integer n to be tested for primality,

(i) Select completely factored, coprime m, m' such that:

$$\begin{aligned} s &= [m, m'] \text{ and } t = \mathrm{ord}_s(n), \\ t &= O(log(n)^{logloglog(n)}), and \\ S &= s \cdot t > \sqrt{n} \text{ or } S > \sqrt[3]{n}, \\ &\quad \text{using techniques like in [Le3].} \end{aligned}$$

Note that the choice $S = 2 \cdot s \cdot t$ is related to lemma 3.58.

(ii) Build a saturated $t-$th cyclotomic extension of $\mathcal{N}$ and working sub extensions thereof.

(iii) Perform Lucas-Lehmer tests for proving the existence of an m' -th extension.

(iv) Perform Jacobi-Sum tests upon the set of characters $G(n)^{\perp}$ (defined in (3.66) and built according to section 4.3.2) for proving existence of an $m-$th extension and combining it to the $m'-$th extension proved to exist in (iii).

(v) Perform the final test $(r, n) = 1, \forall r \in < n \bmod s >$. This test is a consequence of statement II of theorem (3.35).

All these steps contain explicit and implicit pseudoprime tests and the algorithm may hold at any stage, if some necessary condition for primality is not fulfilled. It declares n prime – and provides a (rather long) prime certificate – if it successfully passes all the steps. Steps (iii)-(iv) are separated for the simplicity of the exposition and for relating to the theory. In practice they can be mixed, due to the possibility of building amalgams.

This chapter dedicates a section to the detailed description of the implementation of each step of the above list. It ends with a global statement of the primality test algorithm.

5.1 Choosing the parameters and computing Jacobi-Sums

In the approach followed by the implementations of [CoLe], [BovdH] tables for the function

$$e(t) = \prod_{q|t, q prime} q$$

are precomputed. With help of such tables, a reference value for t and s is chosen, such that t takes the smallest value for which

$$t \cdot e(t) \; > \; \sqrt[i]{n}, \quad \text{with } i = 2 \text{ or } i = 3. \tag{5.1}$$

After that, some factoring work is invested in finding large factors of $n^k - 1$ - for some small values of $k \mid t$ - which are not contained in $e(t)$. The product of these factors is m'. Consequently one reduces t such that $m = e(t)$ and the conditions (i) on s are satisfied. After this reduction, the exponent t must remain a multiple of all the exponents k, for which factors of m' have been defined. In [BovdH], the authors suggest that the process of reduction and adaptation of the parameters of the test might be iterated for optimal results. At the end of this step, one has the parameters s and t and a set Q of primes, such that $q \mid (n^t - 1) \;\; \forall q \in Q$ and $\prod_{q \in Q} \; q \; > s$.

As in the above approach, we use a large precomputed table of the map $t \to e(t)$. This table is ordered primarily according to increasing values of $e(t)$ and secondarily according to values of t. For an explicit value of n we than take advantage of the specific properties of the given test number in following way. For all values of t satisfying (5.1) we compute a *weight function* $w(t)$ and choose the value of t which minimizes $w(t)$. The weight functions take the degrees of the working extensions defined by t into account. We use the two weight functions:

$$w_1(t) = \sum_{p \mid t} (\operatorname{ord}_p(n))^\rho$$

and

$$w_2(t) = \sum_{(q-1) \mid t} \Big(\sum_{p^k \| (q-1)} (\operatorname{ord}_{p^k}(n))^\rho \Big)$$

The number ρ is a measure of the complexity of the method for multiplication in cyclotomic fields used. Its value is 2 for naive multiplication and 1 for convolution methods such as Toom-Cook. While $w_1(t)$ weighs a working extension of degree $p \mid t$ by $(\operatorname{ord}_p(n))^\rho$, which is the multiplication complexity for the saturated $p-$th cyclotomic extension of $\mathcal{N}$, $w_2(t)$ weighs the single Jacobi-Sum tests, using the same measure. The measure $w_2(t)$ is obviously the more accurate one, but also requires more involved computations. It is therefore used only for large numbers n, where the gains due to the accuracy of the weight compensate for the time spent in its evaluation for the optimization of t.

Of course, the optimal t with respect to a weight may not be the least one with $e(t) > \sqrt{n}$, and thus the time for the final trial division is increased. This effect did not influence our experiments, which were moderate and in which the exponentiations predominate. A simple way to cope with this effect is to reorder all t with $e(t) > \sqrt{n}$ increasingly and apply the weight only to an interval in which the increase of the final trial division may be tolerated. For very large tests, a more accurate weight such as:

$$w_3(t) = w_1(t) \cdot \log(n) + c \cdot t$$

should be used. This weight evaluates the number of multiplications $\bmod n$. The constant c must be calibrated for the actual implementation and will be rather small.

The use of weight functions for optimizing t turned out to be very practical. Even with the simple weight w_1 it happens often, that optimal values for t are not the minimal ones.

This happens, for instance, when n has a small order - e.g. 1 of 2 over a larger prime - e.g. $p = 13$ or 17, while it has the full order $p-1$ modulo the smaller primes. In such cases, the larger primes lead to smaller weights and consequently the value of t with minimal weight is not minimal in the order of the natural numbers. The use of weight functions represents an important improvement with respect to the [BovdH] implementation. If complex extensions $\mathbb{Z}[\xi_p]$ are the working extensions, instead of cyclotomic ones, the term $(\mathrm{ord}_p(n))^\rho$ of the weight functions must be replaced by $(p-1)^\rho$; this is the case in the [CoLe] implementation. With this choice, optimal values of t are also minimal in the order of the natural numbers.

Our approach to *computing Jacobi-Sums* is that they do not reflect specific properties of the test number and thus belong to precomputed tables. For all the values of p and q, such that $p^k \mid (q-1) \mid t$ for a value of t in the $e(t)$ map table, we also have the values of $j(\chi, \chi^j),\ j = 1, 2, \dots, p^k - 2$ precomputed in a separate table. The character χ is, complex valued and has conductor q and order p^k. The Jacobi-Sums are polynomials representing elements of $\mathbb{Z}[\xi_{p^k}]$. At run time, this values only need to be mapped into the cyclotomic working extensions. By this approach we shift the super polynomial step of computation of Jacobi-Sums to an off line precomputation stage. It may be argued, that for values of q which are so large, that the precomputed tables become excessive, the lattice reduction method for computing Jacobi-Sums becomes effective, so that the naive approach need never be used in real time computations. We have not pushed our experiments so far though. Using tables for the Jacobi-Sums and thus deferring the major part of their computation to the preprocessing stage is also an improvement upon the [BovdH] implementation: the same table may be used for an exponential amount of test numbers.

5.2 Building working extensions

Once the optimal value t with its corresponding value for $s = e(t)$ is chosen and factors $s' = \prod_{q \in \mathcal{F}} q$ for the Lucas - Lehmer test are found, one has to build working cyclotomic extensions in which Jacobi Sum and Lucas - Lehmer tests are to be performed. This section treats the procedures used for building these extensions.

In the process of building working cyclotomic extensions, one starts by building the saturated extensions $(\mathbf{R}_p, \sigma_p, \zeta_p), \forall p \mid t$ with saturation degrees $k_s(p)$. Given the saturated extension, any p^k-th extension with $k \neq k_s(p)$ can be easily built in the testing process. The extensions are built using the Lucas - Lehmer method. The ring $\mathbf{R} = \mathbb{Z}[\eta_p]$, is defined using some suitable trace of a complex primitive root of unity modulo n. If $\mathrm{ord}_p(n) = p-1$, $\eta_p = \zeta_p$ is itself the $p-$th root of the extension. We say that the cyclotomic extension is *full*.

Fact 5.2 *The standard presentation of a cyclotomic extension in our implementation is following:*

(i) p, the prime order of the extension; k_s, the saturation degree and deg : the extension degree $[\mathbf{R}_p : \mathcal{N}]$,

(ii) $(\eta_p, m_p(x))$, *where* $m_p(x)$ *is the minimal polynomial of* η *over* $\mathcal{N}$.

(iii) *The automorphism matrix* $\mathbf{M}_p$ *of* σ_p *together with the basis transform matrix* $\mathbf{T}_p$ *for switching from a power base to a normal base representation of* $\mathbf{R}_p$.

(iv) ζ_p, *the primitive* $p^{k_s(p)}-\mathrm{th}$ *root of the extension.*

(v) *The minimal polynomial* $\mu_p(x)$ *of* ζ_p *over* $\mathcal{N}$.

Using this representation, it is obvious that for $k < k_s(p)$, a p^k-th root of unity is just $\zeta_p^{p^{k_s(p)-k}}$ and it lays in $\mathbf{R}_p$. For $k > k_s(p)$, the minimal polynomial μ_{p^k} of the root of $x^{p^{k-k_s(p)}} = \zeta_p$ is simply $\mu_{p^k} = \mu(x^{p^{k-k_s(p)}})$. In this case an exception from the standard presentation is made and p^k-th extensions are given by $(\mathcal{N}[\zeta_{p^k}], \sigma_{p^k}, \zeta_{p^k})$, where $\zeta_{p^k} = x \bmod \mu_{p^k}$. One does not have the advantage of a trace base and the coefficients of the matrix σ_{p^k} are large. However $k > k_s(p)$ is a rare case, occurring mostly just for the prime $p = 2$ and the advantages of the saturation exponent presentation are predominant.

The roots ζ_p are computed by trial and error. If a root cannot be found after a fixed number of trials (one should typically choose $c \approx (\log(n))^2$ as upper bound), the algorithm halts with the claim "no decision on the primality of n made". It can be restarted for new random trials. The rationale for the estimate for the bound c is based on the Extended Riemann Hypothesis and can be found in [Ba1]. In Appendix A we treat the deterministic continuation of the algorithm – for the case the present version stops with no decision made.

For building amalgams it is advantageous if two rings $\mathbf{R}_1$ and $\mathbf{R}_2$ such that $\deg(\mathbf{R}_2) \mid \deg(\mathbf{R}_1)$, where $\deg(\mathbf{R}) = [\mathbf{R} : \mathcal{N}]$, also have a natural inclusion map. For achieving this goal, we start by building a division tree of the orders

$$O(t) = \{\mathrm{ord}_4(n)\} \cup \{\mathrm{ord}_p(n) \mid p \text{ is odd and } p|t\}.$$

The cyclotomic extensions are built starting with the maximal order of a single division chain. Extensions with orders dividing the maximal order of the respective chain are then constructed as sub extensions.

Let $p_M \mid t$ be a prime with maximal order in a chain of $O(t)$ and let p lay in the same chain. Thus $\deg(\mathbf{R}_p) \mid \deg(\mathbf{R}_{p_M})$. Given the extension $(\mathbf{R}_{p_M}, \sigma_{p_M}, \zeta_{p_M})$ in its standard presentation (5.2), the extension $(\mathbf{R}_p, \sigma_p, \zeta_p)$ is constructed as sub extension as follows:

1. Let $d = \mathrm{ord}_{p_M}(n) = \deg(\mathbf{R}_{p_M})$ and $d_p = \mathrm{ord}_p(n)$. Then $\eta_p = \sum_{i=1}^{d/d_p} \sigma_{p_M}^{id_p}(\eta_{p_M})$
2. $\sigma_p = \sigma_{p_M}^{d_p}$
3. $\mathbf{R}_p = \mathcal{N}[\eta_p]$
4. ζ_p is computed in $\mathbf{R}_p$ by the Lucas - Lehmer method.

Finally, once all chains of working extensions are constructed, some work must be done for proving that all the extensions built are embedded in a common $t-$th extension. This proof is a prerequisite for the subsequent tests and is itself part of the primality test: if it fails, n is composite. The proof is based on (3.64).

We show how the proof works for two chains. The method shown can then be applied recursively. Let $p_M, p'_M \mid t$ be two primes with maximal orders, $d = \mathrm{ord}_{p_M}(n)$, $d' = \mathrm{ord}_{p'_M}(n)$ and $d_0 = (d, d')$. If $d_0 = 1$, the chains are disjunct and there is nothing to prove. Otherwise, let p be a prime with $\mathrm{ord}_p(n) = d_0$. Build a $p-$th cyclotomic sub extension in both chains. If the $p-$th roots can be constructed, the proof is a consequence of (3.64). In most cases, p will actually be in one of the chains, so only one additional construction needs to be performed for the proof. In fact the choice of the chain to which a prime p belongs, whose order $\mathrm{ord}_p(n)$ divides several maximal orders, is an arbitrary one.

5.3 Arithmetic using fast convolutions

In this section we deal with the implementation problem of arithmetic in cyclotomic extensions. This has an impact upon the stages (ii) - (iv) of the test.

We are concerned with integer arithmetic both in the ring $\mathbb{Z}$ of rational integers and in the ring of polynomials with coefficients in $(\mathbb{Z}/n \cdot \mathbb{Z})$. In both cases we shall use the Montgomery algorithm ([Mg]) for modular reduction, which transforms divisions in multiplications and some trivial reductions. We begin by presenting this algorithm in the setting of a general ring - since we need it in both modular operations mentioned above. Let $\mathbf{R}$ be a commutative, ordered ring, $N \in \mathbf{R}$ and $R > N$ be an element such that following operators:

$$\begin{aligned} \perp : a \in \mathbf{R} \quad &\rightarrow \quad a^{\perp} = a \bmod R \\ \top : a \in \mathbf{R} \quad &\rightarrow \quad a^{\top} = a \div R \end{aligned} \tag{5.3}$$

are easy to calculate. The operation $\div$ is the integer division without remainder. For instance, if $\mathbf{R} = \mathbb{Z}[x]$, $R = x^k$ is a good choice, since polynomial division by R is particularly easy. We represent the classes in $\mathbf{R}/(N\mathbf{R})$ by the definition:

$$\overline{x} = (x \cdot R \bmod N). \tag{5.4}$$

It is easy to see that $\overline{x} + \overline{y} = \overline{(x+y)}$ and $\overline{x} \cdot \overline{y} = \overline{x \cdot y} \cdot R$. Montgomery's idea consists in providing a simple algorithm for computing $f(z) = z \cdot R^{-1} \bmod N$, so that $f(\overline{x} \cdot \overline{y}) = \overline{x \cdot y}$. The input z is subject to the restriction $0 < z < RN$. Suppose v is such that $v \cdot N = -1 \bmod R$. The function f is then computed by following procedure:

REDC(z) $\quad / * 0 < z < R \cdot N * /$

1. $m = (z^{\perp} \cdot v)^{\perp}$.
2. $t = (z + m \cdot N)^{\top}$
3. if $t \geq N$ then $t = t - N$
4. return(t)

In order to check that the algorithm is correct, note that

$$m \cdot N = (z^{\perp} \cdot v)^{\perp} \cdot N = -z^{\perp} \bmod R$$

and thus $z + m \cdot N = 0 \bmod R$ and t is an integer. Furthermore $0 \leq t < 2N$, since $z^{\top} < N$ and $(m \cdot N)^{\top} < N$. Finally $t = z \bmod N$ and step 3. provides for $t < N$. We now present the basic idea of *fast convolution* algorithms. The reader may find an excellent extended treatment of the topic in [Bl1]. Let $a_i, b_i, i = 0, 1, \ldots, n-1$ be two sequences of elements in $\mathbf{R}$. The linear convolution c_k is defined by

$$c_k = \sum_{i=0}^{k} a_i b_{k-i}, \quad k = 0, 1, \ldots, 2n-1,$$

where the coefficients $a_i = b_i = 0$ for $i \geq n$. The sequences a_i, b_i can be regarded as the coefficients of two polynomials of degree n, $a(x) = \sum_{i=0}^{n-1} a_i \cdot x^i$ and $b(x) = \sum_{i=0}^{n-1} b_i \cdot x^i$; c_k are then the coefficients of the product polynomial $c(x) = a(x) \cdot \underline{(}x)$. Furthermore, if $m(x)$ is some polynomial of degree $d > 2(n-1)$, then:

$$c(x) \quad = \quad a(x) \cdot b(x) \bmod m(x) \tag{5.5}$$

The idea of fast convolutions consists in splitting

$$m(x) = \prod_{j=1}^{l} m_j(x)$$

and compute

$$c_j(x) \quad = \quad [(a(x) \bmod m_j(x)) \cdot (b(x) \bmod m_j(x))] \bmod m_j(x).$$

The convolution $c(x)$ can then be retrieved using the Chinese Remainder Theorem.

Suppose now $\mathbf{R} = \mathbb{Z}$ and a_i, b_i are positive and uniformly bounded by some bound B. Then $c_k < n \cdot B^2$ and for any $N \geq n \cdot B^2$ the operations can be performed in $(\mathbb{Z}/N \cdot \mathbb{Z})$ rather than $\mathbb{Z}$. We shall see that this feature is very useful in different methods for fast convolution. The global approach we presented, was invented by Winogradow ([Wn]). We now present some concrete convolution methods:

I. The polynomial $m(x)$ is a Lagrange interpolation polynomial:

$$m(x) = \prod_{i=0}^{2n-2} (x - \epsilon_i)$$

and the interpolation points are usually $\epsilon_i = i$ or $\epsilon_i = i-(n-1)$. This is the **Toom-Cook** method [To], [Co]; $a(x) \bmod m_j(x)$ is in this case $a(x) \bmod (x-\epsilon_j) = a(\epsilon_j)$ and $c(x) \bmod m_j(x) = a(\epsilon_j)\cdot b(\epsilon_j)$. From these interpolation values, the coefficients of $c(x)$ can be retrieved and [Kn] presents an elegant tabular method for finding the convolution sequence. Knuth mentions that this method has the disadvantage that $c(\epsilon_j)$ increase exponentially with n. This problem can however be avoided, if N is chosen as above, subject to the additional condition $(N, \epsilon_j) = 1, \forall j$ and the evaluation of $a(.), b(.)$ and $c(.)$ is performed modulo N. Furthermore, if $\mathbf{R}$ is a ring of polynomials over a finite ring $(\mathbb{Z}/n \cdot \mathbb{Z})$, the values $c(\epsilon_j)$ are naturally bounded by m and there is no problem with using the Toom Cook algorithm. This is particularly the case for cyclotomic extensions.

II. The polynomial $m(x)$ is a cyclotomic polynomial: $m(x) = x^{2n} - 1$. If the $2n$–th roots of unity are known, this method can also be regarded as an interpolation method and the values $a(\epsilon_j), b(\epsilon_j)$ as well as the convolution c_k are computed by **Fast Fourier Transform**. When $\mathbf{R} = \mathbb{Z}$, modular arithmetic with N as above is advantageous, especially if the $2n$–th roots of unity are powers of 2. In that case, the multiplications required by FFT are reduced to binary shifts. The numbers of the form $2^h \pm 1$, where h takes values such that $2^h - 1$ is close to $n \cdot B^2$ are good candidates for N; note that N needs *not* be a prime. Modular reduction is also free for such a choice of N. Strassen and Schönhage proposed in their historical paper [ScSt] to use 2^w as a modulus, for some word length w.

III. While modular arithmetic is recommendable, in order to avoid explosion of the multiplicands for the Toom - Cook method and for simplifying FFT in the cyclotomic method, the multiplicands will however be at least twice as large as the initial coefficients a_i and b_i, and their multiplication is the equivalent of at least 3 direct multiplications of numbers of the size of a_i. This fact needs to be taken into account when evaluating fast convolution methods. **Small Winogradow** convolutions avoid this detriment: the polynomials $m_j(x)$ are no more necessarily linear, they are chosen to have coefficients $0, -1, +1$ and eventually $-2, 2$, so that the coefficients of the multiplicands $a(x) \bmod m_j(x)$ will have roughly the same length as the ones of $a(x)$. Ideal polynomials of degree two for small Winogradow convolutions are $x^2+1, x^2+x+1, x^2-x+1, x^2+x-1, x^2-x-1$. There are efficient small Winogradow convolutions for $n = 3$ up to 8.

IV. Any small convolution can be *iterated* by using the **Agarval-Cooley** method. The idea is to split n in two coprime factors, say $n = n' \cdot n''$ and transform a one-dimensional convolution of degree n into a bidimensional convolution with degrees n' and n''. This leads to simpler convolutions for large n; in the case of FFT it even produces a slight decrease in the number of effective multiplications [Bl1]. A particularly popular iterated small Winogradow convolution is the **Karatsuba - Offman** ([Kn]) long integer multiplication method.

It is usual for arithmetic in galois extensions, to use a variant of the FFT convolution in which the base field arithmetic is replaced by arithmetic in a surrogate Fermat prime ring, of size $> 2\cdot d\cdot p\cdot \log(p)$, where d is the extension degree and p the field characteristic ([Sh2]). This is also the way galois field arithmetic is implemented in the LiDIA library([LiDIA]) by Victor Shoup et.al. Compared to the Toom-Cook method, this approach yields more convenient spectral transforms; it does however increase the base field arithmetic by a factor of at least 4. It is the relation between d and p which decides the trade off between Toom-Cook and FFT: for relatively small d, the factor 4 in the base arithmetic is not compensate by the better spectral transform and thus Toom-Cook is preferable. A simple estimation shows that the break-even point lays about $d = M(p)/\log(p)$, where $M(p)$ is the cost of a field multiplication, varying between $\log(p) \cdot \log\log(p)$ and $\log^2(p)$. With a Karatsuba arithmetic in the base field – such as implemented in the *gmp2.0* arithmetic library used by LiDIA – the break even point will be about $d \approx \sqrt{\log(p)}$. The extension degrees occurring in cyclotomy primality proving lay all beneath this bound, and therefor Toom-Cook is recommendable. I am grateful to Dr. V. Shoup who confirmed in private discussion the above estimates and the behavior of the LiDIA implementation of arithmetic modulo polynomials over finite rings.

The *generic* treatment of convolutions over abstract rings $\mathbf{R}$ suffices for presenting the main principles of the different approaches. When it comes to making the choice for a particular implementation, the properties of the *specific* rings have to be taken into account. In the context of cyclotomy tests, $\mathbf{R}$ may be a cyclotomic extension - in which case, convolutions are used for computing the product of two extension elements represents by polynomials over $\mathcal{N}$. Or it may be the ring $\mathcal{N} = (\mathbb{Z}/n \cdot \mathbb{Z})$ itself and convolutions are used for speeding up the long integer multiplication. In both cases, the multiplication is followed by a modular reduction - in the first case, the modulus is the minimal polynomial generating the extension, in the second it is n. It is thus useful to use Montgomery representation in these contexts. We shall consider the two cases separately and find methods for optimally *combining fast convolutions with Montgomery reduction.*

We first treat the modular multiplication of polynomials over $(\mathbb{Z}/n \cdot \mathbb{Z})$. Let $p(x)$ be a monic polynomial of degree d and $a(x), b(x)$ have lower degree. The convolution polynomial has thus degree $\geq 2d$. As mentioned in II, the **Toom-Cook** algorithm is perfectly adequate in this context. Let the interpolation points be $\epsilon_j = j, \ j = 0, 1, \ldots, 2d$. We have to show that the interpolation theorem holds in a modular ring. It follows directly form the Lagrange interpolation formula, that the Toom - Cook method can be applied iff:

(i) $n > 2d$

(ii) $(n, \epsilon_j) = 1 \ \ \forall j$

For computing $c(x) = a(x) \cdot b(x) \bmod p(x)$ in $(\mathbb{Z}/n \cdot \mathbb{Z})[x]$, first let

$$z(j) = a(j) \cdot b(j) \bmod n, \ j = 0, 1, \ldots, 2d.$$

For the modular reduction we shall use the Montgomery algorithm, with $R = R(x) = \prod_{j=0}^{d} (x - \epsilon_j)$. Suppose $\exists v(x) \in (\mathbb{Z}/n \cdot \mathbb{Z})[x]$ with $p(x) \cdot v(x) = -1 \bmod R(x)$; in the context of primality testing this assumption is meaningful, since $v(x)$ can be obtained with the Euclidean algorithm and whenever a division fails, a factor of n is found and the test algorithm stops. We show how to perform the Montgomery algorithm with a minimum of multiplications. First note that for any polynomial $g(x)$, $g(x)^{\perp} = g(x) \bmod R(x)$, hence $g^{\perp}(i) = g(i)$ for $i = 0, 1, \ldots, d$. Furthermore, $g^{\perp}$ is a polynomial of degree $< d$, so it is completely determined by its values in the d points $i = 0, 1, \ldots, d-1$. Consequently, step 1. of the Montgomery algorithm reduces to multiplying the first d values of $z(x)$ and $v(x) : m(j) = z(j)v(j),\ \forall j \in \{0, 1, \ldots, d\}$.

Suppose $h(x)$ is a polynomial of degree $< 2d$, which is divisible by $R(x)$, thus $h(x) = h^{\top}(x) \cdot R(x)$. Then $h^{\top}$ is uniquely determined by the values

$$h^{\top}(j) \;=\; h(j) \cdot R(j), j = d+1, d+2, \ldots, 2d.$$

Thus $t(x)$ in step 2. of the Montgomery algorithm can also be computed by d multiplications:

$$t(d+j) \;=\; z(d+j) + m(d+j)p(d+j), \qquad \forall j \in \{0, 1, \ldots, d-1\}.$$

Note that $t(x)$ has by definition a degree $< d$, so step 3. of the Montgomery algorithm becomes superfluous. On the other hand, step 1 produces the values $m(j),\ \forall j \in \{0, 1, \ldots, d-1\}$, whereas step 2 requires the values

$$m(j+d)\ \forall j \in \{0, 1, \ldots, d-1\}.$$

The last ones are determined by the first. For computing them, one has to retrieve the coefficients of $m(x)$ and then evaluate this polynomials at the points

$$m(j+d),\ \forall j \in \{0, 1, \ldots, d-1\}.$$

We can state the following:

Algorithm III *(* Modular Multiplication in* $(\mathbb{Z}/n \cdot \mathbb{Z})$ **)*

Let $p(x)$ be a monic polynomial of degree d in $(\mathbb{Z}/n \cdot \mathbb{Z})[x]$ and $a(x), b(x)$ have degree $< d$. Let $R(x) = \prod_{j=0}^{d} (x-j)$ and $v(x)$ be a polynomial of degree $< d$, such that $p(x) \cdot v(x) = -1 \bmod R(x)$. We assume that all above polynomials are given by their values at the points $j = 0, 1, \ldots, 2d$ and present an algorithm which will feature $t_j = t(j)$, where $t(x) = a(x) \cdot b(x) \bmod p(x)$.

1. Compute $z(j) = z_j = a_j \cdot b_j,\ j = 0, 1, \ldots, 2d$
2. Compute $m(j) = m_j = z_j \cdot v_j,\ j = 0, 1, \ldots, d$
3. Retrieve the coefficients of $m(x)$ and compute $m_j,\ j = d+1, d+2, \ldots, 2d$ using the method described by [Kn].
4. Compute $t(j) = t_j = z_j + m_j \cdot p_j,\ j = d+1, d+2, \ldots, 2d.$
5. Retrieve the coefficients of $t^{\top}(x)$ using $t_j^{\top} = t_j \cdot R_j$ and compute t_j, $j = 0, 1, \ldots, d.$

The operation count is following:

(i) $2(2d+1)$ multiplications in $(\mathbb{Z}/n\cdot\mathbb{Z})$, for computing z_j, m_j and t_j.

(ii) Evaluation of $d+1$ coefficients and d values for $m(x)$.

(iii) Evaluation of d coefficients and $d+1$ values for $t^\top(x)$.

Note that at the end of the process the polynomial $t(x)$ is presented by its interpolation values, so it can be used as input for a further application of this algorithm. The algorithm is designed for being used for exponentiations, so the task of determining $v(x)$ belongs to a precomputation phase which is performed once for every $p(x)$. The ring $(\mathbb{Z}/n\cdot\mathbb{Z})/(p(x))$ should thus be defined by the list $\{n, p(x), v(x)\}$.

This approach to polynomial reduction is particularly useful when the modulus polynomial $p(x)$ has long coefficients. It then reduces the number of long integer multiplications used for a reduction modulo a polynomial of degree d from $O(d^2)$ to $O(d)$. *In the case of cyclotomy testing however, the coefficients of $p(x)$ are short integers, and this makes the naive modulo reduction more attractive.* In fact, when using Montgomery reduction, the coefficients of $v(x)$ are in general full length integers $\bmod n$, which would increase complexity!

Modular multiplication of integers is more difficult. The basic idea is splitting a number n in words of length w and representing n as a polynomial: $n(x) = \sum_{i=0}^{k} n_i x^i$, where $x = 2^w$. Multiplication modulo n reduces to multiplication of two polynomials and subsequent reduction of their *values* at $x = 2^w$ modulo n. Choosing a special value for R in the Montgomery algorithm can reduce to half the multiplications in the first step of the procedure **REDC**. In the second one however, a whole multiplication must be performed, when using fast convolution techniques. A modular multiplication thus costs the equivalent of $5/2$ long multiplications when using fast convolution techniques. This fact together with the remark in III must be taken into account, when implementing long integer arithmetic using fast convolutions. The jump from 2 to $5/2$ long multiplications, when changing from naive to fast convolutions techniques must be considered when establishing the lower length for fast convolution. For intermediate range iterated small Winogradow convolutions like the Karatsuba - Offmann algorithm shall be chosen, since they have the quality of preserving the word length of the multiplicands. For large integers FFT techniques over finite fields shall be preferable. "Large" may be 10000 bits or more.

We finally show how to use Montgomery reduction together with nested fast convolutions. Let n have length $B^{2k-2} < l < B^{2k}$, with $B = 2^w$, where w is the machine word length and $a, b < n; x = B^k$. Write $a = a_1 x + a_2$ and $b = b_1 x + b_2$ and choose $R = x^2$ for the Montgomery algorithm. Let $v = v_1 x + v_2$ be such that $vn = -1 \bmod R$. Any fast convolution method can be used for multiplying k word numbers a_i, b_i, v_i $(i = 1, 2)$, whereas for multiplication of $2k$ word numbers, two point Winogradow convolution shall be used, which makes the application of the operators $\perp$ and $\top$ trivial.

The use of fast convolution methods will certainly bring an important improvement of the actual performance of the cyclotomy test compared to the [BovdH] implementation. It may in fact be the most visible improvement at all.

5.4 Building amalgams and performing the tests

According to (4.25), the task of building amalgams consists in joining several Jacobi-Sums together for testing (4.29). For obtaining optimal efficiency, following points must be considered:

(i) The orders of the characters of Jacobi-Sums in one amalgam must be powers of pairwise distinct primes.

(ii) All the Jacobi-Sums in one amalgam must be embedded in a common extension.

The first condition shows that there is a natural upper bound to the number of Jacobi-Sums in one amalgam: this is the number $n(t)$ of distinct primes dividing t. The second suggests that all the degrees of the extensions in which single Jacobi-Sums of an amalgam are elements should divide a maximal one and at least one element of the amalgam should be defined in the extension of the maximal degree. For an optimal amalgam matching, one should thus recursively group Jacobi-Sums belonging to maximal degree extensions and subextensions of degree dividing the maximal degree together. Bosma and van der Hulst show in their thesis, that this naive approach is also optimal, by solving an optimal matching problem.

We give now a formal description of the strategy for building amalgams. Start by making a list $\mathcal{L}$ of the pairs $(p^k, q) \in G_n^{\perp}$. Let the list be ordered according to the division chains for the extensions degrees ord_{p^k} defined in the step of building working extensions, the order being decreasing. While the list $\mathcal{L}$ is not empty, one builds an amalgam $\mathcal{A}$ by following steps:

(i) Set $\mathcal{A} = \emptyset$ and set the pointer $\pi_{\mathcal{L}}$ to the first element $J = (p^k, q) \in \mathcal{L}$. Set the amalgam element counter $c(\mathcal{A}) = 1$ and let $d(\mathcal{A}) = \mathrm{ord}_{p^k}(n)$ be the degree of the extension in which the Jacobi-Sum J lives - the maximal degree of the amalgam.

(ii) If $c(\mathcal{A}) = 1$ go to (iv).

(iii) If $\mathrm{ord}_{p^k}(n)$ is not equal or a divisor of $d(\mathcal{A})$, go to (v).

(iv) Set $\mathcal{A} = \mathcal{A} \cup \{J\}$ and increase $c(\mathcal{A})$ by 1.

(v) If the end of the list $\mathcal{L}$ is reached or if $c(\mathcal{A}) = n(t)$, set $\mathcal{L} = \mathcal{L} \setminus \mathcal{A}$ and return $\mathcal{A}$.

(vi) Increase the pointer $\pi_{\mathcal{L}}$ by one and let J be the pair pointed to by $\pi_{\mathcal{L}}$.

(vii) Go to (iii).

At the end of this procedure, the initial list is partitioned into a set of disjoint amalgams, so performing the test (4.27) on these amalgams is equivalent to performing (4.15) on the initial list $\mathcal{L}$, by theorem (4.25).

Let $\mathcal{F} = \{q : n^w - 1 \mid q \text{ prime and } w \mid t\}$ be the set of known factors of $n^t - 1$ with $(q-1, t) < q - 1$ and $s' = \prod_{q \in \mathcal{F}} q$. Then all the factors in $\mathcal{F}$ will be subjects to Lucas - Lehmer tests according to (3.42) and (3.43).

If all the amalgam and Lucas - Lehmer tests are successfully passed, an $s \cdot s'-$th cyclotomic extension of $\mathcal{N}$ exists by the choice of $G_n^{\perp}$, theorems (3.42), (4.25) and (3.64).

5.5 The final trial division

The final test division is very simple as structure; however, with increasing values of n, it tends to dominate the rest of the test. This stage consists in verifying

$$(r_i, n) = 1,\ \ r_i = n^i \bmod S,\ \ i = 1, 2, \ldots, t-1.$$

It does in fact suffice that r_i is not a divisor of n, since if n were composite, at least one divisor would be equal to its remainder $\bmod s$.

We give here two ideas which help to improve the performance of this step. The first improvement consists in the fact that the number of trial divisions can be reduced to almost none. This can be done by using following idea, remarked also in [BovdH]: if n is composite, it has a prime factor $< \sqrt{n}$, so trial division should be performed only for residues $r_i < \sqrt{n}$. If one chooses $S > t \cdot \sqrt{n}$, which is possible without sensible increase in the size of t, the density of residues $\bmod S$ which are $< \sqrt{n}$ is less then $1/t$ so in average at most one effective trial division will be needed. This simplification has to be anchored in the initial stage of choice of the parameters of the algorithm. Its consequence is that the final stage is virtually reduced to a *long chain of multiplications* by $n \bmod S$.

The second improvement is new and it shows how to also reduce the work for computing the residues $r_i = n^i \bmod S,\ i = 1, 2, \ldots, t-1$. The idea is to take advantage of the fact that the complete factorization of S is known and the orders $\{\mathrm{ord}_q(n) : q|S\}$ split into a small number of prime factors dividing t. The use of the Chinese Remainder Theorem lays at hand. We shall start with some observations in order to develop an optimal way of using the additional information for the test.

(i) The residues $r_i = n^i \bmod S,\ i = 1, 2, \ldots, t-1$ are uniquely determined by the system of "sub residues": $\{r_i(q) = n^i \bmod q :\ i = 1, 2, \ldots, d(q) \text{ and } q|S\}$, where $d(q) = \mathrm{ord}_q(n)$. It appears thus useful to precompute tables for these sub residues.

(ii) When using the Chinese Remainder Theorem for retrieving r_i from the set $\{r_i(q) : q|S\}$ one has to multiply for each $q|S$ a short integer $r_i(q)$ by a long integer $e(q)$, where $e(q) \bmod S$ is a base element for the Chinese Remainder Theorem, i.e.: $e(q) = 1 \bmod q$ and $e(q) = 0 \bmod q',\ \forall q'|S,\ q' \neq q$. The number of factors of S might be larger then the number of machine words required to represent S, so one might end up performing more multiplications while using the Chinese Remainder Theorem then one would have to do while using plain multiplication $\bmod S$. The factors q should thus be somehow grouped in order to reduce the number of operations required for retrieving r_i from the sub residues. The sub residues should be stored multiplied by the base elements $e(q)$, so that no multiplications need to be performed at run time.

(iii) After grouping the factors q into products P_j of *approximate* length 2^w (w might be chosen to be the word length, or its double, etc.), one should precompute the sub residues modulo these products. Due to the grouping, the number of sub residues has increased. One would like to use some kind of "baby step giant step method" in order to optimize the storage/multiplications problem. This consists in following. Say the residues $r_i = n^i \bmod P,\ i = 1, 2, \ldots d(P)$ need to be recorded for some P and $d(P)$ is too large for the storage capacity of the machine. Choose $B = [\sqrt{P}] + 1$, and store the values $r_0(i) = n^i \bmod P$ and $r_1(i) = n^{iB} \bmod P$, for $i = 1, 2, \ldots, B-1$. Then r_i is simply $r_i = r_0(i \bmod B) \cdot r_1(i/B) \bmod B$.

(iv) If one retrieves the residues r_i in their natural order $i = 1, 2, \ldots, t-1$, the values $i \bmod d(q)$ will alternate randomly and multiplications by the full set $e(P_j)$ (we replaced $e(q)$ by $e(P_j)$ with the obvious meaning for $e(P_j)$) might be required at each step. One may spare operations, by regarding the index i as an integer $\bmod t$ and applying the Chinese Remainder Theorem for the indices too. If $\{p^{k(p)} \parallel t\}$ is the set of prime factors of t, one should loop recursively through the indices $\bmod p^{k(p)}$. This should be done in a certain order.

(v) Assume that the primes $p \mid t$ have been reordered, so that

$$h(p_1) \geq h(p_2) \geq \ldots \geq h(p_m).$$

The residues r_i will be computed by using the Chinese Remainder Theorem representation of $i \bmod t$: $i = (i_1, i_2, \ldots, i_m)$, where $i_k = i \bmod p_k^{k(p_k)}$. One calculates the r_i in nested loops, where i_m changes the most frequently, and i_1 the less frequently:

for $i_1 = 1$ **to** $k(p_1)$ **do**
  for $i_2 = 1$ **to** $k(p_2)$ **do**
    $\vdots$
    for $i_m = 1$ **to** $k(p_m)$ **do**
      $i = (i_1, i_2, \ldots, i_m) \bmod t$;
      $r_i = n^i \bmod S$
    done
    $\vdots$
  done
done

In order to estimate the operation count, let us define the function $\kappa(p) = \sum_j \delta_j'(p^{k(p)})$ with $\delta_j'(l) = 1$ if $l \mid \mathrm{ord}_{P_j}(n)$ and 0 otherwise. The function $\kappa(p_k)$ counts the number of products P_j for which the residues $n^i \bmod P_j$ are modified when $i \bmod p_k$ is changing, while $i \bmod p_l$ remains unchanged, for $l \neq k$. Consequently, in the $l-$th loop, exactly $\kappa(p_l^{k(p_l)})$ additions $\bmod S$ will be performed per step. Due to the nesting of the loops, the innermost loop is traversed t times, the next, $t/p_m^{k(p_m)}$ times and in general, the loop l is traversed $\vartheta_l = t/\left(\prod_{h=l+1}^{m} p_h^{k(p_h)}\right)$ times. After having filled the tables of subresidues in a preprocessing step, at runtime, the number of operations (additions $\mod S$) is thus:

$$a(P) = t\kappa(p_m^{k(p_m)}) + \frac{t}{p_m^{k(p_m)}}\kappa(p_{m-1}^{k(p_{m-1})}) + \dots = \sum_{l=1}^{m} \vartheta_l \kappa(p_l^{k(p_l)}). \tag{5.6}$$

(vi) Since the predominant term in (5.6) is the contribution of p_m, one shall first group the primes q with $p_m \mid d(q)$, and add no primes with $(p_m, d(q)) = 1$ to these products. One proceeds then by remaining primes with $p_{m-1} \mid d(q)$, etc.

(vii) The indices i for which the residues r_i are currently being computed are, as mentioned above, represented as tuples, using the Chinese Remainder Theorem. It is thus comfortable, when storing the sub residue tables, to index them the same way, thus avoiding recalculation of the indices $\mod t$.

(viii) If the sub residues are stored with their full values $\mod S$, no multiplications need to be done and the exact size of the products P_j is irrelevant from the point of view of the number of operations. It is more used for calibrating the storage size. In particular, if one chooses 2^w, with w the machine word size, as approximate size for P_j, the value 2^w will not be an upper bound for P_j.

The above list of observations leads to an implementable algorithm for computing the residues $r_i = n^i \bmod S$:

Algorithm IV *(* Computing a Modular Cycle. *)*

1. Let $t = \mathrm{ord}_S(n) = \prod_{i=1}^m p_i^{k(p_i)}$

2. Compute

$$h(p) = \sum_{k=1}^{k(p)} \sum_{q|S} \delta_q(p^k), \ \forall p \mid t,$$

and use this function for reordering the primes p, so that $h(p_1) \geq h(p_2) \geq \dots \geq h(p_m)$.

3. Group the factors $q \mid S$ into products P_j of approximate size C, starting with q such that $p_m \mid d(q)$, etc. Let $P_1, P_2, \dots, P_l$ be the resulting products.

4. Compute the Chinese Remainder Theorem base elements e_j, such that $e_j \bmod P_i = \delta_{ij}$, for $j = 1, 2, \dots, l$, with δ the Kronecker symbol. We have $e_j \in (\mathbb{Z}/S \cdot \mathbb{Z})$.

5. For $j = 1, 2, \ldots, l$, compute the sub residues $r_j(i) = n^i \bmod P_j$, $i = 1, 2, \ldots, d(P_j)$ implicitly, by using the baby step - giant step method and store the values $r_j(i) \cdot e_j \bmod S$ (represented by one or more values). Use the Chinese Remainder Theorem with respect to the factorization of t, for indexing the stored sub residues.

6. Compute the remainders $r_i = n^i \bmod S$, in a nested loop as follows:

for $i_1 = 1$ **to** $k(p_1)$ **do**
  for $i_2 = 1$ **to** $k(p_2)$ **do**
    ⋮
    for $i_m = 1$ **to** $k(p_m)$ **do**
      $i = (i_1, i_2, \ldots, i_m) \bmod t$;
      $r_i = n^i \bmod S$
    done
    ⋮
  done
done

7. If $r_i < \sqrt{n}$, check if $r_i \mid n$. If this is the case, n is composite!

Remark 5.4 *There is a large degree of freedom in the choice of the upper bound C in step 3. If $C \geq \max_q\{q|s\}$, a super polynomial table will result. This table is only depending on t and can thus be precomputed, thus shifting the super polynomial amount of multiplications out of the active trial division. In this stage, only a super polynomial amount of long integer additions will be required. For smaller C, the storage and precomputation size are reduced at the cost of inserting some multiplications - more precisely short by long multiplications - back to the active trial division.*

In [Le4], Lenstra described an ingenuous method for finding divisors of n in residue classes $\bmod S$, where $S > \sqrt[3]{n}$. This allows of course, using smaller t and less Jacobi-Sum tests and decreases the length of the final trial division. It happens of course at a cost: for each residue $r_i = n^i \bmod S$, several relations must be checked, which are more complex then the trial divisibility relation that has eventually to be checked, when S is chosen $> \sqrt{n}$. We shall refer to this method as the *cubic root* method and to the classical one, as the *square root* method for trial division. The crucial exponent in the inequation

$$n > s^{\mu},$$

taking the possible values $\mu = 1/2$ or $\mu = 1/3$ will be referred to, in accordance with [BovdH] as the μ-exponent.

5.5.1 Brief speculative digression

With the above improvements, it is likely that the final trial division stage will take further orders of magnitude, before becoming dominant. It remains however, together with the calculation of Jacobi-Sums, the only super polynomial step of the algorithm. What more is, the later may be deferred to a precomputation stage, since they do not depend on the actual value of the test number n. This is not the case for the final trial division, and the question of reducing this stage to polynomial time is central.

It is appealing to ask the question, whether it is possible to increase S sufficiently, so that one can list a polynomial set of indices i, which can be proved to contain all the indices of residues $r_i < n$. This question can be stated precisely as follows:

Definition 5.5 *Let n be a positive integer and let*

$$t = O\Big(\log(n)^{\log\log\log(n)}\Big), \; S = e(t) > n^{\alpha}, \quad \textit{with } \alpha > 1/2.$$

*A subset $\mathcal{S}$ of $(\mathbb{Z}/t\cdot\mathbb{Z})$ is called μ-**feasible**, if*

(i) $\#\mathcal{S} = (\log(n))^{O(1)}$

(ii) $n^i \; mod \; s = r_i < n^{\mu} \Longrightarrow i \in \mathcal{S}$

(iii) $\mathcal{S}$ can be computed in polynomial time.

A μ-feasible set contains all the residues $r = n^i$ which are $< n^{\mu}$ in absolute value. If a $1/2$ (or $1/3$)-feasible set exists for any n, then obviously the final stage of the cyclotomy test is polynomial. Suppose $S = s_1 \cdot s_2$ with $s_i > \sqrt{n}, i = 1, 2$. If n is composite and an $S-$th cyclotomic extension of $\mathcal{N}$ exists, there is an exponent i mod t, such that

$$n^i \bmod s_1 = n^i \bmod s_2, \tag{5.9}$$

where the numbers of both sides of the above equation are regarded as absolute integers $< \sqrt{n}$; the common value is a $r < \sqrt{n}$, a prime factor of n. The above equation is not only highly improbable, it is also to a high extent independent of the actual value of n. One may thus envisage a strategy for solving the final stage in polynomial time, by sorting out a maximal set of exponents - μ feasible set - for which (5.9) may have a solution; or, inversely, eliminate a super polynomial set of exponents for which (5.9) a priorically may not hold. Needless to say, such an algorithm was not found during the developing time of this thesis. We conclude this digression with a simple example giving the flavor of how such an algorithm might work.

Example 5.7 *Let $S = 143 = 11 \cdot 13$. We shall investigate the possibility of existence of a composite number $n < 11^2$, such that a $143-$th cyclotomic extension of $\mathcal{N}$ exists. In the above notations, we have $s_1 = 11$ and $s_2 = 13$ and n must have a prime factor $r < 11$. We seek thus an exponent $i \;\; mod \;\; 60$, such that*

$$r = n^i \;\; mod \; s_1 = n^i \;\; mod \; s_2 = n^i \;\; mod \; S < 11$$

We have

$$3 = \begin{cases} 2^8 \ mod\ 11; \\ 2^4 \ mod\ 13. \end{cases}$$
$$5 = \begin{cases} 2^4 \ mod\ 11; \\ 2^9 \ mod\ 13. \end{cases}$$
$$7 = \begin{cases} 2^7 \ mod\ 11; \\ 2^{12} \ mod\ 13. \end{cases}$$

While $r = 3$ allows solutions generated by $n = (4,2) = 15 \mod 143$ and $i = 4 \mod 60$, there is no solution for $r = 5$ and $r = 7$, since the parity of the two indexes differs.

In *real life*, the two factors $s_i, i = 1,2$ will be large and highly composite. This example simply shows that some information can be gained from the value of t itself, i.e. before the active test. We close this digression with a sharper version of the μ - feasible set problem:

Definition 5.8 *Let t be a composite built up from "small prime" and let $S = e(t) = s_1 \cdot s_2$ be split in two coprime numbers s_i, $i = 1,2$ of comparable size, such that $\lambda(s_1) = \lambda(s_2) = t$. Let the set of* **common exponents** *be defined by:*

$$\Omega = \{i \mod t : \ \exists \alpha_{1,2} \in (\mathbb{Z}/s_j \cdot \mathbb{Z}), \quad \alpha_1^i \mod s_1 = \alpha_2^i \mod s_2\},$$

the last equality being between absolute integers.

Suppose it is possible to estimate Ω or a polynomial (in $|S|$) superset thereof. If n is an integer for which an $S-$th cyclotomic extension of $\mathcal{N}$ exists and $s_i > \sqrt{n}, i = 1,2$, then all possible prime factors $r < \sqrt{n}$ of n are in $\{n^i \mod S : \ i \in \Omega\}$.

5.6 Global statement of the algorithm

I. Precomputation phase.

1. *Build a table T1 with following entries:*
   - (i) $t = \prod_i p_i^{e_i}$, $p_i^{e_i} < B$ for a chosen bound B.
   - (ii) a linked list to the set $Q(t) = \{q \mid (q-1) \mid t, q$ prime.$\}$
   - (iii) $e(t) = \prod_{q \in Q(t)} q$.

2. *Build a multiple Jacobi-Sum table T2 with following entries:*
   - (i) (p^k, q, d) with $p^k \mid (q-1)$, $d = \text{ord}_{p^k}(n)$ for all $t \in T1$ and $q \in Q(t)$.
   - (ii) $J_i(\chi), i = 1,2,\ldots,p^k$ and $\chi : (\mathbb{Z}/q \cdot \mathbb{Z}) \to <\xi_{p^k}>$, with ξ_{p^k} a complex p^k-th primitive root of unity.

II. Primality test for a candidate n

1. *Choosing parameters*
   1.1 Choosing factors for Lucas - Lehmer test
      (i) For $w < B'$ seek factors $q \mid (n^w - 1)$, for a bound B'.
      (ii) Set $\mathcal{F} = \{q : q \mid (n^w - 1), w < B'\}$ and $s' = \prod_{q \in \mathcal{F}} q$.
   1.2 Choosing parameters for Jacobi-Sum tests
      (i) Choose a weight function w_i ($i = 1$ or 2) and find t and s, such that $e(t) = s > g(n)$ and t is optimal with respect to the weight w_i. The function $g(n)$ is defined by
$$g(n) = \frac{n^{\mu} \cdot f(n)}{s/(e(t), s')},$$
with $f(n) = \log(n)^{\log\log\log(n)}$ and $\mu \in \{1/3, 1/2\}$. The rationale for $g(n)$ is the following: the exponent μ indicates, if plain trial division will be used ($\mu = 1/2$) or the method [Le4]. The choice of $g(n)$ is such that $\operatorname{lcm}(s, s') > n^{\mu} \cdot f(n)$; with $S = \operatorname{lcm}(s, s') \cdot t$, the probability that a random remainder $r \bmod S < n^{\mu}$ is $< 1/(tf(n))$. This fact is used for easing the final trying division. There is a further use for this reserve in S, which shall be explained in the Lucas - Lehmer test.
      (ii) Adjust $\mathcal{F} = \mathcal{F} \setminus \{q : q \mid (s, s')\}$ and $s' = s'/(s, s')$.
      (iii) Discard t from the current copy of the table $T1$. (This is a provision for the case several Lucas - Lehmer test fail and the test must be restarted).
2. *Building work extensions*
   2.1 Let $D(t) = \{(d, p^k, q) : q \in Q(t), p^k \mid (q-1) \text{ and } d = \operatorname{ord}_{p^k}(n)\}$. Order $D(t)$ according to falling division chains for d.
   2.2 For all maximal degrees in d_m in a division chain build a working extension described by (5.2).
   2.3 Build all needed working subextensions of the maximal degree extensions built in 2.2.
   2.4 Prove the inclusion of all working extensions in a common t−th extension, like described in §5.2.
3. *Mapping Jacobi-Sums*
   For all $(d, p^k, q) \in D(t)$ do following:
   3.1 Let $u = u(p^k) = n \bmod p^k$
   3.2 Map $J_u(\chi)$ and $J_{p^k}(\chi)$ from table $T2$ into the working p^k−th extension.
4. *Building amalgams*
   4.1 Let $\mathcal{L} = D(t)$ and $A = \emptyset$.
   4.2 Set $\mathcal{A} = \emptyset$ and set the pointer $\pi_{\mathcal{L}}$ to the first element $J = (p^k, q, d) \in \mathcal{L}$. Set the amalgam element counter $c(\mathcal{A}) = 1$ and let $d(\mathcal{A}) = d$ be the degree of the extension in which the Jacobi-Sum J lives - the maximal degree of the amalgam.

4.3 If $c(\mathcal{A}) = 1$ go to 4.5.

4.4 If $\mathrm{ord}_{p^k}(n)$ is not equal or a divisor of $d(\mathcal{A})$, go to 4.6.

4.5 Set $\mathcal{A} = \mathcal{A} \cup \{J\}$ and increase $c(\mathcal{A})$ by 1.

4.6 If the end of the list $\mathcal{L}$ is reached or if $c(\mathcal{A}) = n(t)$, set $\mathcal{L} = \mathcal{L} \setminus \mathcal{A}$ and $A = A \cup \{\mathcal{A}\}$. If $\mathcal{L} = \emptyset$ stop.

4.7 Increase the pointer $\pi_{\mathcal{L}}$ by one and let J be the pair pointed to by $\pi_{\mathcal{L}}$.

4.8 Go to 4.4.

5. *Performing Jacobi-Sum tests*

5.1 Choose $\mathcal{A} \in A$ and write: $\mathcal{A} = \cup_{i=1}^{j} \{(d_i, p_i^{k_i}, q_i)\}$, $f = \prod_{i=1}^{j} p_i^{k_i}$.

5.2 Let $\alpha_i = J_{p_i^{k_i}}(\chi_i)$ and $\beta_i = J_{u_i}(\chi_i)$, with χ_i and u_i defined in step 3.

5.3 Let $n = fl + u$ and $u = p_i^{k_i} l_i + u_i$, for $i = 1, 2, \ldots j$ be results of Euclidean divisions.

5.4 Define
$$\alpha = \prod_{i=1}^{j} \alpha_i^{f/p_i^{k_i}} \text{ and } \beta = \prod_{i=1}^{j} \alpha_i^{l_i}\beta_i.$$

5.5 Check $\alpha^l\beta \in <\zeta_f>$. If this is not the case, declare n composite and stop.

5.6 Set $A = A \setminus \{\mathcal{A}\}$.

5.7 If $A \neq \emptyset$, go to 5.1.

6. *Performing Lucas - Lehmer tests*

6.1 Choose $q \in \mathcal{F}$, let $w = \mathrm{ord}_q(n)$ and $(\mathbf{R}, \sigma, \zeta)$ be a working $w-$th extension of degree w. Set $k = 0$.

6.2 Choose $\alpha \in \mathbf{R}$, set $k = k + 1$ and:

6.2.1 Check $\alpha^n = \sigma(\alpha)$. If this does not hold, declare n composite and stop.

6.2.2 Set $(n^w - 1)/q = \sum_{i=1}^{t-1} c_i n^i$ with $n = aq + b, c_0 = (b^w - 1)/q$ and $c_i = ab^i$, for $i = 1, 2, \ldots w - 1$, cf. (3.43).

6.2.3 Set $\beta = \prod_{i=0}^{w-1} \sigma^i(\alpha^{c_i})$.

6.2.4 Check $(\beta - 1) \in \mathbf{R}^*$. If this holds go to 6.3.

6.2.5 If $k < M$, for a fixed upper bound of trials M, go to 6.2.

6.2.6 Set $s' = s'/q$ (discard q from s': no root could be found within M trials).

6.2.7 If $S = t \cdot \mathrm{lcm}\ (s, s') > n^\mu$, go to 6.3. This step shows that the reserve $tf(n)$ is not only useful for the final trial division, but it helps coping with failed Lucas - Lehmer tests, without needing to restart the test.

6.2.8 Go to 1.

6.3 Set $\mathcal{F} = \mathcal{F} \setminus \{q\}$.

6.4 If $\mathcal{F} \neq \emptyset$, go to 6.1

7. *The final trial division*

7.1 Let $t = \mathrm{ord}_S(n) = \prod_{i=1}^{m} p_i^{k(p_i)}$.

7.2 Compute

$$h(p) = \sum_{k=1}^{k(p)} \sum_{q|S} \delta_q(p^k), \ \forall p \mid t,$$

and use this function for reordering the primes p, so that $h(p_1) \geq h(p_2) \geq \ldots \geq h(p_m)$.

7.3 Group the factors $q \mid S$ into products P_j of approximate size C - see remark (5.4) for the implications of the choice of C -, starting with q such that $p_m \mid d(q)$, etc. Let $P_1, P_2, \ldots, P_l$ be the resulting products.

7.4 Compute the Chinese Remainder Theorem base elements e_j, such that
$e_j \bmod P_i = \delta_{ij}$, for $j = 1, 2, \ldots, l$, with δ the Kronecker symbol. We have $e_j \in (\mathbb{Z}/S \cdot \mathbb{Z})$.

7.5 For $j = 1, 2, \ldots, l$ compute the sub residues $r_j(i) = n^i \bmod P_j$, $i = 1, 2, \ldots d(P_j)$ implicitly, by using the baby step - giant step method and store the values $r_j(i) \cdot e_j \bmod S$ (represented by one or two values). Use the Chinese Remainder Theorem with respect to the factorization of t, for indexing the stored sub residues.

7.6 Compute the remainders $r_i = n^i \bmod S$, in a nested loop as follows:

for $i_1 = 1$ **to** $k(p_1)$ **do**

  for $i_2 = 1$ **to** $k(p_2)$ **do**

    ⋮

    for $i_m = 1$ **to** $k(p_m)$ **do**

      $i = (i_1, i_2, \ldots, i_m) \bmod t$;

      $r_i = n^i \bmod S$

    done

    ⋮

  done

done

7.7 If $r_i < \sqrt{n}$, check if $r_i \mid n$. If this is the case, n is composite!

WOW

Paul C. Leyland,
the first to comment
the implementation results.

Chapter 6

Implementation

A first implementation was made using the PARI V1.39 library ([PARI]). The implementation was functionally stable but died because of high stack requirements which made tests for number of 500 decimal digits and above impossible.

The current implementation was made under the LiDIA ([LiDIA]) arithmetic library. This is an object oriented arithmetic library, which has several integer arithmetic kernels. The gmp2.0 kernel was chosen for its high portably and very good, assembler enhanced performance. The object oriented structure of LiDIA is comfortable for the development of complex mathematical structures as required by the cyclotomy test. It has a certain performance drop as consequence, but we tried to compensate by good arithmetic choices. Another argument in favor of LiDIA was the fact that it carries a very professional module for modular polynomial arithmetic, written by V. Shoup.

The implementation consists of a class library CYCPROVE and a dedicated, UNIX flavored test program PRIMTEST, with different run options. The set is stable and provides satisfactory results. Several programming improvements will be necessary before making it available for public use. We shall mention them along with the description.

6.1 Overview

The implementation has the class **CyclotomicTest** as a frame. This class – which is initialized with the test number n – has a constructor which builds all required tables, working extensions and roots. The only public method is called for performing all the cyclotomy and the final trial division tests. The further main classes of the program are the following:

cycExt is a class containing the description and construction methods for cyclotomic extensions – the *working* extensions can be built using this class. An extension is defined by its *degree* , the *conductor*, the *minimal polynomial* and the *automorphism matrix*. The **CyclotomicTest** carries a vector with all the extensions, one for each working degree.

cycExtElem is the operative class of an extension and it contains elements of cyclotomic extensions. All arithmetic operations are defined within this class.

Root is derived from the class **cycExtElem** and contains, along with the value of an extension element data such as the *root order* and information about the saturation state of the root. For each degree – and corresponding extension – a list of all the roots required by amalgam tests is stored in the **CyclotomicTest**.

factorList is the class which chooses the optimal parameters s, t for a cyclotomy test, using one of the 3 weights defined in the previous chapter. It builds up a large amount of useful information concerning the saturation degrees of single primes, the used extension degrees for character orders, the list of the prime factors $q|s$, etc. All these tables are data of **CyclotomicTest**.

Amalgam is a small list of data referring to the characters that are joined into an amalgam: the *conductors*, *orders* and *degrees*. The private method *buildAmalgams* of **CyclotomicTest** makes an optimal repartition of characters into amalgams, starting with the highest degree extension and sliding down an extension inclusion tree. The *amalgams* are also listed according to their degree in the class **CyclotomicTest**.

The **CYCPROVE** library runs on the platforms on which the LiDIA library may be built using a GNU g++ compiler. It has been tested on DEC Alpha systems. It allows interactive proving of primality/compositeness for integer candidate numbers, which may be input from console or from files. The proof and prime certificate building follows the basic stages described in the preceding chapter. After a test number N is given, it undergoes a trial division by the first 1000 primes. The implementation restricts the possible prime divisors of the extension degree t to the set of "small primes" $SP = \{2, 3, 5, 7, 11, 13, 17, 19\}$, which allows testing numbers of up to 10000 decimal digits. The degrees of N modulo the primes p in SP are computed and the inclusion tree of working extensions for the given degrees is set. Subsequently, an optimal extension degree t is estimated, using precomputed tables (see next section) and the weights w_i described in §5.1. Next, extension are built and amalgams living in these extensions are optimally combined. The amalgam building is restricted in this constructor phase to symbolic lists of conductors and orders. The values of the Jacobi-Sum products defined by an amalgam are computed later, during the proving process. During the amalgam building "request lists" of roots of unity are established. This way only the roots of unity that will actively be needed in the proof shall also be constructed. Remember that by the amalgam process, elements may be lifted to higher extensions degrees, where they can be combined with several more test bases. The root requests avoid building useless roots for these liftings.

After the amalgam building all information about factors for the Lucas-Lehmer is collected. This way, the Lucas-Lehmer test will follow at the same time with the actual root building process. For the root building we use a binary tree recursive method, which will be described in more detail bellow, and which can carry the gros exponentiation time only once for virtually all the roots in a given extension.

All the above described operation are performed by the constructor of the class **CyclotomicTest** and the construction is completed with the last requested root that is built.

The amalgam checking is performed by the public method *doTest* of **CyclotomicTest**. For each amalgam, Jacobi-Sums over $\mathbb{C}$ are read from files or built on line (see the next section) and than mapped to the according extension. The amalgam check consists in verifying (4.29).

The last step of the *doTest* method consists in the final trial division. By default, this is a $\mu = 1/2$ trial division, but can be configured – via a flag in the constructor of **CyclotomicTest** – to $\mu = 1/3$. The single trial divisions may be grouped into "slices" that can be checked in parallel – on more processors or machines, if the environment allows it.

6.2 Precomputed tables and choice of parameters

The library relays upon two types of precomputed tables: the first are fixed and required for evaluated the optimal parameters of the test: these are the two tables, *factors.doc* and *t_vals.doc*. The table *factors.doc* contains a list of conductors q indexed by the prime powers dividing $q-1$. The table *t_vals.doc* contains a list of values of t together with the binary and decimal logarithms of $e(t) = \prod_{q,(q-1)|t} q$. The indexing of both tables is done by means of *exponent stamps*. An *exponent stamp* is a list of 9 integers $e = (i_j,\ j = 1, 2, \ldots, 9)$, where $i_j \geq 0$ and $i_1 \leq 7$, $i_2 \leq 4$, $i_3 \leq 2$, $i_4 \leq 2$ and $i_j \leq 1$ for $j = 5, \ldots, 9$; it represents the product $E(e) = \prod_j p_j^{i_j}$, where p_j are the primes in SP. For the factor table, the conductor represented by e is $q(e) = E(e) + 1$; for the t-value table, $t = E(e)$. For instance, following line from *factors.doc*

510100000 673

indicates that $q = 673$ is a prime and $q - 1$ is built up from the small primes, namely: $q - 1 = 2^5 \cdot 3 \cdot 7$. The line

522010000 79200 308

in *t_vals.doc* indicates that $t = 79200 = 2^5 \cdot 3^2 \cdot 5^2 \cdot 11$ and $log(e(t)) \approx 308$. In both cases, the first value in the line is an exponent stamp. As the above examples suggest, an exponent stamp may have "holes", i.e. a non zero exponent may be preceded by zeroes. This is meaningful, since we use input dependent weights for choosing an optimal t: for a given target value $e_{min} = e(t) = \log(N)/2$. It may very well happen that the smallest weight is not reached for the smallest t with $e(t) > e_{min}$ and that the exponent stamp of t has holes. In fact this case is in practice rather frequent. It follows from the fact that there is a good chance that, for given N, at least one of the orders of N modulo the small primes at the end of the SP list is small; in that case allowing the corresponding prime in the exponent stamp of t will increase t but reduce the weight.

In order to evaluate an optimal t, one uses the following algorithm:

1. Evaluate d, the decimal logarithm of s required by the test – in accordance with the value μ and the possibly present Lucas-Lehmer factors. Let κ be a surplus factor, allowing to eliminate after choosing the optimal t, the smallest primes q: these do not contribute consistently to the size of s, but may lead to costly amalgam checks. Put thus $d' = (1+\kappa)\cdot d$.

2. Select all the entries in the *t_vals.doc* for which the $d' < \log(e(t)) < 2\cdot d'$. The constant 2 is configurable – the condition eliminates useless searches in the *t_vals.doc* table while seeking the optimal parameters.

3. Choose a weight function W and set $W_{min} = 0$, $t = 0$.

4. For all t in the above selection, evaluate the weight $W(T)$ of t by adding up the weights of all conductors q in the *factors.doc* table, which have an exponent stamp which is lexicographically inferior to e_s, the stamp of t.

4. If $W(T) < W_{min}$, set $W_{min} = W(T)$ and $t = T$.

5. Stop at the end of the selection and return t.

6. After choosing the optimal t, multiply all the q factors in falling order. Stop once the requested size for s is reached and discard the remaining smaller q's.

Remark 6.1 *It is a nice feature to discard selectively the small q's which require Jacobi tests in extensions of highest degree first – this way the advantage of allowing a length surplus in* $e(t)$ *is best paid off. We did not implement this feature. It appears that [BovdH] did, at least in their "large test" of Morain's prime* $(2^{3539}+1)/3$*. As a consequence, they have half as many largest degree amalgam test as we do, for the same optimal* t *in this case.*

The second type of precomputed tables are the facultative, expandable tables. These are Gauss Period and Jacobi-Sums tables. The first are used for building working extensions, the later for evaluating amalgams. Both types of tables have a common root directory each, and for every single conductor q, a subdirectory. In the conductor – subdirectory there is a file for each prime power order $p^k|(q-1)$. These files contain the table data. In the case of the Gauss Periods, the table data are:

1. The minimal polynomial of the Gauss Period η of conductor q and order p^k.

2. The automorphism matrix of $\eta \rightarrow \sigma(\eta)$, in the complex numbers.

3. The generator g of $(\mathbb{Z}/q \cdot \mathbb{Z})^*$ used for computing η. This generator determines the power of σ that shall be taken when reducing modulo n.

Using the Gauss Period data, the working cyclotomic extensions are easily constructed: given an extension degree d, a conductor q such that $d|\mathrm{ord}_q(n)$ is sought. This condition assures that $\eta \bmod n$ will generate an extension of degree d modulo n. The table data provides all the extension description required. For Jacobi-Sums, the table data are:

1. The single Jacobi-Sums $j(\chi, \chi^i)$ for $i = 1, 2, \ldots, p^k - 2$ together with the value $\chi(-1)$ for a primitive character χ of order p^k and conductor q.

Both types of table data can also be computed at run time. The decision of which way to go is configurable. Also, if the program seeks entries that are not found in the existing tables, the values computed at run time can also be written to tables for future runs: this way, the program can *learn*.

6.3 Building working extensions and amalgams

The stage of building extensions and amalgams starts by determining a descending list of all the extension degrees required for the single characters of the running test. The degree list is traversed in descending order, in the following steps:

1. Let D be the current highest degree in the degree list. Construct a list of all root orders living in an extension of degree D, and which have not yet been distributed in any amalgam. These will be called the parent orders. If the parent order list is empty, skip to the next D.

2. Determine a list of all orders which live in extensions of degrees dividing D: this will be called the child order list.

3. For each parent order p^k make a list of the characters $(nodes: \ (q, p^k))$, which have not been yet used in any amalgam and do the same for child orders.

4. If the list of parent order characters is empty, skip to the next degree D. Otherwise construct an extension of degree D, using the Gauss Sum tables. Furthermore, if D has non trivial common divisors with the degrees of previously computed extensions, verify the premises of (3.64) in order to prove that all extensions can be embedded into a common one.

5. Starting with the first parent order, build amalgams by combining

   (i) the next unattributed node for this parent order.

(ii) the next unattributed node for each further parent order.

(iii) child orders that are not yet present in the amalgam (remember, in an amalgam all orders are pairwise coprime).

6. For each used order p^k, store a "request" that a root of order p^k be built in the extension of degree D. The requests will be treated in the root building stage.

7. Close an amalgam when no more parent or child orders can be added, and store it to the amalgam list of the class. Continue the process until no more parent orders are left and shift the list of extension degrees. If this list is not empty, return to 1.

Example 6.2 *Suppose* $t = 2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13^2 \cdot 17 \cdot 19$ *and* N *be such that:*

$$\begin{aligned}\mathrm{ord}_{2^4}(N) = 2;\ \mathrm{ord}_3(N) = 2;\ \mathrm{ord}_5(N) = 4;\\ \mathrm{ord}_7(N) = 3;\ \mathrm{ord}_{11}(N) = 2;\ \mathrm{ord}_{13^2}(N) = 6;\\ \mathrm{ord}_{17}(N) = 4;\ \mathrm{ord}_{19}(N) = 6.\end{aligned}$$

The inclusion tree for this (N, t) *configuration is given by following diagram: The lateral line joining the leaf* $(2^4, 2)$ *to the terminal leaf* $(13, 6)$ *is not an "active" inclusion. It is used for proving the existence of a common cyclotomic extension in which all working extensions are embedded, according to theorem (3.64). The proof is given by providing a* 2^4-th *root in the* $6-$th *degree extension of order* 13.

We shall give now more detail about the building of extensions. We distinguish three types of extensions:

(F.) Full cyclotomic extensions. The degree is $p - 1$ for some odd prime p or 2 and $n = 3 \mod 4$. The minimal polynomial is in this case the rational cyclotomic polynomial $\Phi_p(x)$ for odd p or $x^2 + 1$ for $p = 2$; the automorphism matrix is a rotation matrix.

(S.) Supersaturated extensions of full cyclotomic extensions. The degree is $p^l \cdot (p-1)$ and $\Phi_p(x)$ is irreducible modulo n, for odd p, or $d = 2^k, k > 1$ and $n^2 = 9 \mod 16$. The minimal polynomial is $\Phi_p(x^{p^l})$ for odd p or $x^{2^k} + 1$ for $p = 2$. The automorphism matrix is some block rotation matrix.

(T.) Trace extension – this is the common case. None of the above cases was fulfilled when a traced extension is built (the first two cases are preferable, having simple arithmetic). If κ is an *admissible conductor* for n and degree d, i.e. if it is a prime such that $d | \mathrm{ord}_\kappa(n)$, fetch the data of the Gauss Periods of conductor κ and order d and build the new extension with them.

Note that finding an admissible conductor is possible, by the extended Riemann hypothesis in polynomial time.

6.4 Building roots

Before building roots, Lucas-Lehmer factors are read form files, if existing. These factors are written into "root requests", much the same way as the requests during the amalgam building stage. Furthermore, Lucas-Lehmer might require extensions that were not built for the amalgam test (we want to use all the additional Lucas-Lehmer factors...). The additional extensions are built in the same way described above, while verifying (3.64) for each new extension.

The roots are built by trial and error, following the Lucas-Lehmer method. For speeding the method up, we try to build all requested roots for one given degree in one step. Given the degree d with its extension $(\mathbf{R}, \sigma, \eta)$ and a list of requested root orders $r_i, i = 1, 2, \ldots k$, this goes like this:

1. Choose a base $\alpha \in \mathbf{R}$ and let $\mathcal{R} = \{r_i : i = 1, 2, \ldots k\}$. If $\mathcal{R}$ is a list of orders, let $\pi(\mathcal{R}) = \prod_i \, r_i$ and put $e = n^d - 1$.

2. Compute α^n and verify $\alpha^n = \sigma\alpha$. Then use the formula (3.45) for performing the large exponentiation $\beta = \alpha^{e/R}$.

3. Start a recursive procedure with input $\beta, \mathcal{R}$, doing the following:

   A. If $\sharp\mathcal{R} > 1$, split the list in two non empty sublists $\mathcal{R}', \mathcal{R}''$. Make two recursive calls, with inputs $\beta^{\pi(\mathcal{R}'')}, \mathcal{R}'$ and $\beta^{\pi(\mathcal{R}')}, \mathcal{R}''$, respectively.

   B. If $\sharp\mathcal{R} = 1$, β should be a r_1–th root of unity. Check $\beta^{r_1} = 1$. If this does not hold, declare n composite and stop. If $\beta = 1$, the initial base α failed to provide a primitive root. Return the same list $\mathcal{R}$. If $\beta \neq 1$, it is a required primitive root. Discard the request – it was fulfilled – and, if the root was requested for an amalgam, save it to the root list of the test; do nothing for Lucas-Lehmer roots (only the existence of a root is requested in those cases). Return the empty list.

4. After the two recursive calls, concatenate the returned order lists: $\mathcal{R} = \mathcal{R}' || \mathcal{R}''$. At the bottom of the recursion, this will yield the list of all the orders, for which a root has *failed* to be found. For these orders, the procedure will be continued with a new base α, until either all roots were found or the *composite* halt was issued. The loop should also have an upper bound for the number of trials, in the order of $\log(n) * \log\log(n)$: the ERH lets one expect to find primitive roots after thus many trials ([BaS]).

The above described recursive method takes advantage of the fast formula involving automorphisms (3.45) and reduces the number of trials for finding the roots – when Lucas-Lehmer factors are known, more than a dozen of roots may be found with only one important exponentiation. Thus the precomputing and Lucas-Lehmer test receive an important improvement. Unfortunately, these are not the most time critical stages.

6.5 Performing the pseudoprime tests

When performing pseudoprime tests, a list of amalgams and of individual characters has already been prepared and the complex values of the multiple Jacobi-Sums α, β of lemma (4.13) and α_i, β_i of theorem (4.25) are precomputed in the Jacobi-Sum tables. In order to perform the tests (4.29) one still needs to map those elements into the working extension, by mapping the complex roots of unity to the roots of unity of the maximal extension of the amalgam. Once the mapping performed, the tests follow the exact description of the cited propositions.

6.6 Final trial division

If the square root version of the test ($\mu = 1/2$) is chosen, the final test has to check that

$$(r_i, N) = 1, \quad \forall r_i = N^i \bmod s$$

and halt if this does not hold. The test is performed only for those remainders $r_i < \sqrt{N}$. If t is chosen such that $e(t) > \sqrt{N} \cdot \log(N)$, their number will be negligible (see §5.5). However, all remainders r_i need to be individually computed. For accelerating the computation, we list the remainders $n_i = n \cdot B^i \bmod s : i = 0, 1, \ldots \log_B(s)$, where B is the base for the word representation of the machine – on our DEC - ALPHA, $B = 2^{64}$. Thus the modular multiplication

$$r_{k+1} = r_k \cdot n \bmod s = \sum_j r_{k,j} \cdot B^j \cdot n = \sum_j r_{k,j} \cdot n_j,$$

is reduced to a linear combination over $(\mathbb{Z}/s \cdot \mathbb{Z})^*$ with coefficients $< B$ and the long modular reduction is spared. This cuts the operation count approximately in half.

The set $\{i = 1, 2, \ldots, t\}$ of test powers can be configured into *slices* of given length, with starting points that can be computed in direct access an distributes on more processors or machines.

The cubic root version of the final test has also the slices option. The implementation detail is rather intricate and [BovdH] have covered all the useful implementation tricks: we thus refer to their thesis for implementational detail.

6.7 Arithmetic

The arithmetic of the LiDIA package uses Fast Fourier Transforms for the modular polynomial operations and the GNU gmp2.0 package for long integer arithmetic. Several small improvements in the arithmetic both of GNU and of LiDIA are prone to yield some improvement factor of about 2. These are:

1. Using a dedicated routine for *squaring* in both GMP and LiDIA – squaring can be done at half the cost of long multiplications.

2. Using left shift of the exponent in exponentiation ([Kn]), which is more advantageous when exponentiating small bases.

3. Using slide bits Windows for exponentiation in both programs.

4. Implementing the Toom-Cook algorithm in LiDIA.

These arithmetical improvements together with the selective discarding of small factors q of s – as described in the remark of the section on tables – may lead to a comfortable factor 2-3 of improvement.

As we shall see in the last section describing the implementation results, the current arithmetic is quite satisfactory and allows computing larger examples.

6.8 Times, Certificates and Comments

Our implementation was run on the DEC ALPHA 333 idefix and on the 3 Alpha's 500, Darwin1, 2 and 3. Due also to the power of the machines, we were able to run much faster experiments going beyond the results described in [BovdH]. Since, as van der Hulst also mentioned, the most stable machine independent performance coefficient of a test is the ratio between the full run time for a test for a pseudoprime n and the run time for one modular exponentiation (or, equivalently, a Rabin-Miller test), we shall consider this ratio separately in comparison with the same coefficient for older tests.

We shall end by discussing several large examples – first, of course, the famous Morain prime $(2^{3539} + 1)/3$.

The following tables give run times statistics for sizes of primes between 20 and 800 decimal digits. For each length, we display the average, maximal and minimal times (in sec.), as well as the average time for one modular exponentiation $\bmod n$ and for an exponentiation in a maximal degree extension. The degree used for this average is written in the last column of the table, while the column before last displays the machine independent **ratio**:

$$\frac{\text{Average test time}}{\text{Average modular exponentiation time}}$$

nDec. Digits	**Av. Time** (sec)	**Max Time** (sec)	**Min Time** (sec)	**Mod.Exp** (sec)	**Max Ext** Expo: (sec)	**Ratio**	**Max** Deg
20	0.30	1.05	0.15	0.00	0.04	n.a.	3
50	0.61	0.91	0.36	0.01	0.15	60?	2
100	3.97	7.18	1.49	0.16	1.36	25	5
120	5.63	7.38	2.37	0.20	1.99	28	6
140	9.31	16.81	4.61	0.25	2.79	37	5
160	12.63	24.98	7.08	0.32	3.56	40	3
180	17.72	31.38	4.67	0.38	4.67	47	6
200	23.83	41.40	13.70	0.42	4.67	57	6
250	44.86	92.72	17.35	0.48	7.23	97	7
300	77.59	117.97	45.76	0.54	12.13	144	4
350	171.38	307.77	79.21	1.02	13.35	168	9
400	287.27	454.36	142.88	1.33	17.92	216	4
450	488.98	759.92	231.20	2.37	16.25	206	6
500	730.01	965.97	573.87	3.74	20.87	195	12
600	1035.88	1429.29	569.61	4.66	16.40	222	6
700	2697.36	3689.59	1566,25	6.66	24.96	405	6
800	3900.47	5105.46	2872.56	9.82	20.63	398	8
1000	10680.22	16293.12	5067.33	14.34	28.17	745	6

Table 6.1: *Performance* **CYCLOPROVE**

For correctly interpreting the lower half of the displayed table, one should be aware that just 10 or less tests were run for the larger prime lengths. This is definitely insufficient for yielding statistical evidence and one can understand the fluctuances in the growth of the ratio. Two weeks after computing these statistics, and after having implemented an on-run Lucas factorization which improves the behavior of the program, I was asked to provide proving help. Dr. Roonguthai, a searcher of prime tuples, provided me a list of 24 pseudo-primes of 700 digits - 8 triplets, actually - which needed to be proved as prime. The proof lasted less than 10 hours, at an average of 1490 sec. per prime. The minimum was of 633 sec, the maximum roughly one hour; these results have a better statistical value for the 700 digit entry of the above table. Unfortunately time is insufficient for completing the table with similar intensive statistics.

The true – implementation specific – behavior of the ratio, asymptotically, but first of all in the interesting range of, say, up to 10000 decimal digits is hard to predict.

The tabulated figures might suggest a linear behavior. The complexity reflected by the ratio, reflects the growth in the number of amalgams to be tested and in their repartition with respect to extension degrees. The length of the final test has also a clear increasing weight. It is hard to make an asymptotic prediction for the cumulated growth of these heterogeneous factors. Linear behavior – of course, only for the named range – would be good news and would imply a practical, approximative $O(n^{7/2})$ behavior of the algorithm in this range – the 1/2 stems form the use of Karatsuba multiplication, used by the gmp2.0 library. We should also mention that the statistical tests were run online, without preparing of Lucas factors and are thus less efficient then dedicated large

Digs.	Test A Time	Test A Ratio	Test B Time	Test B Ratio	Test C Time	Test C Ratio	Test D Time	Test D Ratio
100	7.05	486	108.65	201	4108	2598	3.97	25
120	13.75	678	190.83	211	6568	2795	5.63	28
140	23.41	839	418.03	310	10917	3308	9.31	37
160	35.67	958	671.45	348	17762	4155	12.63	40
180	47.86	1029	1017.68	377	27404	5028	17.72	47
200	68.36	1139	1458.87	388	36906	5329	23.83	57

Table 6.2: *Performance in* **Comparison**

examples, in which we precomputed the Lucas factors. A size dependent, embedded factorization of $\Phi_k(n)$ for small values of k is implemented; the search for Lucas factors can also be done off – line. One sees however at the minimal value for 1000 digit numbers, that a time below 1 1/2 hours is possible even without Lucas factors!

We shall now compare the average running time and the machine independent ratio to the values of formal tests, as plotted in [BovdH], p. 263. Note that this source gives the ratio of the division by the time for 4 Rabin-Miller tests (modular exponentiations), whereas we divide by one single modular exponentiation time. We therefor multiplied all the figures in [BovdH] by 4 for the subsequent table.

Test A is the [CoLe] implementation of the Jacobi-Sum test, on a Cray–1, Test B, the [BovdH] implementation on Sun4, Test C Morain's elliptic curve test, as cited in [BovdH] (several improvements of that test might have taken place meanwhile, but we have no data available at present). Finally, Test D is the present implementation. The time will mean the average time, in seconds.

There are many ways to read this data:

1. Our implementation has a rough improvement factor of around 8 over the best ratio of Test B – and thus a better improvement than the one from the Old Jacobi-Sum test ([CoLe]) to the first Lucas-Jacobi implementation of [BovdH].

2. Elliptic curves have not and probably will not for a while reach the point of standing up to the expectation created by the asymptotic polynomial runtime. It is hard to predict what will happen first: progress in hardware power will lead to the possibility of performing computations beyond the break even point where the over polynomial final trial division of cyclotomy becomes overweighted ? Or further research will lead to polynomial time cyclotomy or combined cyclotomy – elliptic curves test ?

3. The Cray – 1 is not such an old machine *after all* .... In fact, comparing the run times for the single modular exponentiations, it appears that the Cray *LIP* modular arithmetic performed 8 better than the LiDIA exponentiations on Alpha 500.

4. The last remark leads to a qualification even of the absolute usefulness of the machine independent ratio: While the measured core exponentiation is mostly programmed very close to the machine – assembler, or in the case of Morain even dedicated long integer processors, the higher layers of the implementation might not be. Accordingly, the ratio may appear larger. In our case, the core arithmetic is gmp2.0 with assembler inlines and is wrapped in C++ by LiDIA. We thus measured a pretty high level time for the modular exponentiation, which is consistent with the fact that the whole application is in C++. A small bias in favor of our implementation may result, which can only consequently be eliminated by performing this arithmetic improvements mentioned in the previous section and measuring times in C layer.

5. An important contribution to our considerable improvement stems from the use of FFT for arithmetic in extensions: the size of the problem is perfectly adapted for the use of fast convolutions and comparing times of exponentiations in extensions of different degrees – figures that do not appear in the above tables – showed that the dependence of the degree is close to linear. On the other hand, the figures published in [BovdH] for the *titanic* prime, show that the time dependence on the degree is quadratic in their implementation.

We now compare the run times used for the proof of $(2^{3539}+1)/3$ by the two cyclotomy implementations: For the CYCLOPROVE implementation, the total running time was of 3873.24 seconds – CA. one hour. We plot bellow the times for the preprocessing and root building stage, the amalgam checking for the different degrees and the final stage.

Preprocessing and root building:	$330.20s$.
39 amalgams in extension of degree 10:	$39 \cdot 58.71 = 2289.81s$.
43 amalgams in extension of degree 4:	$43 \cdot 12.29 = 528.57s$.
39 amalgams in extension of degree 3:	$39 \cdot 12.00 = 468.22s$.
Final $\mu = 1/2$ trial division:	$256.44s$.
Grand Total:	$3873.24s. \approx$ 1 hour.

The juxtaposition of the times for 3-d and $4-$th degree extension times indicate clearly a power of 2 based FFT! This is undoubtedly better than naive field multiplication, but unsatisfactory for several small degree extensions. The times of the [BovdH] implementation on a DEC-3100 were:

Preprocessing and root building:	$92774s$.
20 amalgams in extension of degree 10:	$20 \cdot 34800 = 696000s$.
41 amalgams in extension of degree 4:	$41 \cdot 5840 = 239440s$.
37 amalgams in extension of degree 3:	$37 \cdot 3480 = 128760s$.
Final $\mu = 1/3$ trial division:	$1178710s$.
Grand Total:	$2335684s. \approx$ 27 days

Note that while the numbers of degree 3 and 4 amalgams were roughly the same for both runs, the number of degree 10 amalgams was twice as large in our case, which is probably explained by a better strategy for discarding small q-factors leading to large degree amalgam checks, used by Bosma and van der Hulst. Both tests used the same value of t. This was possible, although we only took $\mu = 1/2$. The reason is that, on a strong machine, we collected about 50 a parallel night run. It appears that the dedicated preprocessing plays an important role for the success of larger tests.

A further *small titan*, the *repunit* prime $\frac{10^{1031}-1}{9}$ – I ow this number to Prof. N. Waldvogel's indication – was proved in just about exactly one hour:

Preprocessing and root building:	$339.80s.$
38 amalgams in extension of degree 6:	$38 \cdot 35.75 = 1358.61s.$
40 amalgams in extension of degree 5:	$40 \cdot 23.14 = 925.60s.$
20 amalgams in extension of degree 4:	$20 \cdot 12.39 = 260.21s.$
21 amalgams in extension of degree 3:	$21 \cdot 12.39 = 260.21s.$
19 amalgams in extension of degree 2:	$19 \cdot 12.39 = 260.21s.$
Final $\mu = 1/2$ trial division:	$502.05s.$
Grand Total:	$3704.66s. \approx 1$ hour

6.9 Breaking the frontier

At the time before printing this thesis we are preparing for some larger tests that can be run before making the required arithmetic improvements. The first goal we wish to achieve, is proving the primality of the last three pseudoprime factors of Mersenne numbers $N = 2^p - 1$, for $p < 10000$, a prime. This factors occur for $p = 6883, 7331$ and 7673, respectively and are slightly larger than 2000 decimal digits. They are provided by Paul Leyland's friendly information and can be found on the net at **ftp://ftp.ox.ac.uk/pub/math**.

Preparing for the large tests, we attacked a small sequence of primes of increasing size – and without special properties. They were tested without prefactorization of Lucas factors, giving thus an image of the complexity evolution close to worst case. At the same time we computed Lucas factors for the 3 Mersenne pseudoprime factors. The results for the 10 powers are as follows: The 1300 digit number $10^{1300} + 11523$.

Preprocessing and root building:	$262.15s.$
77 amalgams in extension of degree 10:	$77 \cdot 92.32 = 7018.81s.$
49 amalgams in extension of degree 9:	$49 \cdot 95.18 = 4663.65s.$
85 amalgams in extension of degree 6:	$85 \cdot 37.94 = 3225.21s.$
92 amalgams in extension of degree 4:	$92 \cdot 21.66 = 1992.70s.$
Final $\mu = 1/2$ trial division:	$6135.40s.$
Grand Total:	$23297.92s. \approx 6\ \ 1/2$ hours.

The 1500 digit number $10^{1500} + 2329$. (The detail for the amalgam proving time was lost by a failure of manipulation).

Preprocessing and root building:	$895.93 s.$
Total amalgam prover time:	16688.58 s.
Final $\mu = 1/2$ trial division:	$15658.94 s.$
Grand Total:	$33241.58 s. \approx 9\ \ 1/4$ hours.

The 1700 digit number $10^{1700} + 469$.

Preprocessing and root building:	$810.16 s.$
102 amalgams in extension of degree 10:	$77 \cdot 196.57 = 20050.41 s.$
40 amalgams in extension of degree 8:	$40 \cdot 156.30 = 6251.99 s.$
106 amalgams in extension of degree 6:	$106 \cdot 137.42 = 14567.35 s.$
34 amalgams in extension of degree 4:	$34 \cdot 21.66 = 1939.82 s.$
Final $\mu = 1/2$ trial division:	$35421.02 s.$
Grand Total:	$79040.75 s. \approx 22$ hours.

The 2000 digit number $10^{2000} + 4561$. This number was proved on the slower Alpha 333 idefix, and used accordingly a higher amount of CPU.

Preprocessing and root building:	$2322.07 s.$
116 amalgams in extension of degree 12:	$116 \cdot 591.59 = 67464.83 s.$
109 amalgams in extension of degree 10:	$109 \cdot 435.80 = 47502.73 s.$
103 amalgams in extension of degree 9:	$103 \cdot 580.00 = 59739.72 s.$
Final $\mu = 1/2$ trial division:	$21769.35 s.$
Grand Total:	$198798.70 s. \approx 55\ \ 1/4$ hours.

The Mersenne factors have been computed in by Prof. Ernst Mayer, Case Western Reserve University, Cleveland. He kindly provided following information about the generation of the Mersenne factor table [LeMa]: The large probable-prime Mersenne cofactors were found by him using a fast discrete weighted transform (DWT)-based [CrFa] Euler-base-3 test of each composite Mersenne number with known factors in the Great Internet Mersenne Prime Search ([GIMPS], [MF]) database. The base-3 test was followed by a Suyama-like post-test, similar to that used for cofactors of Fermat numbers [Ri], of the base-3 residue. For a cofactor F_n of a Mersenne number $M(p)$ with smaller factors yielding the product $F = F_1 \cdot \ldots \cdot F_{n-1}$, the post-test is equivalent to performing simultaneous base- 3^F Fermat and base-3^{2F} Euler pseudoprime tests on F_n. This was done for all $M(p)$ having known factors up to $p = 60,000$, and turned up the following probable-prime cofactors, each of which was further subjected to (and passed) a series of strong pseudoprime tests (we list only the ones having $p > 2000$, i.e. those not in the Cunningham tables at the time of discovery):

M2837	= 22697 ·	138871151 ·	336396730297 ·	P830
M3041	= 24329 ·	5565031 ·		P905
M3359	= 6719 ·			P1007
M4127	= 74287 ·	2080009 ·		P1232
M4243	= 101833 ·			P1273
M5087	= 40697 ·	1678711 ·	114097014833 ·	P1510
M5227	= 1129033 ·	47126633 ·	227482218017 ·	P1549
M5689	= 919724609777 ·			P1701
M6883	= 1885943 ·	2043031664890199 ·		P2051
M7331	= 458072843161 ·			P2196
M7673	= 184153 ·	13918823 ·		P2298
M14561	= 8074991336582835391 ·			PRP4365
M17029	= 418879343 ·			PRP5118
M28759	= 226160777 ·			PRP8649
M28771	= 104726441 ·			PRP8653
M32531	= 65063 ·	25225122959 ·		PRP9778

In the above table, P stands for proven prime, while PRP means probable prime. The $P2051$ was identified after the initial sweep, subsequent to the discovery of the 16-digit factor by E. Prestemon [MeD] using ECM. Note that the large cofactor of $M3359$ was proved prime in 1994 by Keller and Morain using ECPP. The cofactors of the remaining $M(p)$ with p up to 5689 were proven prime earlier this year by Mayer, also using ECPP; the cofactors of $M5087$, $M5227$ and $M5689$ were all hard-prime records at the time of their proof, superseding a 1505-digit number proved prime by Morain in 1992. The next number to be proved was $MC7331$ (the 2196-digit cofactor of $M7331$), done by Mayer and Morain [MM] using a specially modified version of the ECPP software; this proof required 5 weeks of dedicated CPU time on a 400 Mhz DEC Alpha 21164 workstation. Subsequent to this, $MC6883$ was proved in just 26 hours by us using this implementation ... which was less than one fiftieth of the time required to prove the same number prime using ECPP ([May]). Here are the times:

Preprocessing and root building:	$946.89s.$
102 amalgams in extension of degree 10:	$102 \cdot 319.83 = 32622.42s.$
102 amalgams in extension of degree 8:	$102 \cdot 319.64 = 32602.89s.$
103 amalgams in extension of degree 6:	$103 \cdot 135.40 = 59739.72s.$
3 amalgams in extension of degree 4:	$3 \cdot 101.72 = 305.16s.$
Final $\mu = 1/2$ trial division:	$14604.29s.$
Grand Total:	$95027.54s. \approx 26\ \ 1/2$ hours.

The proof of MC7673 – a 2298 decimal digit number – was finally completed on Monday, November 3-d, after a two day's run. It is the first record of a general primality proof that was achieved with this implementation.

Preprocessing and root building:	$2241.05s.$
124 amalgams in extension of degree 10:	$124 \cdot 442.45 = 54864.12s.$
118 amalgams in extension of degree 9:	$118 \cdot 600.56 = 70865.88s.$
128 amalgams in extension of degree 6:	$128 \cdot 203.32 = 26024.62s.$
Final $\mu = 1/2$ trial division:	$19055.85s.$
Grand Total:	$173051.52s. \approx 48$ hours.

The average for degree 9 amalgams, which is by 33% higher than the one for degree 10 amalgams, appears confusing. The explanation is that this test reached far beyond the size of our precomputed Jacobi Sum tables, so that several Jacobi Sums with very large conductors $\sim 10^8$ had to be computed during the run. The number of such Jacobi Sums was larger for degree 9 amalgams, influencing the average as observed.

Several days later, I finished implementing the cubic root ($\mu = 1/3$) variant of Lenstra [Le4] and performed the test for the same number again with $\mu = 1/3$. The proof was completed in 29 hours.

A certificate is something very large of a questionable æsthetic value. Given the fact, that it is a tangible proof for a test having been run, but of a size that is not worth its price in paper, we chose the compromise of creating an internet link [CERTS] with our currently largest certificates – hoping that the link may be maintained in time or the information about its movements be made available to the interested.

6.10 $2^{10000} + 177$ is prime!

Short before printing, the test for the first 10000 digit pseudoprime was started on two machines: one performed the cubic root final test, the second carried out the main stage of the algorithm. The final test was completed in roughly 52 hours. The main stage had to be restarted after a crash – the current version of the implemention writes out the actual amalgam test being perfromed and allows restarting the test with a given amalgam number. The total time for the main stage was of 86 hours. Altogether, the proof of this 3010 decimal digit prime required 138 hours, or 5 3/4 days. This is thus the current record for general primality proving and it outranges by 36% in length the previous one established two weeks ago with ECPP, when proving the primality of $MC7331$.

The first step of a trip around the world
Begins in one's own garden.

Chinese saying

Chapter 7

Asymptotics and Complexity

In this chapter we evaluate the asymptotic expected run - time of the cyclotomy test. The main result is that neither the combination of Jacobi-Sum and Lucas - Lehmer tests, nor the use of lattice reduction for computing Jacobi-Sums or their precomputation do modify the asymptotic behavior of the test initially discovered in [ARP]. We shall use, for ease of notation, the symbol $\mathcal{P}$ for the set of all rational primes. The following theorem is well-known in the context of primality tests [ARP], [CoLe](4.3).

Theorem 7.1 (Prachar, Odlyzko, Pomerance) *There exists an effectively computable positive constant c such that* $\forall\ n > e^e,\ \ \exists t > 0$ *satisfying*

$$t \ < \ (\log n)^{c \cdot \log\log\log n} \quad \textit{and} \quad \Big(\prod_{\{q \in \mathcal{P}, (q-1) | t\}} q \Big)^2 > n. \tag{7.2}$$

Note that with n and t as in the theorem and $s = (\prod_{\{q\in\mathcal{P},(q-1)|t\}} q)$, one has $n^t = 1 \bmod s$, which shows that the number t in the algorithm in §4.3.3 can be chosen such that $t < (\log n)^{c \cdot \log_3 n}$ where $\log_3 n := \log\log\log n$. By using a well known estimate for the number of divisors $d(x)$ of a positive integer x, it is mentioned in [CoLe], §4 that

$$t \ > \ n^{(1-\epsilon)\cdot log_3(n)} \tag{7.3}$$

for the second inequality in (7.2) to hold. We shall make an estimate taking into account the possibilities of the cyclotomy algorithm. That is, we let

$$s(t, M, n) \ = \ \prod_{q \in Q} q^v(q),$$

where $Q = \{q \in \mathcal{P} : q < M, q^{v(q)} \parallel (n^t - 1), v(q) \geq 1\}$ and estimate the average of $\log s(t, M, n)$ over a large interval of values of n . Let $1 < A < B$ such that $A >> t$ and $(B - A) >> t$ and define the average of $\log s(t, M, n)$ by:

$$\mu(t) = 1/(B - A) \cdot \sum_{A<n\leq B} \log(s(t, M, n)) \tag{7.4}$$

Then:

$$\mu(t) \cdot (B - A) \ = \ \sum_{A<n\leq B} \ \sum_{q\in Q(t,M,n)} v(q) \cdot \log q \tag{7.5}$$

If $q \in Q$, then $ord_q(n) \mid t$. For $d \mid (q-1)$ there are exactly $\varphi(d)$ remainder classes $\mod q$ with order d. Consequently, in the interval $[A, B]$ there are $((B-A)/q) \cdot (\varphi(d) + O(1))$ values of n such that $ord_q(n) = d$; with a similar reasoning, we find that

$$((B-A)/q^k) \cdot (\varphi(d) + O(1))$$

classes are such that $ord_{q^k}(n) = d$. Summing up, we have:

$$\begin{aligned} \sum_{A<n\leq B} \sum_{q\mid(n^t-1)} v(q) \cdot \log q \quad &\leq \\ (B-A) \sum_{q\mid(n^t-1), d\mid(q-1)} &(\varphi(d) + O(1)) \cdot (\log q)/q \cdot [q/(q-1)]. \end{aligned} \tag{7.6}$$

and

$$\begin{aligned} \mu(t) \cdot (B-A) \quad &\leq \\ (B-A) \sum_{d\mid t} (\varphi(d) + O(1)) &\sum_{q=1 \bmod d,\ q<M} \left[\frac{\log q}{q} \cdot (q/(q-1) + v_q(t))\right] \end{aligned} \tag{7.7}$$

The factor $(q/(q-1) + v_q(t))$ is bounded by a positive constant c_1 and we can replace the inner sum by its asymptotic value $\log(M)/\varphi(d) + R_1(t)$ [Ch] , where the correction term $R_1(t)$ cannot be expected to be very tight, since d may have relatively large values with respect to the upper summation bound M; (7.7) can be thus rewritten to:

$$\mu(t) \quad = \quad O(d(t) \cdot \log(M)), \tag{7.8}$$

where the function $d(t)$ is upper bounded by:

$$d(t) \quad < \quad 4^{\log t/\log\log t}, \tag{7.9}$$

The formula (7.9) contains important information as to the size of t needed in the cyclotomy algorithm. First note that (7.2) holds for our estimate, if M is such that

$$M = o(e^{(\log n)^\alpha}) \quad \forall \alpha > 0. \tag{7.10}$$

If

$$M = O(e^{(\log n)^\alpha}), \qquad \text{with } \alpha \in (0,1) \tag{7.11}$$

then (7.2) is still valid with a change in the exponent:

$$t \quad > \quad \log n^{(1-\epsilon)\cdot(1-\alpha)\log_3 n/\log 4} \tag{7.12}$$

On the other hand, using fast factorization algorithms for which the amount of work for finding a factor q is $L[q] = O(e^{\sqrt{\log q \cdot \log_2 q}})$, the size of factors that can be found in time polynomial in t is $q = O(\exp(\log t)^2)$, and thus (7.10) still holds. We conclude that:

(i) The bound (7.2) is valid for the cyclotomy algorithm.

(ii) For factors q, such that (7.11) holds, this bound holds with a different constant in the exponent. However, this size of factors cannot be expected to be found in average by the best factoring algorithms at the moment.

Altogether, while combinations of Lucas-Lehmer and Jacobi-Sum algorithms can bring practical improvements of the latter, they do not change the asymptotics (7.2), which are mainly determined by the bound (7.9).

Remark

The complexity of primality testing in multiplicative groups appears to be optimally given by (7.2) and still possible improvements could depend upon

(i) reducing the trial division stage by solving the combinatorial problem of finding feasible sets, defined in §5.5, and

(ii) finding more efficient methods for factoring numbers of the form $\Phi_k(n)$, with Φ_k the k-th cyclotomic polynomial.

Je suis jeune, il est vrai,
Mais aux âmes bien nées,
La valeur n'attend pas
Le nombre des années

Corneille, Le Cide

Chapter 8

CIDE: An improved cyclotomy test

We saw that the cyclotomy test has an uncommon asymptotic behavior: while the main, work intensive stage, is polynomial (in the length of the input), two very simple stages are *super-polynomial*. The asymptotic exponent being $O\Big((\log n)^{\log\log\log(n)}\Big)$, it can be easily assumed to be a fairly small constant in practice. The initial over-polynomial stage could be reduced using Algorithm Ib.

The final stage of the cyclotomy test is equally blunt, yet not polynomial. It essentially reduces to computing a list of power remainders, and verifying that they lay above some given threshold. The only improvement known so far ([Le4]) allows reducing the size of the modulus, with the consequence that the residue list is reduced by some upper bounded constant factor. The reduction happens at the cost of more involved operations, that need to be performed for each single element in the residue list. It is not yet clear from our implementations, where the threshold lays, above which the reduction of t (the size of the residue list) pays off the additional operations per residue. It appears to lay around $t = 10^7$.

We found a new application of elliptic curves, which allows a further reduction of the final stage, such that $s = O(\sqrt[4]{n})$. This happens at the cost doubling the main stage.

Whereas the galois period computation is straight forward and hardly prone to substantial improvements, the use of *dual elliptic pseudoprimes* – the term will be introduced bellow in the section on the reduction of the final stage – is just the first known attempt to combine elliptic curve and cyclotomy primality testing. We hope that its success to improving the last super-polynomial stage of the cyclotomy test may motivate some intensive and deeper study both of elliptic curves tests and of further combinations of cyclotomy and elliptic curves.

We shall make intensive use of elliptic curve primality tests. We assume the reader has the basic knowledge about elliptic curves with complex multiplication and the Goldwasser-Kilian-Atkin-Morain primality test – see [Cox] for a treatment of the first and [GoKi], [AtMo], [Mo] for the second.

Elliptic curve primality testing is polynomial – yet slow even with the use of complex multiplication ([AtMo], [Mo90], [BovdH]). This is due do the fact that a long recursive primality proof needs to be performed: For proving primality of a test number n, one constructs a curve with m points, such that m is divided by a large probable prime $r \ldots$ and proceeds the proof for r. In the hope to eliminate recursion, we considered the case when m itself is a probable prime, rather then being divisible by a large probable prime. This case was never considered previously, probably since it does by nothing reduce the size of the primes to be proved. It has the interesting property of yielding the possibility of reciprocal tests for n and m: we call this *elliptic duality* . Two pseudoprimes m and n which pass elliptic tests with curves with respectively n and m points – i.e. both numbers figure once as test subjects and once as numbers of points – are called *dual elliptic pseudoprimes*. The terms will be made precise bellow. Dual elliptic pseudoprimes are very improbable apparitions – in fact, we started by trying to prove that they can not exist. It can be proved that they are built up of at least 3 primes and the least factors have again the dual property. This facts can be ideally used by cyclotomy. The first makes a cubic root test possible, without any additional operations in the final test. The more hidden advantage consists in the fact that, if cubic root cyclotomy tests are performed not only for the actual test number n, but also for its dual m.

This is a brief exposure of the basic ideas behind our reduction of the final stage. We shall give next the detailed proofs and algorithms.

8.1 Dual Elliptic Pseudo-primes

We shall deal in this and the following sections with elliptic curves having complex multiplications over the integers of an imaginary quadratic field $\mathbb{K} = \mathbb{Q}[\sqrt{-d}]$, with $d = 4k+3 > 3$, a rational integer. If p is a prime and $E(a,b)$ is an elliptic curve with complex multiplication over $\mathbb{K}$ and good reduction at p, then p splits completely in $\mathbb{K} : p = \pi\overline{\pi}$, for some prime number $\pi \in \mathcal{O}(\mathbb{K})$. In this case, the reduction $E_p(a,b) = E(a,b) \mod p$ has $n = \mathbf{N}(\pi \pm 1) = p \pm Tr(\pi) + 1$ points. We say two primes p and q are *dual elliptic primes* (with respect to the discriminant d), if $p = \pi\overline{\pi}$ and $q = (\pi + \epsilon)\overline{(\pi + \epsilon)}$ with $\epsilon = \pm 1$, or, equivalently, if there are two elliptic curves $E(a,b)$ and $E'(a',b')$, such that $\sharp E_p(a,b) = q$ and $\sharp E'_q(a',b') = p$. We define by analogy a pair of dual elliptic pseudoprimes (DEpsp's):

Definition 8.1 *Let m and n be two Rabin-Miller pseudoprimes and suppose there are two elliptic curves $E_m(a,b)$ and $E_n(a',b')$, such that:*

1. *Both curves have complex multiplication in $\mathcal{O}(\mathbb{K})$, the ring of the integers of $\mathbb{K}$.*
2. *The integers m and n split in $\mathcal{O}(\mathbb{K})$ and*
$$m = \mu\overline{\mu}, \quad \text{and } n = (\mu + \epsilon) \cdot \overline{(\mu + \epsilon)},$$
with $\epsilon = \pm 1$.
3. *There is a point $P \in E_m(a,b)$, such that*
$$P \neq \mathcal{O}, \quad \text{and } [n]P = \mathcal{O},$$
with $\mathcal{O}$ being the point at infinity.

4. *There is a point $Q \in E_n(a', b')$, such that*
$$Q \neq \mathcal{O}, \quad \text{and } [m]Q = \mathcal{O}.$$
5. *Both m and n have no prime factor $p < 67$.*
6. *Neither m nor n is a perfect square.*

If these conditions are fulfilled, the pair (m, n) is called a pair of Dual Elliptic pseudo-primes of discriminant d.

Practically, dual elliptic pseudoprimes are found by featuring a pair of Rabin-Miller pseudoprimes (m, n), which both split in a product of two principal ideals in $\mathbb{K}$, such that there is a pair of factors which differ by ± 1. Once such primes found, two elliptic curves must be constructed in order to perform an elliptic pseudoprime test. The easiest fact about dual elliptic pseudoprimes is following

Lemma 8.2 *A pair (m, n) of DEpsp's with discriminant d are simultaneously prime or composite.*

Proof Assume m is prime. Then item 4. of the definition of dual elliptic pseudoprimes is a primality proof for n – thus n is prime too. Conversely, if n is prime, m is also prime as a consequence of 3. of the definition. □

We prove now that the tests required by definition 8.1 imply that, if DEpsp's are composite, than their least prime factor conserves the dual elliptic prime property. We shall assume from now on, without restriction of generality, that $\epsilon = 1$ in the definition of dual elliptic pseudoprimes. This is in order to avoid explosion of the number of cases.

Lemma 8.3 *Let (m, n) be a pair of DEpsp's with discriminant d which are composite and suppose*
$$m = \mu\overline{\mu}, \quad \text{and } n = \nu\overline{\nu} = (\mu + 1) \cdot \overline{(\mu + 1)}.$$
Let π be the least prime in $\mathcal{O}(\mathbb{K})$ dividing μ. Then:

(i) *There is a prime $\rho | \nu$ with $\rho = \pi + \delta$, $\delta = \pm 1$.*

(ii) *If p and q are the least primes dividing m and n respectively, then*
$$|p - q| < 2\sqrt{\max(p, q)}. \tag{8.4}$$

(iii) *If ρ is not the least prime dividing ν, then m and n are built up of at least three primes.*

(iv) *If m and n are built up of two primes each, then there is a prime π, an element $\alpha \in \mathcal{O}(\mathbb{K})$ and a unit δ, such that:*
$$\begin{aligned} \nu &= (\pi + \delta) \cdot (\alpha\pi + \delta) \text{ and} \\ \mu &= \pi \cdot (\alpha(\pi + \delta) + \delta). \end{aligned} \tag{8.5}$$

Proof Given π in the hypothesis, the curve $E_m(a,b)$ has good reduction at $p = \mathbf{N}(\pi)$ and it has $r = \mathbf{N}(\pi+\delta)$ points, for some $\delta = \pm 1$. By item 3. of the definition of DEpsp's, there must be a prime $\lambda = (\nu, \pi+\delta)|(\pi+\delta)$. Let $\pi+\delta = \alpha\cdot\lambda$; we will show that α must be a unit. If this were not the case, then $\mathbf{N}(\lambda+1) = \mathbf{N}\left(\frac{\pi+\delta}{\alpha}+1\right) < p/2+2\sqrt{p} < p-2\sqrt{p}$, for $p > 64$; but the reduction of E' mod l, with $l = \mathbf{N}(\lambda)$ has at most $\mathbf{N}(\lambda+1)$ points and this should be a multiple of some prime dividing μ, as consequence of item 4. of the definition. If α were not a unit, m would thus have a prime factor less than p, which is in contradiction with the choice of p. We have thus $\mathbf{N}(\alpha) = 1$ and may put $\rho = \lambda = \pi+\delta$ – we assumed that $d > 3$ and $\mathbb{K}$ has the only units ± 1. Note that the condition $p > 64$ is satisfied by item 5. of the definition of DEpsp's. This proves (i).

We put $q = \mathbf{N}(\rho)$. If ρ defined above is the least prime dividing n, then we have $|q-p| = \mathbf{Tr}(\pi) < 2\sqrt{p}$. Otherwise, let $\rho'|\nu$ be such that $\mathbf{N}(\rho') = q' < q$. If $r = \sharp E'_q(a',b')$ is the number of points of the curve $E'(a',b')$ taken modulo the prime q', there must be a prime p' dividing m, such that $p|r$; in fact, by a reasoning similar to the one above, we must have $p' = r$ and $\rho' = \pi' \pm 1$. We have the two double inequalities:

$$q' > \left(\sqrt{p'}-1\right)^2 > \left(\sqrt{p}-1\right)^2,$$

and

$$q' < q < \left(\sqrt{p}+1\right)^2.$$

The two inequations yield together (8.4), which proves (ii). Continuing the assumption that ρ is not the least prime divisor of ν (when comparing norms), we shall assume that both m and n are built up of only two primes. Thus $m = p\cdot p'$ and $n = q\cdot q'$. Considering the factors in $\mathcal{O}(\mathbb{K})$, we have already shown that

$$\mu = \pi\cdot\pi',\ \nu = \mu+1 = (\pi+\delta)\cdot(\pi'+\delta'),$$

for some units $\delta, \delta' = \pm 1$. After multiplying out and subtracting the two equations, we get:

$$\delta\cdot\pi' + \delta'\cdot\pi = 1 - \delta\cdot\delta'.$$

If $\delta = \delta'$, this implies $\pi + \pi' = 0$, and m is a perfect square, in contradiction with 6. of the definition of DEpsp's. If $\delta = -\delta'$, the above equation yields

$$\pi' - \pi = 2\delta;$$

and $\rho = \pi+\delta$, while $\rho' = \pi'+\delta' = \pi+2\delta-\delta = \pi+\delta$, showing that n should be a square, in contradiction to 6. Assuming now that only one of the psp's, is built up of three primes, say $n = q\cdot q'\cdot q''$ and $m = p\cdot p'$ we will have from (8.4) that $m = O(p^2)$ whereas $n = O(p^2)\cdot q'' = O(p^3)$, since $q'' > q = O(p)$. This will lead to a contradiction and the exact inequalities are not difficult to deduce, being left to the reader. We have thus shown that if the least primes dividing m and n are not dual to each other, then both numbers are built up from at least three primes, which is (iii).

Let us finally assume that the smallest divisors $p|m$ and $q|n$ are dual to each other and $\rho = \pi+\delta$, as seen in the proof of (i). Suppose that both m and n are built up from two primes and let $q' = \rho'\cdot\overline{\rho}'$ be the second divisor of n, $p' = \pi'\cdot\overline{\pi}'$ the second divisor of m. Using the reduction of $E'(a',b')$ modulo q' we can easily show that $\rho'+\epsilon$ is divisible by either π or π' – where the unit ϵ is defined by the twist of $E'(a', b')$ modulo q'. If the divisor were π' we would reach a contradiction like in the proof of (iii). Assume thus that $\rho' = \alpha\pi + \epsilon$, the divisor being π. Similarly, $\pi = \beta\rho + \epsilon'$. First consider the splitting of ν:

$$\mu + 1 = \nu = \rho \cdot \rho' = (\pi + \delta)(\alpha\pi + \epsilon) = \pi(\alpha\pi + \alpha\delta + \epsilon) + \epsilon\delta$$

By taking the above equation modulo π, we conclude that $\epsilon\delta = 1$ and thus $\epsilon = \delta$, both factors being units ± 1. Having done this simplification, we want to compare the two expressions for μ:

$$\mu = (\alpha\pi^2 + \delta(\alpha + 1)\pi + 1) - 1 = \pi(\beta(\pi + \delta) + \epsilon')$$

and, after dividing π out,

$$(\alpha - \beta)\pi = \epsilon' - \delta - \delta(\alpha - \beta).$$

Assuming $\alpha \neq \beta$, one can divide both sides by $\alpha - \beta$:

$$\pi = \frac{\epsilon' - \delta}{\alpha - \beta} - \delta,$$

and taking norms,

$$\mathbf{N}(\pi) \leq \frac{2}{\mathbf{N}(\alpha - \beta)} + 1 < 3.$$

This is a contradiction to 6. and we must have $\alpha = \beta$; inserting this equality in the above equation we also conclude $\epsilon' = \delta$. This finishes the proof of (iv). $\square$

8.2 Applications to Cyclotomy

We now come to the application of DEpsp's to cyclotomy. Suppose (m, n) are dual elliptic pseudoprimes to discriminant d. It follows from lemma 8.3 that there are two primes $p|m$ and $q|n$ such that

I. If k is the minimum of the numbers of prime factors of m and n, then $p, q < \sqrt[k]{m}$.

II. Furthermore,

$$|p - q| < \sqrt[2k]{m} \tag{8.6}$$

This follows from the fact that the smallest factor p of either m or n, which is higher composite, has a dual elliptic prime q and their difference is smaller than the trace of a prime dividing p in $\mathbb{K}$. This fact can be used for cyclotomy testing. We state following:

Algorithm CIDE *(* Cyclotomy Initialized by Dual Elliptic tests *)*

Let n be a probable prime and let a dual elliptic prime m be defined by (8.1).

1. Find a dual elliptic pseudoprime m to n. If none can be found (in affordable time) skip to a classical cyclotomy test of n.

2. Choose the parameters S, T, s, t, such that $s > t^2\sqrt[4]{n}$ and $S > \sqrt{n}$. Like usual, $T = \mathrm{ord}_S(n)$ and $t = ord_s(n)$.

3. Let m and n pass the main stage of the cyclotomy test for s, t.

4. Build two tables $A = \{m^j \bmod s : j = 1, 2, \ldots, t-1\}$ and $B = \{n^k \bmod s : k = 1, 2, \ldots, t-1\}$, which are sorted in increasing order. (For practical reasons, the upper, say, 8 bytes of each power will suffice).

5. Seek (in $O(\sqrt[4]{n})$ comparisons) pairs (j, k), such that $|m^j - n^k \bmod s| < \sqrt[4]{n}$. The absolute value $|m^j - n^k \bmod s|$ will take the modularity into account, i.e., m^j will be replaced by $s + m^j$, if this reduces the absolute value, etc.

6. If no pair is found, n is prime – and, by lemma 8.2, also m: stop.

7. For all k out of the pairs found in 6., check that

   $$r_{k'} = n^{k'} \bmod S, \ (r_{k'}, n) = 1, \ \forall k' \in (\mathbb{Z}/T \cdot \mathbb{Z}), \ k' = k \bmod t.$$

   If a divisor is found, stop and declare n composite.

8. Perform the central stage for n for all characters in the (S, T) test which were not tested in the (s, t) test and declare n prime if all these central stage tests are passed.

Remark 8.7 *The initial choice of s, t is such that the occurrence of a difference of two elements in A and B which is $< \sqrt[4]{n}$ is highly improbable, in fact having probability $< 1/t^2$. However if n were composite, by I. above, at least one such difference must occur. This explains the steps 1–5.*

Not finding a small difference will conclude the primality proof with $s = O(\sqrt[4]{n})$, while finding one is an indication n could be composite. Note that this is the most unlucky part of the algorithm which actually requires almost the double of the main stage, for achieving as much as a usual cyclotomy test: therefor one starts from the hypothesis n might be composite and checks first all the possible divisors in step 7. If a divisor is found, n is composite and the algorithm halts. Otherwise, the primality proof is only completed, after *proving that all possible divisors of* n *were the ones checked in step 7. – thus performing the* $O(\sqrt{n})$ *main stage in step 8.*

Choosing s *sensibly – but not orders of magnitude – larger then* $\sqrt[4]{n}$ *is a good caution in order to avoid that step 5. finds any solutions, unless* n *is indeed composite. This happens at the cost of finding a dual elliptic pseudoprime* m *to* n*. This cost has still to be evaluated in practice, by using implementations such as Morain's one [Mo90].*

The overall cost of the new algorithm is, in the general case:

1. *Finding one dual elliptic pseudoprime to* n*.*
2. *Performing two central stage of cyclotomy tests with* $s = O(\sqrt[4]{n})$*.*
3. *Building two remainder tables for* $s = O(\sqrt[4]{n})$ *and comparing differences.*

The worst case has an additional central stage of $s = O(\sqrt{n})$ *and few trial divisions.*

Determinism is a decaying bourgeois ideology, pretending the working class could not change its destiny.

Some recent times red bible.

Appendix A

Deterministic primality test

The test described in §5 provides a provable statement about the primality/compositeness of a test number n as soon as all the work extensions have been successfully built. The constructions rely on the Lucas - Lehmer method. Random bases are used for seeking p^k-th roots of unity. Given that such a random base leads to a root of unity with probability $1 - 1/p$, it is very likely that a root will be found in polynomial time. Assuming the extended Riemann hypothesis, this is even a proven fact ([CoLe]).

From a strictly theoretical point of view however, one would wish to have a procedure capable of giving an answer also for the case when certain working extensions could not be constructed. This is the task of the deterministic primality test. Note that relation (3.57) is explicitly used in the proof of theorems (4.13) and (4.25). It is itself a consequence of the existence of the saturated work extensions. If a saturated extension does not exist for a given prime, one can shift computations to complex extensions. The existence proof according to theorems (4.13) and (4.25) will however not hold. If $p|t$, then there is at least one $q|s$ such that $p|\mathrm{ord}_q(n)$; by letting $\mathbf{R} = \mathbb{Z}[\zeta_p]$ for a complex $p-$th root of unity ζ_p and χ be a character $\chi : (\mathbb{Z}/q \cdot \mathbb{Z})^* \to < \zeta_p >$, the element $\alpha = \tau(\chi)^p \in \mathbf{R}$ can be computed by multiple Jacobi-Sums (2.32) and should verify

$$\alpha^{(n^{p-1}-1)/p} = \chi_p(n) \neq 1.$$

If this relation does not hold, n is composite, otherwise, a $p-$th power non residue is found and a saturated $p-$th extension can be constructed using the Lucas-Lehmer method. Furthermore, if $v_p(n^{p-1} - 1) = 1$, a $p-$th root can be taken using the algorithm in §4.1. This shows that a deterministic test is only required for *push* characters, and only in the case when $v_p(n^{p-1} - 1) > 1$ for odd p or $v_2(n - 1) > 2$. The deterministic test described in [Le1] generalizes the idea of the Rabin-Miller test. It replaces (3.56) by a statement on possible divisors $r|n$ in the p-adic numbers $\mathbb{Z}_p$. This leads to proving that the divisors also lay in some cycles generated by a number $\nu \bmod t$, which can be explicitly constructed. Since in general, $\nu \neq n$, the approach suggests that no $s-$th cyclotomic extensions exists (according to theorem (3.35)).

We shall give now a computational presentation of the deterministic algorithm, which was described in [Le1] in more abstract terms and will show how to integrate it in the global algorithm from §5.6. This is to a certain extent, an improvement of [Le1], using just small working extension and integrating the deterministic test naturally and without excessive overhead in the "general purpose" test form §5.6.

Since there is a natural distinction between the odd primes and the prime 2, which occurred already in §4.1, we shall first consider the case of an odd prime p, such that

$$(p,t)=1, \qquad \text{and } v_p(n^{p-1}-1)=\kappa+1>1.$$

With $\mathcal{Q}=\{q|s : \ p|(q-1)/\mathrm{ord}_q(n)\}$ we let $k(q)=v_p(q-1)$, $\forall q\in\mathcal{Q}$ and $k_m=\max_{q\in\mathcal{Q}}\{k(q)\}$.

For each $q\in\mathcal{Q}$, we need a minimal extension in which Gauss-Sums may be computed. If $\wp\subset(\mathbb{Z}/q\cdot\mathbb{Z})^*$ is the maximal p-group and $\eta_q=\xi_q^{(\mathbb{Z}/q\cdot\mathbb{Z})^*/\wp}$, with ξ_q a complex $q-$th root of unity. We shall perform computations in the complex extension

$$\mathbf{R}=\mathbb{Z}[\zeta]/(n\cdot\mathbb{Z}[\zeta]),$$

with ζ a complex $p^{k_m}-$th root of unity, and in the rings

$$\mathbf{Q}_q=\mathbb{Z}[\zeta,\eta_q]/(n\cdot\mathbb{Z}[\zeta,\eta_q].$$

For $q\in\mathcal{Q}$, let

$$n^{(p-1)p^{k(q)-1}}-1=u(q)\cdot p^{\kappa+k(q)},\ (u(q),p)=1,$$

and

$$\lambda_q(\chi)=\tau(\chi_q)^{u(q)}\in\mathbf{Q}_q,\ \chi_q:(\mathbb{Z}/q\cdot\mathbb{Z})^*\to<\zeta^{p^{k_m-k(q)}}>.$$

Note that $\tau(\chi_q)$ may only be computed in the larger extension $\mathbf{Q}_q$ and the exponentiation for finding the value of λ_q will be performed in the same ring. However, for prime n, the value $\lambda_q\in\mathbf{R}$: it lays thus in the smaller extension, as a consequence of its being a $p^{k(q)+\kappa}-$th root of unity. Roots of this order exist in $\mathbf{R}$ for prime n. Consequently, $\lambda_q(\chi)\in\mathbf{R}$ is a necessary primality condition.

The first step of the test is the analog of the Rabin-Miller test and consists in building the sequence:

$$x_i(q)=(\lambda_q(\chi))^{p^i},\ i=0,1,\ldots,k(q)+\kappa,$$

and verifying

1. that $x_{k(q)+\kappa}=1$. This is the condition (4.15) for push characters.
2. that for $j=\min\{i:x_i=1\}$, $x_{j-1}\in<\zeta>$, if $j>0$.
3. that if $\exists l\geq 0: x_l\notin<\zeta>$, then for the maximal such l,

$$(x_l-\zeta^{h\cdot p^{k_m-k(q)}},n)=1,\ h=1,2,\ldots,p^{k_m-k(q)}.$$

The first two conditions are Rabin-Miller, the third provides the information that will be used for combining tests. We now show how this functions. For ease of notation, we shall keep q fixed and give the explicit notation of dependencies on q up. Let

$$J_\chi\subset 1+p\mathbb{Z}_p=\{a\in 1+p\mathbb{Z}_p:\lambda(\chi)^{a-\sigma_a}\in<\zeta>\}, \tag{A.1}$$

with σ_a being the automorphism of $\mathbf{R}$ sending ζ to ζ^a. If the above conditions are verified, then J_χ is not empty and it is a simple consequence of lemma (2.14), that

$$J_\chi = (1 + p^j)^{\mathbb{Z}_p},$$

for a given, yet to determine positive integer j. By definition of x_i above and with $a_i = 1 + p^i$, we have

$$a_i \in J_\chi \iff x_i \in <\zeta> .$$

Consider now a prime $r|n$ and suppose $r \notin J_\chi$. Then there is an $m \in \mathbb{Z}_p^*$ with $1 + p^{j-1} = r^{(p-1)/m}$ and

$$x_{j-1} = \tau(\chi)^{r^{(p-1)m} - \sigma_r^{(p-1)m}} = \chi(r)^{-(p-1)m \cdot r^{(p-1)m}} \mod r\mathbf{R}.$$

This is a contradiction to the above condition 3. We have thus:

$$r^{p-1} \in J_\chi = (1 + p^j)^{\mathbb{Z}_p}.$$

Of course, $\left(n^{p-1}\right)^{\mathbb{Z}_p} = (1 + p^{1+\kappa})^{\mathbb{Z}_p}$ and we deal here with the case when $j < \kappa + 1$:

otherwise, condition (3.57) would be fulfilled and a saturated $p-$th extension would exist, which is all we need. We shall prove now a condition similar to theorem (4.15).

Lemma A.2 *Let $\rho \in <\zeta>$ be given by*

$$\rho^{-ua_j} = x_j.$$

Then

$$\chi(r^{p-1}) = \rho^{\mu_p(r)}, \ \forall \text{ primes } r|n,$$

where $\mu_p(r)$ is such that $r^{p-1} = (1 + p^j)^{\mu_p(r)} \in 1 + p\mathbb{Z}_p$ and there is a multiplicative character $\overline{\chi} : J_\chi \to <\zeta>$ with

$$\chi(r^{p-1}) = \overline{\chi}(r^{p-1}), \quad \forall r|n. \tag{A.3}$$

Proof Let μ_p be defined as above. Then

$$\left(\tau(\chi)^u\right)^{r^{p-1} - \sigma_r^{p-1}} = \chi(r)^{-(p-1)ur^{p-1}} \mod r\mathbf{R},$$

by (2.37). Furthermore,

$$\left(\tau(\chi)^u\right)^{r^{p-1} - \sigma_r^{p-1}} = \lambda(\chi)^{a_j^\mu - \sigma_{a_j}^\mu} = \lambda(\chi)^{(a_j - \sigma_{a_j})(\sum_{i=0}^{\mu-1} a_j^{\mu-i-1}\sigma_{a_j}^i)} = x_j^{\mu_p a_j^{\mu-1}},$$

and finally

$$\chi(r)^{-(p-1)ur^{p-1}} = x_j^{r^{p-1}\mu_p a_j^{-1}} = \rho^{-\mu_p ur^{p-1}} \mod r\mathbf{R}.$$

Since $(ur^{p-1}, p) = 1$ and by lemma (4.23) we have:

$$\chi(r)^{p-1} = \rho^{\mu_p(r)}.$$

Note that ρ does not depend on r. If the character $\overline{\chi}$ is defined by

$$\overline{\chi}(a_j) = \rho,$$

then the statement of the proposition follows. $\square$

Two remarks are needed. First note that both the number $a_j = a(p, q)$ and the character $\overline{\chi}$ defined above depend on both p and q. Second, the value $j = j(q),\ q \in \mathcal{Q}$ depends on q and there is a maximal $j = j(p)$ such that $r^{p-1} \in (1 + p^{j(p)})^{\mathbb{Z}_p}$. We have:

$$\gamma(p) = 1 + p^{j(p)} \rightarrow\ \chi(r) = \overline{\chi}(\gamma_p)^{-\mu_p},\ \forall\chi,$$

where the character $\overline{\chi}$ is accordingly defined and μ_p does not depend on the choice of χ. The characters χ have conductors in $\mathcal{Q}$ and powers of p as orders. It is clear now, that while conditions 1. and 2. should be checked for all $q \in \mathcal{Q}$, since they determine the values $j(p, q)$, condition 3. shall only be checked for one q giving raise to the maximal $j(q)$.

We shall consider now the case $p = 2$ which is slightly diverse, due to the special structure of the p-adic numbers in this case. We define as above,

$$\mathcal{Q} = \{q | s : 2 | (q-1)/\mathrm{ord}_q(n)\},$$

with $v_2(n^2 - 1) = \kappa$, $v_2(q-1) = k(q)$ and $\mathbf{R} = \mathbb{Z}[\zeta]/(n \cdot \mathbb{Z}[\zeta])$ with ζ a complex $2^{\kappa+k(q)}-$th root of unity. We let further $\eta_q = \xi^{(\mathbb{Z}/q\cdot\mathbb{Z})^*/\wp}$, $\forall q \in \mathcal{Q}$; here ξ is a complex $q-$th root of unity and $\wp$ is the maximal 2-group in $(\mathbb{Z}/q \cdot \mathbb{Z})^*$. With this, $\mathbf{Q}_q = \mathbb{Z}[\zeta, \eta_q]/(n\mathbb{Z}[\zeta, \eta_q])$. Finally $n^2 - 1 = 2^\kappa u$ with $(u, 2) = 1$ and $\lambda_q(\chi) = \tau(\chi)^{u(q)}$.

First let $y = \chi(-1)q$ and perform a classical Rabin-Miller test with base y. If the test is not passed, declare n composite and stop. Let $x_i = \lambda_q(\chi)^{2^i}$ and calculate $j(q) = \min\{i : x_i \in <\zeta>\}$.

If $j(q) \geq 4$, one shall verify condition 3. and put $a_2(q) = j(q)$ if it is verified (n is composite otherwise).

If $j = 3$, first check if $\beta = (\chi(-1)q)^{u'(q)} \in \{-1, 1\}$, with $u' = v_2(n-1)$; if this is the case, put $a_2(q) = 7$. If not, check finally condition 3. for x_1, x_2 and $(\beta \pm 1, n) = 1$; put $a_2(q) = 9$.

If $j = 2$, test condition 3. for x_1 and put $a_2(q) = 5$.

If $j = 1$, check condition 3. for x_2 and put $a_2(q) = 3$ if $x_2 \in <\zeta>$ and $a_2(q) = 7$ otherwise.

These calculations will be done only once, namely for $q_0 | s$ such that $j(q_0) = \max_{q\in\mathcal{Q}}\ j(q)$. We have the following analogon to lemma (A.2):

Lemma A.4 *Let $\rho \in <\zeta>$ be given by*

$$\rho^{-ua_j} = \begin{cases} x_j & \text{if } a = a_2(q) = 1 + 2^i, \\ \left(J_7(\chi)\right)^{u(q)}, & \text{if } a = a_2(q) = 7. \end{cases}$$

Then $\chi(r) = \rho^{\mu_p(r)}$, $\forall$ *primes* $r|n$, *where* $\mu_p(r)$ *is such that* $r^{\mu_p(r)} = a_2(q)$ *mod* 2^κ *and there is a multiplicative character* $\overline{\chi} : J_\chi \rightarrow <\zeta>$ *with*

$$\chi(r) = \overline{\chi}(r), \quad \forall r|n,$$

and if

$$-1 \in J_\chi, \text{ then } \overline{\chi}(-1) = \chi(-1).$$

Proof We first prove that $r = a_2(q)^{\mathbb{Z}_2}$. If $j \geq 4$, the prove goes like in the above lemma. If $j \leq 3$, we have following cases:

(i) If $3 \in J_\chi$ and $5 \notin J_\chi$, then $J_\chi = 3^{\mathbb{Z}_2}$.

(ii) If $7 \in J_\chi$ and $5 \notin J_\chi$, then $J_\chi = 7^{\mathbb{Z}_2}$.

(iii) If $3 \notin J_\chi$, $5 \notin J_\chi$ and $7 \notin J_\chi$, then $J_\chi = 9^{\mathbb{Z}_2}$.

(iv) If $J_\chi = 1 + 2\mathbb{Z}_2$ then $J_\chi = 3^{\mathbb{Z}_2} \cup (-3)^{\mathbb{Z}_2}$.

The condition $\beta \in \{-1, 1\}$ implies $-1 \in J_\chi$; for $j(q) = 3$, this shows $7 \in J_\chi$. With these remarks, one can check that $a_2(q)$ as defined above generates J_χ. The further proof goes like in lemma (A.2). □

We can now state a deterministic *add-on* to the primality test in §5.6. This shall be performed before the final trial division step 7. Note that the base for computing the trial division remainders $r_i = \nu^i$ mod s is modified here.

D.1 Let $P = \{p : p|(q-1); q|s$ and no saturated $p-$th extension was found.$\}$

D.2 For all odd $p \in P$ do following:

- D.2.1 Let $v_p(n^{p-1} - 1) = \kappa + 1$. If $\kappa = 0$, next p.
- D.2.2 Let $\mathcal{Q}_p = \{q|s : p|(q-1)\}$
- D.2.3 Let ζ be a complex $p^{k_m}-$th root of unity with $k_m = \max_{q \in \mathcal{Q}_p} v_p(q-1)$ and $\mathbf{R} = \mathbb{Z}[\zeta]/(n\mathbb{Z}[\zeta])$.
- D.2.4 For all $q \in \mathcal{Q}_p$ do following:
  - D.2.4.1 Let $k(q) = v_p(q-1)$, $\wp$ be the p-group in $(\mathbb{Z}/q \cdot \mathbb{Z})^*$, $\eta_q = \xi_q^{(\mathbb{Z}/q \cdot \mathbb{Z})^*/\wp}$ and $\mathbf{Q}_q = \mathbb{Z}[\zeta, \eta_q]/(n\mathbb{Z}[\zeta, \eta_q])$.
  - D.2.4.2 Let χ_q be a generating multiplicative character $\chi_q : (\mathbb{Z}/q \cdot \mathbb{Z})^* \rightarrow <\zeta>$, $\tau(\chi_q) \in \mathbf{Q}_q$ and $\lambda_q(\chi) = \tau(\chi_q)^{u(q)}$, where $n^{(p-1)p^{k(q)-1}} - 1 = u(q)p^{k(q)+\kappa}$, $(u(q), p) = 1$.
  - D.2.4.3 Let $x_i = (\lambda_q(\chi))^{p^i}$ and $j(q) = \min\{i : x_i \in <\zeta>\}$. If $j(q) = 0$, next q.
  - D.2.4.4 Check $x_{\kappa+k(q)} = 1$ and $x_0 \in \mathbf{R}$.

D.2.5 For q such that $j(q)$ is maximal, let $j_p = j(q), a_p = (1 + p^{j(q)})$ and check

$$(x_{j_p-1} - \zeta^{h \cdot p^\kappa}, n) = 1, \ h = 1, \ldots, p^{k(q)}.$$

D.2.6 Choose a generating character $\chi_{p,q}$ and define a character $\overline{\chi_{p,q}}$ such that $\chi_{p,q}(r) = \overline{\chi_{p,q}}(1 + p^{j_p})^{-\mu_p(r)}, \ \forall r|n$.

D.3 If $2 \in P$ do following:

D.3.1 Let $v_2(n^2 - 1) = \kappa + 1$.

D.3.2 Let $\mathcal{Q}_2 = \{q|s : 2|(q-1)\}$

D.3.3 Let ζ be a complex $2^{k_m}-$th root of unity with $k_m = \max_{q \in \mathcal{Q}_2} v_2(q-1)$ and $\mathbf{R} = \mathbb{Z}[\zeta]/(n\mathbb{Z}[\zeta])$.

D.3.4 For all $q \in \mathcal{Q}_2$ do following:

D.3.4.1 Let $k(q) = v_2(q-1)$, $\wp$ be the 2-group in $(\mathbb{Z}/q \cdot \mathbb{Z})^*$, $\eta_q = \xi_q^{(\mathbb{Z}/q \cdot \mathbb{Z})^*/\wp}$ and $\mathbf{Q}_q = \mathbb{Z}[\zeta, \eta_q]/(n\mathbb{Z}[\zeta, \eta_q])$.

D.3.4.2 Let χ_q be a generating multiplicative character $\chi_q : (\mathbb{Z}/q \cdot \mathbb{Z})^* \rightarrow < \zeta >$, $\tau(\chi_q) \in \mathbf{Q}_q$ and $\lambda_q(\chi) = \tau(\chi_q)^{u(q)}$, where $n^{2^{k(q)}} - 1 = u(q)2^{k(q)+\kappa}$, $(u(q), 2) = 1$.

D.3.4.3 Let $x_i = (\lambda_q(\chi))^{2^i}$ and $j(q) = \min\{i : x_i \in < \zeta >\}$. If $j(q) = 0$, next q.

D.3.4.4 Check $x_{\kappa + k(q)} = 1$ and $x_0 \in \mathbf{R}$.

D.3.5 For q such that $j(q)$ is maximal, let $j_2 = j(q)$ and check $(x_{j_2-1} - \zeta^{h \cdot 2^\kappa}, n) = 1, \ h = 1, \ldots, p^{k(q)}$.

D.3.6 Determine a_2 like in lemma (A.4).

D.3.7 Choose a generating character $\chi_{2,q}$ and define a character $\overline{\chi_{2,q}}$ such that $\chi_{2,q}(r) = \overline{\chi_{2,q}}(1 + 2^{j_2})^{-\mu_2(r)}, \ \forall r|n$.

D.4 Set $\nu = n$ and $\mu = 1$.

D.5 For all $p \in P$ do following:

D.5.1 For all $q \in \mathcal{Q}_p$ do following:

D.5.1.1 Fix a generator g of $(\mathbb{Z}/q \cdot \mathbb{Z})^*$ and define $f(q)$ by $g^{f(q)} = \nu \bmod q$.

D.5.1.2 For all $p|(q-1)$, determine the exponent $c(p,q)$ such that

$$\chi_{p,q}(g^{c(p,q)}) = \overline{\chi_{p,q}}(a_p), \text{ if } p \in P,$$

and $c(p,q) = f(q) \mod p^{k(q)}$.

D.5.1.3 Let $c(q) \in (\mathbb{Z}/(q-1) \cdot \mathbb{Z})$ be such that

$$c(q) = c(p,q) \mod p^{k(q)}, \ \forall p|(q-1).$$

Let $\nu_q = g^{c(q)} \mod q$.

D.5.1.4 If $2 \in P$ and $J_2 = 1 + 2\mathbb{Z}_2 = 3^{\mathbb{Z}_2} \cup (-3)^{\mathbb{Z}_2}$, then let $d(p,q) = 0$ for all odd $p|(q-1)$. Define $d(2,q)$ such that

$$\chi_{2,q}(g^{d(2,q)}) = \overline{\chi_{2,q}}(-1).$$

Let $d(q) \in (\mathbb{Z}/(q-1)\cdot\mathbb{Z})$ be such that

$$d(q) = d(p,q) \mod p^{k(q)}, \ \forall p|(q-1).$$

Let $\mu_q = g^{d(q)} \mod q$. Put $\mu = 0$.

D.6 Find the unique residue class modulo s with

$$\nu = \nu_q \mod q \ \forall q|s.$$

D.7 If $\mu \neq 1$ find the unique residue class modulo s with

$$\mu = \mu_q \mod q \ \forall q|s.$$

After performing this additional step for the deterministic test, the residue classes for the final trial division will be:

$$r_i = \nu^i \mod s, \quad i = 1, 2, \ldots, t-1,$$

and if $\mu \neq 1$, also

$$r_i = \mu\nu^i \mod s, \quad i = 1, 2, \ldots, t-1.$$

It follows from the test §5.6 and the lemmas (A.2) and (A.4) that n is prime, if none of the above residue classes is a true divisor of n.

And how do you earn your living ?

My neighbour

Appendix B

Fast Generation of Provable Primes Using Search in Arithmetic Progressions

B.1 Introduction

Primality testing has a long history and has undergone a radical development during the last decade. We shall not go into details of this development but begin with mentioning that prime tests split into compositeness proofs (which are polynomial) and primality proofs, which are more complex. The fastest known primality proof [GoKi] which has been implemented by Atkins and Morain [Mo90], is polynomial, but in practice slower than super polynomial algorithms such as the cyclotomy test [BovdH]. Algorithms proposed for the specific purpose of generating primes for cryptographic use are different due to the technological motivation behind them. Efficiency and simplicity are the main concerns and - as a consequence of the domain of application - "security" of primes is an issue of concern too. Security of a prime p basically means that the discrete logarithm base p and factorization of p out of a product of usually two primes should be, if possible, harder than average. The last condition raised the wish to have large prime factors in $p \pm 1$; this was formalized in conditions for so called "Gordon secure primes" [Go]. It was obvious that with the information about factors of $p \pm 1$ available for a Gordon prime, a proof by Pocklington's lemma was almost for free. The first to make use of this observation was Maurer in [Ma2]. By the date of Maurer's paper, Gordon primes were de facto outdated by the ECM ([Le5]) factoring method: Gordon primes were designed to reduce the odds of $p \pm 1$ factoring methods [Po], but cannot provide any specific protection against elliptic curve factoring. This facts are reflected in [Ri]. For technological applications, Maurer's algorithm lacks both the ease of implementation and the efficiency requirements - being, by the authors statement ([Ma2]), p19 60% slower than Rabin-Miller tests which are also simpler to implement.

Maurer does state in [Ma2], p29, that his algorithm is more efficient than probable

The content of this chapter was first published in the Proceedings of CRYPTO94, [Mi1].

primes, but this statement is not supported by facts and is in contradiction with the rest of the paper. The paper [Ma1] is important for having first indicated that for the specific purpose of cryptographic use, provable primes were worth considering. We propose an algorithm that seeks primes in arithmetic sequences for which a factorization of the ratio is known - this implies a recursive use of the algorithm. For the trial division phase we use Eratosthenes sieve methods, which lead to an increase of the optimal length of trial division; optimal trial division was also evaluated in [Ma1], [BDL]. In the last paper, the authors also consider means of speeding up Maurer's method and notice that the 'almost' uniform distribution required by Maurer has a negative impact on the performance. An elegant analysis of the information entropy of primes produced by "incremental search" - and proved with Rabin-Miller tests - is provided in [BD]. Incremental search is a special case of arithmetic progressions - when the ratio is 2. We shall adapt some of the methods of that article for the analysis of our algorithm.

Probabilistic methods like Rabin-Miller may falsely declare composites for primes and the probability for this event decreases with the iteration of the same test for different bases. In [BDP] the authors show that this probability also depends on the size of the primes produced; tables for the error probability $q_{t,k}$ that a composite with k - binary digits is declared prime after t independent Rabin-Miller tests are quoted also in [BD]; the tables show that the probability of failure of the Rabin-Miller test after t rounds is substantially lower than the 4^{-t} initially proved by Rabin [Ra]. These results suggest to the authors the conclusion that "using the Rabin test remains in many cases the most practical approach" [BD],p.1. We show that recursive primality proofs combined with search in arithmetic progressions is preferable to Rabin-Miller tests, also from the point of view of efficiency, in the range of sizes of primes covered by the tables in [BD] and probably for primes up to at least 1000 bits. For larger primes, the difference becomes negligible.

B.2 Outline of the algorithm

Let $B > 0$ and $n > 0$ be positive integers and $s, c > 1$ real constants. We propose following algorithm for generating provable primes of n digits, together with their certificates:

Algorithm V *(* Prime Generation* **AP** **)*

Input: n. **Constants:** B, c, s.

- **Step 1**. If $n < B$ return a random prime with n bits (generated by trial division).
- **Step 2**. Produce an integer F with $2^{\epsilon n} < F < 2^{c\epsilon n}$ which is completely factored, by recursive use of this algorithm. The constant ϵ may be 1/2, or 1/3 , depending on the prime certification used (see bellow).
- **Step 3**. Draw a random number $t \in (2^{n-2}/F,\ 2^{n-1}/F - sn)$.

- **Step 4**. Find a prime in the arithmetic progression
  $P = \{N : N = N_0 + ia; N_0 = ta + 1; a = 2F; 0 \leq i \leq s\}$.

The primality test for Step 4 splits naturally in three parts which are applied to prime candidates in the progression P until a prime is found - together with a corresponding certificate, or the bound s is passed and the algorithm returns failure.

Part I : **Trial division by primes** $< A$, where A is a given upper bound.

Calculate $a'_p = a \bmod p,\ \forall p < A$.
Calculate $N'_p = N_0 \bmod p,\ \forall p < A$.
Initiate an array *tab* of length s. For all $p < A$, set $tab[i] = 1$ for all solutions of the modular equation $N'_p + ia'_p = 0 \bmod p$. This is obviously an Eratosthenes sieve.

Part II : **Compositeness test** using Rabin-Miller.

Traverse the table *tab* starting with $i = 0$ and perform a Rabin-Miller test with base 2, for the i-th elements in the progression P, such that $tab[i] = 0$. Continue if the test declares "composite", go to Part III otherwise.

Part III : **Primality proof** using the Pocklington lemma.

We recall the Pocklington lemma:

Proposition B.1 *: Let N be an integer, such that $N-1 = F \cdot R$, where F is completely factored. Suppose that,*

$$\forall q \mid F,\ \ \exists \alpha_q \text{ with } \ (\alpha_q^{N-1/q}, N) = 1 \text{ and } \ \alpha_q^{N-1} = 1 \text{ mod } N \tag{B.1}$$

Then all primes $p \mid N$ are of the shape $p = kF + 1$. In particular, if $F > \sqrt{N}$, then N is prime.

Proof Let $\alpha = \prod_{q|F} \alpha_q$. Then $(\alpha_q^{N-1/q}, N) = 1$ and $\alpha_q^{N-1} = 1 \bmod N$. If $r \| N$ is a prime, the above equations hold a fortiori $\bmod r$, thus proving the first assertion: $F \mid (r-1)$. If $F > \sqrt{N}$, it follows that $r > \sqrt{N},\ \forall r \mid N, r$ prime. This is a contradiction, since N must have at least one prime factor $r < \sqrt{N}$. Consequently, N must be prime, which ends the proof. □

In part III of the algorithm, for each $q \| F$, a base α_q verifying (1) is sought among the first primes, starting with 2. If for some base $\alpha_q^{N-1} = 1 \bmod N$ does not hold, N is composite (little Fermat does not hold). If for some q, no base verifying (1) is found before a fixed upper bound R of trials, no primality or compositeness proof can be provided and N is incremented (Part II is proceeded). Finally, if bases α_q are found $\forall q \mid F$, N is prime. The prime certificate consists of the pairs $\{(\alpha_q, q) : q \mid F\}$ together with certificates for each prime q, recursively [Pl]. Providing all these pairs together with the certificates for q being prime gives a proof of N's primality by the above lemma. In

[CQ] a certification method using an $O(n^{1/3})$ factored part of $n-1$ is provided. It requires proving that a certain discriminant is not a perfect square. Suppose $n = Ft + 1$ and $F > \sqrt[3]{n}$, and bases α_q verifying (3.4) have been found for all $q \mid F$. If n is composite, it is built up of two primes $p_i = k_i \cdot F + 1$. Let $n = aF^2 + bF + 1$; by comparing $n = p_1 p_2$ we get $k_1 k_2 = a$ and $k_1 + k_2 = b$. It is then easy to see that n is composite iff $\Delta = b^2 - 4a$ is a perfect square. This again can be checked by verifying if Δ is a perfect square modulo a set of primes $\{p : \prod p > F\}$; if this is the case, $(k_i \bmod F) = k_i < F$. Otherwise n is prime. One can take in general $\{p : p < \log F\}$ as set of primes.

B.3 Optimal trial division and run time analysis

We assume a machine with word length B, the time for a short integer multiplication is t and let $m = n/B$. The time involved in the trial division is: $T_t = t((1+\epsilon)m + \log A)\frac{A}{\log A}$ and is build up of $(1+\epsilon)m$ short divisions for calculating a' and N' and $\log A$ divisions for calculating a modular inverse, for each prime; we shall write $T_t = tm(1+\epsilon+\delta)\frac{A}{\log A}$, with $\delta = \frac{\log A}{m} \to 0$ for $m \to \infty$. Note that the trial divisions are performed only once and do not have to be repeated for all n candidates. Assuming that the prime candidates for AP are equally distributed among the residue classes $\bmod p$ for all small test primes p, the fraction of prime candidates after this step is, by Mertens' theorem $f = \frac{e^{-\gamma}}{\log A}$. The second part then takes in average:

$$T_R = t \cdot f \cdot d \cdot w^2 \cdot m^4 = t \cdot \frac{f \cdot d \cdot n^4}{w^2}, \tag{B.2}$$

where the length of the expected seek interval is $d \cdot n$, and naive multiplication is used for exponentiation. We shall see that $d = 1$, so we subsequently neglect this factor. Optimal table length A may be found by writing $g_P(A) = T_t(A) + T_R(A)$ and taking the derivative. The optimal value found is $A_P = \frac{kn^2 m}{\log(n^2 m)}$, with a constant $k = \frac{e^{-\gamma}}{1+\epsilon+\delta}$ close to 0.4. As a term of comparison, optimal table length in [Ma1] is $O(nm)$. Actually, Maurer's argument goes like this: adding a prime A to the table saves a pseudoprime test with probability $1/A$, so optimal length is reached when the expected saving T_e/A balances the expected extra division which he sets to $1 \cdot T_d$; the argument is incorrect, since both values should be averaged over the whole seek interval. It does however yield a good estimate of the optimal value $A_R = \frac{2e^{-\gamma}}{\alpha(A)} nm$, with $\alpha(A)$ defined in [Ma1], as found by taking the derivative of the adequate function g_R (indices P stay for progression search, R for random search). In [BDL] the optimal table length is even smaller: $O\Big(\frac{nm}{\log(nm)}\Big)$.

An alternative to the sieve method consists in computing the current remainders

$$N_c = N_i + ia \bmod p.$$

This yields the same asymptotics as A_P, with δ replaced by a constant $\alpha = 2wt_a$ where t_a is the ratio between the time for a short addition and a short multiplication. Beside the smaller constant, this approach has the disadvantage that the remainders $\bmod p$ must be stored (three values for each test prime p). Comparing A_P to A_R shows that the use of the Eratosthenes sieve sensibly increases optimal table length, leading to the elimination of more candidates in the trial division phase. One can evaluate this performance improvement: since the number of pseudoprime tests is in average fn both for random search and for search in progressions, in the last case the exponentiations drop by a factor of

$$f_p = \frac{\log A_R}{\log A_P} = O\Big(\frac{\log(nm)}{\log(n^2m/\log(n^2m))}\Big) \to \frac{2}{3} \text{ for } n \to \infty$$

This improvement appears to be more substantial than what can be saved in a probabilistic proof approach by better error estimates, like in [BDP].

For $n = 1024$ the number of primes for the trial division phase is about 2^{15} (with $A \approx 2^{19}$) and this may be argued to be too large for some machines. Using the incremental difference storing for the primes, this requires 32 KB of memory which should be affordable on most current PC's. The saving factor is 0.72 and it results in about 10 pseudoprime tests less! It is theoretically interesting to observe that $A_P = O\Big(\frac{n^4}{(\log n)^2}\Big)$ can be achieved by using a divide and conquer method. The idea is following: group the test primes in $A/(\log A\sqrt{m})$ products of length $\sqrt{m}$ and take first the remainders modulo these products and then the remainders of these remainders modulo the single primes; this yields: $T_t = 2t\sqrt{m}(1+\epsilon+\delta)\frac{A}{\log A}$. Iterating this method leads to the stated result, when the factor $2\sqrt{m}$ is replaced by $(\log m) \cdot m^{1/\log m} = O(\log m)$. This means taking products of length $m/2, m/4, ..., 2$. Of course, the building of the factors belongs to a precomputation phase and the storage space explodes to $O(n^2m^2)$ - the method is not meant for implementation!

Note that the base 2 is a suitable base for the Pocklington lemma, being a q-th power non residue with probability $(1-1/q)$. This is remarkable, since exponentiation base 2 is particularly efficient ([BDL]).We shall consider here the version of the algorithm where F is built up of a single prime. With this, the time for part III is $1-\epsilon$ exponentiations, since for proving that 2 is an adequate F-th power non residue, one only raises to the power $(n-1)/F$, the exponent thus having length $n(1-\epsilon)$. With probability $1/F$ a further base should be tested: we do not take this event into account, since its probability is exponentially low. If $\epsilon = 1/3$, checking that Δ is not a perfect square takes $\sum \log p = O(\log F) = O(n)$ short operations, which are negligible too. We now want to motivate our claim that this algorithm is more efficient than pseudoprime algorithms, for the range of values of n of current interest. Of course, the sieve method can also be used with pseudoprimes in incremental search, although this method was not proposed before. Some implementation might also use suboptimal table length, due to limited memory. We thus do not consider the advantages of trial division as specific for AP. The advantage of our algorithm compared to pseudoprime algorithms will thus relay in the shorter proof, the disadvantage, in recursion. It is these two factors we shall have to compare.

If R is the number of Rabin-Miller tests performed until a pseudoprime is found and T_e is the time for an n-bit exponentiation, the time for the proof is, as seen above, $(1-\epsilon)T_e$ and the time involved in recursion is upper bounded by $T_r = (\frac{\epsilon^4}{1-\epsilon^4}) \cdot RT_e$. The total overhead for proving a prime is thus: $T_r = (\frac{\epsilon^4}{1-\epsilon^4} \cdot R + (1-\epsilon)) \cdot T_e$. With $n = 384$ - which is currently standard for RSA - for a weak implementation, with $\epsilon = 1/2$ and

$A = 1000$ - thus $R \approx 20$, the overhead is $T_p \approx \frac{11}{6} T_e$. If $\epsilon = 1/3$, $T_p < T_e$, even without increasing the tables. With optimal tables, $T_p < T_e$, up to more than 1000 bits.

A standard implementation of our algorithm needs thus less than the time for one additional exponentiation as overhead for a primality proof, for $n \leq 1000$ bits. Compared to that, a Rabin-Miller test with probability of error $< 2^{-48}$ requires three additional exponentiations for 384 bits and two for 600 bits; no values for $n = 1000$ are provided in [BD]. Extrapolating the values from [BD], two Rabin-Miller tests for $n = 1000$ bits will provide an error probability p_e with $2^{-60} < p_e < 2^{-48}$. For primes with more than 1000 bits our algorithm may become more expensive than a pseudoprime algorithm, while keeping the advantage of providing a primality proof. It must be noted that for large primes, the number R of Rabin tests which eliminate composite candidates increases (linearly with n) and the overhead for the primality proof becomes negligible: a good approximation of R is $R(n, A) = \frac{n\ e^{-\gamma} \log 2}{\log A} \approx 0.392 \frac{n}{\log A}$, the logarithm being the natural one. From this and the estimate for the overhead T_p above, it follows,

$$f(n) = \frac{T_p}{R\ T_e} = \frac{\epsilon^4}{1 - \epsilon^4} + \frac{0.392(1-\epsilon)\log A}{n} \approx \frac{1}{80} + \frac{2/3}{n/\log(n)}. \tag{B.3}$$

and $f(n) < 2\%$ for $n > 1000$. Thus AP is never more than 2% slower than probabilistic primes methods, if at all!

B.4 Analysis of the algorithm

This algorithm has two different and independent reasons for producing non uniformly distributed primes. The first is that while searching primes in arithmetical progressions, primes at the end of long gaps are chosen with higher probability. This very phenomenon was investigated by Brandt and Damgard in [BD], for progressions with ratio 2. Their results relay upon the prime r-tuple conjecture of Hardy - Littlewood. This is an asymptotic formula for the number $\pi_{\mathbf{d}}(N)$ of positive integers $n \leq N$ such that $n + d_1, n + d_2, \ldots, n + d_r$ are simultaneously primes. The vector $\mathbf{d}$ is the r-tuple $(d_1, d_2, \ldots, d_r)$. The conjecture says:

$$\pi_{\mathbf{d}}(N) \sim S_{\mathbf{d}}\ \frac{N}{(\log N)^r} \qquad \text{for } N \to \infty. \tag{B.4}$$

with $S_{\mathbf{d}} = \prod_p \frac{p^{r-1}\left(p - \nu_{\mathbf{d}}(p)\right)}{(p-1)^r}$, provided $S_{\mathbf{d}} \neq 0$ and where $\nu_{\mathbf{d}}(p)$ is the number of distinct residue classes modulo p occupied by the numbers in the r-tuple $\mathbf{d}$. Gallagher [Ga] uses this conjecture to prove that:

$$\sum_{\mathbf{d} \in H'} S_{\mathbf{d}} \sim h^r \quad \text{for } h \to \infty \quad \text{where } H' = \{(d_1, d_2, \ldots, d_r) : d \in N, d_i \neq d_j\}. \tag{B.5}$$

In order to use Gallagher's result for primes in arithmetic progressions with ratio F, we must assume the extended Riemann conjecture and $F = o(\sqrt{n})$, for proving the necessary distribution of primes in arithmetic progressions [Da]. With this, Gallagher's result can be generalized to following statement. The number $Q_k(h, N)$ of integers $n < N$ for which the interval $(n, n + hF)$ contains exactly k primes in the progression $1 + tF$ verifies:

$$Q_k(h, N) \sim N\frac{e^{-\lambda}\lambda^k}{k!} \quad \text{for } N \to \infty,\ h \sim \lambda\frac{\varphi(F)}{F}\log N \tag{B.6}$$

and lemma 5 from [BD] can be restated:

Proposition B.2 *Let $G_h(x)$ denote the number of primes p in the progression $1 + tF$, such that $p < x$ and $p - q \leq hF$, where q is the prime preceding p in the progression. Assuming the r-tuple conjecture, the ERH and with $F = o(\sqrt{n})$, for any constant λ,*

$$G_{\lambda\varphi(F)\log(x)/F}\ (x) \ = \ \frac{xF}{\varphi(F)\ \log(x)}(1 - e^{-\lambda}) \cdot (1 + o(1)). \tag{B.7}$$

The factor $\varphi(F)/F$ stems from the fact that $\varphi(F)$ out of F residue classes modulo F contain primes. The proof of this lemma uses (6) and Dirichlet's theorem on distribution of primes in arithmetic progressions [Da]. Let M_k be the set of primes with k bits and for $k \leq B$, let $M'_k = M_k$. For $k > B$, we put: $M'_k = \{p \in M : p = tq+1, q \in M'_{[k/3]+1}\}$. Then M'_k is a subset of the primes that can be produced using AP. Let H''_k be the uncertainty about primes sought in arithmetic progressions by AP and H'_k be the uncertainty of randomly chosen primes in M'_k. Using (7) and methods like in [BD], one can prove that:

$$\frac{H''_k}{H'_k} \sim 1 \quad \text{for } k \to \infty. \tag{B.8}$$

It can also be shown with the same means that the expected length of the seek interval for primes in M'_k is k. This result is not trivial. The average distance between two primes in an arithmetic progression is k, but a prime laying at the end of an "average length interval" is found after only $k/2$ trials, since the starting point of the seek-sequence may lay anywhere between this prime and its predecessor. However, the expected value of the length of the seek interval is not $k/2$ but k and this is a consequence of the fact that primes at the end of longer intervals are chosen with higher probability. So, incidentally, the average number of candidates to be tested for primality is the same in random choice as in progressions, assuming the r-tuple conjecture! In [BDL], this result is stated for incremental search, as an empiric evidence. The paper [BD] provides the tools for such a proof, but does not address the topic. We state a theorem on arithmetic progressions, which contains the empirical result in [BDL] as a sub case, when the ratio of the progression is $F = 2$.

Theorem B.3 *Let $P_k = \{p = \lambda F + u\} \cap M_k$ be the set of k-bit numbers in an arithmetic progression, with $(u, F) = 1$. Assuming the r-tuple conjecture, the extended Riemann conjecture and if $F = o(\sqrt{2}^k)$, then the expected search length for finding a prime by incremental search in P_k, with random starting point is $E(l) = \log(2^k)\frac{\varphi(F)}{F}$.*

Proof Let $l(p) = \frac{p-q}{F}$ be the distance of the prime p to its prime predecessor q in P_k. The probability that a prime p is chosen is $P(p) = \frac{l(p)}{N/(2F)}$: in fact, $l(p)$ out of $N/(2F)$

possible Φstart points lead to the choice of p, so $E(l) = \sum_{p\in P_k} P(p)\frac{l(p)}{2} = \sum_{p\in P_k} \frac{l^2(p)}{N/F}$. Let $\mathbf{L} = \{0 < \lambda_1 < \lambda_2 < \ldots < \lambda_m < \infty\}$ be a partition and k such that the term $o(1)$ in Proposition 2 is $< 1/m^2$. Then

$$E(l) = \sum_{i=0}^{m} \sum_{l\lambda_i < l(p) < l\lambda_{i+1}} \frac{l^2(p)}{N/F} + \sum_{l\lambda_{i+1} < l(p)} \frac{l^2(p)}{N/F}, \quad \text{with } l = \frac{\varphi(F)\log N}{F} \tag{B.9}$$

By Proposition 2, the number of primes with $l\lambda_i < l(p) < l\lambda_{i+1}$ is

$$\frac{NF}{2\varphi(F)\log N}\left(e^{-\lambda_i} - e^{-\lambda_{i+1}}\right)(1+\delta),$$

with $\delta < 2/m^2$. It follows that $E(l) = (\log N)\frac{\varphi(F)}{2F} f(\mathbf{L}) + O(1/m)$, where $f(\mathbf{L})$ is a Riemann sum of the function $h(x) = x^2 e^{-x}$; letting m grow together with k, so that the condition on the error term stays valid, $f(\mathbf{L})$ will converge to the integral $\int_0^\infty f(x) = 2$, which finishes our proof. $\square$

This result needs some comments. It shows that introducing small factors in F will decrease the expected seek length; this seems to suggest a means to reduce the number of pseudoprime tests in our algorithm. However, if $p \mid F$ then $(1+tF, p) = 1$, so p will be ineffective in the trial division stage. Overall, what one gains in the seek interval length, one loses in the trial division. One may thus as well choose F to be a prime and this explains our statement about the expected seek interval.

The second reason for nonuniform distribution is more dramatic: certain primes with n bits are not produced at all (their probability is 0). We finally want to prove that this does not affect the entropy in the sense that the uncertainty about a prime randomly chosen in M'_k is asymptotically equal to the uncertainty of a prime randomly chosen in M_k. For random choice, it is easy to see that the entropy is $H_k = \log(\|M_k\|)$ resp. $H'_k = \log(\|M'_k\|)$. We need to give an estimate of $\|M'_k\|$. By definition, $M'_k = \{p = 2tq+1 | q \in M'_{[k/3]+1}\} \cap M_k$ and it follows that:

$$\frac{2^{\frac{2k}{3}-3}}{k\log 2} \le \frac{\|M'_k\|}{\|M'_{k_1}\|} \le \frac{2^{\frac{2k}{3}-2}}{k\log 2}, \tag{B.10}$$

where $k_i = \left[\frac{k_{i-1}}{3}\right] + 1, k_0 = k, i > 0$. By induction we have: $\frac{k}{3^i} + \frac{1}{2} \le k_i \le \frac{k}{3^i} + \frac{3}{2}$ and we let m be the least index for which $k_m < B$, so that $\|M'_m\| = \frac{2^{k_m - 1}}{k_m \log 2}$. This anchors the recursion and we have, after some manipulations of the above inequalities:

$$\frac{2^k}{(8\log 2\sqrt{3}kB)^m} \le \|M'_k\| \le \frac{2^k}{(2\log 2\sqrt{k}B)^m}. \tag{B.11}$$

By definition of m we have $m = \left[\frac{\log(k/B)}{\log 3}\right] + 1$. Putting $x = 2^k$, (B.11) implies:

$$H'_k = \log x - (\log\log x)^2 \left(\frac{1}{2\log 3} + o(1)\right). \tag{B.12}$$

Since $H_k = \log\left(\frac{x}{2\log x}\right)$, we have a forteriori $\frac{H'_k}{H_k} \sim 1$ for $k \to \infty$; together with (B.10), this yields:

$$\frac{H''_k}{H_k} \sim 1 \qquad \text{for } k \to \infty, \tag{B.13}$$

which is a measure for the distribution of the primes produced by AP.

B.5 Cryptographic Security and Related Topics

It has already been remarked [Ri] that facing recent factorization and discrete logarithm methods, concepts of secure primes like the ones of Gordon [Go] become irrelevant. Actual questions for security of prime generating algorithms remain the following. The distribution of the produced primes, which was measured in the preceding chapter by their entropy. This was shown to be asymptotically equal to the entropy of randomly chosen k-bit primes. The fact that the produced primes are collision free is also a consequence of the above. Finally, the iterated encryption attack for the RSA algorithm seems to suggest that p-1 should have some larger factor ([Ma1]) - although this fact was also relativized by [Ri]. However, cryptography remains a somewhat subjective field. The author of [Sc] has been cited for saying that, while knowing that 'secure primes' are not harder to brake, he would still prefer Gordon primes for the systems he uses. An argument for this attitude may be the fact that algorithms against which Gordon primes offer no additional security may be regarded as more difficult to implement, the crew of possible crackers being thus reduced...

The particularities of AP are particularly favorable for efficient generation of primes with special structure. This can be required in algorithms like the [DSA] or the new signature scheme of Nyberg and Rüppel [NR], which require factors of $p-1$ of fixed length. It is also the case for 'secure primes'.

We end this chapter with an application of AP for finding Gordon strong primes. Let M be a magnitude considered infeasible for algorithms on computers - say, $M = 2^{64}$. We want to produce primes p, such that, there are primes l and l' with: $l \mid (p-1), l' \mid (p+1)$ and $l, l' > M$. Let u_0 and v_0 be the minimal solutions of the equation $vl' - ul = 1$. Following modification in the definition of the progression P, in step 4 of AP gives a solution to the problem: $P = \{N : N = N_0 + \lambda a; N_0 = ta + 2u_0 l + 1; a = 2l \cdot l'; \lambda \geq 0\}$. The choice of t in step 3 must also be adjusted accordingly , so that $t \in \left(\frac{2^{n-1}-2u_0 l}{a}, \frac{2^n-2u_0 l}{a} - sn\right)$ It is easy to verify that a prime in the progression P has the desired properties.

B.6 Performance

The simple version of AP has been implemented on a SUN/IPX machine. It uses sub-optimal table length ($A = 2^{15}$) and naive multiplication. Following table shows the performance of this implementation, with averaged values (over 100 generated primes) for different prime lengths.

n (bits)	**Runtime** (sec)	$r(n) =$ $t(2n)/t(n)$	**Seek Interval**	**Psp tests**	**SeekInt/ log(x)**	**SeekInt/ #Psp.Tests**
256	2.2		173	9.3	0.98	18.6
332	4.0		238	13.0	1.03	18.5
384	7.0		260	14.0	0.98	18.5
512	17.5	8.4	331	17.8	0.93	18.5
664	49.1	11.8	495	26.9	1.07	18.4
768	70.1	11.0	472	25.7	0.89	18.4
1024	213.8	12.2	662	35.7	0.93	18.5

Table B.1: *Performance* **AP**

This table reflects the behavior of predictions in practice. The most stable predicted value, is the ratio (length of the seek - interval)/ (number of pseudoprime tests): it balances around 18.5, whereas the expected value is $\frac{\log A}{e^{-\gamma}} \approx 18.52$. The length of the seek interval also balances around $\log(x)$, but the variance is larger. The $O(n^4)$ behavior of the algorithm is less well reflected, certainly because of the overhead which is independent of the length of the primes found. The ratio $r = t(2n)/t(n)$ - where $t(x)$ is the average time for finding a x-bits prime - has used corrected times, proportional to the relative seek interval. The table reflects a monotonous increase of the apparent specific exponent of the run time. Obviously the data is insufficient and this exponent will approach the expected value 4 for larger primes. Actually this behavior only confirms the known rule that sub quadratic multiplication algorithms are not recommendable for small lengths of the multiplicands.

B.7 Conclusions

We proposed an algorithm for generating provable primes using incremental search in arithmetic progressions. We showed that trial division can be performed using the Eratosthenes sieve method, which increases the number of prime candidates eliminated by the trial division step by an asymptotic factor of 3/2. Independently of the search approach used, we showed that our algorithm is more efficient than probable prime algorithms for primes of at least up to 1000 bits length, whereas for larger primes the loss in efficiency is not more than 2%. The primes produced are always provided with a certificate. The advantages of our algorithm are more substantial when the primes produced are required to have special prime divisors of $p \pm 1$, since this feature can be incorporated for free in the algorithm. The advantages of this algorithm are at the cost of a reduction of the set of primes which can be produced and their nonuniform distribution. We proved though that the information entropy of the primes produced by the algorithm is asymptotically equal to the entropy of randomly chosen primes. We finally presented the performance of a non-optimal implementation of the algorithm on a SUN/IPX machine.

The circle ends where it began.

Who said that?

Appendix C

Classical Lucas - Lehmer tests

The different classical Lucas-Lehmer tests share the feature that no direct reference is made to cyclotomic extensions, and the objects used for testing are certain recurrent sequences rather than explicit elements of extensions. However the recurrent sequences are connected to extensions and explicit elements via their characteristic polynomials. We should also mention that the fact that cyclotomy was never addressed in Lucas-Lehmer tests is surely the reason why information gained from different tests was difficult to combine until Lenstra pointed out the possible connection to the Adleman et al. test ([Le1]). While for actual testing, combining Jacobi-Sum and Lucas-Lehmer tests was described in §4.3.3, the aim of this Appendix is to show that it is possible to generalize Lucas - Lehmer tests in the *classical flavor*, using *recurrent sequences*. We refer to a class of primality tests, which take advantage of the knowledge of factors of $n-1, n^2+n+1, n^2+1$ etc., i.e., of the values that small cyclotomic polynomials take at the point n [WiJu]. Properties of galois fields are implicitly used, while computations are skillfully designed in order to avoid extension fields, by using recursive scalar sequences. We shall attempt to make here an approach which sheds more light into the algebraic background of these methods, while containing them as special cases. This new approach leads to two interesting results which close this appendix. The first is a generalization of Lucas sequences which allow to formulate the general Lucas - Lehmer test 3.42 in terms of recurrent sequences. The second is a generalization of known deterministic tests for numbers of the shape $m \cdot 2^k \cdot 3^l \pm 1$ ([Lu], [BLS], [Mi], etc.) and is based on §4.5.

C.1 Recurrent sequences

Let $\mathbb{K}$ be a field ($\mathbb{K} = \mathbb{Q}$ or $\mathbb{F}_p$, with p a prime) and let $\mathbb{L} = \mathbb{K}[x]/(f(x))$, where $f(x)$ is an irreducible polynomial over $\mathbb{K}$ and $[\mathbb{L} : \mathbb{K}] = s$. Let $g(x) \in \mathbb{L}[x]$, $g(x) = \sum_{i=0}^{k-1} a_i x^i$ and consider the recurrence relations defined over $\mathbb{L}$ by:

$$u_{n+1} = \sum_{j=0}^{k-1} a_j \cdot u_{n-(k-1)+j} \quad \text{for } n \geq k, \text{ and } u_0, u_1, \ldots, u_{k-1} \in \mathbb{L}, \tag{C.1}$$

i.e., the linear recurrence having g as characteristic polynomial. Such recurrence relations were first studied in connection with primality testing by Lucas (although Euler was already aware of some of their properties). In [Lu], $\mathbb{K} = \mathbb{Q}$ and $k = 2$. Lehmer, and then Williams and Judd extended Lucas sequences to the case $\mathbb{L} \neq \mathbb{Q}$, keeping $k = 2$. The case $k = 3$ and $\mathbb{L} = \mathbb{Q}$ was first mentioned by Perrin [Pe] for a special polynomial f and was brought in a more general shape to actuality by Adams and Shanks [AdS]. The interest of recurrent sequences for primality testing results from their periodicity when computed modulo a prime.

Theorem C.2 *Let p be a prime and*

$$\mathbb{K} = \mathbb{F}_p, \mathbb{L} = \mathbb{F}_q = \mathbb{F}_p[x]/(f(x))$$

and $\alpha_1, \alpha_2, \ldots, \alpha_k$, the zeroes of $g(x)$ over a field $\mathbb{M} \supset \mathbb{L}$. Put $l =$ lcm $([\mathbb{L}[\alpha_i] : \mathbb{L}])$, $i = 1, 2, \ldots, k$. Then any sequence defined by (C.1) is periodic over $\mathbb{L}$ and the period τ is a divisor of $p^l - 1$.

Proof Let $a_{k-1}, a_{k-2}, \ldots, a_0$ be the coefficients of g and

$$\mathbf{A} := \begin{pmatrix} a_{k-1} & a_{k-2} & \ldots & a_1 & a_0 \\ 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \ldots & 1 & 0 \end{pmatrix} \tag{C.3}$$

and $\mathbf{u}_n = (u_n, u_{n-1}, \ldots, u_{n-k+1})$. Since $\mathbf{u}_{n+1} = \mathbf{A} \cdot \mathbf{u}_n$, we shall call $\mathbf{A}$ the *shift matrix* associated to (C.1). It is easy to verify by induction that $\mathbf{A}$ has the characteristic polynomial $\chi_{\mathbf{A}}(t) = g(t)$. Since the roots of g are all different, $\mathbf{A}$ may be brought to diagonal form over $\mathbb{M}$:

$$\mathbf{A} = \mathbf{S}^{-1} \cdot \mathbf{D}(\alpha_i) \cdot \mathbf{S}, \tag{C.4}$$

where $\mathbf{D}(\alpha_i)$ is the diagonal matrix, with diagonal entries α_i, $i = 1, 2, \ldots, k$. This leads to:

$$\mathbf{A}^m = \mathbf{S}^{-1} \cdot \mathbf{D}(\alpha_i^m) \cdot \mathbf{S}, \tag{C.5}$$

It follows

$$\mathbf{u}_{m+t} = \mathbf{u}_m, \tag{C.6}$$

for $t = p^l - 1$, $\forall m \in \mathbb{N}$. We still must show that u_n is periodic, that is, that all t satisfying (C.6) are multiples of a smallest one, $\tau \in \mathbb{N}$. Note that (C.6) is equivalent to:

$$\mathbf{A}^t \cdot \mathbf{u}_0 = \mathbf{u}_0, \tag{C.7}$$

Let $T = \{t \in \mathbb{N} : (C.7) \text{ holds}\}$ and $\tau = \min T$. We claim $T = \tau \cdot \mathbb{N}$. The inclusion $T \in t \cdot \mathbb{N}$ is obvious. Suppose, conversely, that $\exists t \in T - \tau \cdot \mathbb{N}$ and $t = s\tau + r$, $r < t$. Then

$$\mathbf{A}^t \cdot \mathbf{u}_0 = \mathbf{u}_0 = (\mathbf{A}^r \cdot \mathbf{A}^{s\tau}) \cdot \mathbf{u}_0 = \mathbf{A}^r \cdot (\mathbf{A}^{s\tau} \cdot \mathbf{u}_0) = \mathbf{A}^r \cdot \mathbf{u}_0,$$

that is, $\mathbf{A}^r \cdot \mathbf{u}_0 = \mathbf{u}_0$, in contradiction to the definition of τ. We know that $p^l - 1 \in T = \tau \cdot \mathbb{N}$ and the assertion of the theorem follows. □

Theorem (C.2) gives a necessary condition for primality, which can be used, provided that methods for the fast computation of the sequence u_n are known. It is in part this requirement which makes that only very few of the cases covered by this theorem are practically studied. En passant, let us mention that a possible-not-so-inefficient method for computing u_n could be the successive squaring of the matrix $\mathbf{A}$. Another important observation is that $p^l - 1$ could be replaced in the statement of the theorem by the exact, but practically incomputable, value of the period τ:

$$\tau = \text{ lcm } (ord_{\mathbb{M}}(\alpha_i)), i = 1, 2, \ldots, k. \tag{C.8}$$

We shall see, when considering generalized Lucas sequences, that the difference from a pseudoprime to a prime test is essentially depending upon the choice of a sequence - resp. a polynomial $g(x)$ - such that the eigenvalues α_i of the matrix (C.3) have "high" order over $\mathbb{M}$. Essentially, the idea of theorem (C.2) is found also in [AdS], in the main theorem 3 of §13. This article deviates however from the other ones using recursive sequences by the fact that pseudoprimality is considered by rather qualitative arguments and no explicit statement is found, as to sufficient conditions for primality. If that were the case it would be natural to expect that knowledge of some large factored part of $n^2 + n + 1$ should be necessary. We shall quit now the general treatment and consider the case $k = 2$ (Lucas sequences, and generalizations thereof).

C.2 Generalized Lucas-Lehmer sequences

When $\mathbb{L}, \mathbb{K}$ and f are like in the previous section and $g(x) = x^2 - P \cdot x + Q$, the Lucas-Lehmer sequences u_n and v_n are defined by the recurrence

$$z_{n+1} = P \cdot z_n - Q \cdot z_{n-1} \qquad (z = u \text{ or } v) \tag{C.9}$$

with the initial conditions :

$$\begin{array}{ll} u_1 = 1; \quad u_2 = P & \qquad \text{and} \\ v_1 = P; \quad v_2 = P^2 - 2 \cdot Q. & \end{array} \tag{C.10}$$

The sequences u_n and v_n are related to the zeroes α and β of $g(x)$ by:

$$\begin{array}{rcll} u_n &=& (\alpha^n - \beta^n)/(\alpha - \beta) & \qquad \text{and} \\ v_n &=& \alpha^n + \beta^n. & \end{array} \tag{C.11}$$

For both sequences, the associated shift matrix is

$$A = \begin{pmatrix} P & -Q \\ 1 & 0 \end{pmatrix}$$

and one can prove by induction on m ([Mi]), that:

$$A^m = \begin{pmatrix} u_{m+1} & -Q \cdot u_m \\ u_m & -Q \cdot u_{m-1} \end{pmatrix} \tag{C.12}$$

where $u_0 := 0$.

Let $\mathbb{L}$ be again a galois field $\mathbb{F}_q = \mathbb{F}_{p^s}$, with $(p, P \cdot Q) = 1$ and let $\Delta = P^2 - 4 \cdot Q$ throughout this section. From (C.12), one reads that $u_n = 0 \leftrightarrow u_{n+1} = -Q \cdot u_{n-1} \leftrightarrow \mathbf{A}^n = -Q \cdot u_{n-1} \cdot \mathbf{I}$. Let $T_p = \{n \mid u_n = 0 \bmod p\}$.

Theorem C.13 *The set $T_p = \tau_p \cdot \mathbb{N}$, where τ_p is the order of $\mathbf{A}$ in the projective group $GL_2(\mathbb{L})/\mathbb{L}^*$. If z_n is one of u_n or v_n, we call τ_p the "pseudoperiod" of z_n, meaning that*

$$z_{n+\tau \cdot s} = (-Q \cdot u_{n-1})^s \cdot z_n. \tag{C.14}$$

The sequence z_n is periodic, with period $\tau_p \cdot \mathrm{ord}_{\mathbb{L}}(-Q \cdot u_{\tau-1})$.

Proof We showed that $u_n = 0 \leftrightarrow \mathbf{A}^n = -Q \cdot u_{n-1} \cdot \mathbf{I}$, which means that $\mathbf{A}^n$ is the unity in $GL_2(\mathbb{L})/\mathbb{L}^*$. On the other hand, if $\mathbf{A}^n = \lambda \cdot \mathbf{I}$, (C.12) implies that $u_n = 0$. Hence $T_p = \{n \mid \mathbf{A}^n = \lambda \cdot \mathbf{I}\}$ and by definition of τ_p, one has $T_p = \tau_p \cdot \mathbb{N}$. Equation (C.14) follows by induction, and the periodicity of z_n follows from (C.14) and the definition of $\mathrm{ord}_{\mathbb{L}}(-Q \cdot u_{\tau-1})$. □

Let (p/q) be the Legendre symbol and define $\epsilon(P, Q)$ by:

$$\epsilon(P, Q) := \begin{cases} +1 & \text{if } \Delta \text{ is a square in } \mathbb{L} \\ -1 & \text{else} \end{cases}$$

If $\mathbb{L} = \mathbb{F}_p$, $\epsilon(P, Q) = (\Delta/p)$. Using again the diagonal form of $\mathbf{A}$, one can make sharper statements on τ_p.

Theorem C.15 *(i) If $\epsilon(P, Q) = -1$, then $\tau_p = \mathrm{ord}_C(\alpha) = \mathrm{ord}_C(\beta)$, where C is the cyclic multiplicative group $\mathbb{L}[\Delta]/\mathbb{L}^*$.*

(ii) If $\epsilon(P, Q) = 1$, then $\tau_p = \mathrm{ord}_{\mathbb{L}}(\alpha/\beta)$.

(iii) In both cases,

$$\tau_p \mid (p^s - \epsilon(P, Q)), \text{ where } s = [\mathbb{L} : \mathbb{K}]. \tag{C.16}$$

Proof Suppose $\epsilon(P, Q) = -1$ and put $\tau = \mathrm{ord}_C(\alpha)$. Then α and β are conjugates over $\mathbb{L}$, and so are α^τ and β^τ; since $\alpha^\tau \in \mathbb{L}^*$, by definition of τ, it follows that $\beta^\tau \in \mathbb{L}^*$ and $\alpha^\tau = \beta^\tau$. Using (A.3), $\mathbf{A}^\tau = \lambda \cdot \mathbf{I}$, for $\lambda = \alpha^\tau \in \mathbb{L}^*$. This proves $\tau \in T_p$.

Conversely, (ii) can be proved similarly, after writing $\mathbf{A} = \beta \cdot \mathbf{S}^{-1}\mathbf{D}(\alpha/\beta, 1) \cdot \mathbf{S}$. Point (iii) follows from the fact that both C and $\mathbb{L}^*$ are cyclic of order $p^s - \epsilon(P, Q)$. □

We wish to extend now our results on the periodicity of z_n to a not necessarily prime module $m \in \mathbb{Z}$, $(m, P \cdot Q \cdot \Delta) = 1$. The first step consists in considering $m = p^t$ for some $t > 1$.

Lemma C.17 *Let $u_n(P,Q)$ be a Lucas-Lehmer sequence. If $p^t \parallel u_n$ for some $n \in \mathbb{N}$ and $t \geq 1$, then $p^{t+1} \parallel u_{np}$.*

Proof The relation $p^t \parallel u_n$ can be written as $u_n = \lambda p^t, (\lambda, p) = 1$, and by introducing this relation in (C.12), one has :

$$A^n = \begin{pmatrix} P \cdot \lambda \cdot p^t - Q \cdot u_{n-1} & -\lambda \cdot Q \cdot p^t \\ \lambda \cdot p^t & -Q \cdot u_{n-1} \end{pmatrix} = \lambda \cdot p^t \cdot A + \mu \cdot I$$

with $\mu = -Q \cdot u_{n-1}$. Direct computation for $\mathbf{A}^{n \cdot p}$ gives:

$$\begin{aligned} \mathbf{A}^{n \cdot p} &= (\lambda p^t \cdot \mathbf{A} + \mu \cdot \mathbf{I})^p = \sum_{k=0}^{p} \binom{p}{k} \cdot (\lambda p^t)^k \cdot \mu^{p-k} \cdot \mathbf{A}^k \\ &= \mu^p \cdot \mathbf{I} + \lambda p^{t+1} \mu^{p-1} \cdot \mathbf{A} + \sum_{k=2}^{p} \binom{p}{k} \cdot (\lambda p^t)^k \cdot \mu^{p-k} \cdot \mathbf{A}^k \end{aligned}$$

Since the last sum allows the factor p^{2t+1} and $(\lambda \mu^{p-1}, p) = 1$, it follows that

$$p^{t+1} \parallel (\mathbf{A}^{np} - \mu^p \cdot \mathbf{I})$$

in the sense that $t+1$ is the highest power of p that divides all elements of the right-hand matrix. Using again (C.12), one has a forteriori $p^{t+1} \parallel u_{np}$. □

Put $\psi(p^t) = p^{t-1} \cdot (p^s - \epsilon(P,Q))$ for p prime, $t \geq 1$. This definition induces a multiplicative function ψ over $\mathbb{N}$; this function is called the Lucas *totient* and is a generalization of Euler's totient function φ to Lucas sequences.

By theorem (C.15) and this lemma, one obtains a general result, which is the main theorem on modular Lucas-Lehmer sequences:

Theorem C.18 *Let $m \in \mathbb{N}$ and $u_n(P,Q)$ be a Lucas-Lehmer sequence, $(m, PQ\Delta) = 1$. Then $u_{\psi(m)} = 0 \bmod m$.*

Proof For m prime, the result follows from Theorem (C.2), and for m a prime-power, it is a consequence of lemma (C.17). The general statement is then proved by applying the Chinese Remainder Theorem. □

We restrict once more our premises to $\mathbb{L} = \mathbb{Q}$ or $\mathbb{F}_p$, in order to state some classical results on Lucas sequences. In this simple cases, two requirements which are specific for the whole class of tests discussed in this section, will appear clearly, i.e.:

(A) Knowing a large factored part of $n^s - 1$, $(s = 1, 2, 3, 4, 6, 8...)$.

(B) Knowing an element of fixed large order, for each prime dividing this factored part, in a suitable extension of $(\mathbb{Z}/n \cdot \mathbb{Z})$.

The Lucas sequences are simply computable, due to following addition and doubling formulae:

$$\begin{aligned} u_{2n} &= u_n \cdot v_n; \qquad u_{m+n} = u_m \cdot v_n + Q^m \cdot u_{n-m} \quad (n > m) \\ v_{2n} &= v_n^2 - 2Q_n; \qquad v_{n+m} = v_n \cdot v_m - Q^m \cdot v_{n-m} \quad (n > m) \end{aligned} \tag{C.19}$$

For the special sequence $u_n(2, -2)$, one has

$$v_{2^n} = 2^{2^n}(r_n - 2), \quad \text{where } r_1 = 4 \text{ and } r_{n+1} = r_n^2 - 2. \tag{C.20}$$

This sequence was used by Lucas for testing Mersenne numbers $M_p = 2^p - 1$, with p prime – it is easy to see that $M_n = 2^n - 1$ can be factored algebraically, for composite n. Using quadratic reciprocity, one can prove that for those M_p which are prime,

a) $(\Delta/M_p) = -1$, showing that $\psi(M_p) = M_p + 1$, and

b) $(Q/M_p) = -1$, showing that these sequences have the pseudo period $\tau = 2^p$.

This leads to following primality criterion for Mersenne numbers :

Theorem C.21 *The Mersenne number M_p is prime iff in the sequence r_n mod M_p defined in (C.19), the first and only occurring* 0 *has index $p - 1$.*

Proof By b), $u_{2^p} = 0$ and $u_{2^{p-1}} \neq 0 \bmod M_p$ and using (C.19), $v_{2^{p-1}} = 0$ and $v_{2^k} \neq 0 \bmod M_p, \quad \forall k < p - 1$. □

More general tests can be obtained, with following Lemma, attributed to Pocklington, and proved before by Lucas [Lu]:

Lemma C.22 (Lucas-Pocklington) *Let $n \in \mathbb{N}, p$ be a prime with $p \mid (n + 1)$ and suppose there is a Lucas sequence $u_n(P, Q)$ with $(\Delta/n) = -1$ and $(\Delta \cdot P \cdot Q, n) = 1$, such that:*

$$u_{n+1} = 0 \ \mathit{mod}\ n \quad \mathit{and} \quad (u_{(n+1)/p}, n) = 1 \tag{C.23}$$

Then, all primes $r \mid n$ are of the shape $r = \lambda p \pm 1$.

Proof If $r \mid n$, from the hypothesis, we have $u_{n+1} = 0 \bmod r$ and $u_{(n+1)/p} \neq 0 \bmod r$. Hence, $p \mid \tau_r \mid (r - (\Delta/r))$, and finally, $r = \lambda \cdot p + (\Delta/r) = \lambda \cdot p \pm 1$. □

This lemma has a similar statement to theorem (3.35), which states that all primes $r \mid n$ are of the shape $r = \lambda p + \epsilon$ where $\epsilon = n^i \bmod p$. It also shows the necessity of knowing primitive roots for testing, since the sequence fulfilling (C.23) may be induced by a polynomial $g(x)$ whose roots are primitive of order p in $(\mathbb{Z}/n \cdot \mathbb{Z})[x]/(g(x))$. This to (A). Argument (B) is made clear by the following

Theorem C.24 (Morrison – [Mo]) *Let $n = F_2 \cdot R_2$, where F_2 is completely factored. Suppose further, that for each $p \mid F_2$ there is a Lucas sequence $u_n(P, Q)$ with $(\Delta, n) = -1$, such that (C.23) holds. Then all primes $r \mid n$ are of the shape $r = \lambda \cdot F_2 \pm 1$.*

Proof The relation (C.23) implies that $p^\beta \mid \tau_r \ \forall p \mid F_2$ with $p^\beta \parallel F_2$ and since $\tau_r \mid (r - \epsilon_r)$, finally, $p^\beta \mid (r - \epsilon_r) \ \forall p \mid F_2$ and consequently $F_2 \mid (r - \epsilon_r)$. □

A direct consequence of Theorem (C.24) is:

Lemma C.25 *If the premises of Theorem (C.24) hold and $F_2 > \sqrt{n} + 1$, then n is prime.*

Proof According to theorem (C.24) all primes $r \mid n$ are divisible by $F_2 - 1 > \sqrt{n}$, which is only possible if n is a prime. □

More refined results, using only a factored part of $O(n^{1/3})$ or even less, are developed in [BLS], by using

a) The fact that if n is not a prime, it splits into a product of at least two primes of the shape $\lambda \cdot F_2 \pm 1$, and

b) If all the prime factors of $n \pm 1$ are computed up to a certain constant B, the least unknown prime dividing R_2 is $> B$.

For combined factors of $n \pm 1$ (that is, factors of $n^2 - 1$), the requirement for the factored part is pushed in the same paper down to $O(n^{2/9})$. Such techniques, which are successful for factors of $n^2 - 1$ seem to grow fast in complexity for the case of cyclotomy tests, where factors of higher values of cyclotomic polynomials at n are used. However, it has been possible to reduce the requirement on s in the Jacobi-Sum test, down to $O(n^{1/3})$ [Le4]. On the other hand, in [WiJu], where generalized Lucas-Lehmer sequences (using polynomials $f(x)$ of degree 3 and $g(x)$ of degree 2) are used in order to take advantage of factors of $n^2 \pm n + 1$, the required factored part of either one or the other cyclotomic polynomial in n is $n^{2/3}$, and no theorems using mixed factors of $n^6 - 1$ are stated. As to remark (B), note that the "Lucas - Pocklington" lemma (C.22) gives a sufficient condition for $\Phi_p(x)$ correctly splitting modulo n:

Lemma C.26 *Suppose the premises of lemma (C.22) hold, and $Q^{n-1} = 1 \bmod n$. Then there exists an $\omega \in (\mathbb{Z}/n \cdot \mathbb{Z})[\Delta]$, such that $\Psi_p(x) = (x^2 - (\omega + \omega^{-1}) \cdot x + 1) \mid \Phi_p(x)$ over $(\mathbb{Z}/n \cdot \mathbb{Z})$.*

Proof Let u_n be a sequence for which (C.23) holds and α, α^* be the roots of its characteristic polynomial $g(x)$. Put $\omega = \alpha^{(n^2-1)/p}$. It follows from theorem (C.13) and lemma (C.22) that $\alpha^{n+1} \in (\mathbb{Z}/n \cdot \mathbb{Z})$ and $\alpha^{(n+1)/p} \notin (\mathbb{Z}/n \cdot \mathbb{Z})$.

Putting $a = \alpha^{n+1} = (\alpha^*)^{n+1} \in (\mathbb{Z}/n \cdot \mathbb{Z})$, and by using $\alpha \cdot \alpha^* = Q$ we get $a^2 = Q^{n+1}$ and $a^{n-1} = Q^{(n+1)(n-1)/2} = (Q^{n-1})^{(n+1)/2} = 1 \bmod n$ hence $\omega^p = 1 \bmod n$. If $\omega = 1$, then $u_{(n^2-1)/p} = 0 \bmod n$ and by theorem (C.13) $u_m = 0$, for $m = (n+1, (n^2-1)/p)$. Since p is a divisor of $n+1$, it does not divide $n-1$ and consequently $m = (n+1)/p$, which is a contradiction to the hypothesis. Consequently, ω is a primitive p -th root of unity in $(\mathbb{Z}/n \cdot \mathbb{Z})[\Delta]$. We still want to show that $\omega^{-1} = \omega^*$. This assertion follows from $\omega^* = (\alpha^*)^{(n^2-1)/p}$ and $\omega \cdot \omega^* = (\alpha \cdot \alpha^*)^{(n^2-1)/p} = (Q^{n-1})^{(n+1)/2p} = 1$, showing that $\omega + \omega^{-1} \in (\mathbb{Z}/n \cdot \mathbb{Z})$ and $\Psi_p(x) \in (\mathbb{Z}/n \cdot \mathbb{Z})[x]$. The lemma now follows from theorem (3.36). □

According to chapter 4, we prove the existence of a cyclotomic extension of prime power order p^k over $\mathbb{N}$, by checking 4.15 in a certain extension $\mathbf{R}$ of $\mathbb{N}$ and implicitly proving the existence of a factor $\Psi_p(x) \mid \Phi_p(x)$ of order $t(s)$ over $\mathbb{N}$.

We conclude this classical excursion by giving a natural generalization of Lucas sequences which allows to state the Lucas-Lehmer tests (3.45) in terms of linear recurrences.

Definition C.27 *Let $\mathbb{L}$ be a field of conductor s with $[\mathbb{L} : \mathbb{Q}] = t$, such that $(t, s) = 1$ and $Gal\,(\mathbb{L}/\mathbb{Q}) = < n \bmod s >$; let $\rho \in \mathbb{C}$ be a primitive t-th root of unity, $g(x) \in \mathbb{Z}[x]$ an irreducible monic polynomial of degree t, which completely splits in $\mathbb{L}$ and $\mathbf{R} = O(\mathbb{L})/n \cdot O(\mathbb{L})$. Let α_i, $i = 1, 2, \ldots, t$ be the zeroes of $g(x)$ in $\mathbb{L}$, numbered such that $\alpha_{i+1} = \psi_n(\alpha_i)$, circularly. The generalized Lucas sequences $u_j(m)$ are defined for $j = 1, 2, \ldots, t$:*

$$u_j(m) = \frac{\sum_{i=1}^{t} \rho^{ij} \cdot \alpha_i^m}{\sum_{i=1}^{t} \rho^{ij} \cdot \alpha_i} \tag{C.28}$$

Obviously, all $u_j(m)$ satisfy the same linear recurrence, with $g(x)$ as characteristic polynomial, while the initial values differ. The denominator has the effect of norming the sequences so that they take values in $\mathbb{Z}[\rho]$ or some t-th cyclotomic extension. This is a consequence of $u_j(m)$ being invariant under cyclic permutations of the α_i.

With this definition we are able to translate (3.45) in terms of recurrent sequences:

Theorem C.29 *Let the notations be the same as in the definition (C.27). Suppose that*

$$u_j(n) = \rho^{-j} \bmod n \quad \text{for } j = 1, 2, \ldots, t \tag{C.30}$$

and

$$\forall p \mid s, \quad \exists j \ : \ u_j(n^t - 1) = 0 \bmod n \ \text{ and } (u_j\Big(\frac{n^t-1}{p}\Big), n) = 1. \tag{C.31}$$

Then an s-th cyclotomic extension of $\mathcal{N}$ exists.

Proof The initial values $u_j(1)$ are Lagrange resolvents and (C.30) shows that $\psi_n(\alpha_i) = \alpha_i^n$, where ψ_n is the Artin symbol. Indeed, writing the t equations in (C.30) out as a linear system, it is a common exercise with Lagrange resolvents, to prove that this system has precisely the circular solution $\alpha_i^n = \alpha_{i+1}$ and thus $\alpha_i^n = \psi_n(\alpha_i)$, so that (3.46) is fulfilled. Furthermore, (C.31) implies (3.47) and the statement follows by theorem (3.45). $\square$

Remark C.32 *Theorem (C.29) is not meant to have practical significance, since matrix multiplication is more expensive then multiplication in field extensions of the same rank. It is however interesting since it shows in a most accurate way, how close modern cyclotomy tests are to Lucas's initial ideas. In fact, by putting $t = 2$ in definition (C.27) we find exactly the Lucas sequences u_n and v_n and (C.30) is then the Lucas test.*

We finally wish to consider primality tests for numbers of the shape

$$N = 2^{e_0} \cdot 3^{e_1} \cdot 5^{e_2} \dots p_k^{e_k} \cdot F \pm 1$$

where p_k is the $k-$th prime and $F < \sqrt{N}$. The case $k = 1$ was treated in [Mi], so let us assume $k \geq 2$. According to Morrison's theorem (C.24), it suffices to find p_i-th non residues for $i = 0, 1, \dots, k$. According to §4.5, this again can be done, provided a quadratic non residues. We shall assume $e_0 > 1$. For $N = F \cdot \prod_i p_i^{e_i} + 1$, the number 3 is a quadratic non residues; for $N = F \cdot \prod_i p_i^{e_i} - 1$, 5 is a quadratic non residues. This facts can be easily verified by quadratic reciprocity. Using the second construction in §4.5, p_i-th non residues can now be constructed for $i = 1, 2, \dots, k$ and used for proving the primality of N by the Morrison theorem.

This test sketch closes the classical excursion to Lucas sequences.

Index

Bibliography

[AdLe] L.M.Adleman, H.W.Lenstra, Jr., Finding irreducible polynomials over finite fields, Proc. 18-th Ann. ACM Symp. on Theory of Computing (STOC) 1986, pp. 350-355

[AdS] W.Adams, D.Shanks: Strong Primality Tests That are not Sufficient; Math. Comp. Vol. 39, Nr. 159, July 1982, pp. 255-300.

[AH] L.M.Adleman, M.A.Huang, Recognizing primes in random polynomial time, Research report, Dept. of Computer Science, Univ. of Southern California, 1988. Extended abstract: Proc. 19-th Ann ACM Symp. on Theory of Computing (STOC) 1987, pp. 462-469

[ARP] L.M. Adleman, C. Pomerance, R.S. Rumely: On distinguishing prime numbers from composite numbers

[AtMo] A.O.L. Atkin, F.Morain: "Elliptic curves and Primality Proving.", Math. Comp., **vol 61**, 1993, pp. 29-68.

[AMM] L.Adleman, G.Miller, K.Manders; On taking roots in finite fields; Proc. 18-th IEEE Symp. on Foundations of Computer Science (1977), pp. 175-178.

[Ba1] E.Bach: "Realistic analysis of some randomized algorithms", Proc. 19-th Ann ACM Symp. on Theory of Computing (STOC) 1987, pp. 453-461

[Ba2] E.Bach: "Explicit Bounds for Primality Testing and Related Problems", Math. Comp. 55 (1990) pp. 355-380

[BaS] E.Bach; J.Shallit: "Algorithmic Number Theory", foundation of computer science series, MIT Press, 1996.

[BBS] L.Blum, M.Blum, M.Shub: "A Simple Unpredictable Pseudo - Random Number Generator", SIAM Journal on Computing, v. 15, n. 2, 1986, pp. 364-83.

[Bb] Bleichenbacher,D., PhD Thesis under development at ETH, Zürich

[BD] Brandt, J; Damgard, I: On Generation of Probable Primes by Incremental Search, Proc. of Crypto 92

[BDL] Brandt, J; Damgard I; Landrock, P: Speeding up Prime Number Generation, Proc. of Asiacrypt 91, Springer Verlag Lecture Notes.

[BDP] Damgard I; Landrock, P; Pomerance, C.: Average Case Bounds for the Strong Probable Prime Test, Math. Comp. Vol.61, no.203, pp.177-194.

[Bl1] Blahut,R.: Fast Algorithm for Digital Signal Processing, Addison Wesley, 1987.

[Bl2] Blahut,R.: Theory and Practice of Error Correcting Codes, Addison Wesley, 1983.

[BLS] J.Brillhart, D.H.Lehmer, J.L.Selfridge: New Primality Criteria and Factorization of $2^m \pm 1$, Math. of Comp., Vol. 29, Number 130, April 1975, pp. 620-647.

[Bo] W.Bosma, Primality testing using elliptic curves, Research Report 85-12, University of Amsterdam

[BovdH] W.Bosma and M.van der Hulst: Primality proving with cyclotomy, Thesis, Universiteit van Amsterdam 1990.

[CERTS] //ftp:ftp.lagaffe.inf.ethz.ch/pub/CYCLO/CERTS

[Ch] K.Chandrasekharan: Einführung in die analytische Zahlentheorie, Springer 1966

[Co] Cook, S.A.: On the Minimum Computation Time of Functions, Thesis, Harvard University, 1966.

[H.Cohn] H.Cohn: A Classical Invitation to Algebraic Numbers and Class Fields, pp 34-45, Springer, 1978

[CoLe] H.Cohen, H.W.Lenstra Jr.: Primality Testing and Jacobi sums, Math. Comp. 1984, pp 297-330.

[Cox] Cox, David A.: "Primes of the Form $x^2 + ny^2$", Wiley & Sons, 1989

[CQ] Couvreur, C; Quisquater, J.J.: An introduction to fast generation of large primes, Philips Journal of Research, vol. 37, pp 231-264, 1982

Plenum Press, New York and London 1990.

[CrFa] Crandal, R; Fagin, B.: Mathematics of Computation **62** (205) 1994, pp. 305-324.

[Da] Davenport, Harold: Multiplicative Number Theory, Springer 1980, Second Edtion.

[DSA] National Institute of Standards and Technology, NIST FIPS PUB 186, "Discrete Signature Standard", US Department of Commerce, Feb. 94

[DLP] Damgard, I.; Landrock, P.; Pomerance, C: Average Case Bounds for the Strong Probable Prime Test, Math.Comp., Vol61, Oct. 1993, pp 177-195.

[ECPP] http://lix.polytechnique.fr/ morain/Prgms/ecpp.francais.html, Site for downloading the elliptic curve primality test software of F.Morain.

[Ed] H.M. Edwards: Galois Theory, Springer 1984

[Ga] Gallagher, P.X.: On the distribution of primes in short interevals, Mathematika, vol. 23, 1976, pp. 4-9

[GIMPS] Great Mersenne Internet Prime Search, http://www.utm.edu/research/primes

[GoKi] S.Goldwasser, J.Kilian: Almost all primes can be quickly certified. Proc. 18-th Annual ACM Symp. on Theory of Computing (1986), 316-329.

[Go] Gordon, J.: Strong primes are easy to find, Advances in Cryptology - EUROCRYPT '84, Lecture Notes in Computer Science, vol. 209, 1984, pp. 216-223.

[Hu1] Huang, M.A.: Factorization fo polynomials over finite fields and factorization of primes in algebraic number fields; Proc. 16-th ACM Symp. on Theory of Computing (1984), pp. 175-182

[Hu2] Huang, M.A.: Riemann Hypothesis and finding roots over finite fields; Proc. 17-th ACM Symp. on Theory of Computing (1985), pp. 121-130.

[IR] Ireland, Kenneth.; Rosen, Michael.: "A Classical Introduction to Modern Number Theory", Second Edition, Springer Graduate Texts in Mathematics 84, 1990

[JSWW] Jones,P.J.; Sato,D. : Wada,H. ; Wiens,D : "Diophantine representation of the set of prime numbers", Amer.Math.Monthly, Vol 83 (1976), pp. 449-164.

[Ka] Kannan,R.: Minkowski's convex body theorem and integer programming; Math. of op. research, Vol. 12, Nr. 3, Aug. 1987, pp. 415-440

[Kn] D.E.Knuth: The art of computer programming, Vol.2, Seminumerical algorithms, Addison-Wesley, Reading, Mass. second edition, 1981.

[Ku] Kurosh: Cours d'algebre superieure, pp 347-348, MIR Editeurs, 1964

[La1] S.Lang: Algebraic Number Theory, Chapter IV , Addison Wesley Series in Mathematics.

[La2] S.Lang: Cyclotomic Fields, Chapter I, Springer 1978

[LeMa] Leyland, P and Mayer,E.: personal communication.

[Le1] H.W.Lenstra Jr.: (Title) Lectures Notes in Mathematics, Vol 901, pp 243-258

[Le2] H.W.Lenstra Jr.: Galois theory and primality testing, Lecture Notes in Mathematics, Vol 1142, Springer

[Le3] H.W.Lenstra Jr.: Euclid's Algorithm in Cyclotomic Fields, J. London Math. Soc. (2) 10 (1975) pp. 457-465.

[Le4] H.W.Lenstra Jr.: Divisors in residue classes, Math. Comp. 1984, pp 331-334.

[Le5] Lenstra, H.W.: Factoring Integers With Elliptic Curves, Annals of Mathematics, Vol. 126, 1987, pp649-673.

[LiDIA] LiDIA Group: "LiDIA - A library for computational number theory", TH Darmstadt, Germany, 1996

[Lh] D.H.Lehmer: Computer technology applied to the theory of numbers, MAA Studies in Mathematics.

[LL] Lenstra, A.K. and Lenstra, H.W.,Jr.: Algorithms in number theory, Technical Report 87-008, May 1987, University of Chicago, Dept. of Computer Science.

[LLL] A.K.Lenstra; H.W.Lenstra Jr.; L.Lovasz: "Factoring Polynomials with Rational Coefficients", Mathematische Annalen, v. 261, n.4, 1982, pp. 515-34.

[Lo] R.Long: Algebraic number Theory, Marcel Dekker, New York and Basel, 1977.

[Lu] E.Lucas: Theorie des fonctions numeriques simplement periodiques, Amer. J. of Math., Vol 1 1878, pp 184-240 and 289-321.

[Ma] Matijasevic,Y.V.: " Primes are nonnegative values of a polynomial in 10 variables", J. Soviet. Math. vol 15 (1981), pp. 33-44.

[Ma1] Maurer, Ueli M.: Fast Generation of Prime Numbers and Secure Public-Key Cryptographic Parameters, Internal Report, Dept. of Comp. Science, Princeton University, 1991.

[Ma2] Maurer, Ueli M.: Fast Generation of Prime Numbers and Secure Public-Key Cryptographic Parameters, Internal Report, Dept. Informatik, ETH Zürich, 1993.

[May] Mayer, E., personal communication.

[Me] Menezes, Alfred J.: "Elliptic Curve Public Key Cryptosystems", Kluwer Academic Publishers, 1993.

[MeD] Mersenne Digest, Volume 1, Number 179, 19 June 1997.

[MF] Freeware for the Great Internet Mersenne Prime Search, http://fractal.mta.ca/prime/freeware/M3

[Mg] Montgomery, P.: Modular Multiplication without Trial Division, Math. Comp. 44 (1985) 519-521.

[Mi] P.Mihăilescu, Folgen von Lucas und deren Anwendungen in Primheitsteste, Diplomarbeit ETH, 1981.

[Mi1] P.Mihăilescu, Fast Generation of Provable Primes Using Search in Arithmetic Progressions, Proceedings CRYPTO94, pp. 282-293.

[MM] Myer, E; Morain, F.: posting to the number theory list, 10/30/1997.

[Mo90] Morain, F.: Distributed primality proving and the primality of $(2^3539 + 1)/3$, Advances in Cryptology, EUROCRYPT '90, Lecture Notes in Computer Science, vol. 473, 1990, pp. 110-123.

[Mo] M.A.Morrison: A note on primality testing using Lucas sequences, Math. Comp. 29 (1975), 181-182.

[NR] Nyberg,K; Rüppel,R:A New Signature Scheme Based on the DSA Giving Message Recovery, Preprint, 1993.

[Ono] T. Ono: An Introduction to Algebraic Number Theory,

[PARI] The PARI library, written at the Universite de Bordeaux, internet.

[Pe] Perrin, R.:"Item 1484", L'intrmdiare des Math., vol. 6, 1899, pp 76-77.

[Pl] Plaisted, D. A.: Fast verification, testing and generation of large primes, Theoretical Computer Science, vol 9, 1979, pp. 1-17.

[Po] Pollard, J.M.:Theorems on factorization and primality testing, Proceedings of the Cambridge Philosophical society, Vol. 76, 1974, pp. 521-528.

[Ra] M.O.Rabin: Probabilistic algorithms in finite fields , SIAM J.Comput. Vol 9, May 1980, pp. 273-280

[Ri] H.Riesel: Prime Numbers and Computer Methods for Factorization, Birkhäuser, 1994

[Ro] Ronyai, L: Factoring Polynomials over Finite Fields, Computer and Automation Institute, Hungarian Academy of Sciences, 1987.

[RSA] Rivest, R.L., Shamir, A., Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM, Vol. 21, No. 2, 1978, pp.120-126.

[Sc] Schneier, B.: Applied Cryptography, Wiley & Sons, 1993

[ScSt] Schönhage, A.; Strassen, V.: Schnelle Multiplikation grosser Zahlen, Computing 7 (1971), 281 - 292.

[Sch] Schoof, R: "Elliptic Curves over Finite Fields and the Computation of Square Roots mod p", Mathematics of Computation, Vol. 44, Vol. 44 (1985), pp. 483-494.

[Se] J.-P. Serre: Cours d'arithmetique.

[Sh] Schoof,R: Elliptic Curves over Finite Fields and the Computation of Square Roots mod p, Math. Comp. 43 (1985), 483-494.

[Sho] V.Shoup: New Algorithms for Finding Irreducible Polynomials over Finite Fields; Proc. 29-th IEEE Symp. on Foundations of Computer Science (1988), pp. 283-290.

[Sh2] V. Shoup: Modular polynomial arithmetic implemented in the LiDIA library.

[SoSt] R.Solovay, V.Strassen: A fast Monte Carlo test for primality, SIAM J.Comput. 6 (1977), 84-85.

[To] Toom,A.L.: Doklady Akad. Nauk SSSR 150 (1963), 496-498.

[Vd] A.T.Vandermonde: Memoire sur la resolution des equations, german transl. in : Abhandlungen aus der reinen Mathematik von Vandermonde, Springer 1888.

[vdW] B.L.van der Waerden: Algebra I, 56, Springer

[VO] Vanstone,S;van Oorschot,P: An Introduction to Error Correcting Codes with Applications, Kluwer Academic Publishers, 1989

[We] A.E Western: On Lucas and Pepin's Test for Primeness of Mersenne Numbers, Journal of the London Math. Society, vol 7/I 1932

[Wi] H.C.Williams: Primality testing on a computer , Ars Combin. 5 (1978), pp 127-185.

[WiJu] H.C.Williams, J.S.Judd: Some algorithms for prime testing, using generalized Lehmer functions, Math. Comp. 30 (1976), 867-886.

[WiZa] H.C.Williams, C.R.Zarnke: Some Prime Numbers of the Forms $2A3^n + 1$ and $2A3^n - 1$, Mathematics of Computation, Vol. 26 Nr. 120, October 1972, pp. 995-998.

[Wn] Winogradow, S. :On Computing the Discrete Fourier Transform, Math. Comp. 32 (1978) pp. 175-199.

[Zip] Zippel, R: "Effective Polynomial Computation", Kluwer Academic Publishers, 1993

Curriculum Vitae

I was born on May 23rd, 1955 in Bucharest. In 1956 Chruschtchow launched destalinization. In 1959 I was inadvertently allowing street friends to cover expenses by betting on my ability to perform three digits multiplications mentally. In 1964 came the big amnesty for political prisoners and the number of relatives increased.

I followed and almost finished my schools in Bucharest. Along with mentally disabling subjects like scientific socialism, I had the privilege of practicing mathematics during four years as an Olympic discipline – in the sportive acceptance of the term – gaining much experience and some modic success.

I left Romania on August 21-st, 1973 and entered on August 24-th into Switzerland, were I received political asylum. I finished school in 1975 at Oberrealschule Rämibüehl, Zürich. In the same year, I started the mathematics studies at ETH, were I received my masters degree in 1981 with a paper on Lucas sequences and a primality test using Eisenstein reciprocity. I functioned from 1979 until 1988 as a teaching assistant for pure and then numerical mathematics, at the respective seminaries of the ETH.

In 1985 I interrupted a PhD in numerical analysis on Newton methods for conformal maps of domains with non smooth boundaries, and decided to dedicate to the present topic. In 1987, Prof.H.W. Lenstra kindly accepted at the suggestion of Prof. V.Strassen, to supervise the present thesis. I received my master in computer science from ETH in 1988 with an implementation of the elliptic curve factoring method.

Between 1982 and 1986 I was working part time in different industries as a programmer and numerical analyst. I have been working full time since 1988 in the domain of information security and cryptography for several major financial institutions and a private consulting company working in the same domain. I am currently a self employed consultant in cryptography.

The political striving for liberty and the changes in Eastern Europe - and especially in Romania, my country of birth - have during the last decade involved much of my energies and activities. This thesis was developed in the last ten years of spare Sundays or spare time.