Elementare Zahlentheorie

Vorlesung von Prof. Dr. B.H. Matzat

SS 1992 Heidelberg

Ausarbeitung von A. Christian

Vorwort

Das vorliegende Sriptum ist die Ausarbeitung einer Vorlesung über Elementare Zahlentheorie, die ich an der TU Berlin im Sommersemester 1987 und in leicht ergänzter Form im Sommersemester 1992 an der Universität Heidelberg gehalten habe. Das Ziel war eine Einführung in die Elementare Zahlentheorie mit Ausrichtung auf Fragen über Primzahlen und diophantische Gleichungen. Insbesondere sollten am Schluß die Nichtexistenz eines Algorithmus für die Lösung allgemeiner diophantischer Geilchungen (X. Hilbertsches Problem) und die Existenz eines Polynoms, dessen positive Werte genau die Menge der Primzahlen durchläuft, bewiesen sein. Diese Zielrichtung legten den Stoff der Vorlesung weitgehend fest.

Das erste Kapitel enthält den Standardstoff der Elementaren Zahlentheorie: Eindeutigkeit der Primzerlegung, Struktur der Restklassenringe und deren Einheitengruppen, simultane Kongruenzen, Satz von Warning über die Anzahl von Kongruenzlösungen diophantischer Gleichungen und das quadratische Reziprozitätsgesetz. Dieser wird ergänzt durch den Primzahltest von Miller und Rabin und den Vier-Quadrate-Satz von Lagrange, der zur Umsetzung diophantischer Probleme im Bereich der ganzen Zahlen in den Bereich der natürlichen Zahlen benötigt wird.

Das zweite Kapitel ist den quadratischen Irrationalzahlen gewidmet. Es beginnt mit einer Einführung der Kettenbrüche und der Charakterisierung quadratischer Irrationalzahlen durch periodische Kettenbrüche. Anschließend wird der Zusammenhang von Kettenbrüchen mit diophantischen Approximationen dargelegt mit einer Anwendung auf Primzerlegungsalgorithmen (Verfahren von Lehman und Lehmer). Der Rest des Kapitels behandelt die Strukturtheorie quadratischer Zahlkörper: Hauptordnung, Einheitengruppe mit Berechnung der Grundeinheit im reell–quadratischen Fall unter Verwendung von Kettenbrüchen, Primidealzerlegung einschließlich Zerlegungsgesetz, Endlichkeit der Klassengruppe mit Beispielen für die Klassengruppenberechnung im imaginär– sowie im reell–quadratischen Fall.

Das dritte und letzte Kapitel hat die von Matijasevič 1973 gezeigte Unlösbarkeit des X. Hilbertschen Problems zum Ziel. Hierfür werden zunächst diophantische Mengen, Relationen und Funktionen eingeführt und die Potenzfunktion unter Verwendung von Lösungen der Pellschen Gleichung, d.h. von Einheiten reell–quadratischer Zahlringe, als diophantische Funktion nachgewiesen. Dann wird gezeigt, daß der beschränkt Allquantor und unter dessen Verwendung auch die Menge der Primzahlen diophantisch ist. Im vorletzten Paragraphen wird der Schlüsselsatz bewiesen, daß eine Funktion genau dann diophantisch ist, wenn sie rekursiv ist. Hiermit läßt sich dann ein Widerspruch zur Lösbarkeit des X. Hilbertschen Problems konstruieren. Im abschließenden Paragraphen schließlich wird unter Verwendung definierender Relationen für die Lösungen der Pellschen Gleichung und der Fakultät ein Satz von definierenden Relationen für die Menge der Primzahlen aufgestellt, der unmittelbar auf die Konstruktion eines Primzahlpolynoms führt.

Als weiterführende Literatur sei empfohlen:

- H. Hasse: Vorlesungen über Zahlentheorie, Springer–Verlag, Berlin 1964
- H. Koch, H. Pieper: Zahlentheorie, VEB Deutscher Verlag der Wissenschaften, Berlin 1976
- J.I.Manin: A course in mathematical logic, Springer–Verlag, New York 1977

- C: Smorynski: Logical number theory I, Springer–Verlag, Berlin 1991

Abschließend möchte ich an dieser Stelle noch Herrn A. Christian danken, der nicht nur die textliche Ausgestaltung der Vorlesung sondern auch den TEX–Satz des Skriptums übernommen und selbständig durchgeführt hat.

B.H. Matzat

Inhaltsverzeichnis

Teil I

Ganzrationale Zahlen

1 Primzahlen

1.1 Teilbarkeit und Primzahlen

Bezeichnungen: Wie üblich bezeichnet $\mathbb{N} := \{1, 2, 3, ...\}$ die Menge der natürlichen Zahlen mit den Verknüpfungen $+$, $\cdot$ und der Ordnungsrelation $\leq$, deren grundlegende Eigenschaften hier als bekannt vorausgesetzt werden.

Ferner bezeichnet $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$ die Menge der endlichen Kardinalzahlen, $-\mathbb{N} := \{\, -n \mid n \in \mathbb{N}\}$ die Menge der negativen ganzen Zahlen und $\mathbb{Z} := -\mathbb{N} \cup \{0\} \cup \mathbb{N}$ die Menge der ganzen Zahlen. Die Verknüpfungen $+, \cdot$ und die Relation $\leq$ in $\mathbb{Z}$ sind verträglich mit denen in $\mathbb{N}$.

Definition 1.1. Es seien a und $b \neq 0$ ganze Zahlen. Die Zahl b heißt **Teiler** von a, wenn eine ganze Zahl q mit $a = qb$ existiert. Entsprechend heißt dann a **Vielfaches** von b. Formelmäßig wird die Teilbarkeit durch $b \mid a$ bzw. deren Negation durch $b \nmid a$ angegeben.

Eine natürliche Zahl $p \neq 1$ heißt **Primzahl**, wenn für ein $b \in \mathbb{N}$ aus $b \mid p$ stets $b = 1$ oder $b = p$ folgt. Die Menge der Primzahlen wird mit $\mathbb{P} := \{\, p \in \mathbb{N} \mid p \text{ ist Primzahl}\}$ bezeichnet.

Bemerkung 1.1. *Für $a, b, c \in \mathbb{Z}$ gelten:*

(a) Aus $b \mid a$ und $c \mid b$ folgt $c \mid a$.

(b) Aus $c \mid a$ und $c \mid b$ folgt $c \mid (a \pm b)$.

Beweis.

(a) Wegen $b \mid a$ existiert ein $q \in \mathbb{Z}$ mit $a = qb$. Wegen $c \mid b$ existiert ein $r \in \mathbb{Z}$ mit $b = rc$. Daraus folgt $a = qrc$ und damit $c \mid a$.

(b) Wegen $c \mid a$ und $c \mid b$ existieren $q, r \in \mathbb{Z}$ mit $a = qc$ bzw. $b = rc$. Daraus folgt $a \pm b = (q \pm r)c$ und damit $c \mid (a \pm b)$. □

Bemerkung 1.2. *Für jede ganze Zahl $a \geq 2$ ist ihr kleinster positiver von 1 verschiedener Teiler eine Primzahl.*

Beweis. Es sei $T := \{\, t \in \mathbb{N} \mid t \mid a,\ t \neq 1\,\}$. Wegen $a \in T$ ist T nicht leer. Da jede nichtleere Teilmenge von $\mathbb{N}$ ein kleinstes Element besitzt, existiert also $z := \min T$.

Wegen $z \mid a$ gilt für jeden positiven Teiler d von z mit $d \neq 1$ stets $d \mid a$. Wegen der Minimalitätseigenschaft von z folgt $d \geq z$ und damit $d = z$. Also ist z eine Primzahl. □

Satz 1.1 (Euklid)**.** *Die Menge der Primzahlen ist unendlich.*

Beweis. Wäre die Menge der Primzahlen endlich, so gäbe es ein $n \in \mathbb{N}$ mit $\mathbb{P} = \{p_1, \dots, p_n\}$. Bildet man die Zahl $q := p_1 \cdot \ldots \cdot p_n + 1$, so folgte wegen $q > 1$ aus Bemerkung 1.2, daß eine Primzahl z mit $z \mid q$ existiert.

Wäre $z \in \{p_1, \dots, p_n\}$, so würde mit Bemerkungt 1.1 aus $z \mid q$ und $z \mid p_1 \cdot \ldots \cdot p_n$ wegen $q - p_1 \cdot \ldots \cdot p_n = 1$ schließlich $z \mid 1$ folgen im Widerspruch zur Definition von z.

Also ist z im Gegensatz zur Annahme eine von $p_1, \dots, p_n$ verschiedene Primzahl. $\square$

Eine einfache Methode zur Bestimmung von Primzahlen liefert das **Sieb des Eratosthenes**:

Aus einer Zahlentafel gewünschter Größe streicht man der Reihe nach die Vielfachen der Primzahlen $p = 2, 3, \dots$, jeweils beginnend mit dem Produkt p^2. Die jeweils kleinste nicht ausgestrichene Zahl $z > p$ ist dann die nächste Primzahl.

Die folgende Tafel enthält die so gewonnenen Primzahlen bis zur Schranke 100:

Abschnitt 1.1

	0	1	2	3	4	5	6	7	8	9
0	×	×			×		×		×	×
1	×		×		×	×	×		×	
2	×	×	×		×	×	×	×	×	
3	×		×	×	×	×	×		×	×
4	×		×		×	×	×		×	×
5	×	×	×		×	×	×	×	×	
6	×		×	×	×	×	×		×	×
7	×		×		×	×	×	×	×	
8	×	×	×		×	×	×	×	×	×
9	×	×	×	×	×	×	×		×	×

1.2 Der Euklidische Algorithmus

Bemerkung 1.3 (Division mit Rest). *Zu einem vorgegebenen Paar ganzer Zahlen a,b mit $b \neq 0$ gibt es genau ein Paar ganzer Zahlen q,r mit*

$$a = qb + r \text{ und } 0 \leq r < |b|.$$

Bezeichnung: $q = [\frac{a}{b}]$ heißt der ganze Quotient, r heißt der kleinste nichtnegative Rest bei der Division von a durch b.

Beweis. Existenz: Es sei $R := \{\, a - qb \mid q \in \mathbb{Z} \,\} \cap \mathbb{N}$. Wegen $R \neq \emptyset$ existiert ein minimales Element $\tilde{r} := \min R$, für das also $1 \leq \tilde{r} \leq |b|$ gilt. Im Falle $1 \leq \tilde{r} < |b|$ setzt man $r := \tilde{r}$ und hat mit dem zugehörigen q die Darstellung $a = qb + r$ gefunden.

Im Falle $\tilde{r} = |b|$ setzt man $r := 0$ und hat mit dem passenden q wieder die gewünschte Darstellung.

Eindeutigkeit: Ist $\tilde{q}, \tilde{r}$ ein Paar ganzer Zahlen mit denselben Eigenschaften wie q, r, so gilt $qb + r = \tilde{q}b + \tilde{r}$, woraus $(q - \tilde{q})b = \tilde{r} - r$ folgt. Also gilt $b \mid (\tilde{r} - r)$, und wegen $|\tilde{r} - r| < |b|$ ergibt sich $\tilde{r} - r = 0$ und damit auch $q = \tilde{q}$. $\square$

Definition 1.2. Seien $z_1, \ldots, z_n$ von Null verschiedene ganze Zahlen. Eine ganze Zahl d heißt **größter gemeinsamer Teiler** von $z_1, \ldots, z_n$, wenn folgende Bedingungen erfüllt sind:

(a) Es gilt $d \mid z_i$ für $i = 1, \ldots, n$.

(b) Aus $t \mid z_i$ für $i = 1, \ldots, n$ folgt $t \mid d$.

Bemerkung 1.4. *Sind d_1 und d_2 größte gemeinsame Teiler von $z_1, \ldots, z_n$, so gilt $d_1 = \pm d_2$.*

Beweis. Aus den Eigenschaften von d_1 und d_2 folgt sowohl $d_2 \mid d_1$ als auch $d_1 \mid d_2$. Es existieren also ganze Zahlen e, f mit $d_1 = ed_2$ und $d_2 = fd_1$, woraus $d_1 = efd_1$ folgt. Wegen $d_1 \neq 0$ erhält man $ef = 1$ und damit $e \in \{1, -1\}$, woraus $d_1 = \pm d_2$ folgt. □

Bezeichnungen: Der größte gemeinsame Teiler ist also genau bis auf das Vorzeichen bestimmt. Für die positive dieser beiden Zahlen schreibt man $\operatorname{ggT}\{z_1, \ldots, z_n\}$.

Satz 1.2. *Seien z_1 und z_2 ganze von Null verschiedene Zahlen. Dann existiert der größte gemeinsame Teiler d von z_1 und z_2 und es gibt ganze Zahlen u und v mit*

$$d = uz_1 + vz_2.$$

Beweis. Zur Konstruktion des größten gemeinsamen Teilers benutzt man den **Euklidischen Algorithmus**:

Offenbar darf $z_2 > 0$ vorausgesetzt werden. Wendet man Division mit Rest auf z_1 und z_2 an, ergibt sich:

$$z_1 = q_1 z_2 + z_3, \quad 0 \leq z_3 < z_2.$$

Im Falle $z_3 = 0$ stoppt das Verfahren.

Im Falle $z_3 > 0$ wendet man Division mit Rest auf z_2 und z_3 an:

$$z_2 = q_2 z_3 + z_4, \quad 0 \leq z_4 < z_3.$$

Da die Folge der Reste $z_2, z_3, \ldots$ streng monoton fällt, stoppt das Verfahren nach endlich vielen Schritten mit den Gleichungen

$$\begin{aligned} z_{r-1} &= q_{r-1} z_r + z_{r+1}, \quad 0 \leq z_{r+1} < z_r \\ z_r &= q_r z_{r+1} \end{aligned}$$

Hieraus liest man $z_{r+1} \mid z_r$ ab. Aus der vorigen Gleichung zusammen mit Bemerkung 1.1 folgt somit $z_{r+1} \mid z_{r-1}$. So fortfahrend erhält man schließlich aus den beiden ersten Gleichungen: $z_{r+1} \mid z_2$ und $z_{r+1} \mid z_1$. Also ist z_{r+1} ein gemeinsamer Teiler von z_1 und z_2.

Für eine Zahl t mit $t \mid z_1$ und $t \mid z_2$ folgt aus der ersten Gleichung $t \mid z_3$. Mit der zweiten Gleichung folgt weiter $t \mid z_4$. So fortfahrend erhält man schließlich $t \mid z_{r+1}$.

Damit ist $d := z_{r+1}$ der größte gemeinsame Teiler von z_1 und z_2.

Zur Konstruktion der Zahlen u und v löst man

$$\begin{aligned} z_r &= z_{r-2} - q_{r-2} z_{r-1} \\ d &= z_{r-1} - q_{r-1} z_r \end{aligned}$$

nach d auf und sieht, daß es ganze Zahlen u_{r-1} und v_{r-1} gibt mit

$$d = v_{r-1}z_{r-1} + u_{r-1}z_{r-2}.$$

So fortfahrend erhält man schließlich aus der ersten Gleichung

$$d = v_2 z_2 + u_2 z_1,$$

was mit $v := v_2$ und $u := u_2$ die gewünschte Darstellung ergibt. $\square$

Beispiel 1.1. Bestimmung des größten gemeinsamen Teilers von 2257 und 1073:

$$\begin{array}{rcccl} 2257 & = & 2 \cdot 1073 & + & 111 \\ 1073 & = & 9 \cdot 111 & + & 74 \\ 111 & = & 1 \cdot 74 & + & 37 \\ 74 & = & 2 \cdot 37 & & \end{array}$$

Also gilt $\text{ggT}\{2257, 1073\} = 37$.

Für die Linearkombination des größten gemeinsamen Teilers ergibt sich:

$$\begin{array}{rcccc} 37 & = & 111 & - & 74 \\ & = & 111 & - & (1073 - 9 \cdot 111) \\ & = & 10 \cdot 111 & - & 1073 \\ & = & 10 \cdot (2257 - 2 \cdot 1073) & - & 1073 \\ & = & 10 \cdot 2257 & - & 21 \cdot 1073 \end{array}$$

1.3 Primzerlegung

Es seien $n \in \mathbb{N}, n > 1$ und p_1 der kleinste Primteiler von n, der nach Bemerkung 1.2 immer existiert. Es ist dann

$$n = n_1 p_1, \quad n_1 \in \mathbb{N}, \quad 1 \leq n_1 < n.$$

Im Falle $n_1 = 1$ hat man eine Primzerlegung erreicht. Sonst zerlegt man in gleicher Weise

$$n_1 = n_2 p_2, \quad n_2 \in \mathbb{N}, \quad 1 \leq n_2 < n_1.$$

Wegen $n_1 > n_2 > n_3 > \cdots$ erhält man nach endlich vielen Schritten eine Primzerlegung von n:

$$n = p_1 \cdot \ldots \cdot p_r$$

Für $n = 1$ setzt man $r = 0$ (leeres Produkt), so daß eine Primzerlegung für jede natürliche Zahl existiert.

Daß die Frage nach der Eindeutigkeit der Primzerlegung nicht voreilig mit ja beantwortet werden darf, zeigt folgendes

Beispiel 1.2. Die Menge $H := \{ 4k + 1 \mid k \in \mathbb{Z} \}$ ist, wie man leicht sieht, multiplikativ abgeschlossen. Die Zahl p heißt H-Primzahl, wenn p in H nur die trivialen Teiler 1 und p besitzt. Daß die Primzerlegung in H nicht eindeutig ist, sieht man daran, daß sich mit den H-Primzahlen 9 , 21 und 49 die Zahl 441 als $441 = 21 \cdot 21$ und $441 = 9 \cdot 49$ darstellen läßt.

Satz 1.3 (Euklidische Charakterisierung der Primzahlen). *Die Zahl $p \in \mathbb{N}\backslash\{1\}$ ist genau dann eine Primzahl, wenn aus $p \mid nm$ stets $p \mid n$ oder $p \mid m$ folgt.*

Beweis. Sei p eine Primzahl und es gelte $p \mid nm$. Im Falle $p \mid n$ ist nichts weiter zu zeigen.

Im Falle $p \nmid n$ gilt $\mathrm{ggT}\{p, n\} = 1$, da p nur triviale Teiler besitzt. Aus Satz 1.2 folgt die Existenz zweier Zahlen $u, v \in \mathbb{Z}$ mit $1 = up + vn$. Hieraus ergibt sich

$$m = ump + vmn.$$

Da p trivialerweise den ersten und nach Voraussetzung auch den zweiten Summanden der rechten Gleichungsseite teilt, ergibt sich $p \mid m$.

Zum Beweis der Umkehrung habe p die im Satz angegebene Eigenschaft und es gelte $p = ab$ mit $a, b \in \mathbb{N}$. Daraus liest man ab, daß sowohl $a \mid p$ und $b \mid p$ als auch eine der beiden Aussagen $p \mid a$ oder $p \mid b$ zutreffen.

Also gilt $a = p$ oder $b = p$ und damit besitzt p nur triviale Teiler. □

Satz 1.4 (Gauß). *Die Primzerlegung einer natürlichen Zahl ist eindeutig bis auf die Reihenfolge der Faktoren.*

Beweis. Für $n = 1$ ist das leere Produkt die einzig mögliche Darstellung. Für $n > 1$ wird der Beweis durch Induktion nach der Anzahl der Faktoren geführt. Es sei

$$n = p_1 \cdot \ldots \cdot p_r = q_1 \cdot \ldots \cdot q_s \quad \text{mit} \quad p_i, q_i \in \mathbb{P}.$$

Für $r = 1$ gilt $n = p_1$ und damit $p_1 \mid q_1 \cdot \ldots \cdot q_s$. Aufgrund der Primzahleigenschaft muß p_1 mit einem der q_i identisch sein. Ohne Einschränkung darf also $p_1 = q_1$ angenommen werden. Daraus folgt $q_2 = \ldots = q_s = 1$ und damit die Eindeutigkeit.

Nun sei die Eindeutigkeit für $r - 1$ Faktoren bewiesen. Aus $p_1 \cdot \ldots \cdot p_r = q_1 \cdot \ldots \cdot q_s$ folgt $p_1 \mid q_1 \cdot \ldots \cdot q_s$ und damit wie oben ohne Einschränkung $p_1 = q_1$. Dann gilt auch $p_2 \cdot \ldots \cdot p_r = q_2 \cdot \ldots \cdot q_s$, woraus aufgrund der Induktionsvoraussetzung $r = s$ und bis auf die Reihenfolge $p_i = q_i$ folgt. □

1.4 Ideale von $\mathbb{Z}$

Definition 1.3. Eine Teilmenge $\emptyset \neq \mathfrak{a} \subseteq \mathbb{Z}$ heißt **Ideal**, wenn sie folgende Eigenschaften besitzt:

(a) Aus $a_1 \in \mathfrak{a}$ und $a_2 \in \mathfrak{a}$ folgt $a_1 - a_2 \in \mathfrak{a}$.

(b) Aus $a \in \mathfrak{a}$ und $z \in \mathbb{Z}$ folgt $za \in \mathfrak{a}$.

Hierfür wird dann $\mathfrak{a} \trianglelefteq \mathbb{Z}$ geschrieben.

Satz 1.5. *Die Ideale von $\mathbb{Z}$ sind von der Form $m\mathbb{Z}$ mit $m \in \mathbb{N}_0$ und umgekehrt.*

Beweis. Sind $a_1 \in m\mathbb{Z}$ und $a_2 \in m\mathbb{Z}$, dann gibt es $z_1, z_2 \in \mathbb{Z}$ mit $a_1 = mz_1$ und $a_2 = mz_2$. Da $mz_1 - mz_2 = m(z_1 - z_2) \in m\mathbb{Z}$ ist und für alle $z \in \mathbb{Z}$ $za_1 = mz_1z \in m\mathbb{Z}$ gilt, folgt $m\mathbb{Z} \trianglelefteq \mathbb{Z}$

Nun sei $\mathfrak{a} \trianglelefteq \mathbb{Z}$. Im Falle $\mathfrak{a} = \{0\}$ ist $\mathfrak{a} = 0 \cdot \mathbb{Z}$.

Im Falle $\mathfrak{a} \neq \{0\}$ gilt $\mathfrak{a} \cap \mathbb{N} \neq \emptyset$, da aus $-n \in \mathfrak{a}$ stets $n \in \mathfrak{a}$ folgt. Also besitzt $\mathfrak{a} \cap \mathbb{N}$ ein minimales Elememt m. Trivialerweise gilt $m\mathbb{Z} \subseteq \mathfrak{a}$. Um $\mathfrak{a} \subseteq m\mathbb{Z}$ zu zeigen, sei $a \in \mathfrak{a}$ beliebig gegeben. Division mit Rest von a durch m ergibt

$$a = qm + r \quad \text{mit } 0 \leq r < m.$$

Wegen $a \in \mathfrak{a}$ und $qm \in \mathfrak{a}$ ist auch $r = a - qm \in \mathfrak{a}$. Wegen der Minimalitätseigenschaft von m hat dies $r = 0$ zur Folge. Also gilt $a = qm$ und damit $a \in m\mathbb{Z}$. □

Satz 1.6 (Fundamentalsatz über den größten gemeinsamen Teiler). *Der größte gemeinsame Teiler d von $z_1, \ldots, z_n \in \mathbb{Z}\backslash\{0\}$ existiert, und es gibt $u_1, \ldots, u_n \in \mathbb{Z}$ mit*

$$d = u_1 z_1 + \cdots + u_n z_n.$$

Beweis. Da $\mathfrak{a} := z_1\mathbb{Z} + \cdots + z_n\mathbb{Z}$ ein Ideal von $\mathbb{Z}$ ist, existiert nach Satz 1.5 eine Zahl $d \in \mathbb{N}_0$ mit $\mathfrak{a} = d\mathbb{Z}$, wobei wegen $z_i \neq 0$ sogar $d \in \mathbb{N}$ angenommen werden kann. Aufgrund von $d \in \mathfrak{a}$ gibt es $u_1, \ldots, u_n$ mit $d = u_1 z_1 + \cdots + u_n z_n$. Es muß noch gezeigt werden, daß d die beiden definierenden Eigenschaften des größten gemeinsamen Teilers erfüllt:

Für alle $i = 1, \ldots, n$ gilt $z_i \in \mathfrak{a}$. Daher gibt es $q_i \in \mathbb{Z}$ mit $z_i = dq_i$, und es folgt $d \,|\, z_i$.

Aus $t \,|\, z_i$ für $i = 1, \ldots, n$ folgt $t \,|\, (u_1 z_1 + \cdots + u_n z_n)$ und damit $t \,|\, d$. □

Anmerkung: Die Berechnung von $\text{ggT}\{z_1, \ldots, z_n\}$ kann durch sukzessive Berechnung von

$$\begin{aligned} d_2 &= \text{ggT}\{z_1, z_2\} \\ d_3 &= \text{ggT}\{d_2, z_3\} \\ &\vdots \\ d &= \text{ggT}\{d_{n-1}, z_n\} \end{aligned}$$

mittels des Euklidischen Algorithmus erfolgen.

(Beweis: Übungsaufgabe!)

2 Kongruenzen

2.1 Kongruenzrelationen

Definition 2.1. Es sei R eine Menge, auf der zwei Verknüpfungen $+$ (Addition) und $\cdot$ (Multiplikation) erklärt sind. $(R, +, \cdot)$ heißt **Ring**, wenn folgende Bedingungen erfüllt sind:

(a) $(R, +)$ ist eine abelsche Gruppe.

(b) $(R, \cdot)$ ist eine Halbgruppe mit Einselement.

(c) Es gelten die Distributivgesetze

$$(a + b)c = ac + bc \text{ und } a(b + c) = ab + ac.$$

Sind keine Verwechslungen möglich, so wird auch R selbst Ring genannt. Gilt darüberhinaus noch das Kommutativgesetz der Multiplikation, so heißt R **kommutativer Ring**.

Beispiel 2.1. Die ganzen Zahlen bilden bezüglich der herkömmlichen Addition und Multiplikation einen kommutativen Ring.

Beispiel 2.2. Sei $\mathbb{Z}[i] := \{ a + bi \mid a, b \in \mathbb{Z} \}$ eine Teilmenge von $\mathbb{C}$ mit der imaginären Einheit $i = \sqrt{-1}$. Addition und Multiplikation darauf seien als Einschränkung der Verknüpfungen in $\mathbb{C}$ definiert. Dann ist $(\mathbb{Z}[i], +, \cdot)$ ein Ring und heißt **Ring der ganzen Gauß'schen Zahlen**.

Beispiel 2.3. Es sei $\mathbb{Z}[X]$ die Menge aller Polynome $f = \sum_{i=0}^{n} a_i X^i$ in einer Variablen X mit ganzzahligen Koeffizienten a_i. Zusammen mit den Verknüpfungen

$$f + g := \sum_{i=0}^{\max\{n,m\}} (a_i + b_i) X^i$$
$$f \cdot g := \sum_{k=0}^{n+m} \Big(\sum_{i+j=k} a_i b_j \Big) X^k$$

bildet $\mathbb{Z}[X]$ einen kommutativen Ring, den **Polynomring einer Variablen über** $\mathbb{Z}$.

Definition 2.2. Es sei $(R, +, \cdot)$ ein kommutativer Ring. Eine Äquivalenzrelation $\equiv$ auf R heißt **Kongruenzrelation**, wenn aus $a_1 \equiv a_2$ und $b_1 \equiv b_2$ stets $a_1 + b_1 \equiv a_2 + b_2$ und $a_1 b_1 \equiv a_2 b_2$ folgt, d.h. wenn $\equiv$ mit den Verknüpfungen auf R verträglich ist.

Eine nichtleere Teilmenge $\mathfrak{a}$ von R heißt **Ideal**, wenn für alle $a_1, a_2 \in \mathfrak{a}$ und $r \in R$ stets $a_1 - a_2 \in \mathfrak{a}$ und $ra_1 \in \mathfrak{a}$ gilt. Ist $\mathfrak{a}$ ein Ideal von R, so wird kurz $\mathfrak{a} \trianglelefteq R$ geschrieben.

Beispiel 2.4. Im Polynomring einer Variablen über $\mathbb{Z}$ bildet

$$\mathfrak{a} := \big\{ 2 \cdot f + X \cdot g \mid f, g \in R \big\}$$

ein Ideal.

Satz 2.1. *Es sei R ein kommutativer Ring.*

(a) *Ist $\equiv$ eine Kongruenzrelation in R, so bildet die Menge $\mathfrak{a} := \{ a \in R \mid a \equiv 0 \}$ ein Ideal in R und es gilt $a \equiv b$ genau dann, wenn $a - b \in \mathfrak{a}$ gilt.*

(b) *Ist $\mathfrak{a}$ ein Ideal in R und setzt man $a \equiv b$, falls $a - b \in \mathfrak{a}$ gilt, so ist $\equiv$ eine Kongruenzrelation in R und es gilt $\{ a \in R \mid a \equiv 0 \} = \mathfrak{a}$.*

Beweis.

(a) Sind $a, b \in \mathfrak{a}$, so gelten $a \equiv 0$ und $b \equiv 0$. Es folgt $a - b \equiv 0$ und damit $a - b \in \mathfrak{a}$. Ist $a \in \mathfrak{a}$ und $r \in R$, so gilt wegen $a \equiv 0$ auch $ra \equiv 0$ und damit $ra \in \mathfrak{a}$. Also ist $\mathfrak{a}$ ein Ideal in R.

Weiterhin ist die Kongruenz $a \equiv b$ gleichbedeutend mit $a - b \equiv 0$, was nach Definition von $\mathfrak{a}$ genau für $a - b \in \mathfrak{a}$ der Fall ist.

(b) Zunächst wird gezeigt, daß $\equiv$ eine Äquivalenzrelation ist: Wegen $0 \in \mathfrak{a}$ gilt $a \equiv a$ für alle $a \in R$. Aus $a \equiv b$ folgt $a - b \in \mathfrak{a}$. Dann gilt auch $b - a \in \mathfrak{a}$ und damit $b \equiv a$. Aus $a \equiv b$ und $b \equiv c$ folgen $a - b \in \mathfrak{a}$ und $b - c \in \mathfrak{a}$. Hieraus folgt $(a-b)+(b-c) = a-c \in \mathfrak{a}$ und damit $a \equiv c$.

Um die Eigenschaften einer Kongruenzrelation nachzuprüfen, gelte $a_1 \equiv a_2$ und $b_1 \equiv b_2$, woraus $a_1 - a_2 \in \mathfrak{a}$ und $b_1 - b_2 \in \mathfrak{a}$ folgen. Wegen $(a_1 - a_2) + (b_1 - b_2) = (a_1 + b_1) - (a_2 + b_2) \in \mathfrak{a}$ gilt damit $a_1 + b_1 \equiv a_2 + b_2$.

Aus $a_1 - a_2 \in \mathfrak{a}$ und $b_1 - b_2 \in \mathfrak{a}$ folgen andererseits $(a_1 - a_2)b_1 \in \mathfrak{a}$ und $a_2(b_1 - b_2) \in \mathfrak{a}$. Damit gilt auch für deren Summe $a_1b_1 - a_2b_2 \in \mathfrak{a}$, woraus $a_1b_1 \equiv a_2b_2$ folgt.

Trivialerweise gilt schließlich $\{\, a \in R \mid a \equiv 0 \,\} = \{\, a \in R \mid a - 0 \in \mathfrak{a} \,\} = \mathfrak{a}$. □

Folgerung 2.1. *Die Kongruenzrelationen in $\mathbb{Z}$ entsprechen bijektiv den Idealen $m\mathbb{Z}$ mit $m \in \mathbb{N}_0$ von $\mathbb{Z}$.*

Beweis. Wird ausgehend von einem Ideal $\mathfrak{a} \trianglelefteq \mathbb{Z}$ gemäß Teil (b) von Satz 2.1 eine Kongruenzrelation definiert, so ist das nach Teil (a) zu der Kongruenzrelation gehörige Ideal gerade $\mathfrak{a}$. Zusammen mit Satz 1.5 ergibt sich die Behauptung. □

Bezeichnung: Für die durch $m \in \mathbb{N}_0$ charakterisierte Kongruenzrelation in $\mathbb{Z}$ schreibt man

$$a \equiv b \pmod{m}$$

(lies: „a kongruent b modulo m“).

Es gilt also $a \equiv b \pmod{m}$ genau dann, wenn $a - b \in m\mathbb{Z}$ bzw. $m \mid (a - b)$ gilt.

Als Beispiel für die Anwendung des Kongruenzbegriffs folgen zwei einfache Teilbarkeitsregeln und eine Aussage über Fermat-Zahlen:

Beispiel 2.5. „Eine Zahl ist genau dann durch 9 teilbar, wenn ihre Quersumme durch 9 teilbar ist.“

Schreibt man die Zahl z in dezimaler Schreibweise $z = \sum_{i=0}^{n} a_i 10^i$, so folgt wegen der Kongruenz $10 \equiv 1 \pmod{9}$, daß $z \equiv \sum_{i=0}^{n} a_i \pmod{9}$ gilt. Da $\sum_{i=0}^{n} a_i$ gerade die Quersumme von z darstellt, ergibt sich die Behauptung.

Beispiel 2.6. „Eine Zahl ist genau dann durch 11 teilbar, wenn ihre alternierende Quersumme durch 11 teilbar ist.“

Diese Tatsache folgt analog, wenn man beachtet, daß wegen $10 \equiv -1 \pmod{11}$ auch $\sum_{i=0}^{n} a_i 10^i \equiv \sum_{i=0}^{n} (-1)^i a_i \pmod{11}$ gilt.

Beispiel 2.7. Zahlen der Form $F_n = 2^{2^n} + 1$ heißen **Fermat-Zahlen**. Die ersten Fermat-Zahlen $F_0 = 3,\ F_1 = 5,\ F_2 = 17,\ F_3 = 257,\ F_4 = 65537$ sind Primzahlen. Entgegen der ursprünglichen Vermutung, alle Fermat-Zahlen seien Primzahlen, kann gezeigt werden, daß $F_5 = 2^{32} + 1$ den Teiler 641 besitzt:

Offensichtlich gilt $2^8 \equiv 256 \pmod{641}$. Durch Quadrieren beider Seiten erhält man

$$2^{16} \equiv (256)^2 \equiv 154 \pmod{641} \quad \text{und } 2^{32} \equiv (154)^2 \equiv -1 \pmod{641}.$$

Also gilt $2^{32} + 1 \equiv 0 \pmod{641}$.

2.2 Restklassenringe

Bemerkung 2.1. *Es seien $(R,+,\cdot)$ ein kommutativer Ring und $\equiv$ eine darauf definierte Kongruenzrelation. Unter $\overline{R} := {}^{R}/_{\equiv}$ werde wie üblich die Quotientenmenge nach der Äquivalenzrelation $\equiv$ verstanden. Werden in $\overline{R}$ die Addition und Multiplikation vertreterweise erklärt:*

$$\overline{a} + \overline{b} := \overline{a+b} \quad \text{und } \overline{a} \cdot \overline{b} := \overline{ab},$$

so bildet $\overline{R}$ einen kommutativen Ring.

Beweis. Zunächst wird gezeigt, daß die Verknüpfungen wohldefiniert sind: Sind a_1 und a_2 beliebige Elemente von $\overline{a}$ und b_1 und b_2 beliebige Elemente von $\overline{b}$, so gilt wegen $a_1 \equiv a_2$ und $b_1 \equiv b_2$ auch $a_1 + b_1 \equiv a_2 + b_2$. Also gilt $\overline{a_1 + b_1} = \overline{a_2 + b_2}$ und damit ist die Definition von $\overline{a} + \overline{b}$ nicht von der speziellen Wahl der Vertreter abhängig.

Analog folgt wegen $a_1 b_1 \equiv a_2 b_2$ auch $\overline{a_1 b_1} = \overline{a_2 b_2}$. Damit ist auch die Multiplikation wohldefiniert. Wegen der vertreterweisen Erklärung der Verknüpfungen übertragen sich alle Ringeigenschaften von R auf $\overline{R}$. □

Bezeichnung: Sei R ein kommutativer Ring, in dem es eine Kongruenzrelation $\equiv$ und ein Ideal $\mathfrak{a}$ gibt, die sich gemäß Satz 2.1 entsprechen. Dann heißt $\overline{R} = {}^{R}/_{\mathfrak{a}} = {}^{R}/_{\equiv}$ der **Restklassenring** von R nach $\equiv$ bzw. $\mathfrak{a}$.

Definition 2.3. Ein Ring R heißt **nullteilerfrei**, wenn für alle $a, b \in R$ aus $ab = 0$ stets $a = 0$ oder $b = 0$ folgt.

Beispiel 2.8. Die Restklassenringe in $\mathbb{Z}$ haben folgende Gestalt:

Für das Nullideal $\mathfrak{a} = \{0\}$ ist $\overline{R} = {}^{\mathbb{Z}}/_{\{0\}} = \mathbb{Z}$.

Für $\mathfrak{a} = \mathbb{Z}$ ist ${}^{\mathbb{Z}}/_{\mathbb{Z}} = \overline{0}$ der Nullring, bei dem Nullelement und Einselement identisch sind.

Weitere Restklassenringe sind ${}^{\mathbb{Z}}/_{2\mathbb{Z}} = \{\overline{0}, \overline{1}\}$, ${}^{\mathbb{Z}}/_{3\mathbb{Z}} = \{\overline{0}, \overline{1}, \overline{2}\}$ und ${}^{\mathbb{Z}}/_{4\mathbb{Z}} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$. Wegen $\overline{2} \cdot \overline{2} = \overline{4} = \overline{0}$ ist ${}^{\mathbb{Z}}/_{4\mathbb{Z}}$ nicht nullteilerfrei.

Anmerkung: Für den Restklassenring ${}^{\mathbb{Z}}/_{n\mathbb{Z}}$ schreibt man manchmal auch kurz Z_n.

Definition 2.4. Ein kommutativer Ring R heißt **Körper**, wenn $(R\backslash\{0\}, \cdot)$ eine Gruppe ist.

Bemerkung 2.2. *Der Restklassenring ${}^{\mathbb{Z}}/_{m\mathbb{Z}}$ ist genau dann ein Körper, wenn m eine Primzahl ist.*

Beweis. Ist m keine Primzahl, so existiert eine nichttriviale Darstellung $m = ab$. Dann gilt aber auch $\overline{0} = \overline{m} = \overline{a}\overline{b}$, das heißt der Restklassenring besitzt Nullteiler. Wäre ${}^{\mathbb{Z}}/_{m\mathbb{Z}}$ ein Körper, so gäbe es ein zu $\overline{a}$ inverses Element $\overline{a}'$ mit $\overline{a}'\overline{a} = 1$ und es würde wegen $\overline{a}'\overline{a}\overline{b} = \overline{b}$ der Widerspruch $\overline{0} = \overline{b}$ folgen.

Ist umgekehrt m eine Primzahl, so ist zu zeigen, daß jede von $\overline{0}$ verschiedene Restklasse $\overline{a}$ ein Inverses besitzt. Dafür sei $a \in \overline{a}$. Wegen $\mathrm{ggT}\{a, m\} = 1$ gibt es nach Satz 1.2 ganze Zahlen u und v mit $ua + vm = 1$. Der Übergang zu den Restklassen ergibt $\overline{ua} = \overline{1}$. Also besitzt $\overline{a}$ ein Inverses. □

Bezeichnung: Ist p eine Primzahl, so wird ${}^{\mathbb{Z}}/_{p\mathbb{Z}} =: \mathbb{F}_p$ als **Primkörper der Charakteristik p** bezeichnet.

2.3 Kongruenzdivision

In diesem Abschnitt wird die Frage behandelt, wann eine Kongruenzgleichung der Form

$$\overline{ax} = \overline{b}$$

lösbar ist, und wie Lösungen zu finden sind.

Bemerkung 2.3. *Ist $(R, +, \cdot)$ ein kommutativer Ring, so bildet die Menge $R^\times$ aller Elemente von R, die ein Inverses besitzen, eine kommutative Gruppe bezüglich der Multiplikation.*

Beweis. Zu zeigen ist nur die Abgeschlossenheit von $R^\times$ und die Existenz inverser Elemente bezüglich der Multiplikation. Für $a, b \in R^\times$ existieren $a', b' \in R^\times$ mit $aa' = 1$ und $bb' = 1$. Wegen $abb'a' = aa' = 1$ folgt $ab \in R^\times$ und wegen $aa' = a'a$ folgt auch $a' \in R^\times$. □

Definition 2.5. $R^\times$ heißt **Einheitengruppe** von R.

Beispiel 2.9. Die Einheitengruppen von $\mathbb{Z}, \mathbb{Z}[i]$ und $\mathbb{Q}$ sind $\mathbb{Z}^\times = \{\pm 1\}, \mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$ und $\mathbb{Q}^\times = \mathbb{Q} \backslash \{0\}$.

Bemerkung 2.4. *Die Einheitengruppe von $R = {}^{\mathbb{Z}}/_{m\mathbb{Z}}$ ist*

$$R^\times = \left\{ \overline{a} \in R \mid \overline{a} = a + m\mathbb{Z} \text{ mit } \operatorname{ggT}\left\{a, m\right\} = 1 \right\}.$$

Beweis. Zunächst ist für $a_1, a_2 \in \overline{a}$ zu zeigen, daß $d_1 := \operatorname{ggT}\{a_1, m\}$ und $d_2 := \operatorname{ggT}\{a_2, m\}$ identisch sind, um die Wohldefiniertheit der Menge zu sichern:

Wegen $a_1 - a_2 \in m\mathbb{Z}$ gibt es eine ganze Zahl g mit $a_1 - a_2 = gm$. Da d_1 Teiler von a_1 und m, also auch von a_2 und m ist, ist d_1 auch ein Teiler von d_2. Analog folgt, daß d_2 ein Teiler von d_1 ist. Also gilt $d_1 = d_2$ wegen der nach Bemerkung 1.4 vereinbarten positiven Normierung.

Nach Satz 1.2 ist $\operatorname{ggT}\{a, m\} = 1$ gleichbedeutend mit der Existenz zweier ganzer Zahlen u und v mit $ua + vm = 1$. Genau dann ist aber $\overline{ua} = \overline{1}$ und damit $\overline{a} \in R^\times$ der Fall. □

Folgerung 2.2. *Die Gleichung $\overline{ax} = \overline{1}$ ist in $({}^{\mathbb{Z}}/_{m\mathbb{Z}})^\times$ genau dann lösbar, wenn $\operatorname{ggT}\{a, m\} = 1$ gilt.*

Beispiel 2.10. Die Gleichung $13 \cdot x \equiv 1 \pmod{32}$ soll auf Lösungen untersucht werden. Mit dem Euklidischen Algorithmus

$$\begin{array}{rcrcr} 32 & = & 2 \cdot 13 & + & 6 \\ 13 & = & 2 \cdot 6 & + & 1 \end{array}$$

folgt $\operatorname{ggT}\{32, 13\} = 1$, und daher existieren Lösungen. Aus der Linearkombination des größten gemeinsamen Teilers

$$\begin{array}{rcrcc} 1 & = & 13 & - & 2 \cdot 6 \\ & = & 13 & - & 2(32 - 2 \cdot 13) \\ & = & -2 \cdot 32 & + & 5 \cdot 13 \end{array}$$

folgt durch Übergang zu Kongruenzen modulo 32, daß $x = 5$ eine Lösung darstellt.

Mit diesem Ergebnis kann man die Lösung der Gleichung mit allgemeiner rechter Seite

$$13 \cdot x \equiv a \pmod{32}$$

bestimmen, denn Multiplikation mit 5 ergibt

$$\begin{aligned} 5 \cdot 13 \cdot x &\equiv 5a \pmod{32} \\ x &\equiv 5a \pmod{32} \quad . \end{aligned}$$

Definition 2.6. Die Elemente von $({}^{\mathbb{Z}}/_{m\mathbb{Z}})^\times$ heißen **prime Restklassen modulo** m. Die Funktion $\varphi : \mathbb{N} \longrightarrow \mathbb{N}_0$ mit $\varphi(m) = \left|({}^{\mathbb{Z}}/_{m\mathbb{Z}})^\times\right|$ heißt **Eulersche** φ**-Funktion**.

Anmerkung: Mit Bemerkung 2.4 ergibt sich, daß $\varphi(m)$ die Anzahl der natürlichen Zahlen bezeichnet, die kleiner als m und zu m teilerfremd sind.

Satz 2.2 (Euler-Fermat)**.** *Ist $\overline{a}$ eine prime Restklasse modulo m, so gilt*

$$\overline{a}^{\varphi(m)} = \overline{1}.$$

Der *Beweis* folgt aus dem folgenden

Satz 2.3. *Ist G eine endliche abelsche Gruppe der Ordnung n und bezeichnet $\imath$ ihr Einselement, so gilt für alle Elemente γ von G die Beziehung $\gamma^n = \imath$.*

Beweis. Trivialerweise gilt $\gamma G \subseteq G$. Da aus $\gamma_i \neq \gamma_j$ immer $\gamma\gamma_i \neq \gamma\gamma_j$ folgt, gilt sogar $\gamma G = G$. Für das Produkt über alle Gruppenelemente gilt also $\prod_{i=1}^n \gamma_i = \prod_{i=1}^n (\gamma\gamma_i) = \gamma^n \prod_{i=1}^n \gamma_i$, woraus $\gamma^n = \imath$ folgt. □

Folgerung 2.3. *Sei p eine Primzahl. Dann gelten*

(a) *Für jedes $\overline{a} \in \mathbb{F}_p^\times$ ist $\overline{a}^{p-1} = \overline{1}$.*

(b) *Für jedes $\overline{a} \in \mathbb{F}_p$ ist $\overline{a}^p = \overline{a}$.*

Beweis.

(a) Da p Primzahl ist, gilt $\varphi(p) = \left|({}^{\mathbb{Z}}/_{p\mathbb{Z}})^\times\right| = \left|\mathbb{F}_p^\times\right| = p - 1$. Die Behauptung folgt damit unmittelbar aus dem Satz von Euler-Fermat.

(b) Für $\overline{a} \in \mathbb{F}_p^\times$ folgt die Behauptung aus Teil (a) durch Multiplikation mit $\overline{a}$. Die verbleibende Restklasse $\overline{0}$ erfüllt die Gleichung trivialerweise. □

3 Die Gruppe der primen Restklassen

3.1 Zyklische Gruppen

Definition 3.1. Ist G eine Gruppe, so wird die Anzahl der Elemente von G als **Gruppenordnung** $|G|$ bezeichnet. Die Gruppe heißt **zyklisch**, wenn jedes Gruppenelement sich als Potenz eines erzeugenden Elements schreiben läßt, wenn also ein Element γ existiert mit $G = \gamma^{\mathbb{Z}} = \{\, \gamma^n \mid n \in \mathbb{Z} \,\}$. Hierfür schreibt man auch $G = \langle \gamma \rangle$. Sind G und H Gruppen und ψ eine Abbildung von G in H, so heißt ψ **(Gruppen-)Homomorphismus**, wenn für alle Elemente α, β aus G stets $\psi(\alpha\beta) = \psi(\alpha)\psi(\beta)$ gilt. Ist die Abbildung ψ zusätzlich bijektiv, so heißt sie **Isomorphismus**. Hierfür wird dann $G \cong H$ geschrieben.

Beispiel 3.1. Die Abbildung $\psi : (\mathbb{Z}, +) \longrightarrow (2\mathbb{Z}, +)$ mit $\psi : n \mapsto 2n$ ist ein Isomorphismus von der Menge der ganzen Zahlen auf die Menge der geraden Zahlen.

Satz 3.1. *Eine zyklische Gruppe G ist entweder zu $(\mathbb{Z}, +)$ oder zu $(\mathbb{Z}/_{m\mathbb{Z}}, +)$ mit einer natürlichen Zahl m isomorph.*

Beweis. Es sei γ ein erzeugendes Element von G. Die Menge $\mathfrak{a} := \{\, n \in \mathbb{Z} \mid \gamma^n = \imath \,\}$ ist ein Ideal in $\mathbb{Z}$, denn sind $n, m \in \mathfrak{a}$ und $z \in \mathbb{Z}$, so gilt wegen

$$\gamma^{n-m} = \gamma^n(\gamma^m)^{-1} = \imath\imath^{-1} = \imath \quad \text{und } \gamma^{zn} = (\gamma^n)^z = \imath^z = \imath$$

auch $n - m \in \mathfrak{a}$ und $zn \in \mathfrak{a}$. Aus Satz 1.5 folgt, daß man das Ideal in der Form $\mathfrak{a} = m\mathbb{Z}$ mit $m \in \mathbb{N}_0$ darstellen kann. Im weiteren unterscheidet man die Fälle $m = 0$ und $m \in \mathbb{N}$:

Für $m = 0$ ist $\mathfrak{a} = \{0\}$ das Nullideal. Die Abbildung

$$\psi : G \longrightarrow \mathbb{Z} \quad \text{mit } \gamma^n \mapsto n$$

ist wohldefiniert, denn aus $\gamma^{n_1} = \gamma^{n_2}$ folgt wegen $\gamma^{n_1 - n_2} = \imath$, daß $n_1 - n_2 \in \mathfrak{a}$ gilt. Daraus folgt aber $n_1 - n_2 = 0$ und damit schließlich $n_1 = n_2$. Die Abbildung ψ ist ein Homomorphismus, da

$$\psi(\gamma^{n_1}\gamma^{n_2}) = \psi(\gamma^{n_1+n_2}) = n_1 + n_2 = \psi(\gamma^{n_1}) + \psi(\gamma^{n_2})$$

gilt. Da offensichtlich ψ bijektiv ist, ist ψ ein Isomorphismus von G auf $\mathbb{Z}$.

Im anderen Fall hat man $\mathfrak{a} = m\mathbb{Z}$ mit einer natürlichen Zahl m. Die Abbildung

$$\psi : G \longrightarrow \mathbb{Z}/_{m\mathbb{Z}} \quad \text{mit } \gamma^n \mapsto n + m\mathbb{Z}$$

ist wohldefiniert, denn aus $\gamma^{n_1} = \gamma^{n_2}$ folgt wegen $\gamma^{n_1-n_2} = \imath$, daß $n_1 - n_2 \in \mathfrak{a}$ gilt, woraus $n_1 + m\mathbb{Z} = n_2 + m\mathbb{Z}$ folgt. Die Abbildung ψ ist ein Homomorphismus wegen

$$\psi(\gamma^{n_1}\gamma^{n_2}) = \psi(\gamma^{n_1+n_2}) = n_1 + n_2 + m\mathbb{Z} = \psi(\gamma^{n_1}) + \psi(\gamma^{n_2}).$$

Da auch hier ψ offensichtlich bijektiv ist, ist ψ ein Isomorphismus von G auf $\mathbb{Z}/_{m\mathbb{Z}}$. □

Definition 3.2. Ist γ Element einer Gruppe G und hat $\mathfrak{a} = \{n \in \mathbb{Z} \mid \gamma^n = \imath\}$ (wie oben gezeigt) die Gestalt $\mathfrak{a} = m\mathbb{Z}$ mit $m \in \mathbb{N}_0$, so heißt m der **Exponent** von γ oder kurz $\exp(\gamma)$. Die Menge $\mathfrak{b} = \{\, n \in \mathbb{Z} \mid \gamma^n = \imath \quad \text{für alle } \gamma \in G \,\}$ ist offensichtlich ein Ideal, besitzt also auch die Darstellung $\mathfrak{b} = e\mathbb{Z}$ mit $e \in \mathbb{N}_0$. Die Zahl e heißt der **Exponent** von G oder kurz $\exp(G)$.

Bemerkung 3.1. *Für eine endliche abelsche Gruppe G ist $\exp(G)$ stets ein Teiler von $|G|$.*

Beweis. Wegen Satz 2.3 gilt für alle $\gamma \in G$ stets $\gamma^{|G|} = \imath$. Daher muß $|G|$ ein Vielfaches von $\exp(G)$ sein. □

Satz 3.2. *Es sei G eine endliche abelsche Gruppe. G ist genau dann zyklisch, wenn der Exponent von G gleich der Gruppenordnung ist.*

Beweis. Zunächst gelte $\exp(G) = |G| =: m$. Wegen

$$m\mathbb{Z} = \{\, n \in \mathbb{Z} \mid \gamma^n = \imath \quad \text{für alle } \gamma \in G \,\} = \bigcap_{\gamma \in G} \{\, n \in \mathbb{Z} \mid \gamma^n = \imath \,\} = \bigcap_{\gamma \in G} \exp(\gamma)\mathbb{Z}$$

ist m das kleinste gemeinsame Vielfache der Exponenten aller Gruppenelemente. Stellt man $m = p_1^{\nu_1} \cdot \ldots \cdot p_r^{\nu_r}$ in der Primzerlegung dar, so gibt es für alle i zwischen 1 und r ein Element $\widetilde{\gamma}_i$, dessen Exponent ein Vielfaches von $p_i^{\nu_i}$ ist. Denn aus $p_i^{\nu_i} \nmid \exp(\gamma)$ für alle $\gamma \in G$ würde folgen, daß m nicht das kleinste gemeinsame Vielfache aller Exponenten wäre. Setzt man

$$\gamma_i := \widetilde{\gamma}_i^{\exp(\widetilde{\gamma}_i)/p_i^{\nu_i}},$$

so gilt sogar $\exp(\gamma_i) = p_i^{\nu_i}$.

Nun wird gezeigt, daß $\gamma := \prod_{i=1}^r \gamma_i$ ein erzeugendes Element der Gruppe ist: Für alle $j = 1, \ldots, r$ gilt wegen $\exp(\gamma_i) = p_i^{\nu_i}$

$$\gamma^{\frac{m}{p_j}} = \prod_{i=1}^{r} \gamma_i^{\frac{m}{p_j}} = \gamma_j^{\frac{m}{p_j}} \neq \imath.$$

Damit gilt aber $\gamma^d \neq \imath$ für alle echten Teiler d von m, weil $\gamma^d = \imath$ den Widerspruch $\gamma^{\frac{m}{p_j}} = \imath$ für ein j zur Folge hätte. Folglich gilt $\exp(\gamma) = m = |G|$. Wegen $\exp(\gamma) = |\{\, \gamma^n \mid n \in \mathbb{Z} \,\}|$ ist γ ein erzeugendes Element von G und G damit eine zyklische Gruppe.

Zum Beweis der Umkehrung sei $G = \langle \gamma \rangle$ als zyklische Gruppe vorausgesetzt, womit $|G| = \exp(\gamma) \mid \exp(G)$ gilt. Nach Bemerkung 3.1 gilt aber auch $\exp(G) \mid |G|$, was $|G| = \exp(G)$ zur Folge hat. □

3.2 Primitivwurzeln

Satz 3.3. *Ist K ein Körper und $f(X) = \sum_{i=0}^n a_i X^i$ ein Polynom mit $a_i \in K$ und $a_n \neq 0$, so hat f höchstens n Nullstellen in K.*

Beweis. Für $n = 1$ hat das Polynom die Gestalt $f(x) = a_1 X + a_0$ und besitzt genau eine Nullstelle, nämlich $-a_0/a_1$. Die Richtigkeit der Behauptung für $n-1$ sei jetzt vorausgesetzt. Ist $x \in K$ eine Nullstelle von f, so gilt

$$f(X) = f(X) - f(x) = \sum_{i=0}^{n} a_i(X^i - x^i) = (X - x)g(X)$$

mit einem Polynom g vom Grad $n - 1$. Nach Induktionsvoraussetzung hat g höchstens $n - 1$ Nullstellen. Damit kann f höchstens n Nullstellen in K besitzen. □

Folgerung 3.1. *Für jede Primzahl p gilt*

$$\prod_{\overline{a}\in\mathbb{F}_p^\times}(X-\overline{a}) = X^{p-1}-\overline{1}.$$

Beweis. Jedes Element $\overline{a}$ aus $\mathbb{F}_p^\times$ ist wegen $\overline{a}^{p-1}-\overline{1}=\overline{0}$ eine Nullstelle von $X^{p-1}-\overline{1}$. Daher gilt

$$X^{p-1}-\overline{1} = \left(\prod_{\overline{a}\in\mathbb{F}_p^\times}(X-\overline{a})\right) g(x).$$

Ein Gradvergleich liefert, daß g einem konstanten Polynom $\overline{g}$ sein muß. Der Vergleich mit dem Koeffizienten von X^{p-1} ergibt $\overline{g}=\overline{1}$. □

Folgerung 3.2 (Satz von Wilson)**.** *Eine natürliche Zahl n ist genau dann eine Primzahl, wenn $(n-1)! \equiv -1 \pmod{n}$ gilt.*

Beweis. Ist n gleich einer Primzahl p, so gilt nach Folgerung 3.1

$$(X-1)(X-2)\cdot\ldots\cdot(X-(p-1)) \equiv X^{p-1}-1 \pmod{p}$$

Die Auswertung an der Stelle p ergibt

$$(p-1)! \equiv p^{p-1}-1 \equiv -1 \pmod{p}.$$

Ist n keine Primzahl, so existiert eine nichttriviale Darstellung $n=ab$. Wegen $a\,|\,(n-1)!$ und $b\,|\,(n-1)!$ gilt auch $n\,|\,(n-1)!$. Daraus folgt $(n-1)! \equiv 0 \not\equiv -1 \pmod{n}$. □

Satz 3.4. *Ist K ein Körper, so ist jede in $K^\times$ enthaltene endliche multiplikative Gruppe G zyklisch.*

Beweis. Es sei $m := \exp(G)$. Jedes Gruppenelement erfüllt die Gleichung $\gamma^m = \imath$ und ist damit Nullstelle von X^m-1. Nach Satz 3.3 gilt $|G|\le m$, aus Bemerkung 3.1 folgt aber $m \le |G|$. Also gilt $|G| = \exp(G)$ und nach Satz 3.2 ist G zyklisch. □

Folgerung 3.3. *$\mathbb{F}_p^\times$ ist eine zyklische Gruppe.*

Definition 3.3. Ein erzeugendes Element $\overline{w}$ von $\mathbb{F}_p^\times$ heißt **primitives Element** von $\mathbb{F}_p^\times$. Ein Vertreter w von $\overline{w}$ heißt **Primitivwurzel modulo** p.

Beispiel 3.2. Für $p=7$ gilt $\mathbb{F}_p^\times = \{\overline{1},\overline{2},\overline{3},\overline{4},\overline{5},\overline{6}\}$.

Wegen $\overline{2}^2 = 4, \overline{2}^3 = \overline{8} = \overline{1}$ ist 2 keine Primitivwurzel. Hingegen ist 3 wegen

$$\overline{3}^2 = \overline{2},\quad \overline{3}^3 = \overline{6},\quad \overline{3}^4 = \overline{4},\quad \overline{3}^5 = \overline{5},\quad \overline{3}^6 = \overline{1}$$

eine Primitivwurzel modulo 7.

Ordnet man gemäß $\overline{a} = \overline{3}^i$ jeder Restklasse modulo 7 den Exponenten i zu, erhält man die folgende Tabelle:

$\overline{a}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
i	6	2	1	4	5	3

Die Zahl i heißt **Index** von $\overline{a}$ bezüglich der Primitivwurzel 3. Die Tabelle wird als **Indextabelle** bezeichnet. Mit ihrer Hilfe können Multiplikationen durch Additionen ersetzt werden (ähnlich wie bei Logarithmen), was sich allerdings erst bei vielen Multiplikationen lohnt. Beispielsweise ergibt sich:

$$\begin{array}{rclclclcl}\overline{2}\cdot\overline{4} & = & \overline{3}^2\cdot\overline{3}^4 & = & \overline{3}^6 & = & \overline{1} & & \\ \overline{4}\cdot\overline{5} & = & \overline{3}^4\cdot\overline{3}^5 & = & \overline{3}^9 & = & \overline{3}^3 & = & \overline{6}\end{array}$$

3.3 Die Struktur von $(\mathbb{Z}/p^n\mathbb{Z})^\times$

Bemerkung 3.2. *Ist p eine Primzahl, so gilt*

$$\varphi(p^n) = (p-1)p^{n-1}.$$

Beweis. Die Anzahl der durch p teilbaren Zahlen zwischen 1 und p^n ist p^{n-1}. Damit gilt $\varphi(p^n) = p^n - p^{n-1} = (p-1)p^{n-1}$. □

Bezeichnung: Für jede ganze Zahl n und jede Primzahl p hat man eine Darstellung

$$n = p^a \cdot m \quad \text{mit } p \nmid m.$$

Die Zahl a heißt **Ordnung von** p in n und wird mit $\mathrm{ord}_p(n)$ bezeichnet. Ist

$$n = a_0 + a_1p + \cdots + a_rp^r \quad \text{mit } \ 0 \le a_i < p$$

die p–Entwicklung von n, so heißt $\mathrm{s}_p := a_0 + a_1 + \cdots + a_r$ die p–**Quersumme** von n.

Bemerkung 3.3. *Für jede natürliche Zahl n gilt*

$$\mathrm{ord}_p(n!) = \frac{1}{p-1}(n - \mathrm{s}_p(n))$$

Beweis. Stellt man n als $n = a_0 + a_1p + \cdots + a_rp^r$ dar, so geht, wie man durch Abzählen der Faktoren erkennt, p in $n! = 1\cdot 2\cdot 3\cdot 4\cdot\ldots\cdot(n-1)\cdot n$ genau $([\frac{n}{p}] + [\frac{n}{p^2}] + \cdots + [\frac{n}{p^r}])$-mal als Faktor auf. Somit ergibt sich

$$\begin{aligned}\mathrm{ord}_p(n!) &= (a_1 + a_2p + \cdots + a_rp^{r-1}) + (a_2 + a_3p + \cdots + a_rp^{r-2}) + \cdots + a_r \\ &= a_1 + a_2(1+p) + a_3(1+p+p^2) + \cdots + a_r(1+p+\cdots+p^{r-1}).\end{aligned}$$

Nach Multiplikation von $(p-1)$ auf beiden Seiten erhält man

$$(p-1)\,\mathrm{ord}_p(n!) = a_1(p-1) + a_2(p^2-1) + a_3(p^3-1) + \cdots + a_r(p^r-1) = n - \mathrm{s}_p(n).$$ □

Satz 3.5. *Für jede Primzahl $p > 2$ ist $(\mathbb{Z}/p^n\mathbb{Z})^\times$ eine zyklische Gruppe. Sie wird erzeugt von $\overline{w}(\overline{1+p})$, wobei w eine Primitivwurzel modulo p vom Exponenten $p-1$ in $(\mathbb{Z}/p^n\mathbb{Z})^\times$ ist.*

Beweis. Es sei $\widetilde{w}$ eine beliebige Primitivwurzel modulo p. Nach dem Satz von Fermat gilt $\widetilde{w}^p \equiv \widetilde{w} \pmod{p}$, woraus $\widetilde{w}^{p^2} \equiv \widetilde{w} \pmod{p}$ folgt. So fortfahrend erhält man schließlich $\widetilde{w}^{p^{n-1}} \equiv \widetilde{w} \pmod{p}$, womit auch $w := \widetilde{w}^{p^{n-1}}$ eine Primitivwurzel modulo p ist.

Betrachtet man nun den Restklassenring $\mathbb{Z}/_{p^n\mathbb{Z}}$, so folgt $\overline{w}^{p-1} = \overline{1}$ aus der Kongruenz

$$w^{p-1} = \widetilde{w}^{(p-1)p^{n-1}} = \widetilde{w}^{\psi(p^n)} \equiv 1 \pmod{p^n}.$$

Daher ist $\exp(\overline{w})$ ein Teiler von $p-1$. Andererseits ist w eine Primitivwurzel modulo p, was $\exp(\overline{w}) \geq p-1$ zur Folge hat. Somit gilt $\exp(\overline{w}) = p-1$.

Für jede Primzahl $p > 2$ gilt

$$(1+p)^{p^{n-1}} = 1 + \binom{p^{n-1}}{1} p + \binom{p^{n-1}}{2} p^2 + \cdots + p^{p^{n-1}} \equiv 1 \pmod{p^n},$$

denn die Ordnung von p in allen Termen der Form $\binom{p^{n-1}}{m} p^m$ mit $1 \leq m \leq p^{n-1}$ läßt sich nach Bemerkung 3.3 wie folgt abschätzen:

$$\begin{aligned} &\mathrm{ord}_p(\binom{p^{n-1}}{m} p^m) = \mathrm{ord}_p(\frac{p^{n-1}!}{m!(p^{n-1}-m)!}) + \mathrm{ord}_p(p^m) \\ = \;& \frac{1}{p-1}\big(p^{n-1} - m - (p^{n-1}-m) - \mathrm{s}_p(p^{n-1}) + \mathrm{s}_p(m) + \mathrm{s}_p(p^{n-1}-m)\big) + m \\ \geq \;& n, \end{aligned}$$

und daher sind alle außer dem ersten Summanden durch p^n teilbar. Analog zeigt man

$$(1+p)^{p^{n-2}} = 1 + \binom{p^{n-2}}{1} p + \binom{p^{n-2}}{2} p^2 + \cdots + p^{p^{n-2}} \equiv 1 + p^{n-1} \not\equiv 1 \pmod{p^n}.$$

Damit gilt $\exp(\overline{1+p}) = p^{n-1}$ in $(\mathbb{Z}/_{p^n\mathbb{Z}})^\times$. Hieraus folgt aber, daß $\overline{z} := \overline{w}(\overline{1+p})$ ein erzeugendes Element von $(\mathbb{Z}/_{p^n\mathbb{Z}})^\times$ ist. Da nämlich $\exp(\overline{1+p})$ und $\exp(\overline{w})$ teilerfremd sind, ist $\overline{z}^i = \overline{1}$ gleichbedeutend mit $\overline{w}^i = \overline{1}$ und $\overline{1+p}^i = \overline{1}$. Dann ist aber sowohl $p-1$ als auch p^{n-1} ein Teiler von i. Also ist auch $\varphi(p^n)$ ein Teiler von i und es gilt $\exp(\overline{z}) = \varphi(p^n) = \left|(\mathbb{Z}/_{p^n\mathbb{Z}})^\times\right|$. Nach Satz 3.2 ist $(\mathbb{Z}/_{p^n\mathbb{Z}})^\times$ damit eine zyklische Gruppe mit $\overline{w}(\overline{1+p})$ als erzeugendem Element. □

Beispiel 3.3. Kongruenzen modulo p^n lassen sich schrittweise durch Kongruenzen modulo p lösen. Gesucht sei beispielsweise die Lösung von

$$2x \equiv 3 \pmod{5^n}.$$

Für $n = 1$ lautet die Kongruenz $2x_1 \equiv 3 \pmod{5}$. Eine Lösung ist $x_1 = 4$.

Für $n = 2$ lautet die Kongruenz $2x_2 \equiv 3 \pmod{25}$. Wegen $x_2 \equiv x_1 \pmod{5}$ besitzt x_2 die Darstellung $x_2 = x_1 + 5a_2 = 4 + 5a_2$. Dann gilt $2x_2 - 3 = 2(4+5a_2) - 3 = 5 + 5 \cdot 2a_2 = 5(1+2a_2) \equiv 0 \pmod{25}$, womit $1 + 2a_2 \equiv 0 \pmod{5}$ gelten muß. Eine Lösung lautet $a_2 = 2$, also gilt $x_2 = 14$.

Für $n = 3$ lautet die Kongruenz $2x_3 \equiv 3 \pmod{5^3}$. Wegen $x_3 \equiv x_2 \pmod{25}$ besitzt x_3 die Darstellung $x_3 = x_2 + 25a_3 = 14 + 25a_3$. Dann gilt $2x_3 - 3 = 25 + 25 \cdot 2a_3 = 25(1+2a_3) \equiv 0$

(mod 5^3), womit $1 + 2a_3 \equiv 0 \pmod 5$ gelten muß. Eine Lösung lautet $a_3 = 2$, also gilt $x_3 = 64$.

Durch Induktion erhält man schließlich

$$x \equiv 4 + 2 \cdot 5 + 2 \cdot 5^2 + \cdots + 2 \cdot 5^{n-1} \pmod{5^n}.$$

Eine alternative Lösungsmöglichkeit sieht wie folgt aus: Aus $2x \equiv 3 \pmod{5^n}$ folgt

$$\begin{aligned} x &\equiv \tfrac{3}{2} \equiv \tfrac{6}{4} \equiv (-6)\tfrac{1-5^n}{1-5} \equiv -(1+5)(1+5+\cdots+5^{n-1}) \\ &\equiv -(1 + 2 \cdot 5 + 2 \cdot 5^2 + \cdots + 2 \cdot 5^{n-1}) \\ &\equiv 4 + 2 \cdot 5 + 2 \cdot 5^2 + \cdots + 2 \cdot 5^{n-1} \pmod{5^n}. \end{aligned}$$

Satz 3.6. *Es gilt* $(\mathbb{Z}/2^n\mathbb{Z})^\times \cong \langle\overline{-1}\rangle \times \langle\overline{5}\rangle$.

Beweis. Für $n = 1$ ergibt sich $(\mathbb{Z}/2\mathbb{Z})^\times = \langle\overline{1}\rangle \cong \langle\overline{1}\rangle \times \langle\overline{1}\rangle$. Es sei also $n \geq 2$. Offenbar gilt $\exp(\overline{-1}) = 2$. Mit einem zum Beweis von Satz 3.5 analogen Schluß erhält man $\exp(\overline{5}) = 2^{n-2}$ wegen

$$\begin{aligned} 5^{2^{n-2}} &= (1+2^2)^{2^{n-2}} = 1 + \binom{2^{n-2}}{1} 2^2 + \binom{2^{n-2}}{2} 2^4 + \cdots \equiv 1 \pmod{2^n} \\ 5^{2^{n-3}} &= (1+2^2)^{2^{n-3}} = 1 + \binom{2^{n-3}}{1} 2^2 + \binom{2^{n-3}}{2} 2^4 + \cdots \equiv 1 + 2^{n-1} \not\equiv 1 \pmod{2^n}. \end{aligned}$$

Gilt $(-1)^i 5^j \equiv (-1)^{i'} 5^{j'}$, wobei offenbar $i, i' \in \{0, 1\}$ und $j, j' \in \{0, 1, \ldots, 2^{n-2} - 1\}$ angenommen werden dürfen, so erhält man $(-1)^{i-i'} \equiv 5^{j'-j} \pmod{2^n}$. Für $i \neq i'$ würde $i - i' \equiv -1 \pmod 4$ gelten, was den Widerspruch

$$(-1)^{-1} \equiv -1 \not\equiv 1 \equiv 5^{j'-j} \pmod 4$$

zur Folge hätte. Also gilt $i = i'$ und damit auch $j = j'$. Folglich gibt es genau $2^{n-1} = \varphi(2^n)$ viele verschiedene Produkte der Form $(-1)^i 5^j$. Daraus ergibt sich die Behauptung. $\square$

Beispiel 3.4. Für $n = 2, 3, 4$ ergeben sich:

$$\begin{aligned} (\mathbb{Z}/4\mathbb{Z})^\times &= \langle\overline{-1}\rangle \times \langle\overline{1}\rangle &\cong& \quad Z_2, \\ (\mathbb{Z}/8\mathbb{Z})^\times &= \langle\overline{-1}\rangle \times \langle\overline{5}\rangle &\cong& \quad Z_2 \times Z_2, \\ (\mathbb{Z}/16\mathbb{Z})^\times &= \langle\overline{-1}\rangle \times \langle\overline{5}\rangle &\cong& \quad Z_2 \times Z_4. \end{aligned}$$

4 Simultane Kongruenzen

4.1 Hauptsatz über simultane Kongruenzen

Definition 4.1. Sind $(R, +, \cdot)$ und $(S, +, \cdot)$ Ringe, so heißt eine Abbildung ψ von R in S ein **(Ring-)Homomorphismus**, wenn für alle Elemente a und b aus R stets

$$\psi(a+b) = \psi(a) + \psi(b) \quad \text{und } \psi(a \cdot b) = \psi(a) \cdot \psi(b)$$

gelten. Ist ein Homomorphismus ψ zusätzlich bijektiv, so heißt er **Isomorphismus**.

Beispiel 4.1. Die Abbildung $\kappa : \mathbb{Z} \longrightarrow {}^{\mathbb{Z}}/_{m\mathbb{Z}}$ mit $a \mapsto \overline{a} := a + m\mathbb{Z}$ ist ein Ringhomomorphismus und wird als **Restklassenhomomorphismus** oder **kanonischer Homomorphismus** bezeichnet.

Satz 4.1 (Hauptsatz über simultane Kongruenzen). *Sind $m_1, \ldots, m_r$ paarweise teilerfremde Zahlen mit $m = \prod_{i=1}^r m_i$, dann ist die Abbildung*

$$\rho : {}^{\mathbb{Z}}/_{m\mathbb{Z}} \longrightarrow \prod_{i=1}^r ({}^{\mathbb{Z}}/_{m_i\mathbb{Z}}) \quad \text{mit } a + m\mathbb{Z} \mapsto (a + m_1\mathbb{Z}, \ldots, a + m_r\mathbb{Z})$$

ein Ringisomorphismus, wobei $\prod_{i=1}^r ({}^{\mathbb{Z}}/_{m_i\mathbb{Z}})$ als kartesisches Produkt mit komponentenweiser Verknüpfung zu verstehen ist. Die Umkehrabbildung ist durch

$$\rho^{-1} : \prod_{i=1}^r ({}^{\mathbb{Z}}/_{m_i\mathbb{Z}}) \longrightarrow {}^{\mathbb{Z}}/_{m\mathbb{Z}} \quad \text{mit } (a_1 + m_1\mathbb{Z}, \ldots, a_r + m_r\mathbb{Z}) \mapsto a + m\mathbb{Z}$$

gegeben mit

$$a = \sum_{i=1}^r a_i e_i \quad \text{und } e_i = (\frac{m}{m_i})^{\varphi(m_i)}.$$

Beweis. Für $i = 1, \ldots, r$ ist die Abbildung

$$\rho_i : {}^{\mathbb{Z}}/_{m\mathbb{Z}} \longrightarrow {}^{\mathbb{Z}}/_{m_i\mathbb{Z}} \quad \text{mit } a + m\mathbb{Z} \mapsto a + m_i\mathbb{Z}$$

ein Homomorphismus, da sie eine Klassenvergröberung darstellt. Aufgrund der komponentenweisen Erklärung der Verknüpfungen ist damit auch ρ ein Homomorphismus. Zum Beweis der Injektivität gelte

$$\rho(a + m\mathbb{Z}) = (0 + m_1\mathbb{Z}, \ldots, 0 + m_r\mathbb{Z}).$$

Dann sind aber $m_1, \ldots, m_r$ Teiler von a, was $m \mid a$ zur Folge hat. Daher gilt

$$a + m\mathbb{Z} = 0 + m\mathbb{Z}.$$

Die Surjektivität von ρ folgt aus der Tatsache, daß ρ zwei Mengen von je m Elementen injektiv aufeinander abbildet. Somit ist ρ ein Isomorphismus. Nun wird gezeigt, daß $\rho \circ \rho^{-1}$ die identische Abbildung in $\prod_{i=1}^r ({}^{\mathbb{Z}}/_{m_i\mathbb{Z}})$ darstellt. Es gilt

$$\rho(\sum_{i=1}^r a_i (\frac{m}{m_i})^{\varphi(m_i)} + m\mathbb{Z}) = \left(\sum_{i=1}^r a_i (\frac{m}{m_i})^{\varphi(m_i)} + m_1\mathbb{Z}, \ldots, \sum_{i=1}^r a_i (\frac{m}{m_i})^{\varphi(m_i)} + m_r\mathbb{Z}\right).$$

Also gilt für die j-te Komponente aufgrund der Teilbarkeit von ${}^{m}/_{m_i}$ durch m_j für $i \neq j$ nach dem Satz von Euler-Fermat

$$\sum_{i=1}^r a_i (\frac{m}{m_i})^{\varphi(m_i)} + m_j\mathbb{Z} = a_j (\frac{m}{m_j})^{\varphi(m_j)} + m_j\mathbb{Z} = a_j + m_j\mathbb{Z}. \qquad \square$$

Beispiel 4.2. Zur Lösung der Kongruenz $x^2 \equiv 36 \pmod{56}$ setzt man $m = 56$, $m_1 = 7$ und $m_2 = 8$ und löst die beiden Kongruenzen

$$\begin{array}{rr} x^2 \equiv 36 \equiv 1 \pmod{7}, & x^2 \equiv 36 \equiv 4 \pmod{8} \\ x \equiv \pm 1 \pmod{7}, & x \equiv \pm 2 \pmod{8} \end{array} .$$

Die Lösungen in $\mathbb{Z}/_{7\mathbb{Z}} \times \mathbb{Z}/_{8\mathbb{Z}}$ lauten demnach

$$x_1' = (-1,-2), \quad x_2' = (1,-2), \quad x_3' = (1,2) \quad \text{und } x_4' = (-1,2).$$

Durch Bestimmung von e_1 und e_2 erhält man alle Lösungen in $\mathbb{Z}/_{56\mathbb{Z}}$:

$$e_1 = (\frac{m}{m_1})^{\varphi(m_1)} \equiv 8^6 \equiv 8 \pmod{56}, \qquad e_2 = (\frac{m}{m_2})^{\varphi(m_2)} \equiv 7^4 \equiv -7 \pmod{56},$$

$$\begin{array}{llllll} x_1 & \equiv & -8+2\cdot 7 & \equiv & 6 & \pmod{56}, \\ x_3 & \equiv & -x_1 & \equiv & -6 & \pmod{56}, \end{array} \qquad \begin{array}{llllll} x_2 & \equiv & 8+2\cdot 7 & \equiv & 22 & \pmod{56}, \\ x_4 & \equiv & -x_2 & \equiv & -22 & \pmod{56}. \end{array}$$

Anmerkung: Mit den Bezeichnungen aus Satz 4.1 gelten für $\overline{e_i} := e_i + m\mathbb{Z}$ die Beziehungen

$$\overline{e_i e_i} = \overline{e_i}, \qquad \overline{e_i e_j} = \overline{0} \quad \text{für } i \neq j \quad \text{und } \overline{e_1} + \cdots + \overline{e_r} = \overline{1}.$$

Die $\overline{e_i}$ bilden daher eine **Zerlegung der Eins von $\mathbb{Z}/_{m\mathbb{Z}}$ in paarweise orthogonale Idempotente**.

Beweis. Es gilt $e_i \equiv 1 \pmod{m_i}$ und $e_i \equiv 0 \pmod{m_j}$ für $j \neq i$, da m_j ein Teiler von $^m/_{m_i}$ ist. Für alle $j = 1, \ldots, r$ gilt damit $\sum_{i=1}^r e_i \equiv 1 \pmod{m_j}$, was $\sum_{i=1}^r e_i \equiv 1 \pmod{m}$ und schließlich $\overline{e_1} + \cdots + \overline{e_r} = \overline{1}$ zur Folge hat.

Aus $m \mid e_i e_j$ für $i \neq j$ folt weiter $e_i e_j \equiv 0 \pmod{m}$ und damit $\overline{e_i e_j} = \overline{0}$.

Aus $e_i e_i \equiv 1 \pmod{m_i}$ und $e_i e_i \equiv 0 \pmod{m_j}$ für $i \neq j$ folgt nach Satz 4.1 $e_i e_i \equiv e_i \pmod{m}$ und damit $\overline{e_i e_i} = \overline{e_i}$. □

4.2 Die Struktur der Einheitengruppe $(\mathbb{Z}/_{m\mathbb{Z}})^\times$

Satz 4.2. *Sind $m_1, \ldots, m_r$ paarweise teilerfremde Zahlen mit $m = \prod_{i=1}^r m_i$, dann ist die Abbildung*

$$\widetilde{\rho} : (\mathbb{Z}/_{m\mathbb{Z}})^\times \longrightarrow \prod_{i=1}^r (\mathbb{Z}/_{m_i\mathbb{Z}})^\times \quad \text{mit } a + m\mathbb{Z} \mapsto (a + m_1\mathbb{Z}, \ldots, a + m_r\mathbb{Z})$$

ein Gruppenisomorphismus, wobei $\prod_{i=1}^r (\mathbb{Z}/_{m_i\mathbb{Z}})^\times$ als kartesisches Produkt mit komponentenweiser Verknüpfung zu verstehen ist.

Beweis. Sind $\overline{a} \in (\mathbb{Z}/_{m\mathbb{Z}})^\times$ und $a \in \overline{a}$, so folgt $\mathrm{ggT}\{a, m\} = 1$ aus Bemerkung 2.4. Daher ist a zu jedem der m_i teilerfremd. Bezeichnet ρ den Ringisomorphismus aus Satz 4.1, so bedeutet dies, daß

$$\rho(\overline{a}) \in \prod_{i=1}^r (\mathbb{Z}/_{m_i\mathbb{Z}})^\times$$

gilt. Also ist $\widetilde{\rho} = \rho|_{(\mathbb{Z}/m\mathbb{Z})^\times}$ eine Abbildung in $\prod_{i=1}^r (\mathbb{Z}/m_i\mathbb{Z})^\times$ mit $\widetilde{\rho}(\overline{a}\overline{b}) = \widetilde{\rho}(\overline{a})\widetilde{\rho}(\overline{b})$ und damit ein Gruppenhomomorphismus. Aus der Injektivität von ρ folgt sofort die Injektivität von $\widetilde{\rho}$. Gelten andererseits $\overline{a} \notin (\mathbb{Z}/m\mathbb{Z})^\times$ und $a \in \overline{a}$, so sind a und m nach Bemerkung 2.4 nicht teilerfremd, besitzen also einen gemeinsamen Primteiler, etwa p. Da p auch in mindestens einem der m_i aufgeht, folgt

$$a + m_i\mathbb{Z} \notin (\mathbb{Z}/m_i\mathbb{Z})^\times.$$

Also ist $\widetilde{\rho}$ auch surjektiv und damit ein Isomorphismus. □

Folgerung 4.1. *Sind $m_1, \ldots, m_r$ paarweise teilerfremde Zahlen mit $m = \prod_{i=1}^r m_i$, so gilt*

$$\varphi(m) = \prod_{i=1}^r \varphi(m_i).$$

Beweis. Aufgrund von Definition 2.6 gilt

$$\varphi(m) = \left|(\mathbb{Z}/m\mathbb{Z})^\times\right| \quad \text{und} \quad \prod_{i=1}^r \varphi(m_i) = \prod_{i=1}^r \left|(\mathbb{Z}/m_i\mathbb{Z})^\times\right| = \left|\prod_{i=1}^r (\mathbb{Z}/m_i\mathbb{Z})^\times\right|.$$

Die Behauptung ergibt sich nun aus Satz 4.1 wegen

$$\left|(\mathbb{Z}/m\mathbb{Z})^\times\right| = \left|\prod_{i=1}^r (\mathbb{Z}/m_i\mathbb{Z})^\times\right|.$$ □

Anmerkung: Funktionen auf $\mathbb{N}$ mit der Eigenschaft aus Folgerung 4.1 heißen **schwach multiplikativ**.

Folgerung 4.2. *Für jede natürliche Zahl m gilt*

$$\varphi(m) = m \prod_{p \mid m} (1 - \frac{1}{p}).$$

Beweis. Es sei $m = \prod_{i=1}^r p_i^{n_i}$ die Primzerlegung von m. Wegen Folgerung 4.1 und Bemerkung 3.2 gilt

$$\varphi(m) = \prod_{i=1}^r \varphi(p_i^{\nu_i}) \quad \text{und } \varphi(p_i^{\nu_i}) = (p_i - 1)p_i^{\nu_i - 1},$$

womit sich die Behauptung ergibt:

$$\varphi(m) = \prod_{i=1}^r p_i^{\nu_i}(1 - \frac{1}{p_i}) = m \prod_{i=1}^r (1 - \frac{1}{p_i}).$$ □

4.3 Diophantische Gleichungen und Kongruenzen

Bezeichnungen: Eine formale Summe der Form

$$f(\underline{X}) = \sum_{\underline{i} \in \mathbb{N}_0^n} a_{\underline{i}} \underline{X}^{\underline{i}} = \sum_{(i_1,\dots,i_n) \in \mathbb{N}_0^n} a_{i_1,\dots,i_n} X_1^{i_1} \cdot \ldots \cdot X_n^{i_n}$$

mit Variablen X_i und Koeffizienten $a_{\underline{i}}$ aus einem kommutativen nullteilerfreien Ring R, von denen höchstens endlich viele von Null verschieden sind, heißt **Polynom in n Variablen (Unbestimmten) über** R. Für die Menge aller dieser Polynome wird

$$R[X_1, \dots, X_n] \quad \text{oder } R[\underline{X}]$$

geschrieben. Ist f nicht das Nullpolynom (bei dem alle $a_{\underline{i}}$ Null sind), so bezeichnet

$$\partial(f) := \max \left\{ i_1 + \cdots + i_n \mid a_{\underline{i}} \neq 0 \right\}$$

den **(Gesamt-)Grad von** f. Sind von der Gleichung $f(\underline{X}) = \underline{0}$ Lösungen in $\mathbb{Z}^n$ gesucht, so nennt man diese Fragestellung **diophantisches Problem**.

Beispiel 4.3. Die Gleichung

$$x^4 + y^4 = z^4 + 13$$

soll auf ganzzahlige Lösungen untersucht werden. Hätte die Gleichung ganzzahlige Lösungen, so wäre auch die Kongruenz

$$x^4 + y^4 - z^4 \equiv 3 \pmod 5$$

lösbar. Aufgrund des Satztes von Euler-Fermat können vierte Potenzen modulo 5 nur die Werte 0 oder 1 annehmen. Also ist die Kongruenz und damit auch die diophantische Gleichung unlösbar.

Beispiel 4.4. Durch Umformung der Gleichung

$$\begin{aligned} 6xy - 3x - 2y + 1 &= 0 \\ (3x - 1)(2y - 1) &= 0 \end{aligned}$$

liest man die Lösungsmenge $\{ ({}^1/_3, b), (a, {}^1/_2) \mid a, b \in \mathbb{Q} \}$ in $\mathbb{Q} \times \mathbb{Q}$ ab. Da keine der Lösungen ganzzahlig ist, besitzt die Gleichung keine Lösungen in $\mathbb{Z} \times \mathbb{Z}$. Die Betrachtung von Kongruenzen führt bei dieser Gleichung nicht zum Ziel, da für jede Primzahl p entweder die Kongruenz

$$3x \equiv 1 \pmod p \quad \text{oder } 2y \equiv 1 \pmod p$$

lösbar ist. Die Lösbarkeit der Kongruenzgleichungen ist also nur eine notwendige, aber im allgemeinen keine hinreichende Bedingung für die Lösbarkeit der Ausgangsgleichung.

Satz 4.3 (Satz von Warning). *Es sei $f(X_1, \dots, X_n) = \sum_{\underline{i} \in \mathbb{N}_0^n} a_{\underline{i}} \underline{X}^{\underline{i}} \in \mathbb{F}_p[\underline{X}]$ ein Polynom, bei dem der Gesamtgrad $\partial(f)$ kleiner ist als die Anzahl der Variablen n. Dann ist die Anzahl der Lösungen in $\mathbb{F}_p^n$ durch p teilbar. Anders gesagt: Für die Lösungsmenge in $\mathbb{F}_p^n$*

$$L := \left\{ (x_1, \dots, x_n) \in \mathbb{F}_p^n \mid f(\underline{x}) = 0 \right\}$$

gilt $|L| \equiv 0 \pmod p$.

Beweis. Es sei g das Polynom mit

$$g(\underline{X}) := 1 - f(\underline{X})^{p-1} \in \mathbb{F}_p[\underline{X}] \quad \text{und } g(\underline{X}) = \sum_{\underline{j} \in \mathbb{N}_0^n} b_{\underline{j}} \underline{X}^{\underline{j}}.$$

Ist $\underline{x}$ Nullstelle von f, so gilt $g(\underline{x}) = 1$. Ist $\underline{x}$ keine Nullstelle von f, so gilt nach dem Satz von Euler-Fermat $f(\underline{x})^{p-1} = 1$ und damit $g(\underline{x}) = 0$. Also gilt

$$\sum_{\underline{x} \in \mathbb{F}_p^n} g(\underline{x}) = |L|\,.$$

Wegen

$$\sum_{\underline{x} \in \mathbb{F}_p^n} (x_1^{j_1} \cdot \ldots \cdot x_n^{j_n}) = (\sum_{x \in \mathbb{F}_p} x^{j_1}) \cdot \ldots \cdot (\sum_{x \in \mathbb{F}_p} x^{j_n})$$

gilt die Beziehung

$$\sum_{\underline{x} \in \mathbb{F}_p^n} g(\underline{x}) = \sum_{\underline{j} \in \mathbb{N}_0^n} b_{\underline{j}} \sum_{\underline{x} \in \mathbb{F}_p^n} \prod_{k=1}^{n} x_k^{j_k} = \sum_{\underline{j} \in \mathbb{N}_0^n} b_{\underline{j}} \prod_{k=1}^{n} (\sum_{x \in \mathbb{F}_p} x^{j_k}).$$

Nach Voraussetzung gilt $\partial(f) < n$, was $\partial(g) < n(p-1)$ zur Folge hat. Zu jedem $\underline{j}$ mit $b_{\underline{j}} \neq 0$ muß es also ein k mit $1 \leq k \leq n$ und ein j_k mit $j_k < p-1$ geben. Im folgenden sei $j := j_k$. Für $j = 0$ gilt $\sum_{x \in \mathbb{F}_p} x^j = \sum_{x \in \mathbb{F}_p} 1 = 0$ in $\mathbb{F}_p$. Für $j \neq 0$ gibt es wegen $\exp(\mathbb{F}_p^\times) = p-1$ ein $y \in \mathbb{F}_p$ mit $y^j \neq 1$. Da mit x auch yx alle Elemente von $\mathbb{F}_p$ durchläuft, gilt

$$S := \sum_{x \in \mathbb{F}_p} x^j = \sum_{x \in \mathbb{F}_p} (yx)^j = y^j \sum_{x \in \mathbb{F}_p} x^j = y^j S,$$

was wegen $y^j \neq 1$ schließlich $S = 0$ zur Folge hat. Damit ist gezeigt, daß für jedes $\underline{j}$ mit $b_{\underline{j}} \neq 0$ mindestens ein Faktor der Form $\sum_{x \in \mathbb{F}_p} x^{j_k}$ gleich 0 ist. Also gilt $|L| = \sum_{\underline{x} \in \mathbb{F}_p^n} g(\underline{x}) = 0$ in $\mathbb{F}_p$. □

Folgerung 4.3. *Besitzt ein Polynom $f(X_1, \ldots, X_n) \in \mathbb{F}_p[\underline{X}]$ mit $\partial(f) < n$ eine Nullstelle in $\mathbb{F}_p^n$, so besitzt es mindestens p Nullstellen in $\mathbb{F}_p^n$.*

Folgerung 4.4 (Satz von Chevalley). *Jedes nicht konstante homogene Polynom*

$$f(X_1, \ldots, X_n) \in \mathbb{F}_p[\underline{X}]$$

mit $\partial(f) < n$ besitzt über $\mathbb{F}_p$ mindestens eine nichttriviale Nullstelle.

Bezeichnet man ein homogenes Polynom vom Gesamtgrad 2 als **quadratische Form**, so gilt speziell auch

Folgerung 4.5. *Jede quadratische Form über $\mathbb{F}_p$ mit mindestens 3 Variablen besitzt ein nichttriviale Lösung.*

5 Quadratische Reste

5.1 Das Legendre-Symbol

Definition 5.1. Es sei p eine ungerade Primzahl. Eine prime Restklasse $\overline{a} \in \mathbb{F}_p^\times$ bzw. deren Vertreter $a \in \mathbb{Z}$ heißt **quadratischer Rest modulo** p, wenn eine Restklasse $\overline{x} \in \mathbb{F}_p^\times$ mit $\overline{x}^2 = \overline{a}$ existiert. Zur Kennzeichnung quadratischer Reste dient das **Legendre-Symbol**

$$\left(\frac{a}{p}\right) := \begin{cases} \ \ 1, & \text{falls } a \text{ quadratischer Rest modulo } p \\ -1, & \text{falls } a \text{ kein quadratischer Rest modulo } p \end{cases},$$

(lies: a über p). Für $p = 2$ wird die Definition des Legendre-Synbols an späterer Stelle nachgetragen. Da es für manche Zwecke günstig ist, ein Legendre-Symbol auch im Fall $p \mid a$ zur Verfügung zu haben, definiert man

$$\left(\frac{a}{p}\right) := 0 \quad \text{für } p \mid a.$$

Bemerkung 5.1. *Ist p eine ungerade Primzahl, so bildet die Menge*

$$Q := \left\{\, \overline{a} \in \mathbb{F}_p^\times \ \mid \overline{a} \quad \text{ist quadratischer Rest} \ \right\}$$

eine Untergruppe von $\mathbb{F}_p^\times$ der Ordnung $\frac{p-1}{2}$.

Beweis. Sind $\overline{a}, \overline{b} \in Q$, so gibt es $\overline{x}, \overline{y} \in \mathbb{F}_p^\times$ mit $\overline{x}^2 = \overline{a}$ und $\overline{y}^2 = \overline{b}$. Wegen $(\overline{xy})^2 = \overline{a}\overline{b}$ ist Q multiplikativ abgeschlossen. Da $\overline{1} \in Q$ und mit $\overline{a} \in Q$ auch $\overline{a}^{-1} \in Q$ gilt, bildet Q damit eine Untergruppe von $\mathbb{F}_p^\times$.

Ist w eine Primitivwurzel modulo p, so sind die geraden Potenzen $\overline{w}^2, \overline{w}^4, \ldots, \overline{w}^{p-1}$ verschieden, also gilt $|Q| \geq \frac{p-1}{2}$. Da eine Primitivwurzel modulo p kein quadratischer Rest ist, gibt es mindestens einen quadratischen Nichtrest und weil mit $\overline{b} \notin Q$ auch $\overline{a}\overline{b} \notin Q$ für alle $\overline{a} \in Q$ gilt, ist die Anzahl der quadratischen Reste ebenso groß wie die Anzahl der quadratischen Nichtreste, was $|Q| = \frac{p-1}{2}$ zur Folge hat. □

Satz 5.1 (Euler-Kriterium)**.** *Ist a eine ganze Zahl und p eine ungerade Primzahl, so gilt*

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$

Beweis. Ist p ein Teiler von a, so ergibt sich die triviale Kongruenz $0 \equiv 0 \pmod{p}$. Im folgenden gelte also $p \nmid a$.

Im Falle $\left(\frac{a}{p}\right) = 1$ gibt es ein $x \in \mathbb{Z}$ mit $a \equiv x^2 \pmod{p}$. Durch Anwendung des Satzes von Euler-Fermat ergibt sich

$$a^{(p-1)/2} \equiv x^{p-1} \equiv 1 \pmod{p}.$$

Im Falle $\left(\frac{a}{p}\right) = -1$ gilt mit einer Primitivwurzel w und einer Zahl $n \in \mathbb{N}$ die Kongruenz $a \equiv w^{2n+1} \pmod{p}$. Hieraus folgt durch nochmalige Anwendung des Satzes von Euler-Fermat

$$a^{(p-1)/2} \equiv w^{(p-1)n} w^{(p-1)/2} \equiv w^{(p-1)/2} \pmod{p}.$$

Setzt man zur Abkürzung $v := w^{(p-1)/2}$, so folgt durch Quadrieren der Kongruenz

$$v^2 \equiv a^{p-1} \equiv 1 \pmod p,$$

was $\overline{v} \in \{\overline{1}, -\overline{1}\}$ in $\mathbb{F}_p$ zur Folge hat. Wegen $\exp(\overline{w}) = p-1$ kann nicht $\overline{v} = \overline{1}$ gelten. Also gilt $\overline{v} = -\overline{1}$ und damit lautet die Kongruenz $a^{(p-1)/2} \equiv -1 \pmod p$. $\square$

Folgerung 5.1. *Für ganze Zahlen a und b und eine ungerade Primzahl p gilt*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Beweis. Im Falle $p \mid ab$ gilt entweder $p \mid a$ oder $p \mid b$, wodurch die Aussage trivial wird. Für $p \nmid ab$ ergibt die zweimalige Anwendung von Satz 5.1

$$\left(\frac{ab}{p}\right) \equiv (ab)^{(p-1)/2} \equiv a^{(p-1)/2} b^{(p-1)/2} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod p. \qquad \square$$

5.2 Das Jacobi-Symbol

Definition 5.2. Es sei m eine ungerade Zahl. Die Menge $H_m := \{h_1, \ldots, h_{(m-1)/2}\}$ heißt **Halbsystem modulo** m, wenn $\mathbb{Z}/m\mathbb{Z}$ die Darstellung

$$\mathbb{Z}/m\mathbb{Z} = \overline{H}_m \cup (-\overline{H}_m) \cup \{\overline{0}\}$$

besitzt, d.h. wenn die Zahlen $\pm h_1, \ldots, \pm h_{(m-1)/2}, 0$ ein vollständiges Restsystem modulo m bilden.

Beispiel 5.1. Die Menge $h_m = \{1, 2, \ldots, \frac{m-1}{2}\}$ ist ein Halbsystem modulo m.

Beispiel 5.2. Ist H_m ein Halbsystem modulo m und a eine ganze Zahl mit $\mathrm{ggT}\{a, m\} = 1$, so ist auch $aH_m = \{ah_i \mid i = 1, \ldots, \frac{m-1}{2}\}$ ein Halbsystem modulo m, da wiederum $\mathbb{Z}/m\mathbb{Z} = \overline{a}\overline{H}_m \cup (-\overline{a}\overline{H}_m) \cup \{\overline{0}\}$ gilt.

Bemerkung 5.2. *Es sei m eine ungerade natürliche Zahl, a eine ganze zu m teilerfremde Zahl und $H_m = \{h_1, \ldots, h_{(m-1)/2}\}$ ein Halbsystem modulo m. Dann gibt es eine Permutation $\pi \in S_{(m-1)/2}$ und Zahlen $v_i \in \{-1, 1\}$ mit*

$$ah_i \equiv v_i h_{\pi(i)} \pmod m.$$

Dabei ist $\prod_{i=1}^{(m-1)/2} v_i$ eine vom gewählten Halbsystem unabhängige Größe.

Beweis. Für jedes i wird v_i und $\pi(i)$ wie folgt gewählt: Im Fall $\overline{a}\overline{h}_i \in \overline{H}_m$ setzt man $v_i = 1$ und wählt $\pi(i)$ passend. Sonst gilt $\overline{a}\overline{h}_i \in -\overline{H}_m$, wobei man $v_i = -1$ setzt und $\pi(i)$ wieder passend gewählt werden kann. Da aH_m nach Beispiel 5.2 ein Halbsystem modulo m bildet, gilt für $i \neq j$ stets $\pi(i) \neq \pi(j)$. Folglich ist π eine Permutation. Es sei $\widetilde{H}_m := \{\widetilde{h}_1, \ldots, \widetilde{h}_{(m-1)/2}\}$ ein zweites Halbsystem modulo m, wobei $\widetilde{h}_i = h_i$ oder $\widetilde{h}_i = -h_i$ angenommen werden darf. Das bedeutet, daß für alle i stets

$$\widetilde{h}_i = s_i h_i \quad \text{mit } s_i \in \{1, -1\}$$

gilt. Hieraus ergeben sich die folgenden Umformungen:

$$a\widetilde{h}_i = as_ih_i = v_is_ih_{\pi(i)} = v_is_is_{\pi(i)}\widetilde{h}_{\pi(i)} =: \widetilde{v}_i\widetilde{h}_{\pi(i)},$$

wobei $\widetilde{v}_i := v_is_is_{\pi(i)}$ gesetzt wurde. Hieraus folgt

$$\prod_{i=1}^{(m-1)/2} \widetilde{v}_i = \Bigg(\prod_{i=1}^{(m-1)/2} v_i \Bigg(\Bigg(\prod_{i=1}^{(m-1)/2} s_is_{\pi(i)}\Bigg) = \prod_{i=1}^{(m-1)/2} v_i,$$

da in dem Produkt jedes s_i zweimal als Faktor auftritt. □

Definition 5.3. Mit den Bezeichnungen von Bemerkung 5.2 wird

$$\left(\frac{a}{m}\right)^* := \prod_{i=1}^{(m-1)/2} v_i$$

als **Jacobi-Symbol** bezeichnet.

Bemerkung 5.3. *Für eine ungerade Primzahl p gilt $\left(\frac{a}{p}\right)^* = \left(\frac{a}{p}\right)$, d.h. das Jacobi-Symbol verallgemeinert das Legendre-Symbol.*

Beweis. Durch Anwendung von Bemerkung 5.2 ergibt sich

$$a^{(p-1)/2} \prod_{i=1}^{(p-1)/2} h_i = \prod_{i=1}^{(p-1)/2} ah_i \equiv \prod_{i=1}^{(p-1)/2} v_ih_{\pi(i)} = (\prod_{i=1}^{(p-1)/2} v_i)(\prod_{i=1}^{(p-1)/2} h_i) \pmod p.$$

Hieraus folgt zusammen mit Satz 5.1 und Definition 5.3

$$a^{(p-1)/2} \equiv \prod_{i=1}^{(p-1)/2} v_i \pmod p \quad \text{und} \quad \left(\frac{a}{p}\right)^* \equiv \left(\frac{a}{p}\right) \pmod p.$$

Da beide Seiten der letzten Kongruenz nur die Werte -1 , 0 und 1 annehmen können, folgt hieraus die Behauptung. □

Bezeichnung: Aufgrund von Bemerkung 5.3 wird auch für das Jacobi-Symbol die Schreibweise $\left(\frac{a}{m}\right)$ verwendet.

Satz 5.2. *(a) Für ungerades $m \in \mathbb{N}$ und $a, b \in \mathbb{N}$ mit $\mathrm{ggT}\{ab, m\} = 1$ gilt*

$$\left(\frac{ab}{m}\right) = \left(\frac{a}{m}\right)\left(\frac{b}{m}\right).$$

(b) Für ungerade $m, n \in \mathbb{N}$ und $a \in \mathbb{N}$ mit $\mathrm{ggT}\{a, mn\} = 1$ gilt

$$\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{m}\right).$$

Beweis.

(a) Es sei $H_m = \{h_1, \dots, h_{(m-1)/2}\}$ ein Halbsystem modulo m. Nach Bemerkung 5.2 gibt es Zahlen $v_i, \widetilde{v}_i$ und Permutationen $\pi, \widetilde{\pi}$ mit

$$ah_i \equiv v_i h_{\pi(i)} \pmod m \tag{5.1}$$

$$bh_i \equiv \widetilde{v}_i h_{\widetilde{\pi}(i)} \pmod m \tag{5.2}$$

Daraus folgt

$$abh_i \equiv bv_i h_{\pi(i)} \equiv v_i \widetilde{v}_{\pi(i)} h_{\widetilde{\pi}\pi(i)} \pmod m$$

Aufgrund von Definition 5.3 gilt

$$\left(\frac{ab}{m}\right) = \prod_{i=1}^{(m-1)/2} v_i \widetilde{v}_{\pi(i)} = (\prod_{i=1}^{(m-1)/2} v_i)(\prod_{i=1}^{(m-1)/2} \widetilde{v}_{\pi(i)}) = \left(\frac{a}{m}\right)\left(\frac{b}{m}\right),$$

da sich das letzte Produkt über alle i erstreckt.

(b) Es seien $H_m = \{h_1, \dots, h_{(m-1)/2}\}$ ein Halbsystem modulo m mit $ah_i \equiv v_i h_{\pi(i)} \pmod m$ und $H_n = \{k_1, \dots, k_{(n-1)/2}\}$ ein Halbsystem modulo n mit $ak_j \equiv \widetilde{v}_j k_{\widetilde{\pi}(j)} \pmod n$. Aus H_m und H_n wird durch

$$H_{m,n} := \left\{ h_i + mr \mid h_i \in H_m, 0 \le r \le n-1 \right\} \cup \left\{ k_j m \mid k_j \in H_n \right\}$$

ein Halbsystem modulo mn konstruiert. Denn es gilt

$$|H_{m,n}| = n\frac{m-1}{2} + \frac{n-1}{2} = \frac{mn-1}{2} \quad \text{und} \quad \overline{H}_{m,n} \cup (-\overline{H}_{m,n}) = \mathbb{Z}/_{mn\mathbb{Z}} \setminus \{0\}.$$

Aus (5.1) ergeben sich die Kongruenzen

$$\begin{aligned} a(h_i + mr) \equiv ah_i &\equiv v_i h_{\pi(i)} \pmod m \\ a(h_i + mr) \equiv v_i h_{\pi(i)} + mr' &\equiv v_i (h_{\pi(i)} + m\widetilde{r}) \pmod{mn} \end{aligned} \tag{5.3}$$

mit einem passenden $\widetilde{r}$. Aus (5.2) folgt

$$amk_j \equiv \widetilde{v}_j m k_{\widetilde{\pi}(j)} \pmod{mn} \tag{5.4}$$

Also erhält man unter Beachtung von (5.3) und (5.4) sowie $n \equiv 1 \pmod 2$

$$\left(\frac{a}{mn}\right) = (\prod_{i=1}^{(m-1)/2} v_i)^n (\prod_{j=1}^{(n-1)/2} \widetilde{v}_j) = (\prod_{i=1}^{(m-1)/2} v_i)(\prod_{j=1}^{(n-1)/2} \widetilde{v}_j) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right). \qquad \square$$

Folgerung 5.2. *Ist $m = \prod_{i=1}^{r} p_i^{e_i}$ die Primzerlegung einer ungeraden Zahl m mit $p_i \nmid a$, so gilt*

$$\left(\frac{a}{m}\right) = \prod_{i=1}^{r} \left(\frac{a}{p_i}\right)^{e_i}.$$

5.3 Das quadratische Reziprozitätsgesetz

Satz 5.3 (Quadratisches Reziprozitätsgesetz). *Sind $m, n \in \mathbb{N}$ ungerade und teilerfremde Zahlen, so gilt*

$$\left(\frac{n}{m}\right)\left(\frac{m}{n}\right) = (-1)^{(m-1)/2 \, (n-1)/2}.$$

Satz 5.4 (1.Ergänzungssatz).

$$\left(\frac{-1}{m}\right) = (-1)^{(m-1)/2}$$

Satz 5.5 (2.Ergänzungssatz).

$$\left(\frac{2}{m}\right) = (-1)^{(m^2-1)/8}$$

Anmerkung: Mittels Kongruenzen ausgedrückt lauten die Sätze: Ist m oder n kongruent 1 modulo 4, so gilt $\left(\frac{n}{m}\right) = \left(\frac{m}{n}\right)$. Sind m und n beide kongruent 3 modulo 4, so gilt $\left(\frac{n}{m}\right) = -\left(\frac{m}{n}\right)$. Genau für m kongruent 1 modulo 4 ist -1 quadratischer Rest modulo m und genau für m kongruent 1 oder 7 modulo 8 ist 2 quadratischer Rest modulo m.

Beispiel 5.3. Mit Hilfe der vorangehenden Sätze und der Tatsache, daß aus $n \equiv n' \pmod m$ stets $\left(\frac{n}{m}\right) = \left(\frac{n'}{m}\right)$ folgt, kann die Berechnung des Jacobi-Symbols schrittweise durchgeführt werden. So führt die Frage, ob 197 ein quadratischer Rest modulo 3001 ist, auf folgende Rechnung:

$$\left(\frac{197}{3001}\right) = \left(\frac{3001}{197}\right) = \left(\frac{46}{197}\right) = \left(\frac{2}{197}\right)\left(\frac{23}{197}\right) = (-1)\left(\frac{197}{23}\right) = (-1)\left(\frac{13}{23}\right) =$$
$$(-1)\left(\frac{23}{13}\right) = (-1)\left(\frac{10}{13}\right) = (-1)\left(\frac{2}{13}\right)\left(\frac{5}{13}\right) = (-1)(-1)\left(\frac{13}{5}\right) = \left(\frac{3}{5}\right) = -1$$

Also ist 197 kein quadratischer Rest modulo 3001.

Beweis. Ergänzungssätze: Durch

$$H_m = \left\{h_1, \ldots, h_{(m-1)/2}\right\} \quad \text{mit } h_i := i$$

ist ein Halbsystem modulo m gegeben. Mit den Bezeichnungen aus Bemerkung 5.2 ergibt sich für $a = -1$:

$$(-1)h_i \equiv v_i h_i \pmod m \qquad \text{für alle } i.$$

Daraus folgt $v_i = -1$ für alle i und man erhält

$$\left(\frac{-1}{m}\right) = \prod_{i=1}^{(m-1)/2} v_i = (-1)^{(m-1)/2}.$$

Für $a = 2$ unterscheidet man die beiden folgenden Fälle: Ist $m \equiv 1 \pmod 4$, so gilt

$$v_i = 1 \quad \text{für } 1 \le i \le \frac{m-1}{4} \qquad \text{und } v_i = -1 \quad \text{für } \frac{m+3}{4} \le i \le \frac{m-1}{2}.$$

Also gilt $\left(\frac{2}{m}\right) = (-1)^{(m-1)/4}$.

Im anderen Fall gilt $m \equiv 3 \pmod 4$ und damit

$$v_i = 1 \quad \text{für } 1 \leq i \leq \frac{m-3}{4} \qquad \text{und } v_i = -1 \quad \text{für } \frac{m+1}{4} \leq i \leq \frac{m-1}{2},$$

woraus $\left(\frac{2}{m}\right) = (-1)^{(m+1)/4}$ folgt.

Beide Fälle lassen sich durch die Kongruenz modulo 8 beschreiben: Für $m \equiv \pm 1 \pmod 8$ gilt $\left(\frac{2}{m}\right) = 1$ und für $m \equiv \pm 3 \pmod 8$ gilt $\left(\frac{2}{m}\right) = -1$. Dies ist wiederum äquivalent zu der kompakten Schreibweise

$$\left(\frac{2}{m}\right) = (-1)^{(m^2-1)/8}.$$

Reziprozitätsgesetz: Durch $H_m = \{1, \ldots, \frac{m-1}{2}\}$ und $H_n = \{1, \ldots, \frac{n-1}{2}\}$ sind Halbsysteme modulo m bzw. n gegeben. Es gilt

$$\left(\tfrac{n}{m}\right) = (-1)^i,$$
$$i = \left|\{\, (h,k) \mid -\tfrac{m}{2} < nh - mk < 0,\ h \in H_m,\ k \in \mathbb{Z} \,\}\right|.$$

Wegen $nh - mk < 0$ muß $k > 0$ gelten. Aus $nh - mk > -\frac{m}{2}$ folgt über die Abschätzung

$$mk < nh + \frac{m}{2} < n\frac{m}{2} + \frac{m}{2} = m\frac{n+1}{2},$$

daß $k < \frac{n+1}{2}$ bzw. $k \leq \frac{n-1}{2}$ gelten muß, was $k \in H_n$ zur Folge hat.

Andererseits gilt

$$\left(\frac{m}{n}\right) = (-1)^j \quad \text{mit } j = \left|\left\{\, (h,k) \mid -\frac{n}{2} < mk - nh < 0,\ h \in H_m,\ k \in H_n \,\right\}\right|,$$

wobei $-\frac{n}{2} < mk - nh < 0$ äquivalent zu $0 < nh - mk < \frac{n}{2}$ ist. Somit gilt

$$\left(\frac{n}{m}\right)\left(\frac{m}{n}\right) = (-1)^{i+j} \quad \text{mit } i + j = \left|\left\{\, (h,k) \mid -\frac{m}{2} < nh - mk < \frac{n}{2},\ h \in H_m, k \in H_n \,\right\}\right|.$$

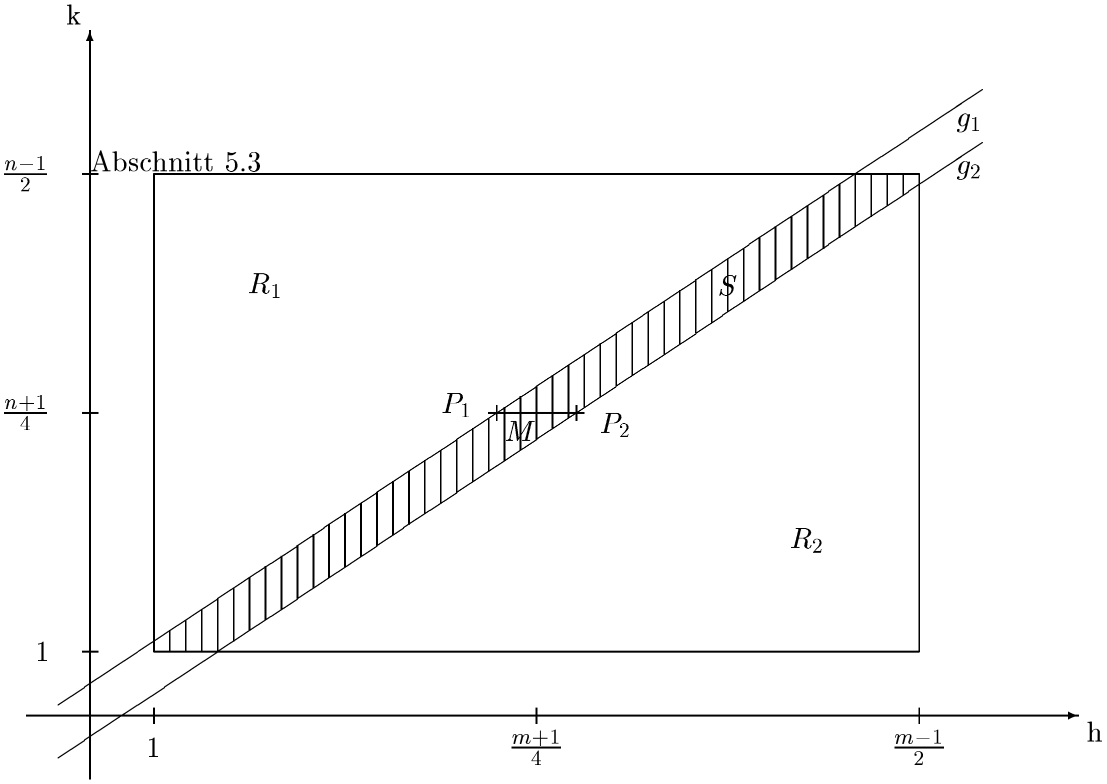
Damit ist die Fragestellung auf das geometrische Problem zurückgeführt, wie viele Punkte mit ganzzahligen Koordinaten in dem durch die Randbedingungen beschriebenen Gebiet liegen.

Die Gleichungen der Geraden g_1 und g_2 haben die Gestalt

$$\begin{array}{lrcl l rcl}
g_1: & -\frac{m}{2} & = & nh - mk & \text{bzw.} & k & = & \frac{n}{m}h + \frac{1}{2}, \\
g_2: & \frac{n}{2} & = & nh - mk & \text{bzw.} & k & = & \frac{n}{m}h - \frac{n}{2m}.
\end{array}$$

Außerdem muß $1 \leq h \leq \frac{m-1}{2}$ und $1 \leq k \leq \frac{n-1}{2}$ gelten. Die Gerade $k = \frac{n+1}{4}$ schneidet g_1 bzw. g_2 in den Punkten P_1 und P_2, deren Koordinaten sich wie folgt ergeben:

$$\frac{n+1}{4} = \frac{n}{m}h + \frac{1}{2},\ h = \frac{m}{n}\frac{n-1}{4} \quad \text{bzw.}\ \frac{n+1}{4} = \frac{n}{m}h - \frac{n}{2m},\ h = \frac{n+1}{4}\frac{m}{n} + \frac{1}{2}$$
$$P_1 = (\frac{n-1}{4}\frac{m}{n}, \frac{n+1}{4}),\ P_2 = (\frac{n+1}{4}\frac{m}{n} + \frac{1}{2}, \frac{n+1}{4}).$$



Für den Mittelpunkt M der Strecke $\overline{P_1P_2}$ ergibt sich

$$\frac{1}{2}(\frac{m}{n}\frac{n-1}{4}+\frac{n+1}{4}\frac{m}{n}+\frac{1}{2})=\frac{mn-m+mn+m+2n}{8n}=\frac{m+1}{4},\ M=(\frac{m+1}{4},\frac{n+1}{4}).$$

Da der in der Skizze schraffierte Bereich S punktsymmetrisch bezüglich M ist, liegen in R_1 ebenso viele Gitterpunkte wie in R_2, etwa r Stück. Für die gesuchte Anzahl der Gitterpunkte in S gilt damit

$$i+j=\frac{n-1}{2}\frac{m-1}{2}-2r.$$

Somit ergibt sich schließlich

$$\left(\frac{n}{m}\right)\left(\frac{m}{n}\right)=(-1)^{(n-1)/2(m-1)/2}\left((-1)^{-r}\right)^2=(-1)^{(n-1)/2(m-1)/2}. \qquad \square$$

6 Primzahltests

6.1 Carmichael-Zahlen

Eine der grundlegenden Aussagen über Primzahlen stellt der Satz von Euler-Fermat dar (Satz 2.2). Die Frage, ob auch die Umkehrung dieses Satzes gilt, die dann ein Primzahlkriterium ähnlich dem Satz von Wilson liefert, führt zu der folgenden Definition:

Definition 6.1. Eine ungerade Zahl $n \in \mathbb{N}\backslash\mathbb{P}$ heißt **Carmichael-Zahl**, wenn für alle Restklassen $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$

$$\overline{a}^{n-1}=\overline{1}$$

gilt.

Bemerkung 6.1. *Die Zahl n ist genau dann Carmichael-Zahl, wenn n die Darstellung*

$$n = p_1 \cdot \ldots \cdot p_r$$

als Produkt von $r > 1$ ungeraden Primzahlen zur ersten Potenz besitzt und für die Primteiler p_i zusätzlich gilt

$$(p_i - 1) \mid (n - 1).$$

Beweis. Ist m eine Carmichael-Zahl, so folgt aus der Definition

$$\exp(\mathbb{Z}/_{n\mathbb{Z}})^\times \mid (n-1).$$

Ist p^e mit $p \in \mathbb{P}$ und $e \geq 1$ ein Teiler von n, so gilt nach dem Hauptsatz über simultane Kongruenzen

$$\exp(\mathbb{Z}/_{p^e\mathbb{Z}})^\times \mid \exp(\mathbb{Z}/_{n\mathbb{Z}})^\times,$$

womit sich zusammen mir Bemerkung 3.2

$$p^{e-1}(p-1) \mid (n-1)$$

ergibt. Die Annahme $e > 1$ führt wegen $p \mid (n-1)$ und $p \mid n$ zu dem Widerspruch $p \mid 1$. Also gilt $e = 1$, und da n ungerade ist, gehen folglich nur ungerade Primfaktoren zur ersten Potenz in n auf, womit

$$(p-1) \mid (n-1)$$

gilt. Besitzt n umgekehrt die geforderte Darstellung

$$n = p_1 \cdot \ldots \cdot p_r,\ 2 \neq p_i \in \mathbb{P},\ (p_i - 1) \mid (n-1) \quad \text{für } i = 1, \ldots, r,$$

so ergibt sich

$$\begin{aligned}
&\exp(\mathbb{Z}/_{n\mathbb{Z}})^\times = \mathrm{kgV}\{\exp(\mathbb{Z}/_{p_i\mathbb{Z}})^\times \mid i = 1, \ldots, r\} = \mathrm{kgV}\{p_i - 1 \mid i = 1, \ldots, r\},\\
&\exp(\mathbb{Z}/_{n\mathbb{Z}})^\times \mid (n-1),
\end{aligned}$$

was $\overline{a}^{n-1} \equiv \overline{1}$ für alle $\overline{a} \in (\mathbb{Z}/_{n\mathbb{Z}})^\times$ zur Folge hat. Also ist n eine Carmichael-Zahl. □

Beispiel 6.1. Die kleinsten Carmichael-Zahlen sind $561 = 3 \cdot 11 \cdot 17$, $1105 = 5 \cdot 13 \cdot 17$ und $1729 = 7 \cdot 13 \cdot 19$.

Anmerkung: Es gibt unendlich viele Carmichael-Zahlen. Diese genügen der Abschätzung

$$\left|\left\{ n \in \mathbb{N} \mid n \leq x,\ n \text{ Carmichael-Zahl} \right\}\right| \geq x^{2/7} \quad \text{für } x \gg 0$$

(Satz von Alford-Granville-Pomerance). Die Umkehrung des Satzes von Fermat ist also nicht für einen Primzahltest geeignet.

6.2 Der Primzahltest von Solovay und Strassen

In diesem Abschnitt wird untersucht, ob das Euler-Kriterium (Satz 5.1) für quadratische Reste für Primzahlen charakteristisch ist.

Definition 6.2. Ist n eine ungerade natürliche Zahl, so heißt eine ganze zu n teilerfremde Zahl a mit

$$\left(\frac{a}{n}\right) \not\equiv a^{(n-1)/2} \pmod{n}$$

ein **Eulerscher Zeuge (für die Zerlegbarkeit) von** n. Mit E_n wird die Menge aller Restklassen $\overline{a}$ bezeichnet, für die a kein Eulerscher Zeuge von n ist.

Anmerkung: Ist a ein Eulerscher Zeuge von n, so kann n nach dem Euler-Kriterium keine Primzahl sein. Also „bezeugt“ a die Zerlegbarkeit von n.

Bemerkung 6.2. *E_n ist eine Untergruppe von $(\mathbb{Z}/n\mathbb{Z})^\times$.*

Beweis. Mit zwei Elementen $\overline{a}, \overline{b} \in E_n$ ist wegen

$$\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right) \equiv a^{(n-1)/2} b^{(n-1)/2} = (ab)^{(n-1)/2}$$

auch $\overline{a}\overline{b} \in E_n$. Da E_n das Einselement $\overline{1}$ und mit $\overline{a}$ auch dessen Inverses $\overline{a}^{\varphi(n)-1}$ enthält, ist E_n eine Untergruppe. □

Satz 6.1. *Für jede ungerade natürliche Zahl n gilt: n ist genau dann eine Primzahl, wenn $E_n = (\mathbb{Z}/n\mathbb{Z})^\times$ gilt.*

Beweis. Ist n eine Primzahl, so gilt das Euler-Kriterium für alle $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$. Folglich gibt es keine Eulerschen Zeugen von n, und es gilt $E_n = (\mathbb{Z}/n\mathbb{Z})^\times$. Gilt umgekehrt für alle zu n teilerfremden Zahlen a

$$a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod{n},$$

so folgt durch Quadrieren

$$a^{n-1} \equiv 1 \pmod{n}.$$

Also ist n entweder Primzahl oder Carmichael-Zahl. Im ersten Fall ist nichts mehr zu zeigen. Nun wird angenommen, n sei Carmichael-Zahl mit der Darstellung

$$n = p_1 \cdot \ldots \cdot p_r, \; r \geq 2, \; p_i \neq p_j \quad \text{für } i \neq j.$$

Der Satz über simultane Kongruenzen sichert die Existenz einer Zahl b mit

$$\left(\frac{b}{p_1}\right) = -1 \quad \text{und } b \equiv 1 \pmod{p_i} \quad \text{für } i = 2, \ldots, r.$$

Daher gilt wegen $\left(\frac{b}{p_i}\right) = 1 \quad$ für $i = 2, \ldots, r$

$$\left(\frac{b}{n}\right) = \left(\frac{b}{p_1}\right) \cdot \ldots \cdot \left(\frac{b}{p_r}\right) = -1. \tag{6.1}$$

Nach Voraussetzung ist b kein Eulerscher Zeuge für n, es gilt also

$$\left(\frac{b}{n}\right) \equiv b^{(n-1)/2} \pmod{n}. \tag{6.2}$$

Aus (6.1) und (6.2) folgt

$$b^{(n-1)/2} \equiv -1 \pmod{n},$$

was im Widerspruch etwa zu $b^{(n-1)/2} \equiv 1 \pmod{p_2}$ steht. Also kann n keine Carmichael-Zahl sein. □

Folgerung 6.1. *Für eine ungerade Zahl $n \in \mathbb{N} \backslash \mathbb{P}$ gilt*

$$|E_n| \leq \frac{1}{2}\varphi(n).$$

Beweis. Wegen Satz 6.1 existiert ein $\overline{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$ mit $\overline{b} \notin E_n$. Daher gilt

$$\left|\overline{b}E_n\right| = \left|\left\{ \overline{b}\overline{a} \ \mid \ \overline{a} \in E_n \right\}\right| = |E_n| \,.$$

Gäbe es ein $\overline{c} \in \overline{b}E_n \cap E_n$, so wäre $\overline{c} = \overline{b}\overline{a}$ mit $\overline{a} \in E_n$, was den Widerspruch $\overline{b} = \overline{c}\overline{a}^{-1} \in E_n$ zur Folge hätte. Also gilt $\overline{b}E_n \cap E_n = \emptyset$, und es ergibt sich

$$|E_n| = \frac{1}{2}\left|E_n \cup \overline{b}E_n\right| \leq \frac{1}{2}\left|(\mathbb{Z}/n\mathbb{Z})^\times\right| = \varphi(n).$$ □

Primzahltest von Solovay und Strassen (1977):

Die ungerade Zahl n soll getestet werden. Dazu wählt man r Zahlen $a_1, \ldots, a_r$ zufällig. (In der Praxis wählt man häufig die ersten r Primzahlen.) Danach testet man $\operatorname{ggT}\{a_i, n\}$ und berechnet die Werte $a_i^{(n-1)/2} \pmod{n}$ und $\left(\frac{a_i}{n}\right)$.

Gilt dann für ein i die Beziehung

$$a_i^{(n-1)/2} \not\equiv \left(\frac{a_i}{n}\right) \pmod{n},$$

so ist n keine Primzahl.

Sonst ist die Vorhersage "$n \in \mathbb{P}$" richtig mit der Fehlerwahrscheinlichkeit $W \leq 1/2^r$.

6.3 Der Primzahltest von Miller und Rabin

Definition 6.3. Ist n eine ungerade natürliche Zahl und $n - 1 = 2^t u$ mit $t \geq 1$ und ungeradem u, so heißt $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$ ein **Zeuge für die Zerlegbarkeit von** n, falls gelten

$$\overline{a}^u \neq \overline{1} \quad \text{und } \overline{a}^{2^s u} \neq -\overline{1} \quad \text{für alle } s = 0, \ldots, t-1. \tag{6.3}$$

Bemerkung 6.3. *Gibt es einen Zeugen für die Zerlegbarkeit von n, so ist n keine Primzahl.*

Beweis. Hätte eine ungerade Primzahl p einen Zeugen für die Zerlegbarkeit $\overline{a}$, so würde wegen

$$p - 1 = 2^t u, \ 2 \not| \, u$$

über den Satz von Fermat folgen, daß

$$\overline{a}^{p-1} = \overline{a}^{2^t u} = \overline{1}$$

gilt. Wegen $\overline{a}^u \neq \overline{1}$ müßte es ein maximales Element s geben mit $0 \leq s < t$ und

$$\overline{b} := \overline{a}^{2^s u} \neq \overline{1}. \tag{6.4}$$

Die durch Quadrieren entstehende Gleichung $\overline{b}^2 = \overline{1}$ hat über dem Körper $\mathbb{F}_p$ nur die Lösungen $\overline{b} = \pm\overline{1}$, die aber aufgrund von (6.3) und (6.4) beide zu einem Widerspruch führen. □

Hieraus erhält man zunächst einen Primzahltest im Taschenrechnerbereich: Ist eine ungerade Zahl n keine Primzahl, so gilt

(a) 2 ist ein Zeuge für die Zerlegbarkeit von n für $n < 2047$.

(b) 2 oder 3 ist ein Zeuge für die Zerlegbarkeit von n für $n < 1373653$.

(c) 2,3,5 oder 7 ist ein Zeuge für die Zerlegbarkeit von n für $n < 2,5 \cdot 10^{10}$ mit Ausnahme von 3215031751 .

Die Verifikation dieser Aussage erfolgt durch Nachrechnen mittels Computer.

Satz 6.2. *Ist n eine ungerade Zahl, so ist jeder Eulersche Zeuge für n auch ein Zeuge für die Zerlegbarkeit von n.*

Beweis. Es gelte

$$n = \prod_{i=1}^{r} p_i^{e_i} \quad \text{und } n-1 = 2^t u \quad \text{mit ungeradem } u. \tag{6.5}$$

Der Satz ist bewiesen, wenn gezeigt ist, daß für jede Restklasse $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$, die kein Zeuge für die Zerlegbarkeit ist, $\overline{a} \in E_n$ folgt. Ist $\overline{a}$ kein Zeuge für die Zerlegbarkeit von n, so ist eine der beiden Bedingungen aus (6.3) verletzt. Zunächst sei $\overline{a}^u = \overline{1}$. Wegen (6.5) folgt daraus

$$\overline{a}^{n-1/2} = \overline{a}^{2^{t-1}u} = \overline{1} \tag{6.6}$$

Andererseits ändert sich der Wert von $\left(\frac{a}{n}\right)$ nicht, wenn man a durch eine modulo n kongruente Zahl ersetzt, also gilt

$$1 = \left(\frac{1}{n}\right) = \left(\frac{a^u}{n}\right) = \left(\frac{a}{n}\right)^u.$$

Da u ungerade ist, muß sogar schon $\left(\frac{a}{n}\right) = 1$ gelten, woraus sich zusammen mit (6.6)

$$\left(\frac{a}{n}\right) \equiv a^{(n-1)/2} \pmod{n},$$

also schließlich $\overline{a} \in E_n$ ergibt.

Ist die zweite Bedingung aus (6.3) verletzt, so existiert ein s mit $0 \leq s \leq t-1$ und

$$\overline{a}^{2^s u} = -\overline{1}. \tag{6.7}$$

Für $i = 1, \ldots, r$ sei d_i der Exponent von $\overline{a}$ in $\mathbb{F}_{p_i}$. Aus $a^{2^s u} \equiv -1 \pmod{p_i}$ ergibt sich

$$d_i \not| \, 2^s u, \; d_i \,|\, 2^{s+1} u.$$

Daher besitzt d_i die Darstellung

$$d_i = s^{s+1} v_i \quad \text{mit ungeradem} \;\; v_i. \tag{6.8}$$

Aufgrund des Satzes von Fermat erhält man wegen $d_i \,|\, (p_i - 1)$ zunächst $2^{s+1} \,|\, (p_i - 1)$, woraus die Existenz eines $k_i \in \mathbb{N}$ mit

$$p_i - 1 = 2^{s+1} k_i \quad \text{bzw. } p_i = 1 + 2^{s+1} k_i \tag{6.9}$$

folgt. Durch Einsetzen und Ausnutzung des binomischen Lehrsatzes folgt

$$n = \prod_{i=1}^{r} p_i^{e_i} \equiv 1 + 2^{s+1} \sum_{i=1}^{r} k_i e_i \pmod{2^{s+2}}.$$

Zusammen mit (6.5) ergibt sich somit

$$\frac{n-1}{2} = 2^{t-1} u \equiv 2^s \sum_{i=1}^{r} k_i e_i \pmod{2^{s+1}}.$$

Nach Division durch 2^s erhält man weiter

$$2^{t-1-s} u \equiv \sum_{i=1}^{r} k_i e_i \pmod{2}.$$

Unter Beachtung von $u \equiv 1 \pmod 2$, (6.5) und (6.7) folgt

$$a^{(n-1)/2} = a^{2^{t-1} u} = (a^{2^s u})^{2^{t-1-s}} = (-1)^{2^{t-1-s}} \equiv (-1)^{\sum_{i=1}^{r} k_i e_i} \pmod{n}. \tag{6.10}$$

Da d_i der Exponent von $\overline{a}$ in $\mathbb{F}_{p_i}$ ist, gilt andererseits

$$a^{d_i/2} \equiv -1 \pmod{p_i}.$$

Hieraus folgt unter Verwendung von (6.8) und (6.9)

$$\left(\frac{a}{p_i}\right) \equiv a^{(p_i-1)/2} = a^{d_i/2 (p_i-1)/d_i} \equiv (-1)^{(p_i-1)/d_i} \equiv (-1)^{(p_i-1)/2^{s+1}} \equiv (-1)^{k_i} \pmod{p_i},$$

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{r} \left(\frac{a}{p_i}\right)^{e_i} = \prod_{i=1}^{r} (-1)^{k_i e_i} = (-1)^{\sum_{i=1}^{r} k_i e_i}.$$

Zusammen mit (6.10) ergibt dies $a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod{n}$, womit schließlich $\overline{a} \in E_n$ gilt. $\square$

Folgerung 6.2. *Für jede ungerade Zahl $n \in \mathbb{N}\backslash\mathbb{P}$ gibt es mindestens $\frac{1}{2}\varphi(n)$ Zeugen für die Zerlegbarkeit in $({}^{\mathbb{Z}}/_{n\mathbb{Z}})^{\times}$.*

Beweis. Die Behauptung ergibt sich aus Folgerung 6.1 zusammen mit Satz 6.2 . □

Beispiel 6.2. Die Zahl $a = 199$ ist ein Zeuge für die Zerlegbarkeit von $n = 225$, aber sie ist kein Eulerscher Zeuge.

Satz 6.3 (Rabin). *Ist $n \in \mathbb{N}\backslash\mathbb{P}$ ungerade mit $n \neq 9$, so besitzt n mindestens $\frac{3}{4}(n-1)$ Zeugen für die Zerlegbarkeit.*

(ohne Beweis)

Primzahltest von Miller und Rabin:

Wähle r Zahlen $a_1, \ldots, a_r$ und teste, ob $\operatorname{ggT}\{n, a_i\} = 1$ gilt. Falls ein a_i ein Zeuge für die Zerlegbarkeit von n ist, so ist n keine Primzahl. Falls kein a_i ein Zeuge für die Zerlegbarkeit von n ist, so ist die Vorhersage "$n \in \mathbb{P}$" richtig mit der Fehlerwahrscheinlichkeit $W \leq {}^{1}/_{4^r}$.

Anmerkung: Aus der erweiterten Riemannschen Vermutung folgt der Satz von Ankeny–Montgomery–Bach: Ist n eine ungerade zerlegbare Zahl, so existiert ein Zeuge $p \in \mathbb{P}$ für die Zerlegbarkeit von n mit

$$0 < p < 2(\log(n))^2.$$

Unter Annahme der erweiterten Riemannschen Vermutung erhält man also die folgende deterministische Variante des Primzahltests von Miller und Rabin:

Teste für alle Primzahlen $p < 2(\log(n))^2$, ob p ein Zeuge für die Zerlegbarkeit von n ist. Wird ein Zeuge für die Zerlegbarkeit gefunden, so ist n keine Primzahl. Im anderen Fall gilt $n \in \mathbb{P}$.

7 Quadratsummendarstellungen

7.1 Summen von zwei Quadraten

Satz 7.1 (Lemma von Thue). *Es seien p eine Primzahl, e und f natürliche Zahlen mit*

$$e, f < p \quad \text{und } ef > p,$$

weiterhin sei x eine ganze Zahl mit $p \nmid x$. Dann existieren natürliche Zahlen u und v mit

$$u < e,\ v < f \quad \text{und } x \equiv \pm\frac{v}{u} \pmod{p}.$$

Beweis. Für die Menge

$$M := \{\, (u,v) \in \mathbb{N} \times \mathbb{N} \mid u \leq e,\ v \leq f \,\}$$

gilt $|M| = ef > p$. Daher gibt es zwei nichtidentische Paare (u_1, v_1) und (u_2, v_2) aus M mit

$$u_1 x - v_1 \equiv u_2 x - v_2 \pmod{p}. \tag{7.1}$$

Wäre $u_1 = u_2$, so würde $v_1 \equiv v_2 \pmod{p}$ und damit der Widerspruch $v_1 = v_2$ folgen. Also gilt $u_1 \neq u_2$. Wäre weiter $v_1 = v_2$, so hätte dies $u_1 x \equiv u_2 x \pmod{p}$ zur Folge. Wegen

$p \nmid x$ würde daraus $u_1 \equiv u_2 \pmod p$ und schließlich $u_1 = u_2$ im Widerspruch zum schon Bewiesenen folgen. Also gilt auch $v_1 \neq v_2$. Durch Umformung von (7.1) erhält man somit

$$x \equiv \frac{v_1 - v_2}{u_1 - u_2} \pmod p,$$

woraus mit $v := |v_1 - v_2| \in \mathbb{N}$ und $u := |u_1 - u_2| \in \mathbb{N}$ die behauptete Kongruenz folgt. □

Satz 7.2. *(a) Die Zahl 2 läßt sich durch $2 = 1^2 + 1^2$ eindeutig als Summe von zwei Quadraten darstellen.*

(b) Jede Primzahl p mit $p \equiv 1 \pmod 4$ läßt sich als Summe von zwei Quadraten darstellen. Diese Darstellung ist eindeutig bis auf die Reihenfolge der Summanden.

(c) Keine Primzahl p mit $p \equiv -1 \pmod 4$ läßt sich als Summe von zwei Quadraten darstellen.

Beweis.

(b) Aus $p \equiv 1 \pmod 4$ folgt nach dem ersten Ergänzungssatz des quadratischen Reziprozitätsgesetzes

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = 1.$$

Also gibt es eine ganze Zahl x mit

$$x^2 \equiv -1 \pmod p \tag{7.2}$$

Mit Hilfe des Lemmas von Thue mit $e = f = [\sqrt{p}] + 1 < p$ folgt die Existenz zweier natürlicher Zahlen u und v mit

$$x \equiv \pm\frac{u}{v} \pmod p \quad \text{und } u, v < \sqrt{p}. \tag{7.3}$$

Aus (7.2) und (7.3) ergibt sich $v^2x^2 \equiv -v^2 \equiv u^2 \pmod p$ bzw. $u^2 + v^2 \equiv 0 \pmod p$. Wegen $0 < u^2 + v^2 < 2p$ erhält man schließlich

$$u^2 + v^2 = p.$$

Zum Beweis der Eindeutigkeit sei

$$p = u^2 + v^2 = \widetilde{u}^2 + \widetilde{v}^2. \tag{7.4}$$

Durch Übergang zur Kongruenz modulo p erhält man

$$(\frac{u}{v})^2 \equiv -1 \equiv (\frac{\widetilde{u}}{\widetilde{v}})^2 \pmod p.$$

Weil $\mathbb{F}_p$ ein Körper ist, folgt hieraus

$$\frac{u}{v} \equiv \pm\frac{\widetilde{u}}{\widetilde{v}} \pmod p.$$

Da sich aufgrund der Beziehung

$$\frac{u}{v} \equiv \frac{v}{u}(\frac{u}{v})^2 \equiv -\frac{v}{u} \pmod p$$

bei der Vertauschung von u und v das Vorzeichen des Quotienten ändert, darf

$$\frac{u}{v} \equiv \frac{\widetilde{u}}{\widetilde{v}} \pmod p$$

angenommen werden. Hieraus folgt $u\widetilde{v} - \widetilde{u}v \equiv 0 \pmod p$, was wegen $|u\widetilde{v} - \widetilde{u}v| < 2p$ zunächst $u\widetilde{v} = \widetilde{u}v$ zur Folge hat. Da wegen (7.4) sowohl u und v als auch $\widetilde{u}$ und $\widetilde{v}$ teilerfremd sind, ergibt sich schließlich $u = \widetilde{u}$ und $v = \widetilde{v}$.

(c) Da ein Quadrat modulo 4 nur die Werte 0 oder 1 annehmen kann, folgt aus $p = u^2+v^2$ stets

$$p \not\equiv -1 \pmod 4.$$

□

Folgerung 7.1. *Die Zahl* $n = \prod_{i=1}^{r} p_i^{k_i}$ *ist genau dann als Summe von zwei Quadraten darstellbar, wenn alle Primfaktoren mit* $p_i \equiv -1 \pmod 4$ *einen geraden Exponenten* k_i *besitzen.*

Beweis. Aufgrund der Beziehung

$$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2$$

und Satz 7.2 können Produkte, in denen nur die 2 und Primzahlen p mit $p \equiv 1 \pmod 4$ als Faktoren auftreten, als Summe von zwei Quadraten dargestellt werden. Treten in der Primzerlegung von n alle Primfaktoren p mit $p \equiv -1 \pmod 4$ nur mit geraden Exponenten auf, so kann n geschrieben werden als

$$n = n_1^2 n_2, \; n_1 = \prod_{p_i \equiv -1 \pmod 4} p_i^{k_i/2}, \; n_2 = a^2 + b^2,$$

woraus die geforderte Summendarstellung folgt:

$$n = n_1^2(a^2 + b^2) = (n_1 a)^2 + (n_1 b)^2.$$

Zum Beweis der Umkehrung sei n als $n = a^2 + b^2$ darstellbar und p_j sei ein Primfaktor von n mit einem ungeraden Exponenten k_j. Mit

$$d := \operatorname{ggT}\{a, b\}, \; a = d\widetilde{a}, \; b = d\widetilde{b} \quad \text{und } n = d^2\widetilde{n}$$

gelten die Beziehungen

$$\operatorname{ggT}\{\widetilde{a}, \widetilde{b}\} = 1, \; \widetilde{n} = \widetilde{a}^2 + \widetilde{b}^2 = \prod_{i=1}^{r} p_i^{\widetilde{k}_i} \quad \text{und } \widetilde{k}_i \equiv k_i \pmod 2.$$

Speziell folgt $\widetilde{k}_j \equiv 1 \pmod 2$ und damit $p_j \mid \widetilde{n}$. Also ist p_j weder ein Teiler von $\widetilde{a}$ noch von $\widetilde{b}$, denn sonst wären $\widetilde{a}$ und $\widetilde{b}$ nicht teilerfremd. Andererseits gilt $\widetilde{a}^2 + \widetilde{b}^2 \equiv 0 \pmod{p_j}$ bzw. $\widetilde{a}^2 \equiv -\widetilde{b}^2 \pmod{p_j}$. Da $p_j \neq 2$ angenommen werden kann, ergibt sich hieraus

$$1 = \left(\frac{\widetilde{a}^2}{p_j}\right) = \left(\frac{-\widetilde{b}^2}{p_j}\right) = \left(\frac{-1}{p_j}\right)\left(\frac{\widetilde{b}^2}{p_j}\right) = (-1)^{(p_j-1)/2},$$

was $p_j \not\equiv -1 \pmod 4$ zur Folge hat.

□

7.2 Summen von vier Quadraten

Satz 7.3 (Lagrange)**.** *Jede natürliche Zahl ist als Summe von vier Quadraten darstellbar.*

Beweis. Für 1 und 2 existieren die Darstellungen

$$1 = 0^2 + 0^2 + 0^2 + 1^2 \quad \text{und } 2 = 0^2 + 0^2 + 1^2 + 1^2.$$

Mit zwei Zahlen

$$m = \sum_{i=1}^{4} a_i^2 \quad \text{und } n = \sum_{i=1}^{4} b_i^2$$

ist auch deren Produkt mn darstellbar als

$$mn = \sum_{i=1}^{4} c_i^2,$$

wobei die c_i die folgende Gestalt besitzen:

$$\begin{aligned} c_1 &= a_1b_1 + a_2b_2 + a_3b_3 + a_4b_4\,,\; c_2 = a_1b_2 - a_2b_1 + a_3b_4 - a_4b_3\,,\\ c_3 &= a_1b_3 - a_3b_1 + a_4b_2 - a_2b_4\,,\; c_4 = a_1b_4 - a_4b_1 + a_2b_3 - a_3b_2. \end{aligned}$$

Somit genügt es, den Satz noch für ungerade Primzahlen zu zeigen. Es sei also p eine ungerade Primzahl. Mit der Bezeichnung $H_p := \{0, 1, 2, \ldots, \frac{p-1}{2}\}$ gilt für alle Paare $h, \widetilde{h} \in H_p$ und $k, \widetilde{k} \in H_p$ mit $h \neq \widetilde{h}$ und $k \neq \widetilde{k}$:

$$h^2 \not\equiv \widetilde{h}^2 \pmod p \quad \text{und} \quad -1 - k^2 \not\equiv -1 - \widetilde{k}^2 \pmod p.$$

Da in jeder Kongruenz $\frac{p+1}{2}$ verschiedene Werte möglich sind, gibt es ein Paar $h, k \in H_p$ mit

$$h^2 \equiv -1 - k^2 \pmod p,$$

woraus die Existenz einer natürlichen Zahl r mit

$$h^2 + k^2 + 1 = rp \tag{7.5}$$

folgt. Mit der Abschätzung

$$1 + h^2 + k^2 < 1 + (\frac{p}{2})^2 + (\frac{p}{2})^2 < p^2$$

ergibt sich

$$r < p. \tag{7.6}$$

Bezeichnet s die kleinste natürliche Zahl, deren Produkt mit p sich als Summe von vier Quadraten darstellen läßt, so gilt wegen (7.5) und (7.6)

$$s < p \tag{7.7}$$

Für $s = 1$ folgt die Behauptung. Es gelte also $s > 1$ und

$$sp = \sum_{i=1}^{4} a_i^2 \tag{7.8}$$

mit minimalem s. Ist s gerade, so gilt

$$\sum_{i=1}^{4} a_i \equiv \sum_{i=1}^{4} a_i^2 \equiv 0 \pmod 2,$$

weshalb ohne Einschränkung der Allgemeinheit

$$a_1 \equiv a_2 \pmod 2 \quad \text{und } a_3 \equiv a_4 \pmod 2$$

vorausgesetzt werden darf. Hieraus folgt aber, daß $\frac{s}{2}p$ als

$$\frac{s}{2}p = (\frac{a_1 + a_2}{2})^2 + (\frac{a_1 - a_2}{2})^2 + (\frac{a_3 + a_4}{2})^2 + (\frac{a_3 - a_4}{2})^2$$

dargestellt werden kann, was im Widerspruch zur Minimalität von s steht.

Ist s ungerade, so ergibt die Division mit Rest von a_i durch s

$$a_i = q_i s + b_i, \ -\frac{s}{2} < b_i < \frac{s}{2}. \tag{7.9}$$

Aus (7.8) folgt, daß es mindestens ein i gibt, für das $s \not| a_i$ gilt, denn sonst würde $s^2 \,|\, a_i^2$ gelten, was über $s^2 \,|\, sp$ schließlich $s \,|\, p$ zur Folge hätte. Dies kann aber wegen (7.7) nicht sein. Wegen $b_i \neq 0$ gilt die Abschätzung

$$0 < \sum_{i=1}^{4} b_i^2 < 4(\frac{s}{2})^2 = s^2. \tag{7.10}$$

Aus (7.8) und (7.9) ergibt sich

$$0 \equiv \sum_{i=1}^{4} a_i^2 \equiv \sum_{i=1}^{4} b_i^2 \pmod s,$$

woraus zusammen mit (7.10)

$$\sum_{i=1}^{4} b_i^2 = \widetilde{s}s \quad \text{mit } \widetilde{s} < s \tag{7.11}$$

folgt. Werden die c_i wie oben definiert, so gilt

$$sp\widetilde{s}s = (\sum_{i=1}^{4} a_i^2)(\sum_{i=1}^{4} b_i^2) = \sum_{i=1}^{4} c_i^2. \tag{7.12}$$

Wegen $a_i \equiv b_i \pmod s$ gilt unter Beachtung der Darstellung der c_i

$$c_i \equiv 0 \pmod s \quad \text{für } i = 1, \ldots, 4.$$

Aus (7.12) ergibt sich somit

$$\widetilde{s}p = \sum_{i=1}^{4} (\frac{c_i}{s})^2, \ \widetilde{s} < s,$$

was wieder einen Widerspruch zur Minimaleigenschaft von s darstellt. □

Anmerkung: Den theoretischen Hintergrund für den Vier-Quadrate-Satz liefert der Schiefkörper der Hamiltonschen Quaternionen.

7.3 Summen von drei Quadraten

Satz 7.4 (Gauß). *Die natürliche Zahl n ist genau dann als Summe von drei Quadraten darstellbar, wenn n nicht die Form*

$$n = 4^l(8k+7) \quad \text{mit } l, k \in \mathbb{N}_0$$

besitzt.

(ohne Beweis)

Teil II

Kettenbrüche und quadratische Irrationalzahlen

8 Kettenbrüche

8.1 Der Kettenbruchalgorithmus

Bezeichnungen: Wie üblich bezeichnet $\mathbb{Q} = (\mathbb{Q}, +, \cdot)$ den durch $\leq$ geordneten Körper der rationalen Zahlen und $\mathbb{R} = (\mathbb{R}, +, \cdot)$ den durch $\leq$ geordneten Körper der reellen Zahlen. ($\mathbb{R}$ ist die Vervollständigung von $\mathbb{Q}$ bezüglich des gewöhnlichen Absolutbetrags, und die Ordnung auf $\mathbb{R}$ ist verträglich mit der auf $\mathbb{Q}$.)

Für $r \in \mathbb{N}$ bezeichnet $a_0 := [r]$ die größte ganze Zahl kleiner gleich r. Es gilt also

$$r =: r_0 = a_0 + \frac{1}{r_1} \quad \text{mit } 1 < r_1 \leq \infty.$$

Für $r_1 \neq \infty$ gilt weiter

$$r_1 = a_1 + \frac{1}{r_2} \quad \text{mit } a_1 = [r_1] \quad \text{und } 1 < r_2 \leq \infty$$

oder allgemein für $r_n \neq \infty$

$$r_n = a_n + \frac{1}{r_{n+1}} \quad \text{mit } a_n = [r_n] \quad \text{und } 1 < r_{n+1} \leq \infty.$$

Definition 8.1. Mit den Bezeichnungen wie oben heißt $[a_0; a_1, a_2, a_3, \ldots, a_n, \ldots]$ **Kettenbruch (Kettenbruchentwicklung)** von r.

Für $r_{n+1} = \infty$ heißt $[a_0; a_1, \ldots, a_n]$ **abbrechender Kettenbruch**.

$$[a_0; a_1, \ldots, a_n] = \frac{p_n}{q_n} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}}}$$

mit teilerfremden ganzen Zahlen p_n und q_n und $q_n > 0$ heißt **n-ter Näherungsbruch**.

Beispiel 8.1. (a) Mit Hilfe des euklidischen Algorithmus ergibt sich für $r = {}^{12}/_5$:

$$\begin{aligned} r &= \frac{12}{5} = 2 + \frac{1}{{}^5/_2} \\ r_1 &= \frac{5}{2} = 2 + \frac{1}{2} \\ r_2 &= 2. \end{aligned}$$

Somit besitzt $r = [2; 2, 2]$ eine Darstellung als abbrechender Kettenbruch.

(b) Für $r = 1 + \sqrt{2}$ ergibt sich wegen

$$\begin{aligned} r &= 2 + (\sqrt{2} - 1) \\ r_1 &= \frac{1}{\sqrt{2} - 1} = \sqrt{2} + 1 = 2 + (\sqrt{2} - 1) \\ r_2 &= \frac{1}{\sqrt{2} - 1} = r_1 \end{aligned}$$

die Darstellung $r = [2; 2, 2, \ldots]$ als **periodischer Kettenbruch**.

(c) Die Eulersche Zahl läßt sich schreiben als $e = [2; 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, \ldots]$. (Für den Beweis siehe z.B. Perron, Lehre der Kettenbrüche)

Bemerkung 8.1. *Der Kettenbruch von $r \in \mathbb{R}$ bricht genau dann ab, wenn $r \in \mathbb{Q}$ gilt.*

Beweis. Bricht der Kettenbruch von r ab, so besitzt r eine Darstellung $r = {}^{p_n}/_{q_n} \in \mathbb{Q}$ als Näherungsbruch.

Gilt umgekehrt $r \in \mathbb{Q}$, so bilden die Nenner der r_i bei der Kettenbruchentwicklung eine streng monoton fallende Folge natürlicher Zahlen. Also bricht der Kettenbruch von r ab.□

Definition 8.2. Die beiden Vektoren $\binom{r}{s}$ und $\binom{\widetilde{r}}{\widetilde{s}}$ heißen **verhältnisgleich** falls $r\widetilde{s} = s\widetilde{r}$ gilt.

Bezeichnung: $\binom{r}{s} \sim \binom{\widetilde{r}}{\widetilde{s}}$. Für $r_n = a_n + {}^1/_{r_{n+1}}$ gilt somit

$$\begin{pmatrix} r_n \\ 1 \end{pmatrix} \sim \begin{pmatrix} a_n r_{n+1} + 1 \\ r_{n+1} \end{pmatrix} = A_n \begin{pmatrix} r_{n+1} \\ 1 \end{pmatrix},$$

wobei $A_n := \left(\begin{smallmatrix} a_n & 1 \\ 1 & 0 \end{smallmatrix}\right)$ mit $\det A_n = -1$ gesetzt wurde. Durch Induktion ergibt sich somit

$$\begin{pmatrix} r \\ 1 \end{pmatrix} \sim A_0 \cdots A_n \begin{pmatrix} r_{n+1} \\ 1 \end{pmatrix} \quad \text{bzw.} \quad \begin{pmatrix} r \\ 1 \end{pmatrix} \sim P_n \begin{pmatrix} r_{n+1} \\ 1 \end{pmatrix} \tag{8.1}$$

mit $P_n := A_0 \cdots A_n$.

Bemerkung 8.2. *Mit den Bezeichnungen von oben gilt*

$$P_n = \begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix} \quad \text{und } \det P_n = (-1)^{n+1}.$$

Beweis. Aus $P_n = A_0 \cdot \ldots \cdot A_n$ und $\det A_i = -1$ folgt $\det P_n = (-1)^{n+1}$. Da sich die Aussage nicht ändert, wenn man statt r den n-ten Näherungsbruch von r betrachtet, kann ohne Einschränkung $r = {}^{p_n}/_{q_n}$ und damit $r_n = a_n$ angenommen werden. Hieraus ergibt sich zusammen mit (8.1)

$$\begin{pmatrix} p_n \\ q_n \end{pmatrix} \sim \begin{pmatrix} r \\ 1 \end{pmatrix} \sim P_{n-1} \begin{pmatrix} r_n \\ 1 \end{pmatrix} = P_{n-1} \begin{pmatrix} a_n \\ 1 \end{pmatrix} = P_{n-1} A_n \begin{pmatrix} 1 \\ 0 \end{pmatrix} = P_n \begin{pmatrix} 1 \\ 0 \end{pmatrix},$$

woraus die Darstellung

$$P_n = \begin{pmatrix} \widetilde{p_n} & * \\ \widetilde{q_n} & * \end{pmatrix} \quad \text{mit} \begin{pmatrix} \widetilde{p_n} \\ \widetilde{q_n} \end{pmatrix} \sim \begin{pmatrix} p_n \\ q_n \end{pmatrix}$$

folgt. Da $\mathrm{ggT}\{p_n, q_n\} = 1$ ist und wegen $\det P_n = (-1)^{n+1}$ auch $\mathrm{ggT}\{\widetilde{p_n}, \widetilde{q_n}\} = 1$ gilt, folgt wegen $q_n > 0$ und $\widetilde{q_n} > 0$ schließlich $p_n = \widetilde{p_n}$ und $q_n = \widetilde{q_n}$. Aus der Darstellung $P_{n-1} = \left(\begin{smallmatrix} p_{n-1} & * \\ q_{n-1} & * \end{smallmatrix}\right)$ folgt somit

$$P_n = P_{n-1} \cdot A_n = \begin{pmatrix} p_{n-1} & * \\ q_{n-1} & * \end{pmatrix} \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} * & p_{n-1} \\ * & q_{n-1} \end{pmatrix}$$

und damit die Behauptung. □

Folgerung 8.1. *Für $n \geq 2$ gilt*

$$p_n = p_{n-1}a_n + p_{n-2} \quad \text{und } q_n = q_{n-1}a_n + q_{n-2}.$$

Beweis. Die Behauptung folgt unmittelbar aus Bemerkung 8.2 und der Beziehung $P_n = P_{n-1}A_n$ □

Anmerkung: Durch die Definitionen $p_{-2} = 0,\ p_{-1} = 1,\ q_{-2} = 1$ und $q_{-1} = 0$ behalten die Rekursionsformeln in Folgerung 8.1 auch für $n = 0, 1$ ihre Gültigkeit. Die p_n, q_n können daher etwa durch folgende Tabelle aus den a_n berechnet werden:

n	-2	-1	0	1	2	3
a_n	$\times$	$\times$				
p_n	0	1				
q_n	1	0				

Satz 8.1. *Für die n-ten Näherungsbrüche ${}^{p_n}/_{q_n}$ von $r \in \mathbb{R}$ gilt*

$$a_0 = \frac{p_0}{q_0} < \frac{p_2}{q_2} < \frac{p_4}{q_4} < \ldots \leq r \leq \ldots < \frac{p_3}{q_3} < \frac{p_1}{q_1} \quad \text{mit } \left| r - \frac{p_n}{q_n} \right| \leq \frac{1}{q_n q_{n+1}}$$

Beweis. Aus (8.1) und der Beziehung $\det P_n = p_n q_{n-1} - q_n p_{n-1} = (-1)^{n+1}$ folgt

$$\begin{aligned} r - \frac{p_n}{q_n} &= \frac{p_n r_{n+1} + p_{n-1}}{q_n r_{n+1} + q_{n-1}} - \frac{p_n}{q_n} \\ &= \frac{q_n p_n r_{n+1} + q_n p_{n-1} - p_n q_n r_{n+1} - p_n q_{n-1}}{q_n(q_n r_{n+1} + q_{n-1})} = \frac{(-1)^n}{q_n(q_n r_{n+1} + q_{n-1})} \end{aligned}$$

Wegen $r_{n+1} \geq a_{n+1}$ und Folgerung 8.1 gilt

$$q_n r_{n+1} + q_{n-1} \geq q_n a_{n+1} + q_{n-1} = q_{n+1},$$

woraus sich die behauptete Abschätzung

$$\left| r - \frac{p_n}{q_n} \right| \leq \frac{1}{q_n q_{n+1}}$$

ergibt. Aus

$$\begin{aligned} p_n q_{n-2} &= (a_n p_{n-1} + p_{n-2}) q_{n-2}, \\ q_n p_{n-2} &= (a_n q_{n-1} + q_{n-2}) p_{n-2} \end{aligned}$$

und der Beziehung $\det P_{n-1} = p_{n-1}q_{n-2} - q_{n-1}p_{n-2} = (-1)^n$ folgt

$$\frac{p_n}{q_n} - \frac{p_{n-2}}{q_{n-2}} = \frac{p_n q_{n-2} - p_{n-2} q_n}{q_n q_{n-2}} = (-1)^n \frac{a_n}{q_n q_{n-2}}.$$

Hieraus ergeben sich die Näherungen wie in Satz 8.1 angegeben. □

8.2 Periodische Kettenbrüche

Definition 8.3. Ein Kettenbruch der Art

$$[a_0; a_1, \ldots, a_k, \overline{a_{k+1}, \ldots, a_l}]$$

heißt **periodischer Kettenbruch**.

Satz 8.2 (Euler–Lagrange). *Eine reelle Zahl r besitzt genau dann einen periodischen Kettenbruch, wenn r eine quadratische Irrationalzahl ist.*

Beweis. Es sei $r = [a_0; a_1, \ldots, a_k, \overline{a_{k+1}, \ldots, a_l}]$ eine reelle Zahl mit periodischem Kettenbruch. Aus $\binom{r}{1} \sim P_k \binom{r_{k+1}}{1}$ folgt

$$r = \frac{p_k r_{k+1} + p_{k-1}}{q_k r_{k+1} + q_{k-1}}.$$

Daher ist r eine quadratische Irrationalzahl genau dann, wenn r_{k+1} eine quadratische Irrationalzahl ist. Ohne Einschränkung kann also r als rein periodisch angenommen werden, etwa

$$r = [\overline{a_0; a_1, \ldots, a_l}].$$

Aus $\binom{r}{1} \sim P_l \binom{r_{l+1}}{1} = P_l \binom{r}{1}$ folgt daher

$$r = \frac{p_l r + p_{l-1}}{q_l r + q_{l-1}},$$

woraus sich

$$q_l r^2 + r(q_{l-1} - p_l) - p_{l-1} = 0$$

ergibt. Also ist r Lösung einer quadratischem Gleichung mit ganzzahligen Koeffizienten. Zusammen mit Bemerkung 8.1 ergibt sich, daß r eine quadratische Irrationalzahl ist. Der Beweis der Umkehrung erfolgt am Ende des Abschnitts. □

Definition 8.4. Ist $r \in \mathbb{R}$ eine quadratische Irrationalzahl, etwa

$$\begin{aligned} & ar^2 + br + c = 0 \quad \text{mit } a \in \mathbb{N},\ b, c \in \mathbb{Z},\ \mathrm{ggT}\left\{a, b, c\right\} = 1 \\ & \text{d.h. } r = -\frac{b}{2a} \pm \frac{1}{2a}\sqrt{b^2 - 4ac}, \end{aligned}$$

so heißt $\mathrm{D}(r) := b^2 - 4ac$ **Diskriminante** von r.

Bemerkung 8.3. *Ist $r \in \mathbb{R}$ eine quadratische Irrationalzahl, so gilt für alle $n \geq 0$*

$$\mathrm{D}(r_n) = \mathrm{D}(r).$$

Beweis. Für $n = 0$ ist nichts zu zeigen. Es gelte nun $\mathrm{D}(r_n) = \mathrm{D}(r) = b^2 - 4ac$. Aus $r_n = a_n + {}^{1}/_{r_{n+1}}$ und $ar_n^2 + br_n + c = 0$ folgen

$$\begin{aligned} a\left(a_n + \frac{1}{r_{n+1}}\right)^2 + b\left(a_n + \frac{1}{r_{n+1}}\right) + c = 0 \\ \underbrace{(aa_n^2 + ba_n + c)}_{\widetilde{a}} r_{n+1}^2 + \underbrace{(2aa_n + b)}_{\widetilde{b}} r_{n+1} + \underbrace{a}_{\widetilde{c}} = 0. \end{aligned}$$

Da mit $\mathrm{ggT}\{a, b, c\}$ auch $\mathrm{ggT}\{\widetilde{a}, \widetilde{b}, \widetilde{c}\}$ gilt, folgt durch

$$\begin{aligned} \mathrm{D}(r_{n+1}) &= \widetilde{b}^2 - 4\widetilde{a}\widetilde{c} \\ &= 4a^2a_n^2 + 4aa_nb + b^2 - 4(a^2a_n^2 + aba_n + ac) \\ &= b^2 - 4ac \\ &= \mathrm{D}(r_n) \end{aligned}$$

die Behauptung. □

Definition 8.5. Ist $r = -{}^{b}/_{2a} + {}^{1}/_{2a}\sqrt{d}$ mit $d = \mathrm{D}(r)$ eine quadratische Irrationalzahl, so heißt

$$r' := -\frac{b}{2a} - \frac{1}{2a}\sqrt{d}$$

die **zu r konjugierte quadratische Irrationalzahl**. Die Zahl r heißt **reduziert**, falls $r > 1$ und $-{}^{1}/_{r'} > 1$ gelten.

Bemerkung 8.4. *Zu einer gegebenen Diskriminante d gibt es nur endlich viele reduzierte quadratische Irrationalzahlen.*

Beweis. Es sei r eine reduzierte quadratische Irrationalzahl mit $\mathrm{D}(r) = d$. Da mit $-{}^{1}/_{r'} > 1$ auch $-1 < r' < 0$ gilt, folgt $r + r' > 0$. Also gilt $-{}^{b}/_{2a} > 0$, woraus wegen $a \in \mathbb{N}$ schließlich $b < 0$ folgt.

Andererseits gilt wegen $-r' > 0$ auch ${}^{b}/_{2a} + {}^{1}/_{2a}\sqrt{d} > 0$, womit sich $b + \sqrt{d} > 0$ und schließlich $b > -\sqrt{d}$ ergibt. Folglich gilt $-\sqrt{d} < b < 0$, und daher gibt es nur endlich viele Möglichkeiten für die Wahl von b. Da wegen $d = b^2 - 4ac$ sowohl a als auch c Teiler von $d - b^2$ sind, gibt es auch nur endlich viele Möglichkeiten für die Wahl von a und c. Daher gibt es nur endlich viele reduzierte r mit $\mathrm{D}(r) = d$. □

Bemerkung 8.5. *Ist $r \in \mathbb{R}$ eine quadratische Irrationalzahl, so existiert ein $n_0 \in \mathbb{N}$, so daß für alle $n \geq n_0$ die Zahl r_n reduziert ist.*

Beweis. Es sei $r = [a_0; a_1, a_2, \ldots]$ die Kettenbruchdarstellung von r. Wegen $\binom{r}{1} \sim P_n \binom{r_{n+1}}{1}$ gilt

$$\begin{pmatrix} r_{n+1} \\ 1 \end{pmatrix} \sim P_n^{-1} \begin{pmatrix} r \\ 1 \end{pmatrix} \quad \text{mit } P_n^{-1} = (-1)^{n+1} \begin{pmatrix} q_{n-1} & -p_{n-1} \\ -q_n & p_n \end{pmatrix}.$$

Hieraus folgt wegen $r_{n+1} > 1$

$$r_{n+1} = \frac{q_{n-1}r - p_{n-1}}{-q_n r + p_n} \quad \text{bzw. } r'_{n+1} = \frac{q_{n-1}r' - p_{n-1}}{-q_n r' + p_n},$$

und zusammen mit $\det P_n = p_n q_{n-1} - q_n p_{n-1} = (-1)^{n+1}$ ergibt sich

$$\begin{aligned}
-\frac{1}{r'_{n+1}} &= \frac{q_n r' - p_n}{q_{n-1}r' - p_{n-1}} \cdot \frac{q_{n-1}}{q_{n-1}} = \frac{q_n q_{n-1} r' - p_n q_{n-1}}{q_{n-1}(q_{n-1}r' - p_{n-1})} \\
&= \frac{q_n q_{n-1} r' - (q_n p_{n-1} + (-1)^{n+1})}{q_{n-1}(q_{n-1}r' - p_{n-1})} = \left(\frac{q_n}{q_{n-1}} - \frac{(-1)^{n+1}}{q_{n-1}(q_{n-1}r' - p_{n-1})} \right), \\
-\frac{1}{r'_{n+1}} - 1 &= \frac{1}{q_{n-1}} \left((q_n - q_{n-1}) - \frac{(-1)^{n+1}}{q_{n-1}\left(r' - {p_{n-1}}/{q_{n-1}}\right)} \right)
\end{aligned}$$

Für $n \to \infty$ strebt ${p_{n-1}}/{q_{n-1}}$ gegen r und q_{n-1} gegen ∞, während $q_n - q_{n-1} \in \mathbb{N}$ gilt. Für hinreichend große n ist wegen $-{1}/{r'_{n+1}} > 1$ damit r_n reduziert. □

Beweis zum Satz von Euler–Lagrange Teil 2. Ist $r \in \mathbb{R}$ eine quadratische Irrationalzahl, so existiert nach Bemerkung 8.5 ein $n_0 \in \mathbb{N}$, so daß für alle $n \geq n_0$ die Zahl r_n reduziert ist. Nach Bemerkung 8.3 gilt jeweils $\mathrm{D}(r_n) = \mathrm{D}(r)$. Da es nach Bemerkung 8.4 nur endlich viele verschiedene reduzierte r_n mit $\mathrm{D}(r_n) = \mathrm{D}(r)$ geben kann, existieren Zahlen k und l mit $r_{k+l} = r_k$. Hieraus folgt aber $r_{k+l+i} = r_{k+i}$ und damit $a_{k+l+i} = a_{k+i}$ für alle $i \in \mathbb{N}$. Folglich ist der Kettenbruch periodisch. □

8.3 Rein periodische Kettenbrüche

Bemerkung 8.6. *Ist $r \in \mathbb{R}$ eine reduzierte quadratische Irrationalzahl, so ist für alle $n \in \mathbb{N}$ auch r_n eine reduzierte quadratische Irrationalzahl.*

Beweis. Da r reduziert ist, gelten $r > 1$ und $r' < 0$. Aus

$$r = a_0 + \frac{1}{r_1} \quad \text{und } r' = a_0 + \frac{1}{r'_1}$$

folgt somit $r_1 > 1$ und wegen $a_0 \geq 1$ auch

$$-\frac{1}{r'_1} = a_0 - r' > 1.$$

Daher ist r_1 reduzierte quadratische Irrationalzahl. Die Behauptung folgt durch Induktion. □

Satz 8.3. *Eine reelle quadratische Irrationalzahl r besitzt genau dann eine rein periodische Kettenbruchentwicklung, wenn r reduziert ist.*

Beweis. Ist $r \in \mathbb{R}$ eine quadratische Irrationalzahl mit rein periodischer Kettenbruchentwicklung $r = [\overline{a_0; a_1, \ldots, a_{l-1}}]$, so gilt $r = r_l = r_{2l} = \cdots$. Nach Bemerkung 8.5 gibt es eine Zahl i, so daß r_{il} reduziert ist. Folglich ist r reduziert.

Für die Umkehrung sei r eine reduzierte quadratische Irrationalzahl. Nach Satz 8.2 besitzt r eine periodische Kettenbruchentwicklung

$$r = [a_0; a_1, \ldots, a_k, \overline{a_{k+1}, \ldots, a_{k+l}}].$$

Angenommen, für die minimale Zahl m mit $r_m = r_{m+l}$ gelte $m > 0$. Aus

$$r_{m-1} = a_{m-1} + \frac{1}{r_m} \quad \text{und } r'_{m-1} = a_{m-1} + \frac{1}{r'_m}$$

folgt

$$-\frac{1}{r'_m} = a_{m-1} - r'_{m-1},$$

und da r_{m-1} nach Bemerkung 8.6 reduziert ist, ergibt sich wegen $-1 < r'_{m-1} < 0$

$$a_{m-1} = \left[-\frac{1}{r'_m}\right] = \left[-\frac{1}{r'_{m+l}}\right] = a_{m+l-1}.$$

Hieraus folgt aber $r_{m+l-1} = r_{m-1}$ und damit ein Widerspruch zur Minimalität von m. □

Bemerkung 8.7. *Ist $r \in \mathbb{R}$ eine reduzierte quadratische Irrationalzahl, etwa*

$$r = [\overline{a_0; a_1, \ldots, a_{l-1}}],$$

so gilt für die konjugierte Zahl r'

$$-\frac{1}{r'} = [\overline{a_{l-1}; a_{l-2}, \ldots, a_0}].$$

Beweis. Es sei

$$-\frac{1}{r'} =: [\overline{\widetilde{a_0}; \widetilde{a_1}, \ldots, \widetilde{a_{j-1}}}].$$

Wegen $r = r_l$ gilt zunächst $r_{l-1} = a_{l-1} + {}^1/_r$ und somit $-{}^1/_{r'} = a_{l-1} - r'_{l-1}$. Da r_{l-1} reduziert ist, folgt wegen $0 < -r'_{l-1} < 1$ die Beziehung

$$a_{l-1} = \left[-\frac{1}{r'}\right] = \widetilde{a_0}.$$

Wegen $-{}^1/_{r'_{l-1}} = a_{l-2} - r'_{l-2}$ gilt weiter

$$a_{l-2} = \left[-\frac{1}{r'_{l-1}}\right] = \widetilde{a_1}.$$

Die Behauptung folgt durch Induktion. □

Beispiel 8.2. Für die Zahl $r = [1; \overline{1}]$ mit rein periodischer Kettenbruchentwicklung gilt

$$r = 1 + \frac{1}{r_1} = 1 + \frac{1}{r},$$

woraus $r^2 - r - 1 = 0$ und schließlich $r = {}^1/_2 + {}^1/_2\sqrt{5}$ folgt.

9 Diophantische Approximation

9.1 Diophantische Approximation und Kettenbrüche

Definition 9.1. Sind $r \in \mathbb{R}$, $p \in \mathbb{Z}$ und $q \in \mathbb{N}$, so heißt $^p/_q$ **diophantische (beste) Approximation von** r, falls für alle $\widetilde{p} \in \mathbb{Z}$ und $\widetilde{q} \in \mathbb{N}$ mit $\widetilde{q} \leq q$ entweder $^p/_q = {}^{\widetilde{p}}/_{\widetilde{q}}$ oder

$$|rq - p| < |r\widetilde{q} - \widetilde{p}|$$

gilt.

Anmerkung: Aus $\left|r - {}^{\widetilde{p}}/_{\widetilde{q}}\right| < \left|r - {}^p/_q\right|$ mit $\widetilde{q} < q$ folgt $|r\widetilde{q} - \widetilde{p}| < |rq - p|$. Ist also $^p/_q$ eine diophantische Approximation von r, so gibt es keine bessere rationale Approximation von r mit Nenner kleiner oder gleich q.

Satz 9.1. *(a) Ist $^p/_q$ eine diophantische Approximation von r, so gibt es eine natürliche Zahl n mit $^p/_q = {}^{p_n}/_{q_n}$. (Jede diophantische Approximation von r ist also ein Näherungsbruch.)*

(b) Ist $^{p_n}/_{q_n}$ ein Näherungsbruch von r mit $n \geq 1$, so ist $^{p_n}/_{q_n}$ eine diophantische Approximation von r.

Beweis.

(a) Es sei $^p/_q$ eine diophantische Approximation von r. Nach Satz 8.1 gilt

$$a_0 = \frac{p_0}{q_0} < \frac{p_2}{q_2} < \ldots \leq r \leq \ldots < \frac{p_3}{q_3} < \frac{p_1}{q_1}.$$

Durch Fallunterscheidung wird nun die Annahme, daß $^p/_q$ kein Näherungsbruch von r ist, zu einem Widerspruch geführt:

1.Fall: Es gelte $^p/_q < {}^{p_0}/_{q_0} = a_0$. Hieraus folgt $\left|r - {}^p/_q\right| > |r - a_0|$ und durch Multiplikation mit q ergibt sich

$$|rq - p| > |r - a_0|,$$

was im Widerspruch dazu steht, daß $^p/_q$ eine diophantische Approximation von r ist.

2.Fall: Es gelte $^p/_q > {}^{p_1}/_{q_1}$. Hieraus ergibt sich

$$\left|r - \frac{p}{q}\right| > \left|\frac{p_1}{q_1} - \frac{p}{q}\right| \geq \frac{1}{qq_1}.$$

Durch Multiplikation mit q und der Abschätzung in Satz 8.1 folgt

$$|rq - p| \geq \frac{1}{q_1} = \frac{1}{q_1 q_0} \geq \left|r - \frac{p_0}{q_0}\right| = |r - a_0|,$$

was wie oben einen Widerspruch darstellt.

3.Fall: Für irgendein n gelte ${}^{p_{n-1}}/_{q_{n-1}} < {}^{p}/_{q} < {}^{p_{n+1}}/_{q_{n+1}}$. Hieraus folgt

$$\frac{1}{qq_{n-1}} \leq \left|\frac{p}{q} - \frac{p_{n-1}}{q_{n-1}}\right| < \left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_{n-1}}{q_{n-1}}\right| \leq \left|r - \frac{p_{n-1}}{q_{n-1}}\right| \leq \frac{1}{q_{n-1}q_n},$$

was $q > q_n$ zur Folge hat. Weiter gilt

$$\left|r - \frac{p}{q}\right| \geq \left|\frac{p_{n+1}}{q_{n+1}} - \frac{p}{q}\right| \geq \frac{1}{qq_{n+1}},$$

woraus sich durch Multiplikation mit q und der Abschätzung in Satz 8.1

$$|rq - p| \geq \frac{1}{q_{n+1}} \geq |rq_n - p_n|$$

und damit wie oben ein Widerspruch ergibt.

Der 4.Fall: Für irgendein n gelte ${}^{p_{n+1}}/_{q_{n+1}} < {}^{p}/_{q} < {}^{p_{n-1}}/_{q_{n-1}}$ wird analog zum 3.Fall behandelt.

(b) Es sei ${}^{p_n}/_{q_n}$ ein Näherungsbruch von r mit $n \geq 1$. Wird

$$\begin{aligned} \mathcal{M}_n(r) &:= \left\{ (p,q) \in \mathbb{Z} \times \mathbb{N} \mid q \leq q_n \quad \text{und } |rq-p| \text{ minimal} \right\}, \\ q^* &:= \min\left\{ q \mid \ \text{es gibt } p \text{ mit } (p,q) \in \mathcal{M}_n(r) \right\} \end{aligned}$$

gesetzt, so ist q^* eindeutig bestimmt. Es sei p^* die zu q^* gehörige Zahl mit $(p,q) \in \mathcal{M}_n(r)$. Angenommen, p^* sei nicht eindeutig bestimmt, es gebe also ein $\widetilde{p^*} \neq p^*$ mit

$$\left|r - \frac{p^*}{q^*}\right| = \left|r - \frac{\widetilde{p^*}}{q^*}\right|.$$

Hieraus folgt aber

$$r = \frac{\widetilde{p^*} + p^*}{2q^*}$$

und schließlich

$$|rq^* - p^*| = \left|\frac{\widetilde{p^*} + p^*}{2} - p^*\right| = \left|\frac{\widetilde{p^*} - p^*}{2}\right| \geq \frac{1}{2}.$$

Andererseits folgt aber aus $q_2 > q_1 > q_0 = 1$, daß $q_2 \geq 3$ gilt, was nach der Abschätzung aus Satz 8.1

$$|rq_1 - p_1| \leq \frac{1}{q_2} \leq \frac{1}{3}$$

und damit einen Widerspruch zur Minimalität von q^* zur Folge hat. Daher ist p^* eindeutig bestimmt und ${}^{p^*}/_{q^*}$ ist nach Definition ein diophantische Approximation von r. Es bleibt zu zeigen, daß ${}^{p^*}/_{q^*} = {}^{p_n}/_{q_n}$ gilt. Nach Teil (a) des Satzes gibt es ein $m \leq n$ mit

$$\frac{p^*}{q^*} = \frac{p_m}{q_m}. \tag{9.1}$$

Angenommen, es gelte $m < n$. Die Beziehung $r_{m+1} < a_{m+1} + 1$ aus dem Kettenbruchalgorithmus und Folgerung 8.1 haben

$$q_m r_{m+1} + q_{m-1} < q_m a_{m+1} + q_{m-1} + q_m = q_{m+1} + q_m$$

zur Folge. Aus der Beziehung aus dem Beweis zu Satz 8.1 ergibt sich somit wegen $m < n$

$$|rq_m - p_m| = \left|\frac{1}{q_m r_{m+1} + q_{m-1}}\right| > \frac{1}{q_{m+1} + q_m} > \frac{1}{q_{n+1} + q_n}.$$

Zusammen mit (9.1) ergibt sich schließlich der Widerspruch

$$\begin{aligned}
\frac{1}{q_n + q_{n-1}} &< |q_m r - p_m| = |q^* r - p^*| \\
&\leq |q_n r - p_n| = \frac{1}{|q_n r_{n-1} + q_{n-1}|} \\
&< \frac{1}{q_n + q_{n-1}}.
\end{aligned}$$

Also ist ${}^{p_n}/_{q_n} = {}^{p^*}/_{q^*}$ eine diophantische Approximation von r.

□

Beispiel 9.1. Durch die Kettenbruchentwicklung sollen Näherungswerte für die Zahl $\pi = 3,14159265358979\ldots$ berechnet werden. Der Kettenbruchalgorithmus ergibt

$$\begin{aligned}
r_0 &= \pi = 3 + (\pi - 3) \\
r_1 &= \frac{1}{\pi - 3} = 7 + \frac{22 - 7\pi}{\pi - 3} \\
r_2 &= \frac{\pi - 3}{22 - 7\pi} = 15 + \left(\frac{\pi - 3}{22 - 7\pi} - 15\right) = 15 + \frac{106\pi - 333}{22 - 7\pi} \\
r_3 &= \frac{22 - 7\pi}{106\pi - 333} = 1 + \ldots
\end{aligned}$$

Mit ${}^{p_1}/_{q_1} = 3 + {}^{1}/_{7} = 3,1328\ldots$ ergibt sich der klassische Näherungswert für π. ${}^{p_2}/_{q_2} = 3,141509\ldots$ und ${}^{p_3}/_{q_3} = 3,1415929\ldots$ liefern bereits Näherungen mit 4 bzw. 6 Stellen Genauigkeit.

9.2 Diophantische Approximation algebraischer Zahlen

Definition 9.2. Eine komplexe Zahl a heißt **algebraische Zahl**, wenn es ein Polynom $f \in \mathbb{Q}[X]$ mit $f(a) = 0$ gibt. Ist n der minimale Grad eines solchen Polynoms, so heißt a algebraische Zahl **vom Grad** n.

Satz 9.2 (Liouville)**.** *Ist a eine irrationale algebraische Zahl vom Grad n, so gibt es eine reelle Zahl $c > 0$, so daß für alle $p \in \mathbb{Z}$ und $q \in \mathbb{N}$*

$$\left|a - \frac{p}{q}\right| \geq \frac{c}{q^n}$$

gilt.

Beweis. Gilt $a \notin \mathbb{R}$, so folgt

$$\left|a - \frac{p}{q}\right| \geq |\mathrm{Im}(a)| \geq \frac{|\mathrm{Im}(a)|}{q^n}$$

und mit $c := |\mathrm{Im}(a)|$ erhält man die behauptete Abschätzung.

Gilt andererseits $a \in \mathbb{R}$, so sei $f \in \mathbb{Q}[X]$ ein Polynom kleinsten Grades mit $f(a) = 0$. Ohne Einschränkung kann

$$f(x) = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$$

angenommen werden. Wäre a mehrfache Nullstelle von f, so wäre a auch Nullstelle von $f' \in \mathbb{Z}[X]$, und es würde sich wegen $\partial(f') < \partial(f)$ ein Widerspruch zu der Wahl von f ergeben. Daher gilt

$$f(X) = (X - a)g(X) \quad \text{mit } g \in \mathbb{R}[X] \quad \text{und } g(a) \neq 0.$$

Aus der Stetigkeit von g folgt die Existenz von $\delta > 0$ mit

$$g(x) \neq 0 \quad \text{für } a - \delta \leq x \leq a + \delta.$$

Sind $p \in \mathbb{Z}$ und $q \in \mathbb{N}$ beliebig vorgegeben, so gilt gilt entweder $\left|a - {}^{p}/_{q}\right| \geq \delta$ oder $\left|a - {}^{p}/_{q}\right| < \delta$. Im ersten Fall gilt für alle $n \in \mathbb{N}$ die Abschätzung $\left|a - {}^{p}/_{q}\right| \geq {}^{\delta}/_{q^n}$. Im zweiten Fall folgt $g({}^{p}/_{q}) \neq 0$ und damit

$$\left|a - \frac{p}{q}\right| = \left|\frac{f({}^{p}/_{q})}{g({}^{p}/_{q})}\right| = \frac{|a_n p^n + a_{n-1}p^{n-1}q + \cdots + a_0 q^n|}{\left|q^n g({}^{p}/_{q})\right|} \geq \frac{1}{q^n M},$$

wobei $M := \max\{\, |g(x)| \mid a - \delta \leq x \leq a + \delta \,\}$ gesetzt wurde.

Daher erhält man mit $c := \min\{\delta, {}^{1}/_{M}\}$ die behauptete Abschätzung. □

Folgerung 9.1. *Es gibt reelle Zahlen, die nicht algebraisch sind.*

Beweis. Es seien $a_0, \ldots, a_k \in \mathbb{N}$, ${}^{p_k}/_{q_k} := [a_0; a_1, \ldots, a_k]$ und $a_{k+1}, \ldots, a_n, \ldots \in \mathbb{N}$ mit $a_{n+1} > q_n^{n-1}$ für $n \geq k$. Setzt man $r := [a_0; a_1, \ldots, a_n, \ldots]$, so gilt nach Satz 8.1 und Folgerung 8.1

$$\left|r - \frac{p_n}{q_n}\right| \leq \frac{1}{q_n q_{n+1}} = \frac{1}{q_n(q_n a_{n+1} + q_{n-1})} \leq \frac{1}{q_n^2 a_{n+1}} < \frac{1}{q_n^{n+1}} \quad \text{für } n \geq k.$$

Wäre r eine algebraische Zahl vom Grad m, so gäbe es ein $c > 0$ mit

$$\left|r - \frac{p_n}{q_n}\right| \geq \frac{c}{q_n^m},$$

was den Widerspruch

$$\frac{c}{q_n^m} < \frac{1}{q_n^{n+1}} \quad \text{für alle } n \geq k$$

zur Folge hätte. Eine so konstruierte nicht algebraische reelle Zahl r heißt **Liouville'sche transzendente Zahl**. □

9.3 Das Primzerlegungsverfahren von Lehman

Satz 9.3 (Lehman). *Ist $6 \neq n \in \mathbb{N}$ eine zusammengesetzte Zahl, so gilt genau eine der beiden folgenden Aussagen:*

(a) *Es gibt $p \in \mathbb{P}$ mit $p \leq \sqrt[3]{n}$ und $p \mid n$*

(b) *Es gibt natürliche Zahlen k, d und m mit*

$$k \leq \sqrt[3]{n},\ d \leq \frac{\sqrt[6]{n}}{4\sqrt{k}} + 1 \quad \text{und} \quad \left(\left[\sqrt{4kn}\right] + d\right)^2 - 4kn = m^2.$$

Dabei ist für $l := \left[\sqrt{4kn}\right] + d$ die Zahl $\mathrm{ggT}\{l+m, n\}$ ein nichttrivialer Teiler von n.

Beispiel 9.2. Die Anwendung des Satzes auf $n = 2257$ ergibt folgendes: Wegen $[\sqrt[3]{n}] = 13$ und $p \nmid n$ für $p \in \{2, 3, 5, 7, 11, 13\}$ muß Aussage (b) des Satzes zutreffen. Da für $1 \leq k \leq 13$ stets $1 \leq d \leq {}^{\sqrt[6]{n}}/_{4\sqrt{k}} + 1 < 2$ gilt, darf $d = 1$ angenommen werden. Das Rechenschema ist nun aus folgender Tabelle ersichtlich:

k	$4kn$	$\left[\sqrt{4kn}\right]$	l	l^2	$l^2 - 4kn$
1	9028	95	96	9216	188
2	18056	134	135	18225	$169 = 13^2 = m^2$

Hieraus ergibt sich der nichttriviale Teiler $\mathrm{ggT}\{135 + 13,\ 2257\} = 37$ von $n = 37 \cdot 61$.

Vorbemerkung: Gilt $n = pq$ mit $\sqrt[3]{n} < q \leq p < \sqrt[3]{n^2}$, so gibt es natürliche Zahlen r und s mit

$$rs \leq \sqrt[3]{n} \quad \text{und} \quad |qr - ps| \leq \sqrt[3]{n}.$$

Beweis. Es sei ${}^{p}/_{q} = [a_0; a_1, a_2, \ldots]$ die Darstellung von ${}^{p}/_{q}$ als abbrechender Kettenbruch mit Näherungsbrüchen ${}^{p_n}/_{q_n}$. Nach Voraussetzung gelten

$$p_0 q_0 = a_0 = \left[\frac{p}{q}\right] < \sqrt[3]{n} \quad \text{und } q > \sqrt[3]{n}.$$

Da die Folge der $p_i q_i$ monoton wachsend ist, gibt es eine natürliche Zahl m mit

$$p_m q_m < \sqrt[3]{n} \quad \text{und } p_{m+1} q_{m+1} \geq \sqrt[3]{n}.$$

Wird $r := p_m$ und $s := q_m$ gesetzt, so gilt nach Satz 8.1

$$\left|\frac{r}{s} - \frac{p}{q}\right| \leq \frac{1}{s q_{m+1}} \quad \text{bzw. } |rq - ps| \leq \frac{q}{q_{m+1}}.$$

Gilt ${}^{q}/_{q_{m+1}} \leq {}^{p}/_{p_{m+1}}$, so folgt wie behauptet

$$|rq - ps| \leq \sqrt{\frac{q}{q_{m+1}} \frac{p}{p_{m+1}}} \leq \sqrt{\frac{n}{\sqrt[3]{n}}} \leq \sqrt[3]{n}.$$

Gilt andererseits ${}^{p}/_{p_{m+1}} < {}^{q}/_{q_{m+1}}$, so läßt sich durch die Darstellung

$$\frac{q}{p} = 0 + \frac{1}{{}^{p}/_{q}} = [0; a_0, a_1, \ldots]$$

und mit den sich aus dem Kettenbruchalgorithmus ergebenden Näherungsbrüchen $\widetilde{p_n}/\widetilde{q_n} = {}^{q_{n+1}}/_{p_{n+1}}$ durch Vertauschung von p und q, r und s schließlich

$$|sp - qr| \leq \frac{p}{p_{m+1}} < \sqrt{\frac{p}{p_{m+1}} \frac{q}{q_{m+1}}} \leq \sqrt[3]{n}$$

folgern. □

Beweis zu dem Satz von Lehman. Gilt Aussage (a) des Satzes nicht, so ist n eine zusammengesetzte Zahl mit $p \nmid n$ für alle $p \leq \sqrt[3]{n}$. Daher gilt $n = pq$ mit $\sqrt[3]{n} < q \leq p < \sqrt[3]{n^2}$. Wird mit den Bezeichnungen aus der Vorbemerkung $k := rs$ gesetzt, so gilt $k \leq \sqrt[3]{n}$. Weiter gilt

$$4kn = 4rspq = (qr + ps)^2 - (qr - ps)^2 =: l^2 + m^2 \quad \text{mit } m \leq \sqrt[3]{n}.$$

Wird $d := l - \left[\sqrt{4kn}\right] \geq 1$ gesetzt, so folgt weiter

$$m^2 = l^2 - 4kn = \left(l - \sqrt{4kn}\right)\left(l + \sqrt{4kn}\right) \geq (d-1)\left(d + \left[\sqrt{4kn}\right] + \sqrt{4kn}\right) \geq 2(d-1)\sqrt{4kn}.$$

Also gilt

$$\begin{aligned} 2(d-1)\sqrt{4kn} &\leq \sqrt[3]{n^2} \\ d &\leq \frac{\sqrt[3]{n^2}}{2\sqrt{4kn}} + 1 = \frac{\sqrt[6]{n}}{4\sqrt{k}} + 1. \end{aligned}$$

Wegen $4kn = (l+m)(l-m)$ und $p, q \nmid 4k$ genügt es, $l + m < n$ zu zeigen. Dies folgt für $n \geq 27$ aus

$$l + m \leq d + \sqrt{4kn} + m \leq 1 + \frac{\sqrt[6]{n}}{4} + 2\sqrt[3]{n^2} + \sqrt[3]{n} < 3\sqrt[3]{n^2} \leq n.$$

Für $n < 27$ ergibt sich die Behauptung des Satzes durch direkte Verifikation mit der Ausnahme $n = 6$. □

Zusatz 9.1. *Die Anzahl der Divisionsversuche ist durch $2\sqrt[3]{n}$ beschränkt. Genauer gilt*

$$\left|\{\, p \mid p \leq \sqrt[3]{p} \,\}\right| + \left|\left\{\, (k,d) \mid 1 \leq k \leq \sqrt[3]{n},\ 1 \leq d \leq \frac{\sqrt[6]{n}}{4\sqrt{k}} + 1 \,\right\}\right| \leq 2\sqrt[3]{n}.$$

Beweis. Offensichtlich gilt

$$\left|\{\, p \mid p \leq \sqrt[3]{n} \,\}\right| \leq \frac{1}{3}\sqrt[3]{n}.$$

Aus der Bedingung für d ergibt sich

$$\sqrt[3]{n} \geq 16(d-1)^2 k.$$

Für $d = 1$ ergibt sich hieraus keine weitere Bedingung für k, während für $d \geq 2$

$$k \leq \frac{\sqrt[3]{n}}{16(d-1)^2}$$

gefolgert werden kann. Durch Summation folgt schließlich

$$\begin{aligned}
\left| \left\{ (k,d) \mid 1 \leq k \leq \sqrt[3]{n},\ 1 \leq d \leq \frac{\sqrt[6]{n}}{4\sqrt{k}} + 1 \right\} \right| &\leq \sqrt[3]{n} \left(1 + \frac{1}{4^2} + \frac{1}{8^2} + \frac{1}{12^2} + \cdots \right) \\
&< \sqrt[3]{n} \left(1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \cdots \right) \\
&= \frac{\pi^2}{6} \sqrt[3]{n} < \frac{5}{3} \sqrt[3]{n},
\end{aligned}$$

womit sich die behauptete Abschätzung ergibt. □

Anmerkung: Für die Anzahl der Rechenschritte zwischen dem naiven Verfahren, auf Teiler t mit $2 \nmid t$ und $3 \nmid t$ zu testen, dem Verfahren, auf Primteiler zu testen, und dem Lehman–Verfahren liefert die folgende Tabelle einen Vergleich:

Verfahren	allgemein	$n = 10^6$	$n = 10^{12}$
$t \mid n$ mit $2 \nmid t$ und $3 \nmid t$	$\frac{1}{3}\sqrt{n}$	333	333333
$p \mid n$ mit $p \in \mathbb{P}$	$\pi(\sqrt{n})$	168	78448
Lehman–Verfahren	$2\sqrt[3]{n}$	200	20000

9.4 Das Verfahren von Lehmer

Anmerkung: Ist n eine natürliche Zahl, so seien p_i/q_i die Näherungsbrüche von $\sqrt{n}$ und $d_i := p_i^2 - nq_i^2$. Gilt dann für ein i, daß $d_i = m^2$ eine Quadratzahl ist, so folgt

$$nq_i^2 = p_i^2 - m^2 = (p_i - m)(p_i + m)$$

und wegen $n \nmid (p_i \pm m)$ ist $d := \operatorname{ggT}\{p_i \pm m, n\}$ ein nichttrivialer Teiler von n.

Beispiel 9.3. Für $n = 1147$ ergibt der Kettenbruchalgorithmus

$$\begin{aligned}
r_0 &= \sqrt{n} = 33 + \left(\sqrt{n} - 33\right) \\
r_1 &= \frac{1}{\sqrt{n} - 33} = \frac{\sqrt{n} + 33}{58} = 1 + \frac{\sqrt{n} - 25}{58}
\end{aligned}$$

Mit $p_0 = 33$ und $q_0 = 1$ erhält man $d_0 = 33^2 - 1147 < 0$, während sich mit $p_1 = 34$ und $q_1 = 1$ für $d_1 = 32^2 - 1147 = 9 =: m^2$ eine Quadratzahl ergibt. Mit $p_1 + m = 37$ und $p_1 - m = 31$ erhält man auf diese Weise die beiden Teiler von $n = 31 \cdot 37$.

Mit der Abschätzung $\left| p_i/q_i - \sqrt{n} \right| < 1/q_i^2$ aus Satz 8.1 gilt

$$\left| \frac{p_i^2}{q_i^2} - n \right| < \frac{1}{q_i^2} \left(\frac{1}{q_i^2} + 2\sqrt{n} \right),$$

was $d_i < 1 + 2\sqrt{n}$ zur Folge hat. Unter der Annahme, daß die d_i gleichverteilt auftreten, ist die relative Häufigkeit, mit d_i eine Quadratzahl zu treffen, etwa $\sqrt{1 + 2\sqrt{n}} \sim \sqrt{2}\sqrt[4]{n}$. Also ist obiger Algorithmus ein (i.a. nicht sicheres) Primzerlegungsverfahren mit etwa $\sqrt{2}\sqrt[4]{n}$ Schritten.

10 Ganze Zahlen in quadratischen Zahlkörpern

10.1 Klassifikation der quadratischen Zahlkörper

Bezeichnungen: Wie üblich bezeichnet $\mathbb{C} = (\mathbb{C}, +, \cdot)$ den Körper der komplexen Zahlen. ($\mathbb{C}$ ist die algebraisch abgeschlossene Hülle von $\mathbb{R}$.) Jeder Teilkörper K von $\mathbb{C}$ umfaßt den Primkörper $\mathbb{Q}$ und kann somit als $\mathbb{Q}$–Vektorraum der Dimension $\dim_{\mathbb{Q}}(K)$ über $\mathbb{Q}$ aufgefaßt werden.

Definition 10.1. Ein Körper K mit $\mathbb{Q} \leq K \leq \mathbb{C}$ heißt **quadratischer Zahlkörper (über $\mathbb{Q}$)**, wenn $\dim_{\mathbb{Q}}(K) = 2$ gilt.

Satz 10.1. *(a) K ist ein quadratischer Zahlkörper genau dann, wenn eine ganze quadratfreie Zahl d existiert mit*

$$K = \left\{ r + s\sqrt{d} \mid r, s \in \mathbb{Q} \right\} = \mathbb{Q} + \mathbb{Q}\sqrt{d} =: \mathbb{Q}(\sqrt{d}\,).$$

(b) Sind $d \neq \widetilde{d}$ ganze quadratfreie Zahlen, so gilt $\mathbb{Q}(\sqrt{d}\,) \neq \mathbb{Q}(\sqrt{\widetilde{d}}\,)$.

Beweis.

(a) Es sei K ein quadratischer Zahlkörper und $x \in K \backslash \mathbb{Q}$. Da 1 und x eine Basis von K als $\mathbb{Q}$–Vektorraum bilden, folgt $K = \mathbb{Q} + \mathbb{Q}x$. Wegen $x^2 \in K$ existieren also $r, s \in \mathbb{Q}$ mit $x^2 = r + sx$. Hiermit erhält man teilerfremde Zahlen $a \in \mathbb{N}$ und $b, c \in \mathbb{Z}$ mit $ax^2 + bx + c = 0$, woraus sich

$$x = -\frac{b}{2a} \pm \frac{1}{2a}\sqrt{\mathrm{D}(x)} \quad \text{mit } \mathrm{D}(x) = b^2 - 4ac$$

ergibt. Wegen $\mathrm{D}(x) \in \mathbb{Z}$ existiert eine natürliche Zahl m mit $\mathrm{D}(x) = m^2 d$ und quadratfreiem $d \in \mathbb{Z}$. Also gilt $x \in \mathbb{Q} + \mathbb{Q}\sqrt{d}$, woraus sich $K \leq \mathbb{Q} + \mathbb{Q}\sqrt{d} = \mathbb{Q}(\sqrt{d}\,)$ ergibt. Da für alle $r, s \in \mathbb{Q}$ stets $r + s\sqrt{d} \in K$ gilt, folgt schließlich $K = \mathbb{Q}(\sqrt{d}\,)$.

Gilt umgekehrt $K = \mathbb{Q}(\sqrt{d}\,)$, so bildet K wegen

$$(r_1 + s_1\sqrt{d}) + (r_2 + s_2\sqrt{d}) = (r_1 + r_2) + (s_1 + s_2)\sqrt{d},$$

$0 \in K$ und $(-r - s\sqrt{d}) + (r + s\sqrt{d}) = 0$ eine additive abelsche Gruppe. Da K wegen

$$(r_1 + s_1\sqrt{d})(r_2 + s_2\sqrt{d}) = (r_1 r_2 + s_1 s_2 d) + (r_1 s_2 + r_2 s_1)\sqrt{d}$$

bezüglich der Multiplikation abgeschlossen ist und jedes Element $r + s\sqrt{d} \neq 0$ wegen

$$(r + s\sqrt{d})\frac{r - s\sqrt{d}}{r^2 - s^2 d} = 1$$

ein multiplikatives Inverses besitzt, ist K ein Teilkörper von $\mathbb{C}$. Da offensichtlich $\dim_{\mathbb{Q}}(K) = 2$ gilt, ist K somit ein quadratischer Zahlkörper.

(b) Gilt $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{\widetilde{d}})$ für ganze quadratfreie Zahlen d und $\widetilde{d}$, so ergibt sich aus $\sqrt{\widetilde{d}} \in \mathbb{Q} + \mathbb{Q}\sqrt{d}$ die Existenz von rationalen Zahlen r und s mit $\sqrt{\widetilde{d}} = r + s\sqrt{d}$, woraus $\widetilde{d} = r^2 + s^2 d + 2rs\sqrt{d}$ folgt. Wegen $\widetilde{d} \in \mathbb{Z}$ ergibt sich hieraus $2rs = 0$. Da $s = 0$ den Widerspruch $\sqrt{\widetilde{d}} \in \mathbb{Q}$ zur Folge hätte, gilt $r = 0$, woraus $\widetilde{d} = s^2 d$ und wegen der Quadratfreiheit von $\widetilde{d}$ schließlich $\widetilde{d} = d$ folgt. □

Bemerkung 10.1. *Ist $K = \mathbb{Q}(\sqrt{d})$ ein quadratischer Zahlkörper, so ist die Abbildung $'$ von K nach K mit*

$$\left(r + s\sqrt{d}\right)' = r - s\sqrt{d}$$

ein Automorphismus von K als Ring bzw. als Körper.

Beweis. Die Abbildung ist eine Bijektion und für $x, y \in K$ gelten $(x + y)' = x' + y'$ sowie $(xy)' = x'y'$. □

Definition 10.2. Ist K ein quadratischer Zahlkörper, so heißt für $x = r + s\sqrt{d}$

$$\mathcal{S}(x) := x + x' = 2r \in \mathbb{Q}$$

Spur von x und

$$\mathcal{N}(x) := xx' = r^2 - s^2 d \in \mathbb{Q}$$

Norm von x. Die hiermit definierten Abbildungen $\mathcal{S}$ und $\mathcal{N}$ von K nach $\mathbb{Q}$ werden entsprechend als **Spur** bzw. **Norm** bezeichnet.

Bemerkung 10.2. *Für alle $x \in K$ gilt $x^2 - \mathcal{S}(x)x + \mathcal{N}(x) = 0$. Ferner gelten*

$$\mathcal{S}(x + y) = \mathcal{S}(x) + \mathcal{S}(y) \quad \text{und } \mathcal{N}(xy) = \mathcal{N}(x)\mathcal{N}(y).$$

Folglich sind die Abbildungen $\mathcal{S}$ und $\mathcal{N}$ additiv bzw. multiplikativ.

Beweis. Die Behauptungen ergeben sich unmittelbar aus der Definition. □

10.2 Die Hauptordnung quadratischer Zahlkörper

Definition 10.3. Ist $K = \mathbb{Q}(\sqrt{d})$ ein quadratischer Zahlkörper, so heißt $x \in K$ **ganze Zahl**, falls $\mathcal{S}(x) \in \mathbb{Z}$ und $\mathcal{N}(x) \in \mathbb{Z}$ gilt. Die Menge der ganzen Zahlen in $\mathbb{Q}(\sqrt{d})$

$$\mathcal{O}_d := \left\{\, x \in \mathbb{Q}(\sqrt{d}) \;\middle|\; x \text{ ganz} \,\right\}$$

heißt **Hauptordnung von** $\mathbb{Q}(\sqrt{d})$.

Satz 10.2. *Für die Hauptordnung von $\mathbb{Q}(\sqrt{d})$ gilt*

$$\mathcal{O}_d = \mathbb{Z} + \mathbb{Z}z = \left\{\, r + sz \;\middle|\; r, s \in \mathbb{Z} \,\right\} \quad \text{mit } z = \begin{cases} \frac{1}{2}(1 + \sqrt{d}) & \text{falls} \quad d \equiv 1 \pmod 4 \\ \sqrt{d} & \text{falls} \quad d \equiv 2, 3 \pmod 4 \end{cases} .$$

Beweis. Es sei $x = r + s\sqrt{d}$ mit $r, s \in \mathbb{Q}$ eine ganze Zahl. Wegen $\mathcal{S}(x) = 2r \in \mathbb{Z}$ gibt es eine Zahl $n \in \mathbb{Z}$ mit $r = {}^{n}/_{2}$. Also gilt $x = {}^{n}/_{2} + s\sqrt{d}$ und wegen $\mathcal{N}(x) = {}^{n^2}/_{4} - s^2 d \in \mathbb{Z}$ gibt es eine Zahl $m \in \mathbb{Z}$ mit $s = {}^{m}/_{2}$. Hieraus folgt über $\mathcal{N}(x) = {}^{(n^2 - m^2 d)}/_{4} \in \mathbb{Z}$ die Beziehung $n^2 \equiv m^2 d \pmod 4$.

Im Falle $d \equiv 2, 3 \pmod 4$ ergeben sich nun wegen $m^2, n^2 \equiv 0, 1 \pmod 4$ die Kongruenzen $m^2, n^2 \equiv 0 \pmod 4$. Dies hat $m, n \equiv 0 \pmod 2$ zur Folge, und hiermit gilt $r, s \in \mathbb{Z}$ bzw. $x \in \mathbb{Z} + \mathbb{Z}\sqrt{d}$. Zusammen mit $\mathbb{Z} + \mathbb{Z}\sqrt{d} \subseteq \mathcal{O}_d$ erhält man $\mathcal{O}_d = \mathbb{Z} + \mathbb{Z}z$ mit $z = \sqrt{d}$.

Im Falle $d \equiv 1 \pmod 4$ ergibt sich die Kongruenz $m^2 \equiv n^2 \pmod 4$, was $m \equiv n \pmod 2$ zur Folge hat. Für $m \equiv n \equiv 0 \pmod 2$ folgt wie im ersten Fall $x \in \mathbb{Z} + \mathbb{Z}\sqrt{d}$. Für $m \equiv n \equiv 1 \pmod 2$ erhält man aber

$$x = \frac{n}{2} + \frac{m}{2}\sqrt{d} = (a + \frac{1}{2}) + (b + \frac{1}{2})\sqrt{d} \quad \text{mit } a, b \in \mathbb{Z},$$

woraus sich $x \in \mathbb{Z} + z\mathbb{Z}$ mit $z = \frac{1}{2}(1 + \sqrt{d})$ ergibt. Gilt umgekehrt $x = (a + {}^{1}/_{2}) + (b + {}^{1}/_{2})\sqrt{d}$ mit $a, b \in \mathbb{Z}$, so folgt $\mathcal{S}(x) = 2a + 1 \in \mathbb{Z}$ und aus

$$\mathcal{N}(x) = \left(a + \frac{1}{2}\right)^2 - \left(b + \frac{1}{2}\right)^2 d = \left(\frac{2a+1}{2}\right)^2 - \left(\frac{2b+1}{2}\right)^2 d \equiv \frac{1-d}{4} \pmod 4$$

folgt wegen $d \equiv 1 \pmod 4$ die Beziehung $\mathcal{N}(x) \in \mathbb{Z}$. Somit gilt $x \in \mathcal{O}_d$. □

10.3 Einheiten in imaginärquadratischen Zahlkörpern

Bemerkung 10.3. *Die Hauptordnung $\mathcal{O}_d$ ist ein Ring und eine ganze Zahl x liegt genau dann in $\mathcal{O}_d^\times$, wenn $\mathcal{N}(x) \in \mathbb{Z}^\times$ gilt.*

Beweis. Wegen $0, 1 \in \mathcal{O}_d \subseteq \mathbb{C}$ genügt es, von den Ringeigenschaften die Abgeschlossenheit bzgl. Addition und Multiplikation zu zeigen. Nach Satz 10.2 ist ersteres trivial, während es für letzteres genügt, $z^2 \in \mathcal{O}_d$ nachzuweisen. Im Falle $d \equiv 2, 3 \pmod 4$ ist dies wegen $z^2 = d$ offensichtlich und für $d \equiv 1 \pmod 4$ gilt

$$z^2 = \frac{1}{4}(1 + \sqrt{d})^2 = \frac{d+1}{4} + \frac{\sqrt{d}}{2} = \frac{d-1}{4} + \frac{1+\sqrt{d}}{2} = \frac{d-1}{4} + z \in \mathcal{O}_d.$$

Nun sei $x \in \mathcal{O}_d^\times$. Dann gilt auch $x^{-1} \in \mathcal{O}_d^\times$ und wegen $\mathcal{N}(x), \mathcal{N}(x^{-1}) \in \mathbb{Z}$ folgt aus $\mathcal{N}(x)\mathcal{N}(x^{-1}) = \mathcal{N}(xx^{-1}) = \mathcal{N}(1) = 1$ die Beziehung $\mathcal{N}(x) \in \{1, -1\} = \mathbb{Z}^\times$. Ist umgekehrt x eine ganze Zahl mit $\mathcal{N}(x) \in \mathbb{Z}^\times$, so gilt $x^{-1} = {}^{x'}/_{\mathcal{N}(x)} \in \mathcal{O}_d$, was $x \in \mathcal{O}_d^\times$ zur Folge hat. □

Definition 10.4. Ein quadratischer Zahlkörper $\mathbb{Q}(\sqrt{d})$ heißt **imaginärquadratisch**, falls $d < 0$ gilt, im Falle $d > 0$ heißt er **reellquadratisch**.

Satz 10.3. *Für die Einheiten imaginärquadratischer Zahlkörper gelten die folgenden Aussagen:*

(a) $\mathcal{O}_{-1}^\times = \{\pm 1, \pm i\}$ mit $i = \sqrt{-1}$,

(b) $\mathcal{O}_{-3}^\times = \{\, z^k \mid k = 0, \ldots, 5 \,\}$ mit $z = \frac{1+\sqrt{-3}}{2}$,

(c) Für $d \neq -1, -3$ gilt $\mathcal{O}_d^\times = \{\pm 1\}$.

Beweis.

(a) Wegen $d = -1 \equiv 3 \pmod 4$ gilt nach Satz 10.2 $\mathcal{O}_{-1} = \mathbb{Z} + \mathbb{Z}i$. Nach Bemerkung 10.3 ist $x = a + bi \in \mathcal{O}_{-1}^\times$ mit $a, b \in \mathbb{Z}$ gleichbedeutend mit $\mathcal{N}(a + bi) = a^2 + b^2 = \pm 1$. Diese Gleichung besitzt aber genau die behaupteten Lösungen $a = 0$ und $b = \pm 1$ sowie $a = \pm 1$ und $b = 0$.

(b) Wegen $d = -3 \equiv 1 \pmod 4$ gilt nach Satz 10.2 $\mathcal{O}_{-3} = \mathbb{Z} + \mathbb{Z}z$ mit $z = \frac{1}{2}(1 + \sqrt{-3})$. Nach Bemerkung 10.3 ist $x = a + bz \in \mathcal{O}_{-3}^\times$ mit $a, b \in \mathbb{Z}$ gleichbedeutend mit

$$\mathcal{N}(a + bz) = \mathcal{N}(a + \frac{b}{2} + \frac{b}{2}\sqrt{-3}) = \mathcal{N}(\frac{\widetilde{a}}{2} + \frac{\widetilde{b}}{2}\sqrt{-3}) = \mathcal{N}(\frac{1}{2})\mathcal{N}(\widetilde{a} + \widetilde{b}\sqrt{-3}) = \pm 1,$$

wobei $\widetilde{a} := 2a + b \in \mathbb{Z}$ und $\widetilde{b} := b \in \mathbb{Z}$ gesetzt wurde. Aufgrund von $\mathcal{N}({}^1/_2) = {}^1/_4$ ist dies gleichbedeutend mit $\mathcal{N}(\widetilde{a} + \widetilde{b}\sqrt{-3}) = \widetilde{a}^2 + 3\widetilde{b}^2 = \pm 4$. Diese Gleichung besitzt aber genau die Lösungen $\widetilde{a} = \pm 1$ und $\widetilde{b} = \pm 1$ sowie $\widetilde{a} = \pm 2$ und $\widetilde{b} = 0$, woraus sich die behaupteten Lösungen ergeben: Aus $\widetilde{a} = 1$ und $\widetilde{b} = \pm 1$ ergibt sich $a = 0$ und $b = 1$ bzw. $a = 1$ und $b = -1$, was $x = \frac{1}{2}(1 \pm \sqrt{-3}) = z^{\pm 1}$ zur Folge hat. Aus $\widetilde{a} = -1$ und $\widetilde{b} = \pm 1$ ergibt sich $a = -1$ und $b = 1$ bzw. $a = 0$ und $b = -1$, woraus $x = \frac{1}{2}(-1 \pm \sqrt{-3}) = z^{\pm 2}$ folgt. Aus $\widetilde{a} = \pm 2$ und $\widetilde{b} = 0$ folgt schließlich $a = \pm 1$ und $b = 0$, womit sich $x = \pm 1 \in \{z^0, z^3\}$ ergibt.

(c) Nun sei $d \leq -2$. Im Falle $d \equiv 2, 3 \pmod 4$ gilt nach Satz 10.2 $\mathcal{O}_d = \mathbb{Z} + \mathbb{Z}\sqrt{d}$. Nach Bemerkung 10.3 ist $x = a + b\sqrt{d} \in \mathcal{O}_d^\times$ mit $a, b \in \mathbb{Z}$ gleichbedeutend mit $\mathcal{N}(a + b\sqrt{d}) = a^2 - db^2 = \pm 1$. Diese Gleichung besitzt aber genau die behaupteten Lösungen $a = \pm 1$ und $b = 0$.

Im Falle $d \equiv 1 \pmod 4$ gilt nach Satz 10.2 $\mathcal{O}_d = \mathbb{Z} + \mathbb{Z}z$ mit $z = \frac{1}{2}(1 + \sqrt{d})$. Nach Bemerkung 10.3 ist $x = a + bz \in \mathcal{O}_d^\times$ mit $a, b \in \mathbb{Z}$ gleichbedeutend mit

$$\mathcal{N}(a + bz) = \mathcal{N}(a + \frac{b}{2} + \frac{b}{2}\sqrt{d}) = \mathcal{N}(\frac{\widetilde{a}}{2} + \frac{\widetilde{b}}{2}\sqrt{d}) = \mathcal{N}(\frac{1}{2})\mathcal{N}(\widetilde{a} + \widetilde{b}\sqrt{d}) = \pm 1,$$

wobei $\widetilde{a} := 2a + b \in \mathbb{Z}$ und $\widetilde{b} := b \in \mathbb{Z}$ gesetzt wurde. Dies ist wiederum gleichbedeutend mit $\mathcal{N}(\widetilde{a} + \widetilde{b}\sqrt{d}) = \widetilde{a}^2 - d\widetilde{b}^2 = \pm 4$. Diese Gleichung besitzt aber für $d \leq -7$genau die Lösungen $\widetilde{a} = \pm 2$ und $\widetilde{b} = 0$, woraus sich wie oben die behaupteten Lösungen ergeben. □

10.4 Einheiten in reellquadratischen Zahlkörpern

Bemerkung 10.4. *Ist $\mathbb{Q}(\sqrt{d})$ ein reellquadratischer Zahlkörper und wird*

$$z := \begin{cases} \frac{1}{2}(1 + \sqrt{d}) & \text{falls} \quad d \equiv 1 \pmod 4 \\ \sqrt{d} & \text{falls} \quad d \equiv 2, 3 \pmod 4 \end{cases}$$

gesetzt, so ist die durch die Kettenbruchentwicklung von z bestimmte Zahl

$$z_1 = \frac{1}{z - [z]}$$

reduziert.

Beweis. Aus $0 < z - [z] < 1$ folgt $z_1 > 1$. Mit $z' = \mathcal{S}(z) - z$ gilt weiter

$$-\frac{1}{z_1'} = [z] - z' = [z] + z - \mathcal{S}(z).$$

Mit $z > 1$, $[z] \geq 1$ und $\mathcal{S}(z) \in \{0,1\}$ ergibt sich hiermit $-{}^1\!/_{z_1'} > 1$. Also ist z_1 reduziert. □

Bemerkung 10.5. *Ist $t \in \mathbb{Q}(\sqrt{d}\,)$ mit $d > 0$ eine reduzierte Zahl mit $\mathrm{D}(t) = \mathrm{D}(z)$, ($z$ sei wie oben definiert), und ist $t = [\overline{a_0; a_1, \ldots, a_n}]$ die nach Satz 8.3 rein periodische Kettenbruchentwicklung von t mit Näherungsbrüchen ${}^{p_k}\!/_{q_k}$, so gilt*

$$e := q_n t + q_{n-1} \in \mathcal{O}_d^\times \quad \text{mit } e > 1.$$

Beweis. Aus $t = t_{n+1}$ und (8.1) folgt

$$\binom{t}{1} \sim P_n \binom{t_{n+1}}{1} = P_n \binom{t}{1}.$$

Daher existiert eine reelle Zahl e mit

$$e\binom{t}{1} = P_n \binom{t}{1} = \binom{p_n t + p_{n-1}}{q_n t + q_{n-1}}.$$

Hieraus ergibt sich $e = q_n t + q_{n-1} \in \mathbb{Q}(\sqrt{d}\,)$ und wegen $t > 1$ gilt $e > 1$. Aus $(P_n - eI)\binom{t}{1} = 0$ folgt $\det(P_n - eI) = 0$, womit sich über

$$0 = \det\begin{pmatrix} p_n - e & p_{n-1} \\ q_n & q_{n-1} - e \end{pmatrix} = e^2 - (p_n + q_{n-1})e + \det P_n$$

die Beziehung $e \in \mathcal{O}_d$ ergibt. Aufgrund von $\mathcal{N}(e) = \det P_n = (-1)^{n+1}$ gilt schließlich sogar $e \in \mathcal{O}_d^\times$. □

Folgerung 10.1. *In reellquadratischen Zahlkörpern gilt $\left|\mathcal{O}_d^\times\right| = \infty$.*

Beweis. Für jedes $n \in \mathbb{Z}$ gilt $e^n \in \mathcal{O}_d^\times$, und aufgrund von $e > 1$ gibt es unendlich viele verschiedene solcher Potenzen. □

Satz 10.4. *Ist $K = \mathbb{Q}(\sqrt{d}\,)$ ein reellquadratischer Zahlkörper und sind $z_1 = {}^1\!/_{(z - [z])}$ wie in Bemerkung 10.4 und $e = q_n z_1 + q_{n-1}$ wie in Bemerkung 10.5 gewählt, so gilt*

$$\mathcal{O}_d^\times = \langle -1 \rangle \times \langle e \rangle = \left\{\, (-1)^i e^j \;\middle|\; i \in \{0,1\},\ j \in \mathbb{Z} \,\right\}.$$

Definition 10.5. Die Zahl e heißt **Grundeinheit** von K.

Beweis. Für die Diskriminante von z gilt

$$D := \mathrm{D}(z) = \begin{cases} d & \text{falls } d \equiv 1 \pmod 4 \\ 4d & \text{falls } d \equiv 2,3 \pmod 4 \end{cases}, \tag{10.1}$$

da sich für $z = \sqrt{d}$ die quadratische Gleichung $z^2 - d = 0$ und für $z = \frac{1}{2}(1 + \sqrt{d})$ die Gleichung $z^2 - z + {}^{(1-d)}/_4 = 0$ zur Bestimmung der Diskriminante ergeben.

Es sei f ein beliebiges Element von $\mathcal{O}_d^\times$ ungleich 1. Da entweder $f > 1, {}^1/_f > 1$, $-f > 1$ oder $-{}^1/_f > 1$ gilt, kann für den Beweis des Satzes ohne Einschränkung $f > 1$ angenommen werden.

Für f kann stets eine Darstellung

$$f = \frac{u + v\sqrt{D}}{2} \quad \text{mit } u, v \in \mathbb{Z},\ u \equiv vD \pmod 2 \tag{10.2}$$

gefunden werden, denn im Falle $d \equiv 2, 3 \pmod 4$ gilt nach Satz 10.2 und (10.1)

$$f = \widetilde{u} + \widetilde{v}\sqrt{d} = \frac{2\widetilde{u} + \widetilde{v}\sqrt{4d}}{2} = \frac{u + v\sqrt{D}}{2},$$

wobei $u := 2\widetilde{u}$ und $v := \widetilde{v}$ mit $u \equiv vD \pmod 2$ gesetzt wurde. Im Falle $d \equiv 1 \pmod 4$ gilt nach Satz 10.2 hingegen

$$f = \frac{u + v\sqrt{d}}{2} \quad \text{mit } u \equiv v \pmod 2,$$

woraus sich mit (10.1) $D \equiv 1 \pmod 2$ und damit die behauptete Darstellung mit $u \equiv vD \pmod 2$ ergibt.

Aus den resultierenden Darstellungen

$$-f = \frac{-u - v\sqrt{D}}{2}, \ \pm\frac{1}{f} = \pm\frac{f'}{\mathcal{N}(f)} = \pm\frac{u - v\sqrt{D}}{2}$$

folgt aufgrund der Wahl von f als größte der vier Zahlen $f, -f, {}^1/_f, -{}^1/_f$ die Beziehung $u, v > 1$.

Ist $t \in \mathcal{O}_d$ reduziert mit $\mathrm{D}(t) = \mathrm{D}(z) = D$ wie in Bemerkung 10.5, so existieren eine natürliche Zahl a und ganze Zahlen b und c mit

$$at^2 + bt + c = 0 \tag{10.3}$$

bzw.

$$at = -\frac{b}{2} + \frac{1}{2}\sqrt{D} \quad \text{mit } D = b^2 - 4ac. \tag{10.4}$$

Aus $D \equiv b \pmod 2$ und (10.2) folgt somit $u \equiv vb \pmod 2$, womit $2 \mid (u - vb)$ gilt. Folglich besitzt die Matrix

$$P := \begin{pmatrix} {}^{(u-vb)}/_2 & -cv \\ av & {}^{(u+vb)}/_2 \end{pmatrix} =: \begin{pmatrix} p & \widetilde{p} \\ q & \widetilde{q} \end{pmatrix}$$

ganzzahlige Einträge. Die folgende Gleichung

$$P\begin{pmatrix} t \\ 1 \end{pmatrix} = f\begin{pmatrix} t \\ 1 \end{pmatrix} \tag{10.5}$$

wird durch elementares Nachrechnen verifiziert: Die erste Zeile $pt + \widetilde{p} = ft$ ist äquivalent zur Gleichung

$$\frac{u - vb}{2}t - cv = \frac{u + v\sqrt{D}}{2}t.$$

Dies wiederum gilt für

$$-\frac{b}{2}t - c = \frac{\sqrt{D}}{2}t = \left(at + \frac{b}{2}\right)t,$$

was wegen (10.3) erfüllt ist. Die zweite Zeile $qt + \widetilde{q} = f$ ist gleichbedeutend mit

$$avt + \frac{u+vb}{2} = \frac{u+v\sqrt{D}}{2},$$

was aufgrund von (10.4) richtig ist.

Unter der Annahme, daß

$$P = \prod_{i=0}^{m} \begin{pmatrix} a_i & 1 \\ 1 & 0 \end{pmatrix}$$

den Anfang einer Kettenbruchentwicklung von

$$\widetilde{t} = [a_0; a_1, \ldots, a_m, t]$$

darstellt, läßt sich wie folgt die Aussage des Satzes schließen: Nach (8.1) und (10.5) gilt

$$\begin{pmatrix} \widetilde{t} \\ 1 \end{pmatrix} \sim P\begin{pmatrix} t \\ 1 \end{pmatrix} = f\begin{pmatrix} t \\ 1 \end{pmatrix} \sim \begin{pmatrix} t \\ 1 \end{pmatrix},$$

woraus $t = \widetilde{t}$ und $t = [\overline{a_0; a_1, \ldots, a_m}]$ folgen. Es sei also $t = [\overline{a_0; a_1, \ldots, a_n}]$ mit minimalem n. Dann gibt es ein $k \in \mathbb{N}$ mit $m = kn$. Hierdurch folgt wegen

$$f\begin{pmatrix} t \\ 1 \end{pmatrix} = P\begin{pmatrix} t \\ 1 \end{pmatrix} = e^k\begin{pmatrix} t \\ 1 \end{pmatrix}$$

die Beziehung $f = e^k$.

Zu zeigen bleibt also noch die Richtigkeit der obigen Annahme. Mit $t = \frac{1}{2a}(-b + \sqrt{D})$ gilt $-t' = \frac{1}{2a}(b + \sqrt{D})$. Da t reduziert ist, gelten $t > 1$ und $0 < -t' < 1$. Aus $-t' > 0$ ergibt sich wegen $a > 0$ die Beziehung $b + \sqrt{D} > 0$ und schließlich

$$b > -\sqrt{D}. \tag{10.6}$$

Aus $-t' < 1$ folgt über $b + \sqrt{D} < 2a$ die Beziehung

$$2a - b > \sqrt{D}, \tag{10.7}$$

während $t > 1$ zunächst $\sqrt{D} - b > 2a$ und damit

$$-b - 2a > -\sqrt{D} \tag{10.8}$$

zur Folge hat. Aus (10.6), (10.7) und (10.8) folgen

$$\begin{aligned} \widetilde{q} &= \frac{u+vb}{2} > \frac{u - v\sqrt{D}}{2} = f' = \frac{\mathcal{N}(f)}{f} \\ &> \begin{cases} 0 & \text{für } \mathcal{N}(f) = 1 \\ -1 & \text{für } \mathcal{N}(f) = -1 \end{cases} \end{aligned}$$

$$
\begin{aligned}
q-\widetilde{q} &= av-\frac{u+vb}{2}=\frac{v(2a-b)-u}{2}>\frac{v\sqrt{D}-u}{2}=-f'=-\frac{\mathcal{N}(f)}{f}\\
&> \begin{cases} -1 & \text{für} \quad \mathcal{N}(f)=1\\ 0 & \text{für} \quad \mathcal{N}(f)=-1\end{cases}\\
p-q &= \frac{u-vb}{2}-av=\frac{u-vb-2av}{2}>\frac{u-v\sqrt{D}}{2}=f'=\frac{\mathcal{N}(f)}{f}\\
&> \begin{cases} 0 & \text{für} \quad \mathcal{N}(f)=1\\ -1 & \text{für} \quad \mathcal{N}(f)=-1\end{cases}
\end{aligned}
$$

Für $\mathcal{N}(f)=1$ ergeben sich somit die Abschätzungen $0<\widetilde{q}\le q$ und $p/q>1$, während für $\mathcal{N}(f)=-1$ die Abschätzungen $0\le\widetilde{q}<q$ und $p/q\ge 1$ gelten. Als rationale Zahl besitzt p/q eine abbrechende Kettenbruchentwicklung

$$
\begin{aligned}
\frac{p}{q} &= [a_0;a_1,\dots,a_{\widetilde{m}}]\\
&=: \begin{cases} [a_0;a_1,\dots,a_m] & \text{falls} \quad \mathcal{N}(f)=(-1)^{\widetilde{m}+1}\\ [a_0;a_1,\dots,a_{\widetilde{m}}-1,1] & \text{falls} \quad \mathcal{N}(f)=(-1)^{\widetilde{m}}\end{cases}.
\end{aligned}
$$

Ist $P_m=\left(\begin{smallmatrix} p_m & p_{m-1}\\ q_m & q_{m-1}\end{smallmatrix}\right)$ die zugehörige Matrix, so gilt $p/q=p_m/q_m$. Wegen $\det P_m=\pm 1$ gilt $\operatorname{ggT}\{p_m,q_m\}=1$, woraus zusammen mit $\operatorname{ggT}\{p,q\}=1$ und $q,q_m>0$ die Beziehungen $p=p_m$ und $q=q_m$ folgen. Weiter gilt

$$pq_{m-1}-p_{m-1}q=(-1)^{m+1}=\mathcal{N}(f)=\det P=p\widetilde{q}-\widetilde{p}q,$$

woraus sich die Beziehung

$$p(q_{m-1}-\widetilde{q})=(\widetilde{p}-p_{m-1})q \tag{10.9}$$

ergibt. Zum Beweis des Satzes bleiben noch $\widetilde{q}=q_{m-1}$ und $\widetilde{p}=p_{m-1}$ zu zeigen. Im Falle $0<\widetilde{q}<q$ folgt wegen $0\le q_{m-1}\le q_m=q$ die Beziehung

$$|\widetilde{q}-q_{m-1}|\le q-1<q$$

und mit $\operatorname{ggT}\{p,q\}=1$ und (10.9) ergibt sich $q\,|\,(q_{m-1}-\widetilde{q})$, was schließlich $q_{m-1}-\widetilde{q}=0$ und damit $\widetilde{p}=p_{m-1}$ zur Folge hat.

Im Falle $0<\widetilde{q}=q$ folgt wegen $p\widetilde{q}-\widetilde{p}q=(-1)^{m+1}$ die Beziehung $q=\widetilde{q}=1$, woraus sich

$$\frac{p}{q}=p=[p]=[p-1;1]$$

ergibt. Also gilt $m=1$ und es folgen $q_{m-1}=q_0=1=\widetilde{q}$ und $p_{m-1}=p_0=\widetilde{p}$.

Im letzten Falle $0=\widetilde{q}<q$ ergeben sich wegen $p\widetilde{q}-\widetilde{p}q=(-1)^{m+1}$ die Beziehungen $q=1$ und $\mathcal{N}(f)=-1$. Somit gelten $p/q=p=[p]$ und $m=0$, woraus $P=\left(\begin{smallmatrix} p & 1\\ 1 & 0\end{smallmatrix}\right)$ folgt. □

Beispiel 10.1. Es soll die Grundeinheit e von $\mathbb{Q}(\sqrt{19})$ berechnet werden. Mit $z=\sqrt{19}=4+(\sqrt{19}-4)$ gilt $t=z_1=1/(\sqrt{19}-4)$, und es ergibt sich die folgende Rechnung:

$$\frac{1}{\sqrt{19}-4}=\frac{\sqrt{19}+4}{3}=2+\frac{\sqrt{19}-2}{3},\qquad \frac{3}{\sqrt{19}-2}=\frac{3(\sqrt{19}+2)}{15}=1+\frac{\sqrt{19}-3}{5},$$

$$\frac{5}{\sqrt{19}-3} = \frac{5(\sqrt{19}+3)}{10} = 3 + \frac{\sqrt{19}-3}{2}, \qquad \frac{2}{\sqrt{19}-3} = \frac{2(\sqrt{19}+3)}{10} = 1 + \frac{\sqrt{19}-2}{5},$$
$$\frac{5}{\sqrt{19}-2} = \frac{5(\sqrt{19}+2)}{15} = 2 + \frac{\sqrt{19}-4}{3}, \qquad \frac{3}{\sqrt{19}-4} = \frac{3(\sqrt{19}+4)}{3} = 8 + (\sqrt{19}-4).$$

Hieraus ergibt sich die Kettenbruchdarstellung $t = [\overline{2; 1, 3, 1, 2, 8}]$. Die Berechnung des 5–ten Näherungsbruchs geht aus folgender Tabelle hervor (siehe Anmerkung nach Folgerung 8.1):

n	-2	-1	0	1	2	3	4	5
a_n	$\times$	$\times$	2	1	3	1	2	8
p_n	0	1	2	3	11	14	39	326
q_n	1	0	1	1	4	5	14	117

Somit ergibt sich

$$e = q_5 t + q_4 = 117 \frac{1}{\sqrt{19}-4} + 14 = 117 \frac{\sqrt{19}+4}{3} + 14 = 170 + 39\sqrt{19}$$

als Grundeinheit von $\mathbb{Q}(\sqrt{19})$.

11 Ideale in quadratischen Zahlkörpern

11.1 Primzerlegung in Ringen

Die folgende Definition dient zur Wiederholung und Ergänzung der Bezeichnungen der Paragraphen 1 und 2:

Definition 11.1. Ist R ein kommutativer Ring, so werden folgende Bezeichnungen eingeführt:

(a) $R^\times := \{ r \in R \mid \text{ es gibt ein } s \in R \text{ mit } rs = 1 \}$ heißt **Einheitengruppe** von R.

(b) Gilt $r, s \in R$, so heißt r **Teiler** von s, wenn es ein $t \in R$ mit $s = rt$ gibt. Die Bezeichnung hierfür lautet $r \mid s$.

(c) Gilt $r, s \in R$, so heißen r und s **assoziiert**, falls $r \mid s$ und $s \mid r$ gilt. Die Bezeichnung hierfür lautet $r \simeq s$.

(d) Ein Element $u \in R$ heißt **unzerlegbar**, wenn für alle $r \in R$ mit $r \mid u$ stets $r \simeq 1$ oder $r \simeq u$ gilt.

(e) Ein Element $p \in R \backslash R^\times$ heißt **prim** (**Primelement**), wenn für alle $r, s \in R$ aus $p \mid rs$ stets $p \mid r$ oder $p \mid s$ folgt.

(f) Ist P ein Vertretersystem von ${\{p \in R \mid p \text{ prim}\}}/{R^\times}$, so heißt R **Ring mit eindeutiger Primzerlegung** (**ZPE–Ring**), wenn jedes Element $r \in R$ bis auf die Reihenfolge der Faktoren eindeutig als

$$r = e \cdot p_1 \cdot \ldots \cdot p_n \quad \text{mit } e \in R^\times,\ p_i \in P$$

darstellbar ist.

Beispiel 11.1. (a) Für $R = \mathbb{Z}$ gilt $R^\times = \{\pm 1\}$ und $P = \mathbb{P}$. Nach Satz 1.4 ist $\mathbb{Z}$ daher ein ZPE–Ring.

(b) Für $R = \mathbb{Z} + \mathbb{Z}i$ gilt $R^\times = \{\pm 1, \pm i\}$ und

$$\begin{aligned} P = &\big\{ i+1 \big\} \cup \big\{ p \in \mathbb{P} \mid p \equiv 3 \pmod 4 \big\} \\ &\cup \big\{ a+bi, a-bi \mid a,b \in \mathbb{N},\ a^2+b^2 = p,\ a > b,\ p \in \mathbb{P},\ p \equiv 1 \pmod 4 \big\}. \end{aligned}$$

Daher ist $\mathbb{Z} + \mathbb{Z}i$ ein ZPE–Ring. (Der Beweis hierfür sei als Übung empfohlen.)

(c) Für $R = \mathbb{Z} + \mathbb{Z}\sqrt{-5} = \mathcal{O}_{-5}$ gilt nach Satz 10.3 $R^\times = \{\pm 1\}$. Weiterhin sind die Elemente $2,\ 3,\ (1-\sqrt{-5}),\ (1-\sqrt{-5})$ unzerlegbar aber nicht prim.

Beweis. Es sei $2 = rs$ mit $r, s \in \mathcal{O}_{-5}$. Für alle Elemente $t = a + b\sqrt{-5}$ mit $a, b \in \mathbb{Z}$ gilt

$$\mathcal{N}(t) = a^2 + 5b^2 \neq \pm 2 \quad \text{und } \mathcal{N}(t) \in \mathbb{Z}.$$

Daher kann aufgrund von $4 = \mathcal{N}(2) = \mathcal{N}(rs) = \mathcal{N}(r)\mathcal{N}(s)$ ohne Einschränkung $\mathcal{N}(r) = 1$ angenommen werden. Folglich gilt $r \in \mathcal{O}_{-5}^\times$, woraus $r \simeq 1$ folgt. Also ist 2 ein unzerlegbares Element. Aber da 2 zwar $6 = (1+\sqrt{-5})(1-\sqrt{-5})$, aber keinen der beiden Faktoren teilt, ist 2 nicht prim. Die restlichen Behauptungen werden analog bewiesen. □

Bemerkung 11.1. *Ist R ein kommutativer Ring und sind $\mathfrak{a}$, $\mathfrak{b}$ und $\mathfrak{c}$ Ideale in R, so gelten folgende Aussagen.*

(a) $\mathfrak{a} + \mathfrak{b} := \{ a + b \mid a \in \mathfrak{a},\ b \in \mathfrak{b} \} \trianglelefteq R$

(b) $\mathfrak{a}\mathfrak{b} := \mathfrak{a} \cdot \mathfrak{b} := \{ \sum_{i=1}^n a_i b_i \mid n \in \mathbb{N},\ a_i \in \mathfrak{a},\ b_i \in \mathfrak{b} \} \trianglelefteq R$

(c) $\mathfrak{a}\mathfrak{b} = \mathfrak{b}\mathfrak{a}$

(d) $\mathfrak{a}(\mathfrak{b}\mathfrak{c}) = (\mathfrak{a}\mathfrak{b})\mathfrak{c}$

(e) $\mathfrak{a}(\mathfrak{b} + \mathfrak{c}) = \mathfrak{a}\mathfrak{b} + \mathfrak{a}\mathfrak{c}$

Beweis. (Übung) □

Definition 11.2. Ist R ein kommutativer Ring, so werden folgende Bezeichnungen eingeführt:

(a) Gilt $\mathfrak{a}, \mathfrak{b} \trianglelefteq R$, so heißt $\mathfrak{a}$ **Teiler von** $\mathfrak{b}$, wenn es ein $\mathfrak{c} \trianglelefteq R$ mit $\mathfrak{a}\mathfrak{c} = \mathfrak{b}$ gibt. Die Bezeichnung hierfür lautet $\mathfrak{a} \mid \mathfrak{b}$.

(b) Ein Ideal $\mathfrak{u} \trianglelefteq R$ heißt **unzerlegbar**, wenn für alle $\mathfrak{a} \trianglelefteq R$ mit $\mathfrak{a} \mid \mathfrak{u}$ stets $\mathfrak{a} = R$ oder $\mathfrak{a} = \mathfrak{u}$ gilt.

(c) Ein Ideal $\mathfrak{p} \trianglelefteq R$ heißt **prim** (**Primideal**), wenn für alle $\mathfrak{a}, \mathfrak{b} \trianglelefteq R$ aus $\mathfrak{p} \mid \mathfrak{a}\mathfrak{b}$ stets $\mathfrak{p} \mid \mathfrak{a}$ oder $\mathfrak{p} \mid \mathfrak{b}$ folgt.

(d) Ein Ideal $\mathfrak{m} \underset{\neq}{\triangleleft} R$ heißt **maximal**, wenn für alle $\mathfrak{a} \trianglelefteq R$ mit $\mathfrak{a} \supseteq \mathfrak{m}$ stets $\mathfrak{a} = \mathfrak{m}$ oder $\mathfrak{a} = R$ gilt.

Satz 11.1. *Ist R ein kommutativer Ring und $\mathfrak{a} \trianglelefteq R$ ein Ideal, so gelten folgende Aussagen:*

(a) *Das Ideal $\mathfrak{a}$ ist ein ein Primideal genau dann, wenn ${}^{R}/_{\mathfrak{a}}$ nullteilerfrei ist.*

(b) *Das Ideal $\mathfrak{a}$ ist ein maximales Ideal genau dann, wenn ${}^{R}/_{\mathfrak{a}}$ ein Körper ist.*

Beweis.

(a) Ist $\mathfrak{a}$ ein Primideal, so folgt aus $ab \in \mathfrak{a}$ stets $a \in \mathfrak{a}$ oder $b \in \mathfrak{a}$. Im Restklassenring ${}^{R}/_{\mathfrak{a}}$ folgt somit aus $\overline{a}\overline{b} = \overline{0}$ stets $\overline{a} = \overline{0}$ oder $\overline{b} = \overline{0}$ und daher ist ${}^{R}/_{\mathfrak{a}}$ nullteilerfrei. Da alle Implikationen auch in der anderen Richtung gelten, gilt auch die Umkehrung.

(b) Ist $\mathfrak{a}$ ein maximales Ideal, so folgt aus $x \notin \mathfrak{a}$ stets $\mathfrak{a} + Rx = R$ und daher existieren Elemente $a \in \mathfrak{a}$ uns $y \in R$ mit $a+yx = 1$. Für die Restklassen in ${}^{R}/_{\mathfrak{a}}$ hat dies $\overline{xy} = \overline{1}$ zur Folge, weshalb $\overline{x} \in ({}^{R}/_{\mathfrak{a}})^{\times}$ gilt. Daher gilt ${}^{R}/_{\mathfrak{a}} \backslash \{\overline{0}\} = ({}^{R}/_{\mathfrak{a}})^{\times}$ und ${}^{R}/_{\mathfrak{a}}$ ist ein Körper. Ist umgekehrt ${}^{R}/_{\mathfrak{a}}$ ein Körper und gilt $x \notin \mathfrak{a}$, so gilt $\overline{x} \in ({}^{R}/_{\mathfrak{a}})^{\times}$, weshalb es ein $y \in R$ mit $\overline{xy} = \overline{1}$ gibt. Folglich gilt $xy - 1 \in \mathfrak{a}$ und es existiert ein $a \in \mathfrak{a}$ mit $xy - a = 1$, woraus $1 \in \mathfrak{a} + Rx$ und schließlich $R = \mathfrak{a} + Rx$ folgen. Also ist $\mathfrak{a}$ ein maximales Ideal.

□

11.2 Erzeugung der Ideale in $\mathcal{O}_d$

Bemerkung 11.2. *Gilt $\mathfrak{o} := \{0\} \neq \mathfrak{a} \trianglelefteq \mathcal{O}_d$ und wird $a := \min(\mathfrak{a} \cap \mathbb{N})$ gesetzt, so gibt es eine Zahl $v \in \mathcal{O}_d \backslash \mathbb{Z}$ mit $\mathfrak{a} = \mathbb{Z}a + \mathbb{Z}v$.*

Beweis. Aufgrund von $\mathfrak{o} \neq \mathfrak{a} \trianglelefteq \mathcal{O}_d$ existiert ein $x \in \mathfrak{a}$ mit $x \neq 0$ und wegen

$$0 \neq xx' = \mathcal{N}(x) \in \mathfrak{a} \cap \mathbb{Z}$$

gilt $\mathfrak{o} \neq \mathfrak{a} \cap \mathbb{Z} =: A \trianglelefteq \mathbb{Z}$. Nach Satz 1.5 gibt es eine Zahl $a \in \mathbb{N}$ mit $A = \mathbb{Z}a$, wobei $a = \min(A \cap \mathbb{N}) = \min(\mathfrak{a} \cap \mathbb{N})$ gilt. Die Hauptordnung läßt sich nach Satz 10.2 schreiben als $\mathcal{O}_d = \mathbb{Z} + \mathbb{Z}z$. Offensichtlich gilt

$$C := \left\{ c \in \mathbb{Z} \mid \text{ es gibt ein } b \in \mathbb{Z} \quad \text{mit } b + cz \in \mathfrak{a} \right\} \trianglelefteq \mathbb{Z},$$

und da mit $a \in A$ auch $az \in \mathfrak{a}$ und somit $a \in C$ gilt, folgt $C \supseteq A \neq \mathfrak{o}$. Daher existiert ein $c \in \mathbb{N}$ mit $C = \mathbb{Z}c$, und wegen $c \in C$ gibt es ein $b \in \mathbb{Z}$ mit $b + cz =: v \in \mathfrak{a}$. Hieraus folgen zunächst $v \in \mathcal{O}_d \backslash \mathbb{Z}$ und $\mathbb{Z}a + \mathbb{Z}v \subseteq \mathfrak{a}$. Umgekehrt existieren für ein beliebiges Element $x \in \mathfrak{a}$ wegen $\mathfrak{a} \subseteq \mathcal{O}_d$ Zahlen $g, h \in \mathbb{Z}$ mit $x = g + hz$. Folglich gilt $h \in C$, und es gibt ein $k \in \mathbb{Z}$ mit $h = kc$. Somit ergibt sich $x = g + kcz = g + k(v - b)$, woraus

$$x - kv = g - kb \in \mathfrak{a} \cap \mathbb{Z} = A = \mathbb{Z}a$$

folgt. Also gilt $x \in \mathbb{Z}a + \mathbb{Z}v$, was die Inklusion $\mathfrak{a} \subseteq \mathbb{Z}a + \mathbb{Z}v$ zur Folge hat. □

Bemerkung 11.3. *Gelten für $u, v \in \mathcal{O}_d$ und $g \in \mathbb{Z}$ die Beziehungen $g \mid uu'$, $g \mid vv'$ und $g \mid (uv' + u'v)$, so folgen $g \mid uv'$ und $g \mid u'v$.*

Beweis. Wird $x := uv'$ gesetzt, so gilt $x' = (uv')' = u'v$. Daher existieren Zahlen $s, t \in \mathbb{Z}$ mit $x^2 + sx + t = 0$, wobei $s = -\mathcal{S}(x) = -(x + x') = -(uv' + u'v)$ und $t = \mathcal{N}(x) = xx' = uu'vv'$ gelten. Aus den Voraussetzungen folgen somit $g \mid s$ und $g^2 \mid t$, weshalb mit $\widetilde{s} := {}^s/_g$ und $\widetilde{t} := {}^t/_{g^2}$ die Beziehung $\widetilde{s}, \widetilde{t} \in \mathbb{Z}$ gilt. Die Division der quadratischen Gleichung für x durch g^2 führt zu

$$\left(\frac{x}{g}\right)^2 + \widetilde{s}\frac{x}{g} + \widetilde{t} = 0,$$

was ${}^x/_g \in \mathcal{O}_d$ und schließlich $g \mid x$ zur Folge hat. Da mit $gy = x$ stets $gy' = x'$ gilt, folgt somit auch $g \mid x'$. $\square$

Bemerkung 11.4. *Ist $\mathfrak{o} \neq \mathfrak{a} \trianglelefteq \mathcal{O}_d$ ein Ideal, das (nach Bemerkung 11.2) die Gestalt $\mathfrak{a} = \mathcal{O}_d u + \mathcal{O}_d v$ mit $u, v \in \mathfrak{a}$ besitzt und wird $g := \operatorname{ggT}\{\mathcal{N}(u), \mathcal{N}(v), \mathcal{S}(u'v)\} \in \mathbb{N}$ gesetzt, so gilt $\mathfrak{a}\mathfrak{a}' = \mathcal{O}_d g$.*

Beweis. Zunächst gilt $\mathfrak{a}\mathfrak{a}' = (\mathcal{O}_d u + \mathcal{O}_d v)(\mathcal{O}_d u' + \mathcal{O}_d v') = \mathcal{O}_d uu' + \mathcal{O}_d uv' + \mathcal{O}_d u'v + \mathcal{O}_d vv'$. Aus $uu' = \mathcal{N}(u) \in \mathfrak{a}\mathfrak{a}'$, $vv' = \mathcal{N}(v) \in \mathfrak{a}\mathfrak{a}'$ und $u'v + v'u = \mathcal{S}(u'v) \in \mathfrak{a}\mathfrak{a}'$ und der Wahl von g folgt nun $g \in \mathfrak{a}\mathfrak{a}'$, womit sich $\mathcal{O}_d g \subseteq \mathfrak{a}\mathfrak{a}'$ ergibt. Andererseits ergeben sich nach Bemerkung 11.3 die Beziehungen $g \mid u'v$ und $g \mid uv'$, woraus die andere Inklusion $\mathfrak{a}\mathfrak{a}' \subseteq \mathcal{O}_d g$ folgt. $\square$

11.3 Primidealzerlegung

Bemerkung 11.5. *Für $\mathfrak{o} \neq \mathfrak{a}, \mathfrak{b}, \mathfrak{c} \trianglelefteq \mathcal{O}_d$ folgt aus $\mathfrak{a}\mathfrak{b} = \mathfrak{a}\mathfrak{c}$ stets $\mathfrak{b} = \mathfrak{c}$.*

Beweis. Aus $\mathfrak{a}\mathfrak{b} = \mathfrak{a}\mathfrak{c}$ folgt zunächst $\mathfrak{a}'\mathfrak{a}\mathfrak{b} = \mathfrak{a}'\mathfrak{a}\mathfrak{c}$. Nach Bemerkung 11.4 existiert somit ein $g \in \mathbb{N}$ mit $\mathcal{O}_d g\mathfrak{b} = \mathcal{O}_d g\mathfrak{c}$, was $g\mathfrak{b} = g\mathfrak{c}$ zur Folge hat. Da in $\mathcal{O}_d$ aus $gb = gc$ stets $b = c$ folgt, gilt daher $\mathfrak{b} = \mathfrak{c}$. $\square$

Bemerkung 11.6. *Für $\mathfrak{o} \neq \mathfrak{a}, \mathfrak{b} \trianglelefteq \mathcal{O}_d$ ist $\mathfrak{a} \mid \mathfrak{b}$ gleichbedeutend mit $\mathfrak{a} \supseteq \mathfrak{b}$.*

Beweis. Gilt $\mathfrak{a} \mid \mathfrak{b}$ so existiert ein $\mathfrak{c} \trianglelefteq \mathcal{O}_d$ mit $\mathfrak{b} = \mathfrak{c}\mathfrak{a} \subseteq \mathcal{O}_d\mathfrak{a} = \mathfrak{a}$. Umgekehrt hat $\mathfrak{a} \supseteq \mathfrak{b}$ die Beziehung $\mathfrak{a}'\mathfrak{b} \subseteq \mathfrak{a}'\mathfrak{a} = \mathcal{O}_d g$ mit $g \in \mathbb{N}$ zur Folge. Da $\mathfrak{c} := {}^1/_g\, \mathfrak{a}'\mathfrak{b}$ ein Ideal in $\mathcal{O}_d$ ist, gilt somit $\mathfrak{a}'\mathfrak{b} = g\mathfrak{c} = \mathcal{O}_d g\mathfrak{c} = \mathfrak{a}'\mathfrak{a}\mathfrak{c}$. Nach Bemerkung 11.5 hat dies $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$ zur Folge, weshalb schließlich $\mathfrak{a} \mid \mathfrak{b}$ gilt. $\square$

Folgerung 11.1. *Für $\mathfrak{o} \neq \mathfrak{a}, \mathfrak{b} \trianglelefteq \mathcal{O}_d$ gilt $\operatorname{ggT}\{\mathfrak{a}, \mathfrak{b}\} = \mathfrak{a} + \mathfrak{b}$.*

Beweis. Nach der Definiton von $\mathfrak{c} := \operatorname{ggT}\{\mathfrak{a}, \mathfrak{b}\}$ gelten $\mathfrak{c} \mid \mathfrak{a}$ und $\mathfrak{c} \mid \mathfrak{b}$, und für alle $\mathfrak{d} \trianglelefteq \mathcal{O}_d$ folgt aus $\mathfrak{d} \mid \mathfrak{a}$ und $\mathfrak{d} \mid \mathfrak{b}$ die Beziehung $\mathfrak{d} \mid \mathfrak{c}$. Nach Bemerkung 11.6 ist dies gleichbedeutend mit $\mathfrak{c} = \mathfrak{a} + \mathfrak{b}$. $\square$

Satz 11.2. *Für $\mathfrak{p} \trianglelefteq \mathcal{O}_d$ sind die folgenden Aussagen äquivalent:*

(a) $\mathfrak{p}$ ist unzerlegbar.

(b) $\mathfrak{p}$ ist maximal.

(c) $\mathfrak{p}$ ist prim.

Beweis. Zunächst sei $\mathfrak{p}$ unzerlegbar. Gilt $\mathfrak{a} \supseteq \mathfrak{p}$, so folgt nach Bemerkung 11.6 $\mathfrak{a} \mid \mathfrak{p}$ und aufgrund der Unzerlegbarkeit von $\mathfrak{p}$ gilt $\mathfrak{a} = \mathfrak{p}$ oder $\mathfrak{a} = \mathcal{O}_d$. Daher ist $\mathfrak{p}$ maximal.

Nun sei $\mathfrak{p}$ als maximal vorausgesetzt und es gelte $\mathfrak{p} \mid \mathfrak{a}\mathfrak{b}$ aber $\mathfrak{p} \nmid \mathfrak{a}$. Hieraus folgen $\mathfrak{p} \supseteq \mathfrak{a}\mathfrak{b}$ und $\mathfrak{p} \not\supseteq \mathfrak{a}$. Daher gilt $\mathfrak{p} + \mathfrak{a} \supsetneq \mathfrak{p}$, und aus der Maximalität von $\mathfrak{p}$ folgt $\mathfrak{p} + \mathfrak{a} = \mathcal{O}_d$. Also existieren $p \in \mathfrak{p}$ und $a \in \mathfrak{a}$ mit $p + a = 1$, und es gilt

$$\mathfrak{b} = \mathfrak{b}1 = \mathfrak{b}(p + a) \subseteq \mathfrak{b}p + \mathfrak{b}a \subseteq \mathfrak{b}\mathfrak{p} + \mathfrak{b}\mathfrak{a} \subseteq \mathfrak{p} + \mathfrak{p} = \mathfrak{p}.$$

Somit folgt $\mathfrak{p} \mid \mathfrak{b}$, und $\mathfrak{p}$ ist ein Primideal.

Schließlich sei $\mathfrak{p}$ ein Primideal, und es gelte $\mathfrak{a} \mid \mathfrak{p}$. Dann gibt es ein $\mathfrak{b}$ mit $\mathfrak{p} = \mathfrak{a}\mathfrak{b}$. Aus $\mathfrak{a} \mid \mathfrak{p}$ und $\mathfrak{b} \mid \mathfrak{p}$ folgen somit die Inklusionen $\mathfrak{a} \supseteq \mathfrak{p}$ und $\mathfrak{b} \supseteq \mathfrak{p}$. Da $\mathfrak{p}$ Primideal ist, folgen wegen $\mathfrak{p} \mid \mathfrak{a}\mathfrak{b}$ andererseits $\mathfrak{p} \mid \mathfrak{a}$ oder $\mathfrak{p} \mid \mathfrak{b}$, womit $\mathfrak{p} \supseteq \mathfrak{a}$ oder $\mathfrak{p} \supseteq \mathfrak{b}$ gilt. Somit gilt $\mathfrak{a} = \mathfrak{p}$ oder $\mathfrak{b} = \mathfrak{p}$, und folglich ist $\mathfrak{p}$ unzerlegbar. □

Satz 11.3. *Jedes Ideal $\mathfrak{o} \neq \mathfrak{a} \trianglelefteq \mathcal{O}_d$ ist bis auf die Reihenfolge der Faktoren eindeutig als Produkt von Primidealen darstellbar.*

Beweis. Für die Mächtigkeit des Restklassenrings von $\mathcal{O}_d$ nach $\mathfrak{a}$ gilt

$$\left| \mathcal{O}_d/\mathfrak{a} \right| \leq \left| \mathcal{O}_d/\mathfrak{a}\mathfrak{a}' \right| = \left| \mathcal{O}_d/\mathcal{O}_d g \right|.$$

Ein Vertretersystem von $\mathcal{O}_d/\mathcal{O}_d g$ ist $V := \{r + sz \mid r, s \in \mathbb{Z},\ 0 \leq r, s < g\}$, wie die folgenden Betrachtungen zeigen: Für zwei Elemente $r_1 + s_1 z \in V$ und $r_2 + s_2 z \in V$ mit $g \mid (r_1 + s_1 z - r_2 - s_2 z)$ gelten wegen $(r_1 - r_2) + (s_1 - s_2)z = g(x + yz) = gx + gyz$ die Beziehungen $g \mid (r_1 - r_2)$ und $g \mid (s_1 - s_2)$. Hieraus folgen aber wegen $|r_1 - r_2| < g$ und $|s_1 - s_2| < g$ schließlich $r_1 = r_2$ und $s_1 = s_2$. Andererseits besitzt jedes Element $x + yz \in \mathcal{O}_d$ einen Vertreter in V, denn durch Division mit Rest $x = \widetilde{x}g + r$ mit $\widetilde{x} \in \mathbb{Z}$ und $0 \leq r < g$ und $y = \widetilde{y}g + s$ mit $\widetilde{y} \in \mathbb{Z}$ und $0 \leq s < g$ folgt

$$x + yz = \widetilde{x}g + r + \widetilde{y}gz + bz \equiv r + sz \in V \bmod \mathcal{O}_d g.$$

Daher ist wegen $\left| \mathcal{O}_d/\mathfrak{a} \right| \leq |V| = g^2$ die Mächtigkeit des Restklassenrings von $\mathcal{O}_d$ nach $\mathfrak{a}$ endlich.

Für $\left| \mathcal{O}_d/\mathfrak{a} \right| = 1$ ist die Behauptung des Satzes klar. Für $\left| \mathcal{O}_d/\mathfrak{a} \right| > 1$ existiert ein maximales Ideal $\mathfrak{p}_1 \trianglelefteq \mathcal{O}_d$ mit $\mathfrak{p}_1 \supseteq \mathfrak{a}$. Folglich gilt $\mathfrak{p}_1 \mid \mathfrak{a}$ und es gibt ein $\mathfrak{a}_1$ mit $\mathfrak{a} = \mathfrak{a}_1\mathfrak{p}$ und $\mathfrak{a} \subsetneq \mathfrak{a}_1$. Wegen $\left| \mathcal{O}_d/\mathfrak{a}_1 \right| < \left| \mathcal{O}_d/\mathfrak{a} \right|$ erhält man auf diese Weise nach endlich vielen Schritten

$$\mathfrak{a} = \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_n \quad \text{mit } \mathfrak{p}_i \text{ maximal.}$$

Die Eindeutigkeit wird wie im Beweis zu Satz 1.4 gezeigt. □

11.4 Das Zerlegungsgesetz für Primideale

Bezeichnung: Mit den Bezeichnungen von Satz 10.2 gelte $f(x) := x^2 - \mathcal{S}(z)x + \mathcal{N}(z) =: x^2 - sx + t = (x - z)(x - z')$ und $\mathrm{D} := \mathrm{D}(z) = s^2 - 4t$

Bemerkung 11.7. *Ist $K = \mathbb{Q}(\sqrt{d}\,)$ ein quadratischer Zahlkörper mit der Diskriminante* D, *so gelten für das Legendre–Symbol $\left(\frac{\mathrm{D}}{p}\right)$ mit $p \in \mathbb{P}$ die folgenden Aussagen:*

(a) $\left(\frac{\mathrm{D}}{p}\right) = -1$ *ist gleichbedeutend mit* ${}^{\mathcal{O}_d}/_{\mathcal{O}_d p} \cong \mathbb{F}_{p^2}$ *(d.h.* ${}^{\mathcal{O}_d}/_{\mathcal{O}_d p}$ *ist ein Körper mit* p^2 *Elementen).*

(b) $\left(\frac{\mathrm{D}}{p}\right) = 1$ *ist gleichbedeutend mit* ${}^{\mathcal{O}_d}/_{\mathcal{O}_d p} \cong \mathbb{F}_p \times \mathbb{F}_p$.

(c) $\left(\frac{\mathrm{D}}{p}\right) = 0$ *ist gleichbedeutend mit* ${}^{\mathcal{O}_d}/_{\mathcal{O}_d p} \cong \mathbb{F}_p + q\mathbb{F}_p$ *(als* $\mathbb{F}_p$*–Vektorraum) mit* $q^2 \equiv 0 \pmod p$.

Beweis. Es genügt, jeweils die Implikationen von links nach rechts zu beweisen. Zur Abkürzung wird $R := {}^{\mathcal{O}_d}/_{\mathcal{O}_d p}$ gesetzt.

(a) Es gelte $\left(\frac{\mathrm{D}}{p}\right) = -1$. Da im Falle $f(x) \equiv 0 \pmod p$ die Kongruenz $x \equiv {}^{s}/_{2} \pm \sqrt{\mathrm{D}} \equiv 0 \pmod p$ gelten würde und D damit ein quadratischer Rest modulo p wäre, besitzt f modulo p keine Nullstellen. Wie im Beweis zu Satz 11.3 gezeigt, besitzt R genau p^2 Elemente und es bleibt zu zeigen, daß R nullteilerfrei ist. Gibt es Elemente $x, y \in \mathcal{O}_d$ mit $x, y \not\equiv 0 \pmod p$ und $xy \equiv 0 \pmod p$, so folgt $\mathcal{N}(x)\mathcal{N}(y) \equiv 0 \pmod p$, weshalb aufgrund der Nullteilerfreiheit in ${}^{\mathbb{Z}}/_{p\mathbb{Z}}$ ohne Einschränkung $\mathcal{N}(x) \equiv 0 \pmod p$ angenommen werden kann. Hat x die Gestalt $x = a + bz$, gilt also

$$\mathcal{N}(x) = (a + bz)(a + bz') = a^2 + abs + b^2 t \equiv 0 \pmod p. \tag{11.1}$$

Die Annahme $b \not\equiv 0 \pmod p$ führt nun wegen $b^2 f(-{}^{a}/_{b}) = a^2 + abs + b^2 t \equiv 0 \pmod p$ zu dem Widerspruch, daß $-{}^{a}/_{b}$ eine Nullstelle von f modulo p ist. Daher gilt $b \equiv 0 \pmod p$, woraus mit (11.1) auch $a \equiv 0 \pmod p$ folgt. Dies hat aber den Widerspruch $x \equiv 0 \pmod p$ zur Folge. Also ist R nullteilerfrei.

(b) Gilt $\left(\frac{\mathrm{D}}{p}\right) = 1$, so existiert ein $w \in \mathbb{Z}$ mit $f(X) \equiv (X - w)(X - w') \pmod p$. Die Abbildungen

$$\varphi : R \longrightarrow \mathbb{F}_p, \ \overline{x + yz} \mapsto x + yw \pmod p, \ \varphi' : R \longrightarrow \mathbb{F}_p, \ \overline{x + yz} \mapsto x + yw' \pmod p$$

sind Homomorphismen, denn für z.B. φ gelten

$$\begin{aligned}
\varphi((x + yz) + (\widetilde{x} + \widetilde{y}z)) &= ((x + \widetilde{x}) + (y + \widetilde{y})w) \\
&= x + yw + \widetilde{x} + \widetilde{y}w \\
&= \varphi(x + yz) + \varphi(\widetilde{x} + \widetilde{y}z) \quad \text{und} \\
\varphi((x + yz)(\widetilde{x} + \widetilde{y}z)) &= \varphi(x\widetilde{x} + y\widetilde{y}(sz - t) + (x\widetilde{y}\widetilde{x}y)z) \\
&= \varphi(x\widetilde{x} - y\widetilde{y}t + (x\widetilde{y} + \widetilde{x}y + y\widetilde{y}s)z) \\
&= x\widetilde{x} - y\widetilde{y} + (x\widetilde{y} + \widetilde{x}y + y\widetilde{y}s)w \\
&= x\widetilde{x} + y\widetilde{y}(sw - t) + (x\widetilde{y} + \widetilde{x}y)w \\
&\equiv x\widetilde{x} + y\widetilde{y}w^2 + (x\widetilde{y} + \widetilde{x}y)w \pmod p \\
&= (x + yw)(\widetilde{x} + \widetilde{y}w) \\
&= \varphi(x + yz)\varphi(\widetilde{x} + \widetilde{y}z).
\end{aligned}$$

Daher ist auch

$$\phi : R \longrightarrow \mathbb{F}_p \times \mathbb{F}_p\,,\ \overline{x+yz} \mapsto (\varphi(\overline{x+yz}), \varphi'(\overline{x+yz}))$$

ein Homomorphismus. Um die Injektivität von ϕ zu zeigen, sei $\phi(\overline{x+yz}) = (0,0)$. Somit gelten $x + yw = 0$ und $x + yw' = 0$, woraus $y(w - w') = 0$ folgt. Wegen $w - w' \neq 0$ hat dies $y \equiv 0 \pmod p$ zur Folge, womit auch $x \equiv 0 \pmod p$ gilt. Damit gilt $x + yz \in \mathcal{O}_d p$, was $\overline{x+yz} = \overline{0}$ zur Folge hat. Also ist ϕ injektiv. Aufgrund von $|R| = p^2 = |\mathbb{F}_p \times \mathbb{F}_p|$ ist ϕ auch surjektiv und damit bijektiv.

(c) Gilt $\left(\frac{\mathrm{D}}{p}\right) = 0$, so existiert ein $w \in \mathbb{Z}$ mit $f(X) \equiv (X - w)^2 \pmod p$. Wird $q := z - w$ gesetzt, so gilt

$$q^2 = (z-w)^2 \equiv f(z) \equiv 0 \pmod p,$$

weshalb 1 und q eine $\mathbb{Z}$–Basis von $\mathcal{O}_d$ bilden. Hieraus folgt $\mathcal{O}_d \cong \mathbb{Z} + q\mathbb{Z}$, woraus $R = \mathbb{F}_p + q\mathbb{F}_p$ mit $q^2 \equiv 0 \pmod p$ folgt. □

Satz 11.4. *Ist $K = \mathbb{Q}(\sqrt{d}\,)$ ein quadratischer Zahlkörper mit der Diskriminante* D, *so gelten für das Legendre–Symbol $\left(\frac{\mathrm{D}}{p}\right)$ mit $p \in \mathbb{P}$ die folgenden Aussagen:*

(a) $\left(\frac{\mathrm{D}}{p}\right) = -1$ ist gleichbedeutend mit $\mathcal{O}_d p = \mathfrak{p}$ mit einem Primideal $\mathfrak{p} \trianglelefteq \mathcal{O}_d$. .

(b) $\left(\frac{\mathrm{D}}{p}\right) = 1$ ist gleichbedeutend mit $\mathcal{O}_d p = \mathfrak{p}\mathfrak{p}'$ mit Primidealen $\mathfrak{p} \neq \mathfrak{p}' \trianglelefteq \mathcal{O}_d$.

(c) $\left(\frac{\mathrm{D}}{p}\right) = 0$ ist gleichbedeutend mit $\mathcal{O}_d p = \mathfrak{p}^2$ mit einem Primideal $\mathfrak{p} \trianglelefteq \mathcal{O}_d$.

Hierbei gilt $\left|\mathcal{O}_d/\mathfrak{p}\right| = p^2$ in (a) und $\left|\mathcal{O}_d/\mathfrak{p}\right| = p$ in (b) und (c).

Beweis. Nach Bemerkung 11.7 ist $\left(\frac{\mathrm{D}}{p}\right) = -1$ genau dann der Fall, wenn $\mathcal{O}_d/\mathcal{O}_d p$ nullteilerfrei und von der Mächtigkeit p^2 ist. Dies ist aber nach Satz 11.1 gleichbedeutend damit, daß $\mathcal{O}_d p$ ein Primideal mit $\left|\mathcal{O}_d/\mathfrak{p}\right| = p^2$ ist.

Gilt $\mathcal{O}_d p = \mathfrak{p}^2$ mit einem Primideal $\mathfrak{p} \trianglelefteq \mathcal{O}_d$, so existiert wegen $\mathfrak{p} \supsetneqq \mathfrak{p}^2$ ein $q \in \mathfrak{p}\backslash\mathfrak{p}^2$. Es gelten also $q \not\equiv 0 \pmod p$ und $q^2 \equiv 0 \pmod p$. Daher tritt Fall (c) in Bemerkung 11.7 ein und es folgt $\left(\frac{\mathrm{D}}{p}\right) = 0$. Gilt umgekehrt $\left(\frac{\mathrm{D}}{p}\right) = 0$, so existiert ein $q \in \mathcal{O}_d/\mathcal{O}_d p$ mit $q \not\equiv 0 \pmod p$ und $q^2 \equiv 0 \pmod p$. Wird $\mathfrak{p} := \mathcal{O}_d p + \mathcal{O}_d q$ gesetzt, so gilt $\mathfrak{p}^2 \subseteq \mathcal{O}_d p \subsetneqq \mathfrak{p}$. Hieraus folgt $\mathcal{O}_d p \,|\, \mathfrak{p}^2$, womit sich $\mathfrak{p} \neq \mathcal{O}_d$ und schließlich $\left|\mathcal{O}_d/\mathfrak{p}\right| = p$ ergeben. Somit gilt $\left|\mathcal{O}_d/\mathfrak{p}^2\right| = p^2 = \left|\mathcal{O}_d/\mathcal{O}_d p\right|$, was zusammen mit der schon gezeigten Inklusion $\mathfrak{p}^2 = \mathcal{O}_d p$ zur Folge hat.

Für einen direkten Beweis der Aussage (b) würde man den Hauptsatz 4.1 über simultane Kongruenzen in der allgemeineren Fassung für kommutative Ringe mit 1 benötigen, wie er in der Algebra I bewiesen wird. Unter Verwendung der vollständigen Fallunterscheidung in der Folgerung 12.2 im nächsten Paragraphen ergibt sie sich aber als direkte Konsequenz aus den bereits bewiesenen Teilen (a) und (c). □

12 Die Klassengruppe quadratischer Zahlkörper

12.1 Die Norm von Idealen

Definition 12.1. Ist $\mathbb{Q}(\sqrt{d})$ ein quadratischer Zahlkörper und gilt $\mathfrak{o} \neq \mathfrak{a} \trianglelefteq \mathcal{O}_d$, so heißt $\mathcal{N}(\mathfrak{a}) := \left| {}^{\mathcal{O}_d}/_{\mathfrak{a}} \right|$ **Norm von** $\mathfrak{a}$.

Bemerkung 12.1. *Ist $\mathfrak{o} \neq \mathfrak{a} \trianglelefteq \mathcal{O}_d$ ein Ideal mit $\mathfrak{a} = \mathbb{Z}a + \mathbb{Z}v$ und gilt $v = b + cz$ mit $a, c \in \mathbb{N}$ minimal und $b \in \mathbb{Z}$, so folgt $\mathcal{N}(\mathfrak{a}) = ac$.*

Beweis. Wird $V := \{r + sz \mid 0 \leq r < a,\ 0 \leq s < c\}$ gesetzt, so gilt $|V| = ac$, und es bleibt zu zeigen, daß V ein Vertretersystem von ${}^{\mathcal{O}_d}/_{\mathfrak{a}}$ ist. Zunächst sind alle Elemente von V paarweise inkongruent modulo $\mathfrak{a}$, denn für Elemente $r + sz \in V$ und $\widetilde{r} + \widetilde{s}z \in V$ mit $(r + sz) - (\widetilde{r} + \widetilde{s}z) \in \mathfrak{a}$ gilt $(r - \widetilde{r}) + (s - \widetilde{s})z \in \mathfrak{a}$, womit sich $a \mid (r - \widetilde{r})$ und $c \mid (s - \widetilde{s})$ ergeben. Hieraus folgen aber wegen $|r - \widetilde{r}| < a$ und $|s - \widetilde{s}| < c$ schließlich $r = \widetilde{r}$ und $s = \widetilde{s}$. Andererseits besitzt jede Restklasse $\overline{g} \in {}^{\mathcal{O}_d}/_{\mathfrak{a}}$ einen Vertreter in V, denn für $g = x + yz$ mit $x, y \in \mathbb{Z}$ erhält man durch Division mit Rest $y = \widetilde{y}c + s$ mit $\widetilde{y} \in \mathbb{Z}$ und $0 \leq s < c$. Hiermit ergibt sich

$$g - \widetilde{y}v = x + yz - \widetilde{y}(b + cz) = x + \widetilde{y}cz + sz - \widetilde{y}b - \widetilde{y}cz = x - \widetilde{y}b + sz.$$

Durch Division mit Rest erhält man weiter $x - \widetilde{y}b = \widetilde{x}a + r$ mit $\widetilde{x} \in \mathbb{Z}$ und $0 \leq r < a$, womit sich

$$g - \widetilde{y}v - \widetilde{x}a = x - \widetilde{y}b + sz - \widetilde{x}a = r + sz \in V$$

ergibt. Aufgrund von $\widetilde{y}v - \widetilde{x}a \in \mathfrak{a}$ folgt nun aber $g \equiv r + sz \bmod \mathfrak{a}$. □

Bemerkung 12.2. *Ist $\mathfrak{o} \neq \mathfrak{a} \trianglelefteq \mathcal{O}_d$ ein Ideal mit $\mathfrak{a} = \mathbb{Z}a + \mathbb{Z}v$ und gilt $v = b + cz$ mit $a, c \in \mathbb{N}$ minimal und $b \in \mathbb{Z}$, so gelten*

$$\widetilde{a} := \frac{a}{c} \in \mathbb{N},\ \widetilde{b} := \frac{b}{c} \in \mathbb{Z} \quad \text{und } \widetilde{b}^2 + \mathcal{S}(z)\widetilde{b} + \mathcal{N}(z) \equiv 0 \bmod \mathfrak{a}.$$

Beweis. Wird $s := \mathcal{S}(z)$ und $t := \mathcal{N}(z)$ gesetzt, so gilt $z^2 - sz + t = 0$. Aufgrund von $\mathfrak{a} \trianglelefteq \mathcal{O}_d$ gilt $z\mathfrak{a} \subseteq \mathfrak{a}$, woraus $za \in \mathbb{Z}a + \mathbb{Z}v$ und $zv \in \mathbb{Z}a + \mathbb{Z}v$ folgen. Hieraus ergeben sich über

$$za = \frac{v - b}{c}a = -\frac{b}{c}a + \frac{a}{c}v$$

die Beziehungen $c \mid a$ und $c \mid b$, womit $\widetilde{a} \in \mathbb{N}$ und $\widetilde{b} \in \mathbb{Z}$ gelten. Weiterhin folgt aus

$$\begin{aligned} zv &= z(b + cz) = zb + cz^2 = zb + c(sz - t) = z(b + cs) - ct \\ &= \frac{(v - b)(b + cs) - c^2t}{c} = \frac{-b^2 - bcs - c^2t + v(b + cs)}{c} = -\frac{b^2 + bcs + c^2t}{ac}a + \frac{b + cs}{c}v \end{aligned}$$

die Beziehung $ac \mid (b^2 + bcs + c^2t)$, was $ac \mid (c^2\widetilde{b}^2 + \widetilde{b}c^2s + c^2t)$ und schließlich $\widetilde{a} \mid (\widetilde{b}^2 + s\widetilde{b} + t)$ zur Folge hat. □

Folgerung 12.1. *Mit den Bezeichnungen von Bemerkung 12.2 gilt $\mathfrak{a} = c\widetilde{\mathfrak{a}}$ mit $\widetilde{\mathfrak{a}} = \mathbb{Z}\widetilde{a} + \mathbb{Z}\widetilde{v}$ und $\widetilde{v} = \widetilde{b} + z$*

Bezeichnung: Ideale der Form von $\widetilde{\mathfrak{a}}$ heißen **primitive Ideale**.

Bemerkung 12.3. *Für $\mathfrak{o} \neq \mathfrak{a} \trianglelefteq \mathcal{O}_d$ gilt $\mathfrak{a}\mathfrak{a}' = \mathcal{O}_d\mathcal{N}(\mathfrak{a})$.*

Beweis. Hat $\mathfrak{a}$ die Gestalt $\mathfrak{a} = \mathbb{Z}a + \mathbb{Z}v$ und gilt $v = b + cz$ mit $a, c \in \mathbb{N}$ minimal und $b \in \mathbb{Z}$, so wird $\widetilde{\mathfrak{a}} = \mathbb{Z}\widetilde{a} + \mathbb{Z}\widetilde{v}$ mit $\widetilde{a} = {}^a/_c$, $\widetilde{v} = \widetilde{b} + z$ und $\widetilde{b} = {}^b/_c$ gesetzt. Nach Bemerkung 12.1 gelten $\mathcal{N}(\mathfrak{a}) = ac$ und $\mathcal{N}(\widetilde{\mathfrak{a}}) = \widetilde{a}$, was $\mathcal{N}(\mathfrak{a}) = c^2\mathcal{N}(\widetilde{\mathfrak{a}})$ zur Folge hat. Wegen $\mathfrak{a}\mathfrak{a}' = (c\widetilde{\mathfrak{a}})(c\widetilde{\mathfrak{a}})' = c^2\widetilde{\mathfrak{a}}\widetilde{\mathfrak{a}}'$ kann daher $\mathfrak{a}$ ohne Einschränkung als primitiv, etwa als $\mathfrak{a} = a\mathbb{Z} + v\mathbb{Z}$ mit $v = b + z$ vorausgesetzt werden. Nach Bemerkung 11.4 gilt nun $\mathfrak{a}\mathfrak{a}' = \mathcal{O}_d g$ mit $g = \mathrm{ggT}\{\mathcal{N}(a), \mathcal{N}(v), \mathcal{S}(av')\}$ und den Beziehungen

$$\begin{aligned}
\mathcal{N}(a) &= a^2, \\
\mathcal{N}(v) &= (b+z)(b+z') = b^2 + b\mathcal{S}(z) + \mathcal{N}(z) =: c \quad \text{und} \\
\mathcal{S}(av') &= \mathcal{S}(a(b+z')) = a(2b + \mathcal{S}(z)).
\end{aligned}$$

Da nach Bemerkung 12.2 ein $\widetilde{c} \in \mathbb{Z}$ mit $c = a\widetilde{c}$ existiert, gilt $g = a\,\mathrm{ggT}\{a, \widetilde{c}, 2b + \mathcal{S}(z)\} =: a\widetilde{g}$. Wegen $\mathfrak{a}\mathfrak{a}' = \mathcal{O}_d g = \mathcal{O}_d a\widetilde{g} = \mathcal{O}_d\mathcal{N}(\mathfrak{a})\widetilde{g}$ bleibt nur noch $\widetilde{g} = 1$ zu zeigen. Es sei also p eine Primzahl mit $p \mid a$ und $p \mid (2b + \mathcal{S}(z))$. Im Falle $p \neq 2$ folgt aus

$$4c = 4b^2 + 4b\mathcal{S}(z) + 4\mathcal{N}(z) = (2b + \mathcal{S}(z))^2 - \mathcal{S}(z)^2 + 4\mathcal{N}(z)$$

aufgrund von $p^2 \mid (2b + \mathcal{S}(z))^2$ und $p^2 \nmid \mathrm{D}(z) = \mathcal{S}(z)^2 - 4\mathcal{N}(z)$ die Beziehung $p^2 \nmid c$. Wegen $c = a\widetilde{c}$ und $p \mid a$ hat dies $p \nmid \widetilde{c}$ und schließlich $p \nmid \widetilde{g}$ zur Folge. Im anderen Falle $p = 2$ gilt $2 \mid \mathcal{S}(z)$ und nach Satz 10.2 folgen $d \equiv 2, 3 \pmod 4$ und $\mathcal{S}(z) = 0$. Hiermit ergibt sich wegen $b^2 \equiv 0, 1 \pmod 4$ die Beziehung $c = b^2 + \mathcal{N}(z) = b^2 - d \not\equiv 0 \pmod 4$. Also gilt $4 \nmid c$, und wie im ersten Fall folgt $2 \nmid \widetilde{g}$, was insgesamt $\widetilde{g} = 1$ zur Folge hat. □

Satz 12.1. *Für $\mathfrak{o} \neq \mathfrak{a}, \mathfrak{b} \trianglelefteq \mathcal{O}_d$ gelten die folgenden Aussagen:*

(a) $\mathcal{N}(\mathfrak{a}\mathfrak{b}) = \mathcal{N}(\mathfrak{a})\mathcal{N}(\mathfrak{b})$

(b) *Für $x \in \mathcal{O}_d$ gilt $\mathcal{N}(\mathcal{O}_d x) = |\mathcal{N}(x)|$.*

Beweis.

(a) Nach Bemerkung 12.3 gilt $\mathcal{O}_d\mathcal{N}(\mathfrak{a}\mathfrak{b}) = (\mathfrak{a}\mathfrak{b})(\mathfrak{a}\mathfrak{b})' = (\mathfrak{a}\mathfrak{a}')(\mathfrak{b}\mathfrak{b}') = \mathcal{O}_d\mathcal{N}(\mathfrak{a})\mathcal{O}_d\mathcal{N}(\mathfrak{b}) = \mathcal{O}_d\mathcal{N}(\mathfrak{a})\mathcal{N}(\mathfrak{b})$, womit $\mathcal{N}(\mathfrak{a}\mathfrak{b}) = \mathcal{N}(\mathfrak{a})\mathcal{N}(\mathfrak{b})$ folgt.

(b) Aus $\mathcal{O}_d\mathcal{N}(\mathcal{O}_d x) = (\mathcal{O}_d x)(\mathcal{O}_d x)' = (\mathcal{O}_d x)(\mathcal{O}_d x') = \mathcal{O}_d x x' = \mathcal{O}_d\mathcal{N}(x)$ folgt $\mathcal{N}(\mathcal{O}_d x) = |\mathcal{N}(x)|$. □

Folgerung 12.2. *Ist $\mathfrak{p} \trianglelefteq \mathcal{O}_d$ ein Primideal, so gilt genau eine der folgenden Aussagen:*

(a) $\mathfrak{p} = \mathcal{O}_d p$ *mit* $\mathcal{N}(\mathfrak{p}) = p^2$.

(b) $\mathfrak{p}\mathfrak{p}' = \mathcal{O}_d p$ *mit* $\mathcal{N}(\mathfrak{p}) = p$ *und* $\mathfrak{p} \neq \mathfrak{p}'$.

(c) $\mathfrak{p}^2 = \mathcal{O}_d p$ *mit* $\mathcal{N}(\mathfrak{p}) = p$.

Beweis. Nach Bemerkung 11.4 gibt es eine natürliche Zahl g mit $\mathfrak{p}\mathfrak{p}' = \mathcal{O}_d g$. Ist $g = \prod_{i=1}^{r} p_i^{e_i}$ die Primzerlegung von g, so folgt wegen

$$\mathfrak{p}\mathfrak{p}' = \mathcal{O}_d \prod_{i=1}^{r} p_i^{e_i} = \prod_{i=1}^{r} (\mathcal{O}_d p_i)^{e_i}$$

und der Primidealeigenschaft von $\mathfrak{p}$, daß es ein i gibt mit $\mathfrak{p} \mid \mathcal{O}_d p_i =: \mathcal{O}_d p$. Somit gilt nach Satz 12.1 die Beziehung $\mathcal{N}(\mathfrak{p}) \mid \mathcal{N}(\mathcal{O}_d p) = |\mathcal{N}(p)| = p^2$. Im folgenden unterscheidet man drei Fälle. Im Falle $\mathcal{N}(\mathfrak{p}) = p^2$ gilt $\mathcal{N}(\mathfrak{p}) = \mathcal{N}(\mathcal{O}_d p)$ und wegen $\mathfrak{p} \supseteq \mathcal{O}_d p$ tritt Fall (a) ein. Im Falle $\mathcal{N}(\mathfrak{p}) = p$ gilt $\mathfrak{p}\mathfrak{p}' = \mathcal{O}_d \mathcal{N}(\mathfrak{p}) = \mathcal{O}_d p$, woraus sich für $\mathfrak{p} \neq \mathfrak{p}'$ Fall (b) und für $\mathfrak{p} = \mathfrak{p}'$ Fall (c) ergibt. Der letzte Fall $\mathcal{N}(\mathfrak{p}) = 1$ führt wegen $\mathfrak{p} = \mathcal{O}_d$ zu einem Widerspruch. □

12.2 Die Endlichkeit der Klassengruppe

Bemerkung 12.4. *Ist $K = \mathbb{Q}(\sqrt{d}\,)$ ein quadratischer Zahlkörper, so gibt es für $m \in \mathbb{N}$ nur endlich viele Ideale $\mathfrak{a} \trianglelefteq \mathcal{O}_d$ mit $\mathcal{N}(\mathfrak{a}) = m$.*

Beweis. Mit $\mathcal{N}(\mathfrak{a}) = m$ gilt nach Bemerkung 12.3 $\mathfrak{a}\mathfrak{a}' = \mathcal{O}_d m$, woraus $\mathfrak{a} \mid \mathcal{O}_d m$ folgt. Nach Satz 11.3 und Folgerung 12.2 besitzt $\mathcal{O}_d m$ nur endlich viele Teiler. □

Satz 12.2. *Ist $K = \mathbb{Q}(\sqrt{d}\,)$ ein quadratischer Zahlkörper, so gibt es für $\mathfrak{o} \neq \mathfrak{a} \trianglelefteq \mathcal{O}_d$ ein Element $a \in \mathfrak{a}$ mit $|\mathcal{N}(a)| \leq (1 + |d|)\mathcal{N}(\mathfrak{a})$.*

Beweis. Werden $m := \left[\sqrt{\mathcal{N}(\mathfrak{a})}\right]$ und $V =: \{\, x + yz \mid 0 \leq x, y \leq m \,\}$ gesetzt, so existieren wegen $|V| = (m+1)^2 > \mathcal{N}(\mathfrak{a})$ Elemente $r_1 = x_1 + y_1 z \in V$ und $r_2 = x_2 + y_2 z \in V$ mit $r_1 \neq r_2$ und $r_1 - r_2 \in \mathfrak{a}$. Somit gilt $x_1 - x_2 + (y_1 - y_2)z =: a_1 + a_2 z =: a \in \mathfrak{a}$ mit

$$\mathcal{N}(a) = aa' = a_1^2 + a_1 a_2 \mathcal{S}(z) + a_2^2 \mathcal{N}(z).$$

Für $d \equiv 2, 3 \pmod 4$ gelten nun nach Satz 10.2 die Beziehungen $\mathcal{S}(z) = 0$ und $\mathcal{N}(z) = -d$, was

$$|\mathcal{N}(a)| \leq m^2 + m^2\,|d| \leq (1 + |d|)m^2 \leq (1 + |d|)\mathcal{N}(\mathfrak{a})$$

zur Folge hat. Für $d \equiv 1 \pmod 4$ gelten $\mathcal{S}(z) = 1$ und wie im Beweis zu Satz 10.4 gezeigt $\mathcal{N}(z) = {}^{(1-d)}/_{4}$. Wegen $|d| \neq 1$ ergibt sich hieraus wegen

$$\begin{aligned} |\mathcal{N}(a)| &\leq m^2 + m^2 + m^2 \left|\frac{1-d}{4}\right| \leq m^2 + m^2 + m^2 \frac{1+|d|}{4} \\ &= \left(\frac{9+|d|}{4}\right) m^2 \leq (1+|d|)m^2 \leq (1+|d|)\mathcal{N}(\mathfrak{a}) \end{aligned}$$

die Behauptung. □

Definition 12.2. Ist $K = \mathbb{Q}(\sqrt{d}\,)$ ein quadratischer Zahlkörper und gilt $\mathfrak{a}, \mathfrak{b} \trianglelefteq \mathcal{O}_d$ dann heißt $\mathfrak{a}$ **äquivalent** zu $\mathfrak{b}$, wenn es Elemente $a, b \in \mathcal{O}_d$ mit $\mathfrak{a}a = \mathfrak{b}b$ gibt. Die Bezeichnung hierfür lautet $\mathfrak{a} \sim \mathfrak{b}$. (Hierdurch wird eine Äquivalenzrelation auf der Menge der Ideale in $\mathcal{O}_d$ definiert.) Eine Äquivalenzklasse von Idealen heißt **Idealklasse**, und die Menge $\mathfrak{C}_d$ der Idealklassen heißt **Klassengruppe**. Diese Bezeichnung wird durch Bemerkung 12.6 gerechtfertigt. Die Anzahl der Idealklassen in $\mathcal{O}_d$ heißt **Klassenzahl von** $\mathbb{Q}(\sqrt{d}\,)$ und wird mit $h(\mathbb{Q}(\sqrt{d}\,))$ bezeichnet.

Bemerkung 12.5. *Gilt $\mathfrak{a} \trianglelefteq \mathcal{O}_d$, so ist $\mathfrak{a} \sim \mathcal{O}_d$ genau dann der Fall, wenn $\mathfrak{a}$ ein Hauptideal ist.*

Beweis. Ist $\mathfrak{a}$ ein Hauptideal, so existiert ein $a \in \mathcal{O}_d$ mit $\mathfrak{a}1 = \mathfrak{a} = \mathcal{O}_d a$, woraus $\mathfrak{a} \sim \mathcal{O}_d$ folgt. Gilt umgekehrt $\mathfrak{a} \sim \mathcal{O}_d$, so existieren $a, b \in \mathcal{O}_d$ mit $\mathfrak{a}a = \mathcal{O}_d b$. Wird $m := aa' \in \mathbb{Z}$ gesetzt, so gilt $\mathfrak{a}m = \mathfrak{a}aa' = \mathcal{O}_d ba'$, was $\mathfrak{a} = \mathcal{O}_d {}^{ba'}/_{m}$ zur Folge hat. Aufgrund von $\mathfrak{a} \subseteq \mathcal{O}_d$ gilt somit ${}^{ba'}/_{m} \in \mathcal{O}_d$, weshalb $\mathfrak{a}$ ein Hauptideal ist. □

Folgerung 12.3. *Ist $K = \mathbb{Q}(\sqrt{d})$ ein quadratischer Zahlkörper, so gilt $h(\mathbb{Q}(\sqrt{d})) = 1$ genau dann, wenn $\mathcal{O}_d$ ein Hauptidealring ist.*

Bemerkung 12.6. *Die Menge der Idealklassen bildet eine abelsche Gruppe bezüglich der Multiplikation.*

Beweis. Zunächst folgt aus $\mathfrak{a}_1 \sim \mathfrak{a}_2$ und $\mathfrak{b}_1 \sim \mathfrak{b}_2$ die Beziehung $\mathfrak{a}_1\mathfrak{b}_1 \sim \mathfrak{a}_2\mathfrak{b}_2$, weshalb die Multiplikation auf der Menge der Idealklassen vertreterweise definiert werden kann. Die Klasse $\mathfrak{E}$ von $\mathcal{O}_d$ ist nach Bemerkung 12.5 gleich der Menge aller Hauptideale in $\mathcal{O}_d$, und da wegen $\mathfrak{a}\mathcal{O}_d = \mathfrak{a}$ für alle Idealklassen $\mathfrak{A}$ die Beziehung $\mathfrak{A}\mathfrak{E} = \mathfrak{A}$ gilt, stellt $\mathfrak{E}$ das neutrale Element der Multiplikation dar. Ist schließlich $\mathfrak{A}$ eine beliebige Idealklasse mit $\mathfrak{a} \in \mathfrak{A}$, so ist nach Bemerkung 12.3 $\mathfrak{a}\mathfrak{a}' = \mathcal{O}_d\mathcal{N}(\mathfrak{a})$ ein Hauptideal, womit $\mathfrak{A}\mathfrak{A}' = \mathfrak{E}$ gilt. Also besitzt jede Idealklasse $\mathfrak{A}$ die Klasse $\mathfrak{A}'$ als Inverses. □

Satz 12.3. *In jeder Idealklasse $\mathfrak{A}$ von $\mathcal{O}_d$ gibt es ein Ideal $\mathfrak{a}$ mit $\mathcal{N}(\mathfrak{a}) \leq 1 + |d|$.*

Beweis. Ist $\mathfrak{o} \neq \mathfrak{a} \in \mathfrak{A}$, so gibt es nach Satz 12.2 ein Element $a \in \mathfrak{a}$ mit $|\mathcal{N}(a)| \leq (1 + |d|)\mathcal{N}(\mathfrak{a})$. Aufgrund von $\mathfrak{a} \supseteq \mathcal{O}_d a$ gilt $\mathfrak{a} \,|\, \mathcal{O}_d a$, weshalb es ein $\mathfrak{b} \trianglelefteq \mathcal{O}_d$ mit $\mathfrak{a}\mathfrak{b} = \mathcal{O}_d a$ gibt. Nach Satz 12.1 folgt hieraus

$$\mathcal{N}(\mathfrak{a})\mathcal{N}(\mathfrak{b}) = \mathcal{N}(\mathfrak{a}\mathfrak{b}) = \mathcal{N}(\mathcal{O}_d a) = |\mathcal{N}(a)|\,,$$

womit sich

$$\mathcal{N}(\mathfrak{b}) = \frac{|\mathcal{N}(a)|}{\mathcal{N}(\mathfrak{a})} \leq \frac{(1 + |d|)\mathcal{N}(\mathfrak{a})}{\mathcal{N}(\mathfrak{a})} = 1 + |d|$$

ergibt. Die Idealklasse $\mathfrak{B}$ von $\mathfrak{b}$ enthält also ein Ideal mit der geforderten Normabschätzung. Da aufgrund von $\mathfrak{A}\mathfrak{B} = \mathfrak{E}$ die Klasse $\mathfrak{B}$ invers zu $\mathfrak{A}$ ist, durchläuft mit $\mathfrak{A}$ auch $\mathfrak{B}$ alle Idealklassen von $\mathcal{O}_d$, womit die Behauptung gezeigt ist. □

Satz 12.4. *Die Klassenzahl eines quadratischen Zahlkörpers $\mathbb{Q}(\sqrt{d})$ ist endlich.*

Beweis. Nach Satz 12.3 besitzt jede Idealklasse einen Vertreter $\mathfrak{a}$ mit $\mathcal{N}(\mathfrak{a}) \leq 1 + |d|$. Da es aber nach Bemerkung 12.4 nur endlich viele solcher Ideale $\mathfrak{a}$ geben kann, ist die Anzahl der Idealklassen in $\mathcal{O}_d$ endlich. □

12.3 Berechnung der Klassengruppe

In diesem Abschnitt soll an einigen Beispielen gezeigt werden, wie die Klassengruppe von imaginärquadratischen und reellquadratischen Zahlkörpern $\mathbb{Q}(\sqrt{d}\,)$ konkret berechnet werden kann.

Zunächst wird die Diskriminante $\mathrm{D} = \mathrm{D}(z)$ von $\mathbb{Q}(\sqrt{d}\,)$ bestimmt, die für die Anwendung des Zerlegungsgesetzes Satz 11.4 benötigt wird. (Vergleiche Satz 10.2 und Beweis zu Satz 10.4.) Das gesuchte Vertretersystem V von $\mathfrak{C}_d$ kann nach Satz 12.3 so gewählt werden, daß

$$V \subseteq \{\, \mathfrak{o} \neq \mathfrak{a} \trianglelefteq \mathcal{O}_d \mid \mathcal{N}(\mathfrak{a}) \leq 1 + |d| \,\}$$

gilt. Zur Bestimmung von V werden zunächst mit Hilfe von Folgerung 12.2 die Primideale $\mathfrak{p} \trianglelefteq \mathcal{O}_d$ mit $\mathcal{N}(\mathfrak{p}) \leq 1 + |d|$ gesucht und durch deren Produkte die Ideale $\mathfrak{a} \trianglelefteq \mathcal{O}_d$ mit $\mathcal{N}(\mathfrak{a}) \leq 1 + |d|$ zusammengesetzt. Anschließend wird durch Aufstellen von Normgleichungen untersucht, welche dieser Ideale äquivalent sind und welche Relationen zwischen den nichtäquivalenten Vertretern bestehen. So erhält man eine Beschreibung der Gruppenstruktur von $\mathfrak{C}_d$.

Beispiel 12.1. Die Klassengruppe von $\mathbb{Q}(\sqrt{-1}\,)$: Es gilt $d = -1$ und $D = -4$. Für die Primideale der Norm $\leq 1 + |-1| = 2$ gilt

$$2\mathcal{O}_{-1} = \mathfrak{p}_2^2, \quad \text{da } \left(\frac{-4}{2}\right) = 0,$$

woraus

$$V \subseteq \{\mathcal{O}_{-1}, \mathfrak{p}_2\}$$

folgt. Wegen $\mathcal{N}(1+i) = 2$ gilt $\mathfrak{p}_2 = (1+i)\mathcal{O}_{-1}$. Dies hat $\mathfrak{p}_2 \sim \mathcal{O}_{-1}$ und somit $\mathfrak{C}_{-1} = 1$ zur Folge.

Beispiel 12.2. Die Klassengruppe von $\mathbb{Q}(\sqrt{-17}\,)$: Es gilt $d = -17$ und $D = -68$. Zur Abkürzung sei $\mathcal{O} := \mathcal{O}_{-17}$. Für die Primideale der Norm $\leq 1 + |-17| = 18$ gilt nach dem Zerlegungsgesetz

$$\begin{array}{rcll}
2\mathcal{O} & = & \mathfrak{p}_2^2, & \text{da } \left(\frac{-68}{2}\right) = 0, \\
3\mathcal{O} & = & \mathfrak{p}_3\mathfrak{p}_3', & \text{da } \left(\frac{-68}{3}\right) = 1, \\
5\mathcal{O} & = & \mathfrak{p}_5 \sim \mathcal{O}, & \text{da } \left(\frac{-68}{5}\right) = -1, \\
7\mathcal{O} & = & \mathfrak{p}_7\mathfrak{p}_7', & \text{da } \left(\frac{-68}{7}\right) = 1, \\
11\mathcal{O} & = & \mathfrak{p}_{11}\mathfrak{p}_{11}', & \text{da } \left(\frac{-68}{11}\right) = 1, \\
13\mathcal{O} & = & \mathfrak{p}_{13}\mathfrak{p}_{13}', & \text{da } \left(\frac{-68}{13}\right) = 1, \\
17\mathcal{O} & = & \mathfrak{p}_{17}^2, & \text{da } \left(\frac{-68}{17}\right) = 0,
\end{array}$$

woraus

$$V \subseteq \{\mathcal{O},\ \mathfrak{p}_2,\ \mathfrak{p}_3,\ \mathfrak{p}_3',\ \mathfrak{p}_7,\ \mathfrak{p}_7',\ \mathfrak{p}_{11},\ \mathfrak{p}_{11}',\ \mathfrak{p}_{13},\ \mathfrak{p}_{13}',\ \mathfrak{p}_{17},\ \mathfrak{p}_2\mathfrak{p}_3,\ \mathfrak{p}_2\mathfrak{p}_3',\ \mathfrak{p}_2\mathfrak{p}_7,\ \mathfrak{p}_2\mathfrak{p}_7',\ \mathfrak{p}_3^2,\ \mathfrak{p}_3'^2\}$$

folgt. Nun wird die Norm von $x_a := a + \sqrt{-17}$ für $a = 0, 1, 2, 3, 4$ betrachtet: Aus

$$\begin{array}{lll}
\mathcal{N}(x_0) = 17, & \mathcal{N}(x_1) = 18 = 2 \cdot 9, & \mathcal{N}(x_2) = 21 = 3 \cdot 7, \\
\mathcal{N}(x_3) = 26 = 2 \cdot 13, & \mathcal{N}(x_4) = 33 = 3 \cdot 11 &
\end{array}$$

ergeben sich bei geeigneter Bezeichnung von $\mathfrak{p}_i, \mathfrak{p}'_i$ die Beziehungen

$$\begin{aligned}
\mathcal{O}x_0 &= \mathfrak{p}_{17}, && \\
\mathcal{O}x_1 &= \mathfrak{p}_2\mathfrak{p}_3^2 \quad \text{und} \quad & \mathcal{O}x'_1 &= \mathfrak{p}_2\mathfrak{p}_3'^2, \\
\mathcal{O}x_2 &= \mathfrak{p}'_3\mathfrak{p}_7 \quad \text{und} \quad & \mathcal{O}x'_2 &= \mathfrak{p}_3\mathfrak{p}'_7, \\
\mathcal{O}x_3 &= \mathfrak{p}_2\mathfrak{p}_{13} \quad \text{und} \quad & \mathcal{O}x'_3 &= \mathfrak{p}_2\mathfrak{p}'_{13}, \\
\mathcal{O}x_4 &= \mathfrak{p}_3\mathfrak{p}_{11} \quad \text{und} \quad & \mathcal{O}x'_4 &= \mathfrak{p}_3\mathfrak{p}'_{11}.
\end{aligned}$$

Hierbei ist zu beachten, daß die Wahl von $\mathfrak{p}_3$ als Teiler von $\mathcal{O}x_1$ das Ideal $\mathfrak{p}'_3$ als Teiler von $\mathcal{O}x_2$ festlegt, da im Falle $\mathfrak{p}_3 \,|\, \mathcal{O}x_2$ der Widerspruch $\mathfrak{p}_3 \,|\, (x_2 - x_1)\mathcal{O} = \mathcal{O}$ folgen würde. Daher gelten die folgenden Relationen:

$$\begin{aligned}
\mathfrak{p}_{17} &\sim \mathcal{O}, && \\
\mathfrak{p}_2\mathfrak{p}_3^2 &\sim \mathcal{O} \quad \text{und} \quad & \mathfrak{p}_2\mathfrak{p}_3'^2 &\sim \mathcal{O}, \\
\mathfrak{p}'_3\mathfrak{p}_7 &\sim \mathcal{O} \quad \text{und} \quad & \mathfrak{p}'_3\mathfrak{p}_7 &\sim \mathcal{O}, \\
\mathfrak{p}_2\mathfrak{p}_{13} &\sim \mathcal{O} \quad \text{und} \quad & \mathfrak{p}_2\mathfrak{p}_{13} &\sim \mathcal{O}, \\
\mathfrak{p}_3\mathfrak{p}_{11} &\sim \mathcal{O} \quad \text{und} \quad & \mathfrak{p}_3\mathfrak{p}'_{11} &\sim \mathcal{O}.
\end{aligned}$$

Aus $\mathfrak{p}_2\mathfrak{p}_3^2 \sim \mathcal{O}$ folgt wegen $\mathfrak{p}_2^2 \sim \mathcal{O}$ die Beziehung

$$\mathfrak{p}_3^2 = \mathcal{O}\mathfrak{p}_3^2 \sim \mathfrak{p}_2^2\mathfrak{p}_3^2 \sim \mathfrak{p}_2\mathcal{O} = \mathfrak{p}_2$$

und in ähnlicher Weise ergeben sich

$$\mathfrak{p}_3'^2 \sim \mathfrak{p}_2,\ \mathfrak{p}_3 \sim \mathfrak{p}_7,\ \mathfrak{p}'_3 \sim \mathfrak{p}'_7,\ \mathfrak{p}_2 \sim \mathfrak{p}_{13},\ \mathfrak{p}_2 \sim \mathfrak{p}'_{13},\ \mathfrak{p}'_3 \sim \mathfrak{p}_{11},\ \mathfrak{p}_3 \sim \mathfrak{p}'_{11}.$$

Also gilt $V \subseteq \{\mathcal{O}, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}'_3\}$. Um nachzuweisen, daß die restlichen vier Vertreter nicht äquivalent sind, genügt es wegen $\mathfrak{p}_2 \sim \mathfrak{p}_3^2$, die Beziehung $\mathfrak{p}_2 \not\sim \mathcal{O}$ zu zeigen. Die Annahme $\mathfrak{p}_2 \sim \mathcal{O}$ hat aber die Existenz ganzer Zahlen a und b mit $\mathfrak{p}_2 = \mathcal{O}(a + b\sqrt{-17})$ und somit den Widerspruch

$$2 = \mathcal{N}(\mathfrak{p}_2) = \mathcal{N}(a + b\sqrt{-17}) = a^2 + 17b^2$$

zur Folge. Also gilt $\mathfrak{C}_{-17} = \langle \mathfrak{p}_3\mathcal{O}_{-17} \rangle \cong Z_4$.

Beispiel 12.3. Für die Klassengruppe von $\mathbb{Q}(\sqrt{-5}\,)$ gilt $\mathfrak{C}_{-5} \cong Z_2$. (Vergleiche Beispiel 11.1.) Der Beweis hierfür sei als Übung empfohlen.

Beispiel 12.4. Die Klassengruppe von $\mathbb{Q}(\sqrt{5}\,)$: Es gilt $d = 5$ und $D = 5$. Für die Primideale der Norm $\leq 1 + |5| = 6$ gilt nach dem Zerlegungsgesetz

$$\begin{aligned}
2\mathcal{O} &= \mathfrak{p}_2 \sim \mathcal{O}, && \text{da } \left(\tfrac{5}{2}\right) = -1, \\
3\mathcal{O} &= \mathfrak{p}_3 \sim \mathcal{O}, && \text{da } \left(\tfrac{5}{3}\right) = -1, \\
5\mathcal{O} &= \mathfrak{p}_5^2, && \text{da } \left(\tfrac{5}{5}\right) = 0,
\end{aligned}$$

woraus

$$V \subseteq \{\mathcal{O}, \mathfrak{p}_5\}$$

folgt. Wegen $\mathcal{N}(\sqrt{5}) = -5$ gilt aber $\mathfrak{p}_5 = \sqrt{5}\mathcal{O}$. Also gilt auch $\mathfrak{p}_5 \sim \mathcal{O}$ und somit $\mathfrak{C}_5 = 1$.

Beispiel 12.5. Die Klassengruppe von $\mathbb{Q}(\sqrt{15})$: Es gilt $d = 15$ und $D = 60$. Für die Primideale der Norm $\leq 1 + |15| = 16$ gilt nach dem Zerlegungsgesetz

$$\begin{array}{rcll} 2\mathcal{O} & = & \mathfrak{p}_2^2, & \text{da } \left(\frac{60}{2}\right) = 0, \\ 3\mathcal{O} & = & \mathfrak{p}_3^2, & \text{da } \left(\frac{60}{3}\right) = 0, \\ 5\mathcal{O} & = & \mathfrak{p}_5^2, & \text{da } \left(\frac{60}{5}\right) = 0, \\ 7\mathcal{O} & = & \mathfrak{p}_7\mathfrak{p}_7', & \text{da } \left(\frac{60}{7}\right) = 1, \\ 11\mathcal{O} & = & \mathfrak{p}_{11}\mathfrak{p}_{11}', & \text{da } \left(\frac{60}{11}\right) = 1, \\ 13\mathcal{O} & = & \mathfrak{p}_{13} \sim \mathcal{O}, & \text{da } \left(\frac{60}{13}\right) = -1, \end{array}$$

woraus

$$V \subseteq \left\{\mathcal{O},\ \mathfrak{p}_2,\ \mathfrak{p}_3,\ \mathfrak{p}_5,\ \mathfrak{p}_7,\ \mathfrak{p}_7',\ \mathfrak{p}_{11},\ \mathfrak{p}_{11}',\ \mathfrak{p}_2\mathfrak{p}_3,\ \mathfrak{p}_2\mathfrak{p}_5,\ \mathfrak{p}_2\mathfrak{p}_7,\ \mathfrak{p}_2\mathfrak{p}_7',\ \mathfrak{p}_3\mathfrak{p}_5\right\}$$

folgt. Nun wird die Norm von $x_a := a + \sqrt{15}$ für $a = 0, 1, 2, 3, 4$ betrachtet: Aus

$$\begin{array}{ll} \mathcal{N}(x_0) = -15 = -3 \cdot 5, \quad \mathcal{N}(x_1) = -14 = -2 \cdot 7, \quad \mathcal{N}(x_2) = -11, \\ \mathcal{N}(x_3) = -6 = -2 \cdot 3, \quad \mathcal{N}(x_4) = 1 \ (x_4 \text{ ist sogar Grundeinheit in } \mathbb{Q}(\sqrt{15})) \end{array}$$

ergeben sich bei geeigneter Bezeichnung von $\mathfrak{p}_i, \mathfrak{p}_i'$ die Beziehungen

$$\begin{array}{lll} \mathcal{O}x_0 = \mathfrak{p}_3\mathfrak{p}_5, & & \\ \mathcal{O}x_1 = \mathfrak{p}_2\mathfrak{p}_7 & \text{und} & \mathcal{O}x_1' = \mathfrak{p}_2\mathfrak{p}_7', \\ \mathcal{O}x_2 = \mathfrak{p}_{11} & \text{und} & \mathcal{O}x_2' = \mathfrak{p}_{11}', \\ \mathcal{O}x_3 = \mathfrak{p}_2\mathfrak{p}_3. & & \end{array}$$

Daher gelten die folgenden Relationen:

$$\begin{array}{lll} \mathfrak{p}_3\mathfrak{p}_5 \sim \mathcal{O}, & & \\ \mathfrak{p}_2\mathfrak{p}_7 \sim \mathcal{O} & \text{und} & \mathfrak{p}_2\mathfrak{p}_7' \sim \mathcal{O}, \\ \mathfrak{p}_{11} \sim \mathcal{O} & \text{und} & \mathfrak{p}_{11}' \sim \mathcal{O}, \\ \mathfrak{p}_2\mathfrak{p}_3 \sim \mathcal{O}. & & \end{array}$$

Somit ergeben sich

$$\mathfrak{p}_5 \sim \mathfrak{p}_3,\ \mathfrak{p}_7 \sim \mathfrak{p}_2,\ \mathfrak{p}_7' \sim \mathfrak{p}_2,\ \mathfrak{p}_3 \sim \mathfrak{p}_2.$$

Also gilt $V \subseteq \{\mathcal{O}, \mathfrak{p}_2\}$. Die Annahme $\mathfrak{p}_2 \sim \mathcal{O}$ hat aber die Existenz ganzer Zahlen a und b mit $\mathfrak{p}_2 = \mathcal{O}(a + b\sqrt{-17})$ zur Folge. Hier führt die Kongruenzmethode (vergl. Beispiel 4.3) zum Ziel: Betrachtet man die Gleichung modulo 3, so ergibt sich der Widerspruch $a^2 \equiv 2 \pmod 3$. Also gilt $\mathfrak{C}_{15} = \langle \mathfrak{p}_2\mathcal{O}_{15} \rangle \cong Z_2$.

Teil III

Diophantische Gleichungen

13 Diophantische Mengen und Relationen

13.1 Motivation: Das X. Hilbertsche Problem

Ist $f(X_1,\dots,X_n) = f(\underline{X}) \in \mathbb{Z}[\underline{X}]$ ein Polynom in n Variablen, so heißt $\underline{x} \in \mathbb{Z}^n$ **Lösung der diophantischen Gleichung** $f(\underline{X}) = 0$, falls $f(\underline{x}) = 0$ gilt.

Die Frage nach der Existenz eines Algorithmus, der in endlich vielen Schritten entscheidet, ob eine gegebene diophantische Gleichung eine Lösung besitzt, wird als **X. Hilbertsches Problem** bezeichnet.

Bemerkung 13.1. *Folgende Aussagen sind äquivalent:*

(a) *Es gibt einen Algorithmus, der für alle $f(\underline{X}) \in \mathbb{Z}[\underline{X}]$ entscheidet, ob eine Lösung in $\mathbb{Z}^n$ existiert.*

(b) *Es gibt einen Algorithmus, der für alle $f(\underline{X}) \in \mathbb{Z}[\underline{X}]$ entscheidet, ob eine Lösung in $\mathbb{N}^n$ existiert.*

Beweis. Zunächst sei Aussage (b) vorausgesetzt. Ein Polynom $f(\underline{X}) \in \mathbb{Z}[\underline{X}]$ hat eine Lösung in $\mathbb{Z}^n$ genau dann, wenn

$$g(\underline{X}) := \prod_{\underline{\nu}\in\{\pm 1\}^n} f(\nu_1 X_1,\dots,\nu_n X_n)$$

eine Lösung in $\mathbb{N}_0^n$ besitzt. Dies ist aber gleichbedeutend damit, daß

$$h(\underline{X}) := g(X_1-1,\dots,X_n-1)$$

eine Lösung in $\mathbb{N}^n$ besitzt, was nach Voraussetzung entschieden werden kann.

Nun gelte Aussage (a). Ein Polynom $f(\underline{X}) \in \mathbb{Z}[\underline{X}]$ hat eine Lösung in $\mathbb{N}^n$ genau dann, wenn $g(\underline{X}) := f(X_1+1,\dots,X_n+1)$ eine Lösung in $\mathbb{N}_0^n$ besitzt. Nach dem Vier-Quadrate-Satz 7.3 ist dies aber gleichbedeutend damit, daß

$$h(Z_1,\dots,Z_{4n}) := g(Y_1,\dots,Y_n) \quad \text{mit } Y_i := Z_i^2 + Z_{i+n}^2 + Z_{i+2n}^2 + Z_{i+3n}^2$$

eine Lösung in $\mathbb{Z}^{4n}$ besitzt, was nach Voraussetzung entschieden werden kann. □

Anmerkung: Es genügt also, die Lösbarkeit diophantischer Gleichungen in $\mathbb{N}^n$ zu untersuchen.

13.2 Diophantische Mengen

Definition 13.1. Es sei $f(X_1,\dots,X_n) \in \mathbb{Z}[\underline{X}]$ ein Polynom. Die Menge

$$\mathrm{V}_f := \{\, (x_1,\dots,x_n) \in \mathbb{N}^n \mid f(\underline{x}) = 0 \,\}$$

wird als **Nullstellenmenge** (**Varietät**) von f in $\mathbb{N}^n$ bezeichnet. Für $m \leq n$ sei

$$\pi_m(\mathrm{V}_f) := \{\, (x_1, \ldots, x_m) \in \mathbb{N}^m \mid (x_1, \ldots, x_n) \in \mathrm{V}_f \,\}$$

die **Projektion** von V_f auf die ersten m Komponenten.

Eine Menge $D \subseteq \mathbb{N}^m$ heißt **diophantische Menge**, falls es ein Polynom $f \in \mathbb{Z}[X_1, \ldots, X_n]$ mit $n \geq m$ gibt, so daß $D = \pi_m(\mathrm{V}_f)$ gilt.

Beispiel 13.1. (a) $\mathbb{N}^n$ und $\emptyset$ sind diophantische Mengen vermöge den Polynomen $f(\underline{X}) = 0$ bzw. $f(\underline{X}) = 1$.

(b) $\{a\}$ mit $a \in \mathbb{N}$ ist diophantische Menge vermöge $f(X) = X - a$.

Die Menge $\{\, (x_1, x_2) \in \mathbb{N}^2 \mid x_1 = x_2 \,\}$ wird als Diagonale von $\mathbb{N}^2$ bezeichnet und ist diophantisch vermöge $f(X_1, X_2) = X_1 - X_2$.

(c) Für $f(X_1, X_2, X_3) = X_1 + X_3 - X_2$ ist $\pi_2(\mathrm{V}_f)$ die Menge der (x_1, x_2), für die es ein $x_3 \in \mathbb{N}$ mit $x_1 + x_3 = x_2$ gibt. Daher ist $\{\, (x_1, x_2) \in \mathbb{N}^2 \mid x_1 < x_2 \,\}$ diophantische Menge.

(d) Für $f(X_1, X_2, X_3) = X_2 - X_1 X_3$ ist $\pi_2(\mathrm{V}_f) = \{\, (x_1, x_2) \in \mathbb{N}^2 \mid x_1 \,|\, x_2 \,\}$ diophantische Menge.

(e) Für $f(X_1, X_2) = X_1 - n(X_2 - 1) - a$ mit $a, n \in \mathbb{N}$ ist $\pi_1(\mathrm{V}_f) = \{\, x_1 \in \mathbb{N} \mid x_1 \equiv a \pmod{n} \,\}$ diophantische Menge.

(f) Die Menge $\{\, n \in \mathbb{N} \mid n$ ist zusammengesetzt $\}$ ist diophantisch vermöge dem Polynom $f(X_1, \ldots, X_5) = (X_1 - X_2 X_3)^2 + (1 + X_4 - X_2)^2 + (1 + X_5 - X_2)^2$.

Satz 13.1. *Sind $D_1, D_2 \in \mathbb{N}^m$ diophantische Mengen, so sind auch $D_1 \cup D_2$ und $D_1 \cap D_2$ diophantische Mengen.*

Beweis. Die folgende Vorbemerkung zeigt, daß bei dem Polynom zu einer diophantischen Menge beliebig viele neue Variablen hinzugefügt werden können: Eine diophantische Menge $D = \pi_m(\mathrm{V}_f)$ zu $f = f(X_1, \ldots, X_n)$ mit $n \geq m$ läßt sich für beliebiges $s \geq n$ auch als $D = \pi_m(\mathrm{V}_{\widetilde{f}})$ zu $\widetilde{f} = \widetilde{f}(Y_1, \ldots, Y_s) = f(Y_1, \ldots, Y_m, Y_{r+1}, \ldots, Y_{r+n-m})$ mit $m \leq r \leq s - n + m$ darstellen. Dies wird dadurch erreicht, daß als Koeffizienten der „neuen“ Variablen jeweils null gewählt wird.

Somit kann ohne Einschränkung $D_1 = \pi_m(\mathrm{V}_{f_1})$ und $D_2 = \pi_m(\mathrm{V}_{f_2})$ mit $f_1, f_2 \in \mathbb{Z}[X_1, \ldots, X_n]$ angenommen werden.

Nun sei $g := f_1 f_2$. Wegen $\mathrm{V}_g = \mathrm{V}_{f_1} \cup \mathrm{V}_{f_2}$ ist

$$\pi_m(\mathrm{V}_g) = \pi_m(\mathrm{V}_{f_1} \cup \mathrm{V}_{f_2}) = \pi_m(\mathrm{V}_{f_1}) \cup \pi_m(\mathrm{V}_{f_2}) = D_1 \cup D_2$$

eine diophantische Menge.

Wird andererseits $g := f_1^2 + f_2^2$ gesetzt, so gilt wegen $\mathrm{V}_g = \mathrm{V}_{f_1} \cap \mathrm{V}_{f_2}$ die Beziehung

$$\pi_m(\mathrm{V}_g) = \pi_m(\mathrm{V}_{f_1} \cap \mathrm{V}_{f_2}) \subseteq \pi_m(\mathrm{V}_{f_1}) \cap \pi_m(\mathrm{V}_{f_2}) = D_1 \cap D_2.$$

Der Satz ist somit bewiesen, wenn f_1 und f_2 so gewählt werden können, daß auch die andere Inklusion gilt. Aufgrund der Vorbemerkung kann ohne Einschränkung

$$\begin{aligned} f_1 &= f_1(X_1, \ldots, X_m, X_{m+1}, \ldots, X_n, X_{n+1}, \ldots, X_r) \\ f_2 &= f_2(X_1, \ldots, X_m, \widetilde{X_{m+1}}, \ldots, \widetilde{X_n}, \widetilde{X_{n+1}}, \ldots, \widetilde{X_r}) \end{aligned}$$

mit $n - m = r - n$ und $\widetilde{X_{n+i}} = X_{m+i}$ für $1 \leq i \leq r - n$ angenommen werden. Hierbei sind die Koeffizienten der X_i für $n + 1 \leq i \leq r$ und die Koeffizienten der $\widetilde{X_i}$ für $m + 1 \leq i \leq n$ jeweils gleich null.

Es gelte nun $\underline{x} = (x_1, \ldots, x_m) \in \pi_m(\mathrm{V}_{f_1}) \cap \pi_m(\mathrm{V}_{f_2})$. Folglich gibt es $x_i, \widetilde{x_i} \in \mathbb{N}$ für $m + 1 \leq i \leq r$ mit

$$\begin{aligned} f_1(x_1, \ldots, x_m, x_{m+1}, \ldots, x_n, x_{n+1}, \ldots, x_r) &= 0 \\ f_2(x_1, \ldots, x_m, \widetilde{x_{m+1}}, \ldots, \widetilde{x_n}, \widetilde{x_{n+1}}, \ldots, \widetilde{x_r}) &= 0 \end{aligned}$$

Da ihre Koeffizienten gleich null sind, können für $n + 1 \leq i \leq r$ die Komponenten x_i durch $\widetilde{x_i}$ ersetzt werden. Ebenso können für $m + 1 \leq i \leq n$ die Komponenten $\widetilde{x_i}$ durch x_i ersetzt werden.

Somit ist $(x_1, \ldots, x_m, x_{m+1}, \ldots, x_n, \widetilde{x_{n+1}}, \ldots, \widetilde{x_r})$ eine gemeinsame Nullstelle von f_1 und f_2, womit $\underline{x} \in \pi_m(\mathrm{V}_{f_1} \cap \mathrm{V}_{f_2})$ gezeigt ist. $\square$

13.3 Diophantische Relationen

Definition 13.2. Eine Aussage $R(x_1, \ldots, x_n)$ über n natürliche Zahlen x_i heißt **(n-stellige) diophantische Relation** (**diophantisches Prädikat**), wenn es eine diophantische Menge D gibt, so daß $R(\underline{x})$ gleichbedeutend ist mit $\underline{x} \in D$.

Eine Abbildung $f : \mathbb{N}^n \longrightarrow \mathbb{N}$ heißt **diophantische Abbildung** ([diophantisch!diophantische Funktion]diophantische Funktion), wenn der Graph von f

$$\mathrm{Graph}_f := \big\{(x_1, \ldots, x_n, f(x_1, \ldots, x_n))\big\}$$

diophantisch ist.

Anmerkungen: Die Aussage $f(\underline{x}) = y$ ist genau dann eine diophantische Relation, wenn f eine diophantische Abbildung ist.

Jedes Polynom $f = f(X_1, \ldots, X_n)$ ist diophantische Abbildung vermöge

$$g(X_1, \ldots, X_n, Y) := f(X_1, \ldots, X_n) - Y.$$

Beispiel 13.2. Die folgenden Relationen sind diophantisch nach Beispiel 13.1:

(a) $x = a$ für $a \in \mathbb{N}$,

(b) $x_1 = x_2$,

(c) $x_1 < x_2$,

(d) $x_1 \mid x_2$,

(e) x ist zusammengesetzt.

Satz 13.2. *Sind R_1 und R_2 diophantische Relationen, so sind auch $R_1 \wedge R_2$ und $R_1 \vee R_2$ diophantische Relationen.*

Beweis. Entspricht R_i der diophantischen Menge D_i für $i = 1, 2$, so kann ohne Einschränkung $R_1, R_2 \in \mathbb{N}^m$ angenommen werden. Dann entsprechen $R_1 \wedge R_2$ der Menge $D_1 \cap D_2$ und $R_1 \vee R_2$ der Menge $D_1 \cup D_2$, die nach Satz 13.1 diophantisch sind. □

Folgerung 13.1. *Ist $R(x_1, \ldots, x_n)$ eine diophantische Relation und sind $f_i(\underline{x_i}) = f_i(x_{i1}, \ldots, x_{is_i})$ diophantische Funktionen, so ist $Q(\underline{x_i}, \ldots, \underline{x_n}) := R(f_1(\underline{x_i}), \ldots, f_n(\underline{x_n}))$ eine diophantische Relation.*

Beweis. Die Relation Q ist äquivalent zu

$$R(x_1, \ldots, x_n) \ \wedge \ (f_1(\underline{x_i}) = x_1) \ \wedge \ \ldots \ \wedge \ (f_n(\underline{x_n}) = x_n),$$

wobei jedes Konjunktionsglied eine diophantische Relation ist. Die Behauptung folgt somit aus Bemerkung 13.2. □

Beispiel 13.3. (a) Die Relation $x_1 \neq x_2$ ist äquivalent zu $(x_1 < x_2) \ \vee \ (x_2 < x_1)$ und damit diophantisch.

(b) Die Relation $x_1 \leq x_2$ ist äquivalent zu $(x_1 < x_2) \vee (x_1 = x_2)$ und damit diophantisch.

(c) Die Relation $x_1 \equiv x_2 \pmod{x_3}$ ist diophantisch, denn für $f(X_1, \ldots, X_n) = X_1 - X_2 - X_3X_4$ ist

$$\pi_3(\mathrm{V}_f) = \{\, (x_1, x_2, x_3) \mid x_1 \equiv x_2 \pmod{x_3} \quad \text{und } x_1 > x_2 \,\}$$

eine diophantische Menge. Folglich ist $(x_1 \equiv x_2 \pmod{x_3}) \ \wedge \ (x_1 > x_2)$ eine diophantische Relation. Analog wird gezeigt, daß $(x_1 \equiv x_2 \pmod{x_3}) \wedge (x_2 > x_1)$ eine diophantische Relation ist. Nun ist aber $x_1 \equiv x_2 \pmod{x_3}$ äquivalent zu

$$((x_1 \equiv x_2 \pmod{x_3}) \wedge (x_1 > x_2)) \ \vee \ ((x_1 \equiv x_2 \pmod{x_3}) \wedge (x_2 > x_1)) \ \vee \ (x_1 = x_2)$$

und daher diophantisch.

Bemerkung 13.2. *Ist $R(x_1, \ldots, x_n, y_1, \ldots, y_m)$ eine diophantische Relation, so ist auch Die Aussage $Q(\underline{x})$: Es gibt ein $\underline{y} \in \mathbb{N}^m$ mit $R(\underline{x}, \underline{y})$ eine diophantische Relation.*

Beweis. Ist $\pi_{m+n}(\mathrm{V}_f)$ die diophantische Menge zu R, so ist $\pi_m(\mathrm{V}_f)$ die diophantische Menge zu Q. □

Beispiel 13.4. Die Relation $x_1 = \left[{}^{x_2}/_{x_3}\right]$ ist diophantisch, denn sie ist äquivalent zu der Aussage

$$\text{Es gibt ein } y \in \mathbb{N} \quad \text{mit } (x_1x_3 = x_2 + (y - 1) \ \wedge \ y \leq x_3).$$

14 Die Potenzfunktion

Ziel dieses Paragraphen ist es zu zeigen, daß die Menge $\{\, (n, k, n^k) \mid n, k \in \mathbb{N} \} \subseteq \mathbb{N}^3$ diophantisch ist, oder gleichbedeutend, daß die Abbildung $f : \mathbb{N}^2 \longrightarrow \mathbb{N}$ mit $(n, k) \mapsto n^k$ eine diophantische Funktion ist.

14.1 Die Pellsche Gleichung

Ist $a \geq 2$ eine natürliche Zahl, so wird die Gleichung

$$X^2 - (a^2 - 1)Y^2 = 1$$

als **Pellsche Gleichung** (P_a) bezeichnet. Triviale Lösungen von (P_a) sind $(1, 0)$ und $(a, 1)$. Für Lösungen $(x, y) \in \mathbb{N}^2$ sind wegen $x^2 = (a^2 - 1)y^2 + 1$ die Funktionen $x(y)$ und $y(x)$ streng monoton wachsend. Wegen $(1, 0) \notin \mathbb{N}^2$ wird daher die Lösung $(a, 1)$ als **minimale Lösung** bezeichnet. Im quadratischen Zahlkörper $\mathbb{Q}(\sqrt{a^2 - 1}\,)$ ist

$$e_1 := a + \sqrt{a^2 - 1}$$

wegen $\mathcal{N}(e_1) = a^2 - (a^2 - 1) = 1$ eine Einheit. (Achtung: $a^2 - 1$ ist im allgemeinen nicht quadratfrei.)

Bezeichnung: Für $n \in \mathbb{N}_0$ und $a \geq 2$ seien $X_n(a) \in \mathbb{N}$ und $Y_n(a) \in \mathbb{N}_0$ durch die Zerlegung von $e_1^n = (a + \sqrt{a^2 - 1})^n =: X_n(a) + Y_n(a)\sqrt{a^2 - 1}$ in Summanden ohne und mit Wurzel definiert. Für jedes $n \in \mathbb{N}$ ist $(X_n(a), Y_n(a))$ eine Lösung von (P_a) wegen

$$1 = \mathcal{N}(e_1)^n = \mathcal{N}(e_1^n) = X_n(a)^2 - Y_n(a)^2(a^2 - 1).$$

Bemerkung 14.1. *Ist $(x, y) \in \mathbb{N}^2$ eine Lösung von (P_a), so gibt es ein $n \in \mathbb{N}$ mit*

$$x + y\sqrt{a^2 - 1} = X_n(a) + Y_n(a)\sqrt{a^2 - 1} = (a + \sqrt{a^2 - 1})^n = e_1^n.$$

Beweis. Da $(a, 1)$ minimale Lösung ist, gelten die Beziehungen $x \geq a$ und $y \geq 1$. Folglich gilt $1 < e_1 \leq x + y\sqrt{a^2 - 1}$ und es gibt eine natürlichen Zahl n mit

$$e_1^n \leq x + y\sqrt{a^2 - 1} < e_1^{n+1}.$$

Da $e_1^{-1} = a - \sqrt{a^2 - 1}$ als Inverses einer positiven reellen Zahl auch positiv ist, folgt hieraus

$$1 \leq (x + y\sqrt{a^2 - 1})e_1^{-n} < e_1. \tag{14.1}$$

Setzt man $(x + y\sqrt{a^2 - 1})e_1^{-n} =: r =: u + v\sqrt{a^2 - 1}$ mit $u, v \in \mathbb{Z}$, so ist r wegen

$$rr' = (x + y\sqrt{a^2 - 1})e_1^{-n}(x - y\sqrt{a^2 - 1})e_1^n = x^2 - y^2(a^2 - 1) = 1$$

eine Einheit in $\mathbb{Q}(\sqrt{a^2 - 1}\,)$ mit $r^{-1} = u - v\sqrt{a^2 - 1}$.

Die Annahme $u, v < 0$ führt zu $r < 0$ im Widerspruch zu (14.1). Im Falle $u \geq 0, v < 0$ folgt wegen $\sqrt{a^2 - 1} > 1$ die Beziehung $r^{-1} = u - v\sqrt{a^2 - 1} > 1$, die wiederum im Widerspruch zu (14.1) steht. Gilt andererseits $u < 0, v \geq 0$, so folgt $-r^{-1} = -u + v\sqrt{a^2 - 1} > 0$, was im Widerspruch zu $-r^{-1} < -e_1^{-1} < 0$ steht. Also gilt $u, v \in \mathbb{N}_0$ und da (u, v) wegen

$$u^2 - v^2(a^2 - 1) = (u + v\sqrt{a^2 - 1})(u - v\sqrt{a^2 - 1}) = rr' = 1$$

eine Lösung von (P_a) ist und e_1 zur minimalen Lösung $(a, 1)$ gehört, folgt aus $r < e_1$ schließlich $(u, v) = (1, 0)$. Damit gilt $r = 1$, woraus sich $(x + y\sqrt{a^2 - 1}) = e_1^n$ ergibt. □

Anmerkung: Ist a^2-1 quadratfrei, so zeigt Bemerkung 14.1, daß $e_1 = a + \sqrt{a^2-1}$ Grundeinheit von $\mathbb{Q}(\sqrt{a^2-1})$ ist.

Bemerkung 14.2. *Ist f eine natürliche Zahl, so gibt es $x, y \in \mathbb{N}$ mit $x^2 - y^2 f^2(a^2-1) = 1$.*

Beweis. Es sei $d := f^2(a^2-1)$ und $t \in \mathbb{Q}(\sqrt{d})$ eine reduzierte Zahl mit $\mathrm{D}(t) = \mathrm{D}(\sqrt{d}) = 4d$. (Nach Bemerkung 10.4 kann t z.B. als erster Rest in der Kettenbruchentwicklung von $\sqrt{d}$ gewählt werden.) Nach Satz 8.3 besitzt t eine rein periodische Kettenbruchentwicklung etwa der Periode n mit Näherungsbrüchen ${}^{p_k}/_{q_k}$, wobei nach Bemerkung 10.5 die Beziehung

$$e := q_n t + q_{n-1} \in \mathcal{O}_d^\times \quad \text{bzw. } \mathcal{N}(e) = \pm 1$$

gilt. Aus der Periodizität von t ergibt sich $\binom{t}{1} = P_n \binom{t}{1}$, woraus

$$t = \frac{p_n t + p_{n-1}}{q_n t + q_{n-1}}$$

und schließlich $q_n t^2 + (q_{n-1} - p_n)t - p_{n-1} = 0$ folgt. Mit $y := \mathrm{ggT}\{q_n, q_{n-1} - p_n, p_{n-1}\} \in \mathbb{N}$ gilt somit

$$t = \frac{p_n - q_{n-1}}{2q_n} + \frac{y}{2q_n}\sqrt{\mathrm{D}(t)},$$

woraus sich

$$\begin{aligned} e = q_n t + q_{n-1} &= \frac{1}{2}(p_n - q_{n-1}) + \frac{1}{2}y\sqrt{\mathrm{D}(t)} + q_{n-1} \\ &= \frac{1}{2}(p_n + q_{n-1}) + yf\sqrt{a^2-1} \\ &=: x + yf\sqrt{a^2-1} \end{aligned}$$

ergibt, wobei $\frac{1}{2}(p_n + q_{n-1}) =: x$ gesetzt wurde.

Wegen $\mathcal{S}(e) = e + e' = p_n + q_{n-1}$ und $\mathcal{N}(e) = \pm 1$ ist e ganz über $\mathbb{Z}$ und aufgrund von $x = e - yf\sqrt{a^2-1} \in \mathbb{Q}$ ist auch x ganz über $\mathbb{Z}$. Folglich gilt $x \in \mathbb{Z}$ und damit sogar $x \in \mathbb{N}$. Im Falle $\mathcal{N}(e) = 1$ folgt die Behauptung nun wegen $1 = \mathcal{N}(e) = x^2 - y^2 f^2(a^2-1)$ direkt, während sie sich im Falle $\mathcal{N}(e) = -1$ über $1 = \mathcal{N}(e^2) = \mathcal{N}(\widetilde{x} + \widetilde{y} f\sqrt{a^2-1})$ mit $\widetilde{x}, \widetilde{y} \in \mathbb{N}$ ergibt. □

14.2 Kongruenzen für die Lösungen der Pellschen Gleichung

Ziel dieses Abschnitts ist es zu zeigen, daß die Relationen $x = X_k(a)$ und $y = Y_k(a)$ diophantisch sind.

Bemerkung 14.3. *Für $a \geq 2$ gelten die folgenden Beziehungen:*

(a)

$$Y_{nk}(a) = \sum_{\substack{j=1 \\ 2 \nmid j}}^{k} \binom{k}{j} X_n(a)^{k-j} Y_n(a)^j \sqrt{a^2-1}^{\,j-1} \tag{14.2}$$

(b) Aus $a \equiv b \pmod{c}$ folgt $Y_k(a) \equiv Y_k(b) \pmod{c}$.

(c) $Y_k(a) \equiv k \pmod{(a-1)}$

Beweis. Nach Bemerkung 14.1 gilt

$$\begin{aligned} X_{nk}(a) + Y_{nk}(a)\sqrt{a^2-1} &= e_1^{nk} = (e_1^n)^k \\ &= \left(X_n(a) + Y_n(a)\sqrt{a^2-1}\right)^k \\ &= \sum_{j=0}^{k} \binom{k}{j} X_n(a)^{k-j} Y_n(a)^j \sqrt{a^2-1}^{\,j}. \end{aligned}$$

Da bei den Summanden zu geradem j die Wurzel quadriert wird, ergibt eine Zerlegung in Anteile mit und ohne Wurzel

$$Y_{nk}(a)\sqrt{a^2-1} = \sum_{\substack{j=1 \\ 2 \nmid j}}^{k} \binom{k}{j} X_n(a)^{k-j} Y_n(a)^j \sqrt{a^2-1}^{\,j},$$

womit Teil (a) folgt.

Für jedes $a \geq 2$ gelten $X_1(a) = a$ und $Y_1(a) = 1$. Also folgen aus $a \equiv b \pmod{c}$ die Beziehungen

$$\begin{aligned} X_1(a) &\equiv X_1(b) \pmod{c} \\ Y_1(a) &\equiv Y_1(b) \pmod{c} \end{aligned}$$

Setzt man in (14.2) $n = 1$, so ergibt sich die Kongruenz $Y_k(a) \equiv Y_k(b) \pmod{c}$, womit (b) gezeigt ist.

Um schließlich (c) zu zeigen, wird in (14.2) $n = 1$ gesetzt und die Gleichung modulo $(a-1)$ betrachtet. Wegen $a^2 - 1 \equiv 0 \pmod{(a-1)}$ ist nur der Summand für $j = 1$ nichttrivial. Aus $X_1(a) = a \equiv 1 \pmod{(a-1)}$ und $Y_1(a) = 1$ folgt somit

$$Y_k(a) \equiv \binom{k}{1} = k \pmod{(a-1)},$$

womit (c) gezeigt ist. □

Bemerkung 14.4. *Für $a \geq 2$ folgt aus $Y_n(a)^2 \mid Y_m(a)$ stets $Y_n(a) \mid m$.*

Beweis. Wird zur Abkürzung $x_n := X_n(a)$, $y_n := Y_n(a)$ und $d := a^2 - 1$ gesetzt und durch Division mit Rest $m = kn + r$ mit $0 \leq r < n$ geschrieben, so gilt

$$\begin{aligned} x_m + y_m\sqrt{d} &= e_1^m = (e_1^n)^k e_1^r \\ &= (x_n + y_n\sqrt{d})^k (x_r + y_r\sqrt{d}) \\ &= \left(\sum_{j=0}^{k} \binom{k}{j} x_n^{k-j} y_n^j \sqrt{d}^{\,j}\right)(x_r + y_r\sqrt{d}). \end{aligned}$$

Eine Zerlegung in Summanden mit und ohne Wurzel ergibt

$$y_m\sqrt{d} = \sum_{\substack{j=0 \\ 2\,|\,j}}^{k} \binom{k}{j} x_n^{k-j} y_n^j \sqrt{d}^j y_r \sqrt{d} + \sum_{\substack{j=1 \\ 2\,\not|\,j}}^{k} \binom{k}{j} x_n^{k-j} y_n^j \sqrt{d}^j x_r,$$

woraus sich die Beziehung

$$y_m = \sum_{\substack{j=0 \\ 2\,|\,j}}^{k} \binom{k}{j} x_n^{k-j} y_n^j \sqrt{d}^j y_r + \sum_{\substack{j=1 \\ 2\,\not|\,j}}^{k} \binom{k}{j} x_n^{k-j} y_n^j \sqrt{d}^{j-1} x_r$$

ergibt. Betrachtet man diese Gleichung modulo y_n, so ist nur der Summand für $j = 0$ nichttrivial. Da nach Voraussetztung $y_n \,|\, y_m$ gilt, ergibt sich hiermit

$$0 \equiv y_m \equiv x_n^k y_r \pmod{y_n}.$$

Da jeder gemeinsame Teiler von x_n und y_n auch $\mathcal{N}(e_1^n) = \pm 1$ teilt, muß $\mathrm{ggT}\{x_n, y_n\} = 1$ gelten, was $y_n \,|\, y_r$ zur Folge hat. Da andererseits aus $r < n$ aufgrund der Monotonie auch $y_r < y_n$ folgt, ergibt sich $y_r = 0$ und damit $r = 0$, womit $m = kn$ gilt. Betrachtet man nun (14.2) modulo y_n^2, so ist nur der Summand für $j = 1$ nichttrivial. Zusammen mit der Voraussetztung ergibt sich

$$0 \equiv y_m = y_{nk} \equiv k x_n^{k-1} y_n \pmod{y_n^2},$$

woraus sich $y_n \,|\, k x_n^{k-1}$ ergibt. Aufgrund von $\mathrm{ggT}\{x_n, y_n\} = 1$ gilt nun $y_n \,|\, k$, was schließlich $y_n \,|\, m$ zur Folge hat. □

Bemerkung 14.5. *Für $a > 2$ folgt aus $Y_i(a) \equiv Y_j(a) \pmod{X_n(a)}$ stets $i \equiv \pm j \pmod{2n}$.*

Beweis. Für $n, m \in \mathbb{N}_0$ mit $n \le m$ gilt mit den Bezeichnungen aus Bemerkung 14.4 wegen $e_1^{-m} = x_m - y_m\sqrt{d}$ die Beziehung

$$x_{n\pm m} + y_{n\pm m}\sqrt{d} = e_1^{n\pm m} = e_1^n e_1^{\pm m} = (x_n + y_n\sqrt{d})(x_m \pm y_m\sqrt{d}).$$

Hieraus ergeben sich durch Zerlegung in Summanden mit und ohne Wurzel und (P_a) die folgenden Kongruenzen:

$$\begin{aligned} y_{n\pm m} = x_m y_n \pm x_n y_m &\equiv y_n x_m \pmod{x_n} && (14.3)\\ x_{n\pm m} = x_n x_m \pm y_n y_m d &\equiv \pm y_n y_m d \pmod{x_n} && (14.4)\\ 1 = x_n^2 - d y_n^2 &\equiv -d y_n^2 \pmod{x_n} && (14.5) \end{aligned}$$

Die schrittweise Anwendung von (14.3), (14.4) und (14.5) ergibt

$$y_{2n\pm m} = y_{n+(n\pm m)} \equiv y_n x_{n\pm m} \equiv \pm y_n^2 y_m d \equiv \mp y_m \pmod{x_n},$$

woraus mit der Bezeichnung

$$\mathcal{Y}_k := \{y_k \pmod{x_n}, -y_k \pmod{x_n}\}$$

die Beziehung $\mathcal{Y}_{2n\pm m} = \mathcal{Y}_m$ folgt.

Zu jedem $k \in \mathbb{N}_0$ existiert ein k^* mit $0 \le k^* \le n$, für das entweder $k \equiv k^* \pmod{2n}$ oder $k \equiv -k^* \pmod{2n}$ und damit $\mathcal{Y}_k = \mathcal{Y}_{k^*}$ gilt. Nach Voraussetzung gilt $\mathcal{Y}_i = \mathcal{Y}_j$ woraus $\mathcal{Y}_{i^*} = \mathcal{Y}_{j^*}$ und weiter

$$x_n \,|\, (y_{i^*} + y_{j^*}) \quad \text{oder } x_n \,|\, (y_{i^*} - y_{j^*})$$

folgt. Aufgrund der Monotonie gilt wegen $0 \le i^*, j^* \le n$ auch $0 \le y_{i^*}, y_{j^*} \le y_n$, und da sich aufgrund von $a \ge 3$ über die Abschätzung

$$x_n^2 = 1 + (a^2-1)y_n^2 > 8y_n^2 > 4y_n^2$$

die Beziehung $y_n < {}^1\!/_2\, x_n$ ergibt, gilt schließlich

$$|y_{i^*} \pm y_{j^*}| < 2 \cdot \frac{1}{2} x_n = x_n.$$

Da aber x_n entweder die Summe oder die Differenz teilt, folgt somit $y_{i^*} \pm y_{j^*} = 0$ und wegen $y_{j^*} \ge 0$ gilt $y_{i^*} = y_{j^*}$. Aufgrund der strengen Monotonie hat dies aber $i^* = j^*$ und damit $i \equiv \pm j \pmod{2n}$ zur Folge. □

Bemerkung 14.6. *Für $a > 2$ ist die Relation $y = Y_k(a)$ äquivalent zu der Relation $R(y,k,a)$ mit*

$$R(y,k,a): \quad \text{es gibt } x, \widetilde{x}, \approx\!\!x, \widetilde{y}, \approx\!\!y, b \quad \text{mit } R_1 \wedge R_2 \wedge \ldots \wedge R_8,$$

wobei die R_i folgende Relationen sind:

$$\begin{array}{llll} R_1: & y \ge k & R_5: & b = a + \widetilde{x}^2(\widetilde{x}^2 - a) \\ R_2: & x^2 - y^2(a^2-1) = 1 & R_6: & \overset{\approx}{x}{}^2 - \overset{\approx}{y}{}^2(b^2-1) = 1 \\ R_3: & \widetilde{y} \equiv 0 \pmod{2x^2y^2} & R_7: & \overset{\approx}{y} \equiv y \pmod{\widetilde{x}^2} \\ R_4: & \widetilde{x}^2 - \widetilde{y}^2(a^2-1) = 1 & R_8: & \overset{\approx}{y} \equiv k \pmod{2y}. \end{array}$$

Beweis. Wird $y = Y_k(a)$ vorausgesetzt, so ist die Existenz von Zahlen $x, \widetilde{x}, \overset{\approx}{x}, \widetilde{y}, \overset{\approx}{y}$ und b zu zeigen, die die Relationen R_1 bis R_8 erfüllen. Zunächst gelten wegen $y = Y_k(a) \ge k$ und mit $x := X_k(a)$ die Relationen R_1 und R_2.

Wird $f := 2x^2y^2$ gesetzt, so existieren nach Bemerkung 14.2 Zahlen x', y' mit $x'^2 - y'^2 f^2(a^2-1) = 1$. Mit $\widetilde{x} := x'$ und $\widetilde{y} := y'f$ gelten nun R_3 und R_4.

Werden b durch Relation R_5 und $\overset{\approx}{x} := X_k(b)$, $\overset{\approx}{y} := Y_k(b)$ definiert, so gelten R_5 und R_6.

Aus R_5 folgt $b \equiv a \pmod{\widetilde{x}^2}$, was nach Bemerkung 14.3 (b) die Beziehung $Y_k(b) \equiv Y_k(a) \pmod{\widetilde{x}^2}$ und damit R_7 zur Folge hat.

Nach Bemerkung 14.3 (c) gilt $\overset{\approx}{y} = Y_k(b) \equiv k \pmod{(b-1)}$. Zum Beweis der Relation R_8 reicht es also, $2y \,|\, (b-1)$ zu zeigen. Da nach R_3 aber $\widetilde{y} \equiv 0 \pmod{2y}$ gilt, ergibt sich mit R_4 die Kongruenz $\widetilde{x}^2 \equiv 1 \pmod{2y}$. Zusammen mit R_5 erhält man $b \equiv a + 1(1-a) \equiv 1 \pmod{2y}$, woraus $2y \,|\, (b-1)$ folgt.

Zum Beweis der Umkehrung sei die Relation R vorausgesetzt. Aus R_2 und Bemerkung 14.1 folgt die Existenz von $n \in \mathbb{N}$ mit $x = X_n(a)$ und $y = Y_n(a)$. Es ist also noch $n = k$ zu zeigen. Aus R_4 und R_6 folgt die Existenz von $\widetilde{n}, \overset{\approx}{n} \in \mathbb{N}$ mit

$$\widetilde{x} = X_{\widetilde{n}}(a), \; \widetilde{y} = Y_{\widetilde{n}}(a) \quad \text{und } \overset{\approx}{y} = Y_{\overset{\approx}{n}}(b).$$

Mit Bemerkung 14.3 (c) gilt $\widetilde{\widetilde{y}} = Y_{\widetilde{\widetilde{n}}}(b) \equiv \widetilde{\widetilde{n}} \pmod{(b-1)}$ und da sich wie oben aus den Relationen R_3, R_4 und R_5 die Beziehung $2y \mid (b-1)$ ergibt, folgen $\widetilde{\widetilde{y}} \equiv \widetilde{\widetilde{n}} \pmod{2y}$ und zusammen mit R_8

$$k \equiv \widetilde{\widetilde{n}} \pmod{2y}. \tag{14.6}$$

Andererseits gilt mit Relation R_5 die Beziehung $b \equiv a \pmod{\widetilde{x}}$, woraus sich zusammen mit Bemerkung 14.3 (b)

$$Y_{\widetilde{\widetilde{n}}}(b) \equiv Y_{\widetilde{\widetilde{n}}}(a) \pmod{\widetilde{x}}$$

ergibt. Da mit R_7 aber auch

$$Y_{\widetilde{\widetilde{n}}}(b) = \widetilde{\widetilde{y}} \equiv y = Y_n(a) \pmod{\widetilde{x}}$$

gilt, folgt wegen $\widetilde{x} = X_{\widetilde{n}}(a)$ somit

$$Y_n(a) \equiv Y_{\widetilde{\widetilde{n}}}(a) \pmod{X_{\widetilde{n}}(a)}.$$

Mit Bemerkung 14.5 ergibt sich hieraus

$$n \equiv \pm\widetilde{\widetilde{n}} \pmod{2\widetilde{n}}. \tag{14.7}$$

Weiter folgt mit R_3 die Beziehung $y^2 \mid \widetilde{y}$ bzw. $Y_n(a)^2 \mid Y_{\widetilde{n}}(a)$, womit sich nach Bemerkung 14.4

$$y \mid \widetilde{n} \tag{14.8}$$

ergibt. Aus (14.6), (14.7) und (14.8) folgt nun

$$k \equiv \widetilde{\widetilde{n}} \equiv \pm n \pmod{2y}.$$

Da $0 < n \leq Y_n(a) = y$ und mit R_1 die Beziehung $0 < k \leq y$ gilt, ergibt sich

$$|k \pm n| \leq 2y.$$

Im Falle $k \equiv -n \pmod{2y}$ folgt somit $k + n = 2y$ und damit $n = k = y$, während sich im Falle $k \equiv n \pmod{2y}$ direkt $k = n$ ergibt. □

Satz 14.1. *Die Relationen $a > 2 \wedge x = X_n(a)$ und $a > 2 \wedge y = Y_n(a)$ sind diophantisch.*

Beweis. Die Relation $a > 2 \wedge y = Y_n(a)$ ist nach Bemerkung 14.6 äquivalent zu $R(y, k, a) \wedge a > 2$, die nach den Bemerkungen 13.2 und 13.2 diophantisch ist.

Die Relation $a > 2 \wedge x = X_n(a)$ andererseits ist äquivalent zu $a > 2 \wedge y = Y_n(a) \wedge x^2 - (a^2-1)y^2 = 1$ und damit diophantisch. □

14.3 Anwendung auf die Potenzfunktion

Bemerkung 14.7. *Für $a \geq 2$ und $a \geq n$ gilt*

$$n^k \equiv X_k(a) - (a-n)Y_k(a) \pmod m \quad \text{mit } m = 2an - n^2 - 1.$$

Beweis. Der Beweis erfolgt durch Induktion nach k. Wie oben sei zur Abkürzung $x_n := X_n(a)$, $y_n := Y_n(a)$ und $d := a^2 - 1$ gesetzt.

Für $k = 0$ gilt die Behauptung wegen $n^0 = 1$, $x_0 = 1$ und $y_0 = 0$ trivialerweise.

Für der Induktionsschluß beachtet man die Zerlegung von

$$\begin{aligned} x_{k+1} + y_{k+1}\sqrt{d} &= e_1^{k+1} \\ &= (x_k + y_k\sqrt{d})(a+\sqrt{d}) \\ &= ax_k + (a^2-1)y_k + (x_k + ay_k)\sqrt{d}, \end{aligned}$$

in Anteile mit und ohne Wurzel, woraus die Darstellungen

$$x_{k+1} = ax_k + (a^2-1)y_k \quad \text{und } y_{k+1} = x_k + ay_k$$

folgen. Somit ergibt sich mit der Induktionsvoraussetzung wegen

$$\begin{aligned} x_{k+1} - (a-n)y_{k+1} &= ax_k + (a^2-1)y_k + (n-a)(x_k + ay_k) \\ &= nx_k + (na-1)y_k \\ &\equiv n(n^k + (a-n)y_k) + (na-1)y_k \\ &= n^{k+1} + (2an - n^2 - 1)y_k \\ &= n^{k+1} + my_k \\ &\equiv n^{k+1} \pmod m \end{aligned}$$

die Behauptung. □

Satz 14.2. *Die Potenzfunktion $\mathbb{N}^2 \longrightarrow \mathbb{N}$ mit $(n,k) \mapsto n^k$ ist diophantisch.*

Beweis. Betrachtet man die Pellsche Gleichung (P_{n+2}), so gilt $e_1 = n+2+\sqrt{(n+2)^2-1} > n+1$. Hieraus folgt

$$\begin{aligned} a &:= X_k(n+2) + (n+2)Y_k(n+2) \;>\; X_k(n+2) + \sqrt{(n+2)^2-1}\,Y_k(n+2) \\ &= e_1^k \;>\; (n+1)^k, \end{aligned}$$

womit sich für $k \geq 1$

$$\begin{aligned} m &:= (a-n)n + an - 1 \;>\; ((n+1)^k - n)n + (n+1)^k n - 1 \\ &> (n+1)^k n \;>\; n^k \end{aligned}$$

ergibt. Nach Bemerkung 14.7 ist die Relation $z = n^k$ somit äquivalent zu der Relation

$$\begin{gathered} z \equiv X_k(a) - (a-n)Y_k(a) \pmod m \\ \wedge\, m = (a-n)n + an - 1 \;\wedge\; z < m \\ \wedge\, a = X_k(n+2) + (n+2)Y_k(n+2), \end{gathered}$$

die wiederum mit der folgenden Relationen gleichbedeutend ist

$$\begin{aligned}
&z \equiv x-(a-n)y \pmod m \ \wedge\ x = X_k(a) \wedge y = Y_k(a)\\
&\wedge\, m = (a-n)n + an - 1 \ \wedge\ z < m\\
&\wedge\, a = u + (n+2)v \ \wedge\ u = X_k(n+2) \ \wedge\ v = Y_k(n+2),
\end{aligned}$$

und da alle Konjunktionsglieder diophantisch sind, ist $z = n^k$ eine diophantische Relation bzw. $(n,k) \mapsto n^k$ eine diophantische Abbildung. □

Anmerkung: Dieses Ergebnis zeigt, daß die Exponentialfunktion n^k polynomialer Natur ist.

15 Der beschränkte Allquantor

15.1 Der Produktsatz

Bemerkung 15.1. *Die Relation* $n \geq k \ \wedge\ z = \binom{n}{k}$ *ist diophantisch.*

Beweis. Wählt man eine beliebige Hilfszahl $m \in \mathbb{N}$ mit $m > 2^n$, so gilt

$$\frac{(m+1)^n}{m^k} = \frac{\sum_{j=0}^n \binom{n}{j} m^j}{m^k} = \sum_{j=k+1}^{n} \binom{n}{j} m^{j-k} + \binom{n}{k} + r$$

mit

$$r = \sum_{j=0}^{k-1} \binom{n}{j} \frac{1}{m^{k-j}} \leq \frac{1}{m} \sum_{j=0}^{k-1} \binom{n}{j} \leq \frac{1}{m} \sum_{j=0}^{n} \binom{n}{j} \leq \frac{1}{m}(1+1)^n = \frac{2^n}{m} < 1,$$

womit sich

$$\left[\frac{(m+1)^n}{m^k}\right] \equiv \binom{n}{k} \pmod m \tag{15.1}$$

ergibt. Wegen $\binom{n}{k} \leq 2^n < m$ ist somit gezeigt, daß die Relation

$$R_1 : n \geq k \ \wedge\ z = \binom{n}{k}$$

die Relation

$$R_2 : n \geq k \ \wedge\ m > 2^n \ \wedge\ z < m \ \wedge\ z \equiv \left[\frac{(m+1)^n}{m^k}\right] \pmod m$$

zur Folge hat. Gilt umgekehrt R_2, so hat (15.1) $z \equiv \binom{n}{k} \pmod m$ zur Folge, womit sich wegen $z < m$ und $\binom{n}{k} \leq 2^n < m$ die Relation R_1 ergibt. Nach Satz 14.2, Bemerkung 13.2 und den Beispielen 13.3 und 13.4 ist die Relation R_2 diophantisch, womit die Behauptung gezeigt ist. □

Bemerkung 15.2. *Die Relation $z = n!$ ist diophantisch.*

Beweis. Es sei $m \in \mathbb{N}$ eine Hilfszahl mit $m > (2n)^{n+1}$. Wegen Bemerkung 15.1 genügt es,

$$n! = [x] \quad \text{mit } x := \frac{m^n}{\binom{m}{n}}$$

zu zeigen. Aufgrund von

$$\begin{aligned} x &= \frac{m^n n!}{m(m-1)\cdots(m-n+1)} \\ &= n! \frac{m}{m} \frac{m}{m-1} \cdots \frac{m}{m-n+1} \\ &= n! \cdot 1 \cdot (1-\frac{1}{m})^{-1}(1-\frac{2}{m})^{-1} \cdots (1-\frac{n-1}{m})^{-1} \end{aligned}$$

ergibt sich die Abschätzung $x > n!$. Da für jedes $\delta \in \mathbb{R}$ mit $0 < \delta < {}^1/_2$ stets $(1-\delta)^{-1} \leq 1 + 2\delta$ gilt, folgt andererseits

$$\begin{aligned} x &= n! \cdot 1 \cdot (1-\frac{1}{m})^{-1}(1-\frac{2}{m})^{-1} \cdots (1-\frac{n-1}{m})^{-1} \\ &\leq n! \cdot 1 \cdot (1+\frac{2}{m})(1+\frac{4}{m})^{-1} \cdots (1+\frac{2(n-1)}{m})^{-1} \\ &< n!(1+\frac{2n}{m})^n \\ &= n! \sum_{j=0}^{n} \binom{n}{j} (\frac{2n}{m})^j \leq n!(1+\frac{2n}{m}\sum_{j=1}^{n}\binom{n}{j}) \\ &\leq n!(1+\frac{2n}{m}2^n) < n!(1+\frac{2n2^n}{(2n)^{n+1}}) \\ &\leq n!(1+\frac{1}{n^n}) < n!+1, \end{aligned}$$

womit $n! = [x]$ gezeigt ist. □

Satz 15.1 (Produktsatz). *Die Relation $R(a,b,y,z) : z = \prod_{n=1}^{y}(a+bn)$ ist diophantisch.*

Beweis. Wird zunächst

$$m := (a+by)! + 1 > \prod_{n=1}^{y}(a+bn) = z$$

gesetzt, so gilt wegen $b \,|\, (a+by)!$ die Beziehung $\mathrm{ggT}\{m,b\} = 1$. Also existiert (nach Folgerung 2.2) ein $q \in \mathbb{N}$ mit $bq \equiv a \pmod m$, womit sich

$$z \equiv \prod_{n=1}^{y}(bq+bn) = b^y \prod_{n=1}^{y}(q+n) \pmod m$$

ergibt. Somit ist gezeigt, daß die Relation

$$R(a,b,y,z) : z = \prod_{n=1}^{y} (a+bn)$$

die Relation

$$\begin{aligned} \tilde{R}(a,b,y,z) \quad : \quad & m = (a+by)! + 1 \\ & \wedge\, z \equiv b^y \prod_{n=1}^{y} (q+n) \pmod{m} \;\wedge\; z < m \;\wedge\; bq \equiv a \pmod{m} \end{aligned}$$

zur Folge hat.

Gilt umgekehrt $\tilde{R}$, so folgt

$$z \equiv b^y \prod_{n=1}^{y} (q+n) = \prod_{n=1}^{y} (bq+bn) \equiv \prod_{n=1}^{y} (a+bn) \pmod{m},$$

womit sich wegen $z < m$ und $\prod_{n=1}^{y}(a+bn) < m$ die Relation R ergibt. Nach Bemerkung 15.2 ist die Relation

$$x = \prod_{n=1}^{y} (q+n) = \frac{(q+y)!}{q!}$$

diophantisch, womit auch $\tilde{R}$ diophantisch ist. □

Folgerung 15.1. *Die Relation $c \geq d \;\wedge\; z = \prod_{n-1}^{d}(c-n)$ ist diophantisch.*

Beweis. Im Falle $c \geq d+2$ ergibt sich nach Satz 15.1 mit $y = d$, $b = 1$ und $a = c-d-1$ die diophantische Relation

$$z = \prod_{n=1}^{d} (c-d-1+n) = (c-d)\cdots(c-1) = \prod_{n=1}^{d} (c-n),$$

während sich im Falle $c = d+1$ die nach Bemerkung 15.2 diophantische Relation

$$z = \prod_{n=1}^{d} (d+1-n) = d!$$

und für $c = d$ die diophantische Relation $z = 0$ ergibt. Die Behauptung ergibt sich nun mit Bemerkung 13.2. □

15.2 Der Satz über den beschränkten Allquantor

Ziel dieses Abschnitts ist es zu zeigen, daß der beschränkte Allquantor diophantische Relationen erhält.

Definition 15.1. Ist $R(k,y,x_1,\ldots,x_r)$ eine Relation zwischen natürlichen Zahlen, so sei die Relation
$$R'(y,x_1,\ldots,x_r) : \forall k \leq y : \quad R(k,y,x_1,\ldots,x_r)$$
definiert als
$$\text{für alle } k \text{ gilt } R(k,y,x_1,\ldots,x_r) \ \vee \ k > y.$$
Hierin heißt $\forall k \leq y :$ **beschränkter Allquantor**.

Bezeichnung: Im folgenden sei f ein festes Polynom aus $\mathbb{Z}[K,Y,X_1,\ldots,X_r,Z_1,\ldots,Z_s]$, weiter sei $\underline{X} := (X_1,\ldots,X_n)$, $\underline{Z} := (Z_1,\ldots,Z_s)$ und für $z_1 \leq u, z_2 \leq u, \ldots, z_s \leq u$ werde kurz $\underline{z} := (z_1,\ldots,z_s) \leq u$ geschrieben.

Bemerkung 15.3. *Die folgenden Relationen sind äquivalent:*

(a) $\forall k \leq y :$ es gibt $\underline{z} \in \mathbb{N}^s$ mit $f(k,y,\underline{x},\underline{z}) = 0$,

(b) es gibt $u \in \mathbb{N}$ mit $\forall k \leq y :$ es gibt $\underline{z} \in \mathbb{N}^s$ mit $\underline{z} \leq u \ \wedge \ f(k,y,\underline{x},\underline{z}) = 0$.

Beweis. Die Aussage (b) impliziert (a) trivialerweise. Gilt umgekehrt Relation (a), so gibt es für jedes $k \leq y$ ein $\underline{z}^{(k)} \in \mathbb{N}^s$ mit $f(k,y,\underline{x},\underline{z}) = 0$. Daher folgt (b) mit
$$u := \max\left\{ z_i^{(k)} \mid 1 \leq k \leq y,\ 1 \leq i \leq s \right\}. \qquad \square$$

Bemerkung 15.4. *Es gibt ein Polynom $g \in \mathbb{Z}[Y,\underline{X},U]$ mit*
$$(\forall k \leq y : \quad \forall \underline{z} \leq u : \quad |f(k,y,\underline{x},\underline{z})| \leq g(y,\underline{x},u)) \ \wedge \ g(y,\underline{x},u) > \max\left\{y,u\right\}.$$

Beweis. Wird $f = \sum_{i=1}^m f_i$ in Monome
$$f_i(K,Y,\underline{X},\underline{Z}) = c_i K^{a_i} Y^{b_i} \underline{X}^{\underline{e}_i} \underline{Z}^{\underline{n}_i} \quad \text{mit } c_i \in \mathbb{Z},\ a_i, b_i \in \mathbb{N}_0\,,\ \underline{e}_i \in \mathbb{N}_0^r\,,\ \underline{n}_i \in \mathbb{N}_0^s$$
zerlegt, und wird g durch
$$g_i(Y,\underline{X},U) := |c_i|\, Y^{a_i+b_i} \underline{X}^{\underline{e}_i} U^{n_i} \quad \text{mit } n_i := \sum_{j=1}^{r} n_{ji}$$
$$g(Y,\underline{X},U) := Y + U + \sum_{i=1}^{m} g_i(Y,\underline{X},U)$$
definiert, so gelten
$$g(y,\underline{x},u) \geq y + u > \max\left\{y,u\right\}$$
und
$$\forall k \leq y : \quad \forall \underline{z} \leq u : \quad |f(k,y,\underline{x},\underline{z})| \leq \sum_{i=1}^{m} |f_i(k,y,\underline{x},\underline{z})| \leq \sum_{i=1}^{m} g_i(y,\underline{x},u) < g(y,\underline{x},u). \qquad \square$$

Bemerkung 15.5. *Die folgenden Relationen sind äquivalent:*

(a) $Q(y,\underline{x},u) : \forall k \leq y :$ es gibt $\underline{z} \in \mathbb{N}^s$ mit $\underline{z} \leq u \ \wedge \ f(k,y,\underline{x},\underline{z}) = 0$

(b) $\widetilde{Q}(y,\underline{x},u)$: es gibt $\underline{a} \in \mathbb{N}^s$, $t,m,l \in \mathbb{N}$ mit $R_1 \wedge \ldots \wedge R_6$

mit den folgende Relationen R_i*:*

$R_1:$	$t = g(y,\underline{x},u)!$	$R_4:$	$\underline{a} \geq u$
$R_2:$	$m \equiv \prod_{k=1}^{y}(1+kt)$	$R_5:$	$f(l,y,\underline{x},\underline{a}) \equiv 0 \pmod m$
$R_3:$	$m = 1 + lt$	$R_6:$	$m \mid \prod_{j=1}^{u}(a_i - j)$ für $i = 1,\ldots,s.$

wobei g *wie in Bemerkung 15.4 durch* f *definiert ist.*

Beweis. Zunächst gelte die Relation Q. Werden t und m wie in den Relationen R_1 und R_2 definiert, so gelten R_1 und R_2 und wegen $m \equiv 1 \pmod t$ gibt es ein $l \in \mathbb{N}$ mit $m - 1 = lt$, womit R_3 gilt.

Nun soll gezeigt werden, daß $m = \mathrm{kgV}\{\, 1 + kt \mid 1 \leq k \leq y \,\}$ gilt. Gibt es für $1 \leq k, \widetilde{k} \leq y$ eine Primzahl p mit $p \mid (1+kt)$ und $p \mid (1+\widetilde{k}t)$, so gelten $p \mid (\widetilde{k}-k)t$ und $p \nmid t$. Da p Primzahl ist, folgt hieraus aber $p \mid (\widetilde{k}-k)$ mit $p \leq \widetilde{k} - k < y$. Da nach Definition von g aber $y < g(y,\underline{x},u)$ gilt, ergibt sich der Widerspruch

$$p \mid g(y,\underline{x},u)! = t.$$

Daher gilt $\mathrm{ggT}\{1+kt, 1+\widetilde{k}t\} = 1$, womit $m = \mathrm{kgV}\{\, 1+kt \mid 1 \leq k \leq y \,\}$ gezeigt ist. Nach Voraussetzung gibt es zu jedem $k \leq y$ ein $\underline{z}^{(k)} \in \mathbb{N}^s$ mit $\underline{z}^{(k)} \leq u$ und $f(k,y,\underline{x},\underline{z}^{(k)}) = 0$, und nach dem Hauptsatz über simultane Kongruenzen 4.1 gibt es für jedes $i = 1,\ldots,s$ eine Zahl a_i mit

$$z_1^{(k)} \equiv a_i \pmod{(1+kt)}. \tag{15.2}$$

Da zu a_i beliebige Vielfache von m addiert weden können, kann dabei ohne Einschränkung $a_i \geq u$ vorausgesetzt werden kann, womit R_4 gilt. Betrachtet man für $k = 1,\ldots,y$ die Relation R_3 modulo $1+kt$, so ergibt sich $1 + kt \equiv 0 \equiv 1 + lt \pmod{(1+kt)}$, was wegen $t \nmid (1+kt)$ die Beziehung $k \equiv l \pmod{(1+kt)}$ zur Folge hat. Damit gilt

$$0 = f(k,y,\underline{x},\underline{z}^{(k)}) \equiv f(l,y,\underline{x},\underline{a}) \pmod{(1+kt)} \quad \text{für } k = 1,\ldots,y,$$

was nach dem Hauptsatz über simultane Kongruenzen die Relation R_5 zur Folge hat.

Da nach 15.2 für $k = 1,\ldots,y$ und $i = 1,\ldots,s$ die Beziehung

$$(1+kt) \mid (a_i - z_i^{(k)})$$

mit $a_i \geq u$ und $z_i^{(k)} \leq u$ gilt, folgt

$$(1+kt) \mid \prod_{j=1}^{u}(a_i - j),$$

womit sich R_6 ergibt.

Nun sei Relation $\widetilde{Q}$ vorausgesetzt. Für ein festes k mit $k \leq y$ sei p eine Primzahl mit $p \mid (1+kt)$. Nach R_2 und R_3 gilt somit $1 + lt \equiv 0 \pmod{(1+kt)}$, womit sich wie oben $l \equiv k \pmod p$ ergibt. Schreibt man durch Division mit Rest

$$a_i = q_i p + z_i \quad \text{mit } 0 < z_i \leq p, \tag{15.3}$$

hat dies wegen $p \mid m$ zusammen mit R_5

$$f(k, y, \underline{x}, \underline{z}) \equiv 0 \pmod{p} \tag{15.4}$$

zur Folge. Aus der Annahme $p \leq g(y, \underline{x}, u)$ ergibt sich mit R_1 die Beziehung $p \mid t$, was im Widerspruch zu $p \mid (1 + kt)$ steht. Also gilt zusammen mit Bemerkung 15.4

$$p > g(y, \underline{x}, u) > \max\{y, u\}, \tag{15.5}$$

und mit der Abschätzung

$$|f(k, y, \underline{x}, \underline{z})| \leq g(y, \underline{x}, u)$$

aus Bemerkung 15.4 und (15.4) folgt

$$f(k, y, \underline{x}, \underline{z}) = 0.$$

Weiter gilt wegen $p \mid m$ und R_6 die Beziehung

$$p \mid \prod_{j=1}^{u} (a_i - j),$$

und da p Primzahl ist, gibt es ein $j \in \{1, \ldots, u\}$ mit $p \mid (a_i - j)$. Dies hat $a_i \equiv j \pmod{p}$ und mit (15.3) die Kongruenz $z_i \equiv j \pmod{p}$ zur Folge. Da aber nach (15.3) und (15.5) die Abschätzungen

$$1 \leq z_i \leq p$$
$$1 \leq j \leq u < g(y, \underline{x}, u) < p$$

gelten, ergibt sich somit $z_i = j$, womit $\underline{z} \leq u$ folgt. □

Satz 15.2. *Ist $R(k, y, \underline{x})$ eine diophantische Relation, so ist auch*

$$Q(y, \overline{x}) : \forall k \leq y : \quad R(k, y, \underline{x})$$

eine diophantische Relation.

Beweis. Ist die zu R gehörende diophantische Menge

$$\pi_{2+r} \mathrm{V}_f \quad \text{mit } f \in \mathbb{Z}[K, Y, X_1, \ldots, X_r, Z_1, \ldots, Z_s],$$

so ist $Q(y, \overline{x})$ gleichbedeutend mit mit

$$\forall k \leq y : \quad \text{es gibt } \underline{z} \in \mathbb{N}^s \text{ mit } f(k, y, \underline{x}, \underline{z}) = 0.$$

Nach den Bemerkungen 15.3 und 15.5 ist dies äquivalent zu der Relation

$$\text{es gibt } u \in \mathbb{N} \text{ mit } \widetilde{Q}(y, \underline{x}, u),$$

wobei $\widetilde{Q}$ wie in Bemerkung 15.5 definiert ist. Nun sind R_1 (Bemerkung 15.2), R_2 (Satz 15.1), R_3 bis R_5 (Paragraph 13) und R_6 (Folgerung 15.1) diophantisch, und mit Bemerkung 13.2 folgt, daß $\widetilde{Q}$ und damit auch Q diophantische Relationen sind. □

15.3 Die Menge der Primzahlen

Satz 15.3. *Die Menge $\mathbb{P}$ der Primzahlen ist diophantisch.*

Beweis. Die Relation $p \in \mathbb{P}$ ist äquivalent zu

$$\forall y \leq p: \quad (y = 1 \ \vee \ y = p \ \vee \ y \not| p),$$

und da $y \not| p$ gleichbedeutend ist mit

$$\forall x \leq p: \quad yx \neq p,$$

folgt die Behauptung aus dem Vorausgehenden. □

Bemerkung 15.6. *Ist $D \subseteq \mathbb{N}$ eine diophantische Menge, so gibt es ein Polynom $g \in \mathbb{Z}[X_1, \ldots, X_n]$ mit $D = g(\mathbb{N}^n) \cap \mathbb{N}$.*

Beweis. Es sei $D = \pi_1(\mathrm{V}_f)$ mit $f \in \mathbb{Z}[X_1, \ldots, X_n]$ und

$$g(X_1, \ldots, X_n) := X_1(1 - f(\underline{X})^2).$$

Gilt nun $x_1 \in D \subseteq \mathbb{N}$, so gibt es $x_2, \ldots, x_n \in \mathbb{N}$ mit $f(x_1, \ldots, x_n) = 0$, womit $g(x_1, \ldots, x_n) = x_1$ und damit $x_1 \in g(\mathbb{N}^n)$ folgt.

Gilt umgekehrt $z \in g(\mathbb{N}^n) \cap \mathbb{N}$, so gibt es ein $\underline{x} \in \mathbb{N}^n$ mit $z = g(\underline{x})$. Wegen $x_1 \in \mathbb{N}$ hat dies $1 - f(\underline{x}) \in \mathbb{N}$ und damit $f(\underline{x}) = 0$ zur Folge. Somit gilt $z = x_1 \in \pi_1(\mathrm{V}_f) = D$. □

Folgerung 15.2. *Es gibt ein Polynom $g(X_1, \ldots, X_n) \in \mathbb{Z}[X_1, \ldots, X_n]$, dessen positiven Werte genau die Primzahlen sind.*

Anmerkung: Ein solches Primzahlpolynom wird im abschließenden Paragraphen 17 konstruiert.

16 Rekursive Funktionen

16.1 Die Gödelsche Folgenfunktion

Definition 16.1. Die Abbildung $P : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ mit

$$(x, y) \mapsto \Delta(x + y - 2) + x \quad \text{mit } \Delta(z) := 1 + 2 + \cdots + z = \frac{z(z+1)}{2}$$

heißt **Cantorsche Paarabbildung**.

Anmerkung: Die Cantorsche Paarabbildung ist eine bijektive Abbildung von $\mathbb{N} \times \mathbb{N}$ nach $\mathbb{N}$.

Bemerkung 16.1. *Die Cantorsche Paarabbildung $P : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ und ihre Umkehrabbildung $P^{-1} : \mathbb{N} \longrightarrow \mathbb{N} \times \mathbb{N}$ mit $z \longrightarrow (L(z), R(z))$ sind diophantisch. Ferner gelten $L(z) \leq z$ und $R(z) \leq z$.*

Beweis. Wegen $2P = (X+Y-2)(X+Y-1) + 2X \in \mathbb{Z}[X,Y]$ ist P eine diophantische Abbildung und mit $z = P(x,y)$ gelten $L(z) \leq z$ und $R(z) \leq z$. Da die Relationen $x = L(z)$ und $y = R(z)$ äquivalent sind zu

$$\begin{array}{llll} \text{es gibt } y \in \mathbb{N} & \text{mit } z = P(x,y) & \text{und } x \leq z & \text{bzw.} \\ \text{es gibt } x \in \mathbb{N} & \text{mit } z = P(x,y) & \text{und } y \leq z, & \end{array}$$

sind $L(z)$ und $R(z)$ diophantisch. □

Definition 16.2. Die Abbildung $F : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ mit

$$(k,m) \mapsto L(m) \pmod{(1 + kR(m))} \quad \text{mit } 1 \leq L(m) \leq 1 + kR(m)$$

heißt **Gödelsche Folgenfunktion**.

Satz 16.1. *Die Gödelsche Folgenfunktion ist diophantisch und hat die folgenden Eigenschaften:*

(a) Für alle $k, m \in \mathbb{N}$ gilt $F(k,m) \leq m$.

(b) Für alle $\underline{a} \in \mathbb{N}^n$ gibt es ein $m \in \mathbb{N}$, so daß $F(k,m) = a_k$ für $k = 1, \ldots, n$ gilt.

Beweis. Nach Bemerkung 16.1 ist F diophantisch und es gilt $F(k,m) \leq L(m) \leq m$, womit (a) gezeigt ist.

Wird $y := n! a_1 \cdot \ldots \cdot a_n$ gesetzt, so gilt $\mathrm{ggT}\{\, 1 + ky \mid 1 \leq k \leq n \,\} = 1$, denn gibt es für $1 \leq k < \widetilde{k} \leq n$ eine Primzahl p mit $p \mid (1+ky)$ und $p \mid (1 + \widetilde{k}y)$, so gelten $p \mid (\widetilde{k} - k)y$ und $p \nmid y$. Da p Primzahl ist, folgt hieraus aber $p \mid (\widetilde{k} - k)$ mit $p \leq \widetilde{k} - k < n$, was den Widerspruch $p \mid y$ zur Folge hat.

Nach dem Satz über simultane Kongruenzen gibt es ein $x \in \mathbb{N}$ mit $x \equiv a_k \pmod{(1 + ky)}$ für $k = 1, \ldots, n$. Wird nun $m := P(x,y)$ gesetzt, so gilt

$$F(k,m) \equiv L(m) = x \equiv a_k \pmod{(1+ky)} \quad \text{mit } 1 \leq a_k \leq y = R(m) < 1 + kR(m) = 1 + ky,$$

womit $a_k = F(k,m)$ gezeigt ist. □

16.2 Definition rekursiver Funktionen

Definition 16.3. Die Funktionen

$$\begin{array}{llll} \mathrm{C} & : \mathbb{N} \longrightarrow \mathbb{N}, & x \mapsto 1 & \text{(konstante Funktion)} \\ \mathrm{S} & : \mathbb{N} \longrightarrow \mathbb{N}, & x \mapsto x + 1 & \text{(Nachfolgerfunktion)} \\ \mathrm{P}_{n,k} & : \mathbb{N}^n \longrightarrow \mathbb{N}, & (x_1, \ldots, x_n) \mapsto x_k & \text{(Projektionen)} \\ F & : \mathbb{N}^2 \longrightarrow \mathbb{N}, & & \text{(Gödelsche Funktion)} \end{array}$$

heißen **rekursive Grundfunktionen**

Anmerkung: Auf F kann auch verzichtet werden.

Bemerkung 16.2. *Die rekursiven Grundfunktionen lassen sich in endlich vielen Rechenschritten auswerten.*

Beweis. Für C, S und $\mathrm{P}_{n,k}$ ist die Behauptung klar. Da $x = L(m)$ äquivalent ist zu

$$x \leq m \;\wedge\; \text{ es gibt } y \leq m \text{ mit } m = P(x,y),$$

ist $L(m)$ in endlich vielen Schritten auswertbar. Analoges gilt für $R(m)$, und schließlich läßt sich $F(k,m)$ aus $R(m)$ und $L(m)$ in endlich vielen Rechenschritten durch den Euklidischen Algorithmus auswerten. □

Definition 16.4. (a) Sind $f : \mathbb{N}^n \longrightarrow \mathbb{N}$ und $g := (g_1, \ldots, g_n)$ mit $g_k : \mathbb{N}^m \longrightarrow \mathbb{N}$ Funktionen, so heißt $h = f \circ g : \mathbb{N}^m \longrightarrow \mathbb{N}$ mit

$$h(\underline{x}) = h(x_1, \ldots, x_m) := f(g_1(x_1, \ldots, x_m), \ldots, g_n(x_1, \ldots, x_m))$$

Komposition von f und g.

(b) Sind $f : \mathbb{N}^n \longrightarrow \mathbb{N}$ und $g : \mathbb{N}^{n+2} \longrightarrow \mathbb{N}$ Funktionen, so heißt $h : \mathbb{N}^{n+1} \longrightarrow \mathbb{N}$ mit

$$\begin{aligned} h(1, \underline{x}) &:= f(\underline{x}) \\ h(t+1, \underline{x}) &:= g(t, h(t, \underline{x}), \underline{x}) \end{aligned}$$

primitive Rekursion von f und g.

(c) Sind $f, g : \mathbb{N}^{n+1} \longrightarrow \mathbb{N}$ Funktionen mit der Eigenschaft, daß es für alle $\underline{x} \in \mathbb{N}$ ein $y \in \mathbb{N}$ mit $f(\underline{x}, y) = g(\underline{x}, y)$ gibt, so heißt $h : \mathbb{N}^n \longrightarrow \mathbb{N}$ mit

$$h(\underline{x}) := \min \{\, y \in \mathbb{N} \mid f(\underline{x}, y) = g(\underline{x}, y) \,\}$$

Minimalisierung von f und g.

Komposition, primitive Rekursion und Minimalisierung heißen **rekursive Grundoperationen**. Eine Funktion heißt **rekursiv**, wenn sie durch Anwendung endlich vieler rekursiver Grundoperationen aus den rekursiven Grundfunktionen erhalten wird.

Bemerkung 16.3. *Rekursive Funktionen lassen sich in endlich vielen Rechenschritten auswerten.*

Beweis. Nach Bemerkung 16.2 genügt es zu zeigen, daß Funktionen, die in endlich vielen Rechenschritten ausgewertet werden können, bei Anwendung der rekursiven Grundoperationen wieder in solche übergehen.

(a) Komposition: Sind f und $g_1, \ldots, g_n$ endlich berechenbar, so ist auch $f \circ g$ endlich berechenbar.

(b) Primitive Rekursion: Sind f und g endlich berechenbar, so ist $h(1, \underline{x}) = f$ und mit $h(t, \underline{x})$ auch $h(t+1, \underline{x})$ endlich berechenbar. Die Behauptung folgt nun durch Induktion.

(c) Minimalisierung: Sind f und g endlich berechenbar, so wird für $y = 1, 2, \ldots$ geprüft, ob $f(\underline{x}, y) = g(\underline{x}, y)$ gilt. Nach Voraussetzung tritt dies nach endlich vielen Schritten ein, womit $y = h(\underline{x})$ endlich berechenbar ist. □

Anmerkung: Die Auswertungsvorschrift einer rekursiven Funktion heißt **Algorithmus**. Die Umkehrung von Bemerkung 16.3 („Jede endlich berechenbare Funktion ist rekursiv“) wird als **Church'sche These** bezeichnet.

16.3 Der Hauptsatz

Satz 16.2. *Eine Funktion ist genau dann diophantisch, wenn sie rekursiv ist.*

Beweis.

(a) Behauptung 1: Eine rekursive Funktion ist diophantisch.

Die Grundfunktionen C , S und $\mathrm{P}_{n,k}$ sind diophantisch nach Paragraph 13, und F ist rekursiv nach Satz 16.1. Es genügt also zu zeigen, daß diophantische Funktionen bei Anwendung der rekursiven Grundoperationen wieder in solche übergehen:

(i) Komposition: nach Folgerung 13.1.

(ii) Primitive Rekursion: Es seien f und g diophantische Funktionen und h die primitive Rekursion von f und g. Nach Satz 16.1 gibt es ein $m \in \mathbb{N}$ mit

$$h(1, \underline{x}) = F(1, m), \ldots, h(n, \underline{x}) = F(n, m),$$

und damit ist $y = h(n, \underline{x})$ gleichbedeutend mit

$$\begin{aligned} \text{es gibt } m \in \mathbb{N} \quad \text{mit} \quad & F(1, m) = f(\underline{x}) \ \wedge \ F(n, m) = y \ \wedge \\ & \forall t < n: \ \ F(t+1, m) = g(t, F(t, m), \underline{x}), \end{aligned}$$

wobei alle auftretenden Relationen diophantisch sind.

(iii) Minimalisierung: Ist h die Minimalisierung zweier diophantischer Funktionen f und g, so ist $y = h(\underline{x})$ gleichbedeutend mit

$$f(\underline{x}, y) = g(\underline{x}, y) \ \wedge \ \forall t < y: \ \ f(\underline{x}, t) \neq g(\underline{x}, t),$$

wobei alle auftretenden Relationen diophantisch sind.

(b) Behauptung 2: Polynomfunktionen $f \in \mathbb{N}[\underline{X}]$ sind rekursiv.

(i) Die Addition $\mathrm{Ad}(x, y) = x + y$ kann durch

$$\begin{aligned} \mathrm{Ad}(x, 1) &:= x + 1 = \mathrm{S}(x) \\ \mathrm{Ad}(x, t+1) &:= x + t + 1 \\ &= \mathrm{Ad}(x, t) + 1 = g(t, \mathrm{Ad}(x, t), x) \quad \text{mit } g = \mathrm{S} \circ \mathrm{P}_{3,2} \end{aligned}$$

definiert werden und ist damit rekursiv.

(ii) Die Multiplikation $\mathrm{Mu}(x, y) = xy$ kann durch

$$\begin{aligned} \mathrm{Mu}(x, 1) &:= x = \mathrm{P}_{1,1}(x) \\ \mathrm{Mu}(x, t+1) &:= xt + x \\ &= \mathrm{Mu}(x, t) + x = g(t, \mathrm{Mu}(x, t), x) \quad \text{mit } g = \mathrm{Ad} \circ (\mathrm{P}_{3,2}, \mathrm{P}_{3,3}) \end{aligned}$$

definiert werden und ist damit rekursiv.

(iii) Die konstanten Funktionen $\mathrm{C}_k(x) = k$ können durch Induktion als

$$\begin{aligned} \mathrm{C}_1(x) &:= \mathrm{C}(x) \\ \mathrm{C}_{k+1}(x) &:= k+1 \\ &= \mathrm{C}_k(x) + 1 = (\mathrm{Ad} \circ (\mathrm{C}_k, \mathrm{C}_1))(x) \end{aligned}$$

definiert werden und sind damit rekursiv.

Jedes Polynom $f \in \mathbb{N}[\underline{X}]$ ist durch endlich Anwendung von C_k, Mu und Ad aus den Projektionen $\mathrm{P}_{n,k}$ zu erhalten und damit rekursiv.

(c) Behauptung 3: Diophantische Funktionen sind rekursiv.

Ist $f \in \mathbb{Z}[\underline{X}]$ eine diophantische Funktion, so ist $f(\underline{x}) = y$ gleichbedeutend damit, daß es ein Polynom $g \in \mathbb{Z}[\underline{X}, Y, \underline{Z}]$ und $\underline{z} = (z_1, \ldots, z_s)$ mit $g(\underline{x}, y, \underline{z}) = 0$ gibt. Eine Zerlegung in Anteile mit positiven und negativen Koeffizienten zeigt die Existenz zweier Polynome $p, q \in \mathbb{N}[\underline{X}, Y, \underline{Z}]$ mit $p(\underline{x}, y, \underline{z}) = q(\underline{x}, y, \underline{z})$, wobei p und q nach Behauptung 2 rekursiv sind. Nach Satz 16.1 gibt es ein $m \in \mathbb{N}$ mit

$$F(1,m) = y \ \wedge \ F(2,m) = z_1 \wedge, \ldots, \ \wedge F(s+1,m) = z_s.$$

Wird also

$$\widetilde{p}(m, \underline{x}) := p(\underline{x}, F(1,m), \ldots, F(s+1,m))$$

gesetzt, so ist $\widetilde{p}$ rekursiv. Definiert man $\widetilde{q}$ auf analoge Weise durch q, so ist

$$M(\underline{x}) := \min \left\{ m \in \mathbb{N} \mid \widetilde{p}(m, \underline{x}) = \widetilde{q}(m, \underline{x}) \right\}$$

die Minimalisierung von $\widetilde{p}$ und $\widetilde{q}$ und damit rekursiv. Da schließlich

$$f(\underline{x}) = y = F(1,m) = F(1, M(\underline{x}))$$

gilt, ist f rekursiv. □

16.4 Die Unlösbarkeit des X. Hilbertschen Problems

Bemerkung 16.4. *(a) Die Menge $\mathcal{E}(\mathbb{N})$ der endlichen Folgen natürlicher Zahlen ist abzählbar.*

(b) Die Menge $\mathcal{E}(\mathbb{Z})$ der endlichen Folgen ganzer Zahlen ist abzählbar.

Beweis.

(a) Wird für $\underline{a} = (a_1, \ldots, a_k) \in \mathcal{E}(\mathbb{N})$

$$m(\underline{a}) := \min \left\{ m \in \mathbb{N} \mid a_1 = F(1,m), \ldots, a_k = F(k,m) \right\} \in \mathbb{N}$$

gesetzt, so ist $\underline{a}$ durch $m(\underline{a})$ und $k = k(\underline{a})$ und damit auch durch $P(m,k)$ eindeutig bestimmt. Also gibt es eine injektive Abbildung $\alpha : \mathcal{E}(\mathbb{N}) \longrightarrow \mathbb{N}$ womit $\mathcal{E}(\mathbb{N})$ abzählbar ist.

(b) Ist $\beta : \mathbb{Z} \longrightarrow \mathbb{N}$ die bijektive Abbildung mit

$$z \mapsto \begin{cases} 2z & \text{für} \quad z > 0 \\ -2z+1 & \text{für} \quad z \leq 0 \end{cases},$$

so ist $\alpha \circ \beta : \mathcal{E}(\mathbb{Z}) \longrightarrow \mathbb{N}$ eine injektive Abbildung, womit $\mathcal{E}(\mathbb{Z})$ abzählbar ist. $\square$

Folgerung 16.1. *Die Menge aller Polynome mit ganzzahligen Koeffizienten*

$$\mathbb{Z}[\underline{\underline{X}}] := \bigcup_{n \geq 1} \mathbb{Z}[X_1, \ldots, X_n]$$

ist eine abzählbare Menge.

Beweis. Jedes $f \in \mathbb{Z}[\underline{\underline{X}}]$ läßt sich als endliche Summe von $c_{\underline{i}}\underline{X}^{\underline{i}}$ mit Monomen $\underline{X}^{\underline{i}}$ schreiben. Da jedem Monom $\underline{X}^{\underline{i}} = X_1^{i_1} \cdot \ldots \cdot X_n^{i_n}$ umkehrbar eindeutig die Folge $i_1+1, \ldots, i_n+1 \in \mathcal{E}(\mathbb{N})$ zugeordnet werden kann, ist die Menge $\mathcal{M}$ aller Monome abzählbar nach Bemerkung 16.4 (a). Also gilt $\mathcal{M} = \{ M_i \mid i \in \mathbb{N} \}$, und f läßt sich als endliche Summe von $c_i M_i$ mit $c_i \in \mathbb{Z}$ schreiben. Wird nun f die Folge (c_i) zugeordnet, so ergibt sich eine umkehrbar eindeutige Abbildung zwischen $\mathbb{Z}[\underline{\underline{X}}]$ und $\mathcal{E}(\mathbb{Z})$, womit nach Bemerkung 16.4 (b) folgt, daß $\mathbb{Z}[\underline{\underline{X}}]$ abzählbar ist. $\square$

Satz 16.3. *Das X. Hilbertsche Problem ist unlösbar, d.h. die Frage nach der Existenz von Nullstellen einer diophantischen Gleichung ist algorithmisch nicht lösbar.*

Beweis. Nach Folgerung 16.1 besitzt $\mathbb{Z}[\underline{\underline{X}}]$ eine Darstellung $\mathbb{Z}[\underline{\underline{X}}] = \{f_1, f_2, \ldots\}$. Weiter sei

$$\mathcal{D} := \{ D_n \mid n \in \mathbb{N} \} \quad \text{mit } D_n := \pi_1(\mathrm{V}_{f_n})$$

die Menge aller diophantischer Mengen und $g : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ durch

$$g(x,n) := \begin{cases} 1 & \text{falls} \quad x \in D_n \\ 2 & \text{falls} \quad x \notin D_n \end{cases}$$

definiert. Die Annahme, daß das X. Hilbertsche Problem lösbar ist, hätte nun zur Folge, daß $x \in \mathrm{D}_n$ berechnet werden kann. Damit wäre g eine rekursive und nach Satz 16.2 auch eine diophantische Funktion. Folgende Überlegung zeigt aber, daß g nicht diophantisch sein kann: Es sei

$$X := \{ x \in \mathbb{N} \mid x \notin D_x \}.$$

Wäre X diophantisch, so gäbe es ein $m \in \mathbb{N}$ mit $X = D_m$ und nach Definition von X wäre $m \in \mathrm{D}_m$ gleichbedeutend mit $m \notin X = D_m$, was einen Widerspruch darstellt.

Daher ist X nicht diophantisch. Da aber $x \in X$ gleichbedeutend ist mit $g(x,x) = 2$, was wiederum gleichbedeutend ist mit

$$g(x,y) = z \ \wedge \ x = y \ \wedge \ z = 2,$$

hat die Annahme, daß g diophantisch ist zur Folge, daß X diophantisch ist, was einen Widerspruch zu dem schon Bewiesenen darstellt. Also ist g nicht diophantisch und das X. Hilbertsche Problem ist nicht lösbar. $\square$

17 Konstruktion eines Primzahlpolynoms

17.1 Ergänzungen zur Pellschen Gleichung

Bemerkung 17.1. *Werden wie in Bemerkung 14.1* $(a+\sqrt{d})^k =: x_k + y_k\sqrt{d}$ *mit* $d := a^2-1$ *gesetzt, so gelten* $(x_0,y_0) = (1,0)$, $(x_1,y_1) = (a,1)$ *und für* $k \geq 2$

$$\begin{aligned} x_{k+1} &= 2ax_k - x_{k-1} \\ y_{k+1} &= 2ay_k - y_{k-1}. \end{aligned}$$

Beweis. Die ersten beiden Gleichungen ergeben sich direkt aus der Definition. Nach dem Beweis zu Bemerkung 14.5 gelten die Beziehungen

$$\begin{aligned} x_{k\pm l} &= x_k x_l \pm y_k y_l d \\ y_{k\pm l} &= x_l y_k \pm x_k y_l. \end{aligned}$$

Wird nun $l = 1$ gesetzt, so folgt aus der ersten Gleichung

$$\begin{aligned} x_{k+1} &= ax_k + y_k d \\ x_{k-1} &= ax_k - y_k d, \end{aligned} \tag{17.1}$$

woraus sich durch Addition $x_{k+1} = 2ax_k - x_{k-1}$ ergibt, während die zweiten Gleichung

$$\begin{aligned} y_{k+1} &= ay_k + x_k \\ y_{k-1} &= ay_k - x_k \end{aligned} \tag{17.2}$$

und durch Subtraktion $y_{k+1} = 2ay_k - y_{k-1}$ zur Folge hat. □

Bemerkung 17.2. *Für alle* $a \geq 2$, $k \in \mathbb{N}_0$ *und* $m \in \mathbb{N}$ *gilt mit* $x_k := X_k(a)$ *und* $y_k := Y_k(a)$ *stets*

$$x_k - y_k(a-m) \equiv m^k \pmod{2am - m^2 - 1}.$$

Für $a > m^k$ *gilt darüberhinaus*

$$x_k - y_k(a-m) \geq m^k.$$

Beweis. Der Beweis der ersten Behauptung erfolgt durch Induktion nach k, denn für $k = 0$ ergibt sich wegen $x_0 = 1$ und $y_0 = 0$ eine triviale Beziehung und für den Induktionsschluß gilt zusammen mit Bemerkung 17.1

$$\begin{aligned} x_{k+1} - y_{k+1}(a-m) &= 2a(x_k - (a-m)y_k) - (x_{k-1} - (a-m)y_{k-1}) \\ &\equiv 2am^k - m^{k-1} \pmod{2am - m^2 - 1} \\ &= m^{k-1}(2am-1) \\ &\equiv m^{k-1}m^2 = m^{k+1} \pmod{2am - m^2 - 1}. \end{aligned}$$

Gilt nun $a > m^k$, so folgt zusammen mit (17.1) und (17.2)

$$\begin{aligned} x_k - ay_k + my_k &= ax_{k-1} + (a^2-1)y_{k-1} - a(ay_{k-1} + x_{k-1}) + m(ay_{k-1} + x_{k-1}) \\ &= (ma-1)y_{k-1} + mx_{k-1} \\ &> (m^{k+1} - 1)y_{k-1} + mx_{k-1}, \end{aligned}$$

woraus sich die zweite Behauptung durch Fallunterscheidung ergibt: Für $k = 0$ ist die Behauptung trivial und für $k = 1$ gilt

$$(m^{k+1} - 1)y_{k-1} + mx_{k-1} = (m^0 - 1) \cdot 0 + m \cdot 1 = m \geq m^1$$

Für $k > 1$ und $m = 1$ ergibt sich

$$(m^{k+1} - 1)y_{k-1} + mx_{k-1} = (1 - 1)y_{k-1} + 1 \cdot x_{k-1} \geq x_1 = a > m^k,$$

während für $k > 1$ und $m > 1$ die Abschätzung

$$(m^{k+1} - 1)y_{k-1} + mx_{k-1} \geq (m^{k+1} - 1) \geq m^k$$

folgt. □

Bemerkung 17.3. *Analog zu der in Bemerkung 14.3 (b) gezeigten Kongruenz gilt auch*

$$X_k(a) \equiv X_k(b) \pmod{c} \quad \text{für } a \equiv b \pmod{c}.$$

Beweis. Die Behauptung wird durch triviale Verifikation für $k = 0, 1$ und Induktionsschluß mit Hilfe von Bemerkung 17.1 gezeigt. □

Satz 17.1. *Für alle $a \geq 2$ ist die Relation $y = Y_n(a)$ gleichbedeutend mit*

$$Q(y, n, a): \quad \text{es gibt } c, d, r, u, x \quad \text{mit } Q_1 \wedge Q_2 \wedge Q_3 \wedge Q_4,$$

wobei die Q_i folgende Relationen sind:

$$\begin{aligned}
Q_1 &: \ y \geq n \\
Q_2 &: \ x^2 = (a^2 - 1)y^2 + 1 \\
Q_3 &: \ u^2 = (a^2 - 1)4r^2y^4 + 1 \\
Q_4 &: \ (x + (c-1)u)^2 = \left((a + u^2(u^2 - a))^2 - 1\right)(n + 2(d-1)y)^2 + 1.
\end{aligned}$$

Beweis. Wird Bemerkung 14.6 mit der Umbenennung $k \longrightarrow n$, $\widetilde{x} \longrightarrow u$, $\widetilde{y} \longrightarrow v$, $\approx{x} \longrightarrow s$ und $\approx{y} \longrightarrow t$ verwendet, so ist noch die Äquivalenz von R mit Q zu zeigen. Offensichtlich gelten $R_1 = Q_1$ und $R_2 = Q_2$.

Werden R_3 und R_4 vorausgesetzt, so folgt $v \equiv 0 \pmod{2y^2}$, wobei die stärkere Aussage $v \equiv 0 \pmod{2x^2y^2}$ im zweiten Beweisteil von Bemerkung 14.6 nicht verwandt wurde. Daher gibt es ein $r \in \mathbb{N}$ mit $v = 2ry^2$, und es gilt $u^2 - 4r^2y^4(a^2 - 1) = 1$, womit Q_3 gezeigt ist. Umgekehrt folgt aber aus Q_3 die Beziehung R_4 mit $v = 2ry^2$ und die schwächeren Kongruenz $v \equiv 0 \pmod{2y^2}$.

Werden nun R_5 bis R_8 vorausgesetzt, so gilt nach R_6

$$s^2 = (b^2 - 1)t^2 + 1 \tag{17.3}$$

wobei nach R_5

$$b = a + u^2(u^2 - a) \tag{17.4}$$

gilt. Hieraus folgt aber $a \equiv b \pmod{u}$ und nach Bemerkung 17.3 zusammen mit Q_2 und (17.3) gilt $s \equiv x \pmod{u}$, womit es eine Zahl $c \in \mathbb{N}$ mit

$$s = x + (c-1)u \tag{17.5}$$

gibt. Weiter gilt nach R_8 noch $t \equiv n \pmod{2y}$, und daher gibt es ein $d \in \mathbb{N}$ mit

$$t = n + 2(d-1)y. \tag{17.6}$$

Setzt man nun (17.5), (17.4) und (17.6) in (17.3) ein, so erhält man Q_4.

Gilt nun umgekehrt Q_4 und werden s, b und t wie in (17.5), (17.4) und (17.6) definiert, so gelten offensichtlich R_5, R_8 und R_6. □

17.2 Definierende Relationen für die Fakultät

Bemerkung 17.4. *(a) Für alle $k, n \in \mathbb{N}$ folgt aus $(2k)^k \leq n$ stets*

$$\frac{(n+1)^k}{\binom{n}{k}} < k! + 1.$$

(b) Für alle $k, n, p \in \mathbb{N}$ folgt aus $(2k)^k \leq n$ und $n^k < p$ stets

$$k! < \frac{(n+1)^k p^k}{r} < k! + 1,$$

wobei r der kleinste positive Rest von $(p+1)^n$ modulo p^{k+1} ist.

Beweis.

(a) Es gelten die folgenden Abschätzungen:

$$\begin{aligned} \frac{(n+1)^k}{\binom{n}{k}} &= \frac{k!}{n(n-1)\cdot\ldots\cdot(n-k+1)/(n+1)^k} \\ &\leq \frac{k!}{(n+1-k)^k/(n+1)^k} = \frac{k!}{\left(1 - k/_{n+1}\right)^k} < \frac{k!}{\left(1 - k/_n\right)^k}. \end{aligned}$$

Da für $0 \leq \epsilon \leq \frac{1}{q}$ stets $(1-\epsilon)^q \geq 1 - q\epsilon$ gilt, folgt weiter

$$\frac{k!}{\left(1 - k/_n\right)^k} \leq \frac{k!}{1 - k^2/_n}.$$

Für $0 \leq \delta \leq \frac{1}{2}$ gilt stets $\frac{1}{1-\delta} \leq 1 + 2\delta$, und somit ergibt sich

$$\frac{k!}{1 - k^2/_n} \leq k!\left(1 + \frac{2k^2}{n}\right) \leq k!\left(1 + \frac{2k^2}{(2k)^k}\right) \leq k!\left(1 + \frac{1}{k!}\right),$$

wobei die letzte Umformung klar ist für $k = 1$ und sich für $k > 1$ aus

$$\frac{2k^2}{(2k)^k} = \frac{1}{2^{k-1}k^{k-2}} \leq \frac{1}{k!}$$

ergibt.

(b) Sind k, n und p wie vorausgesetzt gegeben, so folgt aus der Hilfsrechnung

$$\begin{aligned}(np)^{k+1}-1 &= n^k np^{k+1}-1\\ &\leq (p-1)np^{k+1}-1\\ &= np^{k+2}-np^{k+1}-1\\ &< np^{k+2}-p^{k+1}\\ &= (np-1)p^{k+1}\end{aligned}$$

die Abschätzung

$$r := \sum_{i=0}^{k}\binom{n}{i}p^i \leq \sum_{i=0}^{k} n^i p^i = \frac{(np)^{k+1}-1}{np-1} < p^{k+1}.$$

Aufgrund der Zerlegung

$$(p+1)^n = \sum_{i=0}^{k}\binom{n}{i}p^i + p^{k+1}\sum_{i=k+1}^{n}\binom{n}{i}p^{i-k-1}$$

ist r somit der kleinste positive Rest von $(p+1)^n$ modulo p^{k+1}. Hieraus erhält man die Ungleichungskette

$$\begin{aligned}k!r &= k!\left(\sum_{i=0}^{k}\binom{n}{i}p^i\right)\\ &\leq k!\left(k\binom{n}{k-1}p^{k-1}+\binom{n}{k}p^k\right)\\ &\leq k!\left(k\frac{n^{k-1}}{(k-1)!}p^{k-1}+\frac{n^k}{k!}p^k\right)\\ &= k^2n^{k-1}p^{k-1}+n^kp^k\\ &< kn^kp^{k-1}+n^kp^k \quad \text{wegen } k<n\\ &< kp^k+n^kp^k \quad \text{wegen } n^k<p\\ &= (k+n^k)p^k\\ &\leq (1+n)^kp^k,\end{aligned}$$

womit sich die linke Ungleichung ergibt.

Die rechte Ungleichung ergibt sich nach Teil (a) wegen

$$\frac{(n+1)^k}{r}p^k = \frac{(n+1)^k}{\sum_{i=0}^{k}\binom{n}{i}p^{i-k}} < \frac{(n+1)^k}{\binom{n}{k}} < k!+1. \qquad \square$$

Bemerkung 17.5. *(a) Ist $e \geq 2$ und $e^3(e+2)(n+1)^2+1$ eine Quadratzahl, so gilt $e-1+e^{e-2} \leq n$.*

(b) Für jedes $e \in \mathbb{N}$ gibt es ein $n \in \mathbb{N}$, so daß $e^3(e+2)(n+1)^2+1$ eine Quadratzahl ist.

Beweis. Wird $a := e+1$ gesetzt, so ist $(a-1)^3(a+1)(n+1)^2+1 = (a^2-1)(a-1)^2(n+1)^2+1$ eine Quadratzahl größer als 1, womit $(a-1)(n+1)$ eine Lösung der Pellschen Gleichung (P_a) ist. Daher gibt es ein $k \geq 1$ mit

$$(a-1)(n+1) = Y_k(a).$$

Da nach Bemerkung 14.3 (c) $Y_k(a) \equiv k \pmod{(a-1)}$ gilt, ergibt sich hieraus $k \equiv 0 \pmod{(a-1)}$, woraus $(a-1) \mid k$ und wegen $k \neq 0$ schließlich $a-1 \leq k$ folgt. Mit der Hilfsbehauptung

$$(2a-1)^k \leq Y_{k+1}(a) \leq (2a)^k \quad \text{für } a \geq 3,\ k \geq 0$$

folgt nun

$$(a-2)(a-1) + (a-1)^{a-2} < (2a-1)^{a-2} \leq Y_{a-1}(a) \leq Y_k(a) = (a-1)(n+1),$$

woraus sich $a - 2 + (a-1)^{a-3} < n+1$ und durch Rückersetzung $a = e-1$ die Aussage (a) ergibt. Die Hilfsbehauptung folgt nun durch Induktion nach k: Für $k = 0$ ist sie wegen $Y_1(a) = 1$ trivialerweise erfüllt. Wird nun die Richtigkeit der Aussage (beide Ungleichungen!) bis $k-1$ vorausgesetzt, so gelten zusammen mit Bemerkung 17.1

$$Y_{k+1}(a) = 2aY_k(a) - Y_{k-1}(a) \geq 2a(2a-1)^{k-1} - (2a)^{k-2} \geq (2a-1)^k$$

und

$$Y_{k+1}(a) = 2aY_k(a) - Y_{k-1}(a) \leq 2a(2a)^{k-1} - (2a-1)^{k-2} \leq (2a)^k.$$

Die Aussage (b) ergibt sich durch Ersetzung $a = e+1$ wie oben aus der Tatsache, daß die Pellsche Gleichung $X^2 - dY^2 = 1$ für $d \neq 0$ stets nichttriviale Lösungen besitzt. $\square$

Satz 17.2. *Für natürliche Zahlen k und f ist die Relation $f = k!$ gleichbedeutend mit*

$$Q(k,f): \text{es gibt } q,w,z,h,j,n,p \in \mathbb{N} \text{ mit } S_1 \ \wedge \ \ldots \ \wedge \ S_6$$

mit den folgenden Relationen S_i:

$S_1:\quad q = (w-1)z + h + j$	$S_4:\quad p = (n+1)k$
$S_2:\quad z = f(h+j) + h$	$S_5:\quad q = (p+1)^n$
$S_3:\quad (2k)^3(2k+2)(n+1)^2 + 1$ ist Quadratzahl	$S_6:\quad z = p^{k+1}$

Beweis. Sei zunächst $f = k!$. Nach Bemerkung 17.5 (b) gibt es ein n, so daß $(2k)^3(2k+2)(n+1)^2+1$ eine Quadratzahl ist, womit S_3 gilt. Werden nun p , q und z durch S_4 bis S_6 definiert und wird r als der kleinste positive Rest von q modulo z erklärt, so folgt mit S_6 , Bemerkung 17.4 (b) und S_4

$$h := z - fr = p^{k+1} - rk! > p^{k+1} - (n+1)^k p^k = 0,$$

womit $h \in \mathbb{N}$ gilt. Wird weiter $j := r - h$ gesetzt, so folgt mit Bemerkung 17.4 (b) und S_4

$$j = r - p^{k+1} + rk! = r(k!+1) - p^{k+1} > (n+1)^k p^k - p^{k+1} = 0,$$

womit $j \in \mathbb{N}$ gilt. Schließlich folgt aus $q - h - j = q - r \equiv 0 \pmod{z}$ und $q - z \geq 0$ die Existenz einer Zahl w mit $q - h - j = (w-1)z$, womit S_1 gilt. Schließlich ergibt sich S_2 aus $z = fr + h = f(h+j) + h$.

Werden umgekehrt S_1 bis S_6 vorausgesetzt, so gilt wegen S_1 $q \equiv h+j \pmod z$. Da aus S_2 die Beziehung $0 < h+j < z$ folgt, ist $r := h+j$ somit der kleinste nichtnegative Rest von q modulo z. Mit S_2 ergibt sich somit

$$f \leq \frac{z}{h+j} \leq f+1.$$

Nach S_6 und S_4 gilt aber

$$\frac{z}{h+j} = \frac{p^{k+1}}{r} = \frac{(n+1)^k p^k}{r},$$

womit zusammen mit Bemerkung 17.4 $k! < {}^{z}/_{h+j} < k!+1$ und somit $f = k!$ folgt. □

17.3 Definierende Relationen für Primzahlen

Satz 17.3. *Für $k \in \mathbb{N}$ ist die Relation $k+1 \in \mathbb{P}$ gleichbedeutend mit*

$$\text{es gibt } a \dots z \in \mathbb{N} \text{ mit } P_1 \ \wedge \ \dots \ \wedge \ P_{14}$$

mit den folgenden Relationen P_i:

$$\begin{aligned}
P_1 :&\quad q = (w-1)z + h + j\\
P_2 :&\quad z = (gk+g-1)(h+j) + h\\
P_3 :&\quad (2k)^3(2k+2)(n+1)^2 + 1 = f^2\\
P_4 :&\quad e = p + q + z + 2n\\
P_5 :&\quad e^3(e+2)(a+1)^2 + 1 = o^2\\
P_6 :&\quad x^2 = (a^2-1)y^2 + 1\\
P_7 :&\quad u^2 = 4(a^2-1)r^2y^4 + 1\\
P_8 :&\quad (x+(c-1)u)^2 = ((a+u^2(u^2-a))^2-1)(n+2(d-1)y)^2 + 1\\
P_9 :&\quad m^2 = (a^2-1)l^2 + 1\\
P_{10} :&\quad l = k + (i-1)(a-1)\\
P_{11} :&\quad n + l + v = y\\
P_{12} :&\quad m = p + l(a-n-1) + (b-1)(2a(n+1) - (n+1)^2 - 1)\\
P_{13} :&\quad x = q + y(a-p-1) + (s-1)(2a(p+1) - (p+1)^2 - 1)\\
P_{14} :&\quad pm = z + pl(a-p) + (t-1)(2ap - p^2 - 1)
\end{aligned}$$

Beweis. Zunächst seien P_1 bis P_{14} vorausgesetzt. Aus P_3 folgt nach Bemerkung 14.5 (a) die Beziehung $n \geq 2k - 1 + (2k)^{2k-2} \geq 2$ und somit

$$n > k. \tag{17.7}$$

Ebenso folgt aus P_4 und P_5 die Beziehung

$$a \geq e - 1 + e^{e-2} = p + q + z + 2n - 1 + (p+q+z+2n)^{p+q+z+2n-2} \geq 2. \tag{17.8}$$

Somit kann a in vielen Abschätzungen als eine obere Schranke verwendet werden. Da aus P_{11} die Relation $y \geq n$ folgt, sind zusammen mit P_6, P_7 und P_8 die Relationen Q_1 bis Q_4 aus Satz 17.1 erfüllt und es folgt $y = Y_n(a)$, womit sich mit P_6 die Beziehung $x = X_n(a)$ ergibt.

Nach P_9 gibt es eine Zahl $\widetilde{k} \in \mathbb{N}$ mit $m = X_{\widetilde{k}}(a)$ und $l = Y_{\widetilde{k}}(a)$. Nun soll $k = \widetilde{k}$ gezeigt werden: Da nach P_{11} $l < y$ gilt, folgt aufgrund der Monotonie $\widetilde{k} < n$. Da sich aus (17.8) $n < a$ ergibt, gilt $\widetilde{k} < a$ und somit $\widetilde{k} \leq a-1$. Andererseits folgt zusammen mit (17.7) und $n < a$ die Abschätzung $k \leq a-1$. Aus P_{10} und Bemerkung 14.3 (c) folgt schließlich

$$k \equiv l = Y_{\widetilde{k}(a)} \equiv \widetilde{k} \pmod{a-1},$$

womit sich $k = \widetilde{k}$ ergibt. Also gelten $m = X_k(a)$ und $l = Y_k(a)$.

Ziel ist es nun, die Relationen S_1 bis S_6 aus Satz 17.2 zu zeigen. Die Relationen S_1 bis S_3 gelten wegen P_1 bis P_3, wenn in S_2 statt f die Zahl $\widetilde{f} := gk + g - 1$ gesetzt wird. Nach P_{12} und Bemerkung 17.2 gilt

$$p \equiv m - l(a-n-1) \equiv X_k(a) - Y_k(a)(a-n-1) \equiv (n+1)^k \pmod{2a(n+1) - (n+1)^2 - 1}.$$

Da nach (17.8) $p < a$ gilt, folgt mit (17.7) und nochmals (17.8) $(n+1)^k < (n+1)^n < a$. Aus (17.8) folgt aber auch $n+2 \leq a$ womit sich

$$a < a(n+1) = 2a(n+1) - a(n+1) \leq 2a(n+1) - (n+1)^2 - 1$$

ergibt. Hieraus folgt schließlich $p = (n+1)^k$ und somit S_4.

Auf die gleiche Weise erhält man aus P_{13} und den aus (17.8) stammenden Abschätzungen $q < a$, $(p+1) < a$ und $a < 2a(p+1) - (p+1)^2 - 1$ die Relation S_5.

Nach P_{14} und Bemerkung 17.2 gilt

$$z \equiv pm - pl(a-p) = pX_k(a) - pY_k(a)(a-p) \equiv pp^k = p^{k+1} \pmod{2ap - p^2 - 1}.$$

Da nach (17.8) $z < a$ und $p^n < a$ gelten, folgt mit (17.7) $p^k < a$. Wiederum nach (17.8) gilt $p + 2 \leq a$, womit sich

$$a < ap = 2ap - ap \leq 2ap - p^2 - 1$$

ergibt. Hieraus folgt schließlich $z = p^{k+1}$ und somit S_4.

Mit Satz 17.2 gilt nun $\widetilde{f} = k!$ mit $\widetilde{f} := gk + g - 1$, womit sich $k! + 1 = g(k+1)$ ergibt. Dies hat aber $(k+1) \mid (k!+1)$ und somit $k! \equiv -1 \pmod{k+1}$ zur Folge. Nach dem Satz von Wilson (Folgerung 3.2) bedeutet dies aber, daß $k+1$ eine Primzahl ist.

Nun sei umgekehrt $k+1$ eine Primzahl. Nach dem Satz von Wilson gilt somit $(k+1) \mid (k!+1)$ und daher gibt es eine Zahl $g \in \mathbb{N}$ mit $k!+1 = g(k+1)$. Da nun $k! = gk+g-1$ gilt, folgt nach Satz 17.2 die Existenz von Zahlen $q, w, z, h, j, n, p, f \in \mathbb{N}$ mit $S_1 \wedge \ldots \wedge S_6$, wobei in S_2 $gk+g-1$ statt f und für S_3 $(2k)^3(2k+2)(n+1)^2+1 = f^2$ gesetzt wird. Somit gelten die Relationen P_1 bis P_3.

Wird nun e wie in P_4 definiert, so gibt es nach Bemerkung 17.5 (b) Zahlen $a, o \in \mathbb{N}$ mit $e^3(e+2)(a+1)^2+1 = o^2$, womit P_5 gilt. Weiter folgt wegen $e \geq 2$ nach Bemerkung 17.5 (a) $a \geq e - 1 + e^{e-2} \geq 2$. Wird nun y durch $y := Y_n(a)$ definiert, so gibt es nach Satz 17.1 Zahlen $c, d, r, u, x \in \mathbb{N}$, die die Relationen P_6 bis P_8 erfüllen. (Insbesondere gilt $x = X_n(a)$.)

Mit $m := X_k(a)$ und $l := Y_k(a)$ gilt auch P_9. Da aufgrund der Monotonie nun $k \leq Y_k(a) = l$ und nach Bemerkung 14.3 (c) auch $l = Y_k(a) \equiv k \pmod{(a-1)}$ gelten, gibt es eine Zahl $i \in \mathbb{N}$ mit $l = k + (i-1)(a-1)$, womit P_{10} gilt.

Die Zwischenbehauptung $Y_{k+1}(a) - Y_k(a) > k-1$ wird durch Induktion nach k gezeigt: Für $k=1$ ergibt sich wegen $a \geq 2$ die wahre Aussage $Y_2(a) - Y_1(a) = 2a-1 > 2$ und für $k > 1$ gilt nach Bemerkung 17.1 wegen $a \geq 2$ und der Induktionsannahme

$$\begin{array}{rcl} Y_{k+1}(a) - Y_k(a) & = & 2aY_k(a) - Y_{k-1}(a) - Y_k(a) \\ & = & (2a-1)Y_k(a) - Y_{k-1}(a) \\ & = & (Y_k(a) - Y_{k-1}(a)) + 2(a-1)Y_k(a) \\ & \geq & (Y_k(a) - Y_{k-1}(a)) + 1 \\ & \geq & k+1. \end{array}$$

Aus P_3 folgt nach Bemerkung 17.5 (a) die Beziehung $n \geq 2k - 1 + (2k)^{2k-2}$, womit $k < n$ gilt. Mit der Zwischenbehauptung erhält man die Ungleichung

$$n + l = n + Y_k(a) \leq n + Y_{n-1}(a) < Y_n(a) = y$$

und daher gibt es eine Zahl $v \in \mathbb{N}$ mit $n + l + v = y$, womit P_{11} gezeigt ist.

Aus den Relationen P_4 und P_5 folgt wie im ersten Teil des Beweises die Abschätzung (17.8), womit sich zusammen mit S_4 bis S_6 die folgenden Beziehungen ergeben:

$$\begin{array}{ccccl} a & > & p & = & (n+1)^k \\ a & > & q & = & (p+1)^n \\ a & > & z & = & p^{k+1} \end{array} .$$

Nach Bemerkung 17.2 (a) gilt die Kongruenz

$$m - l(a-(n+1)) = X_k(a) - Y_k(a)(a-(n+1)) \equiv (n+1)^k = p \pmod{2a(n+1)-(n+1)^2-1}$$

und nach Bemerkung 17.2 (b) gibt es eine Zahl $b \in \mathbb{N}$ mit

$$m - l(a-(n+1)) = p + (b-1)(2a(n+1) - (n+1)^2 - 1),$$

womit P_{12} gezeigt ist. In analoger Weise erhält man

$$x - y(a-(p+1)) = X_n(a) - Y_n(a)(a-(p+1)) \equiv (p+1)^k = q \pmod{2a(p+1)-(p+1)^2-1}$$

und die Existenz einer Zahl $s \in \mathbb{N}$ mit

$$x - y(a-(p+1)) = q + (s-1)(2a(p+1) - (p+1)^2 - 1),$$

womit P_{13} gezeigt ist. Schließlich erhält man P_{14} auf gleichem Wege, da aus

$$m - l(a-p) = X_k(a) - Y_k(a)(a-p) \equiv p^k \pmod{2ap - p^2 - 1}$$

durch Multiplikation mit p die Beziehung

$$mp - lp(a-p) \equiv z \pmod{2ap - p^2 - 1}$$

folgt und somit eine Zahl $t \in \mathbb{N}$ mit

$$mp - lp(a-p) = z + (t-1)(2ap - p^2 - 1)$$

existiert. □

17.4 Das Primzahlpolynom

Satz 17.4. *Ist F_i das durch die Relation P_i in Satz 17.3 definierte Polynom, so ist die Menge der positiven Werte des Polynoms*

$$F(a,\dots,z) := (k+1)(1-\sum_{i=1}^{14} F_i^2)$$

für $(a,\dots,z) \in \mathbb{N}^{26}$ gerade die Menge der Primzahlen.

Index