Elementare Zahlentheorie

Wintersemester 2024/25

Dr. Hendrik Kasten und Dr. Denis Vogel

9. Januar 2025

Inhaltsverzeichnis

0 Einleitung **3**

0.1 Zahlbereiche . . . 3

0.2 Über Zahlentheorie . . . 4

1 Teilbarkeit **5**

1.1 Teiler und Vielfache . . . 5

1.2 Der Fundamentalsatz der Arithmetik . . . 12

1.3 Vollkommene Zahlen . . . 15

2 Zahlentheoretische Funktionen **18**

2.1 Der Ring der zahlentheoretischen Funktionen . . . 18

2.2 Multiplikativität . . . 20

2.3 Der Möbius'sche Umkehrsatz . . . 25

2.4 Die Euler'sche φ-Funktion . . . 27

3 Rechnen mit Restklassen **30**

3.1 Restklassenringe . . . 30

3.2 Teilbarkeitsregeln . . . 34

3.3 Prime Restklassen und der Satz von Euler-Fermat . . . 36

3.4 Zyklische Gruppen . . . 41

3.5 Die Zyklizität von $\mathbb{F}_p^\times$ . . . 46

3.6 Die Struktur der primen Restklassengruppen für Primpotenzen . . . 50

3.7 Der Chinesische Restsatz . . . 56

3.8 Das RSA-Verfahren . . . 65

4 Diophantische Gleichungen **69**

4.1 Pythagoräische Tripel und der Große Satz von Fermat 69

4.2 Lösungsstrategien 72

4.3 Lineare diophantische Gleichungen 79

5 Das Quadratische Reziprozitätsgesetz und seine Anwendungen **83**

5.1 Das Reziprozitätsgesetz 83

5.2 Primzahlen mit vorgegebener Restklasse 92

5.3 Summen von Quadraten 95

5.4 Der Primzahltest von Solovay-Strassen 100

6 Kettenbrüche und quadratische Zahlkörper **106**

6.1 Die Kettenbruchentwicklung reeller Zahlen 106

6.2 Periodische Kettenbrüche 117

6.3 Die Pell'sche Gleichung und diophantische Approximation 125

6.4 Die Einheitengruppe des Ganzheitsringes quadratischer Zahlkörper 137

KAPITEL 0

Einleitung

0.1 Zahlbereiche

Wir gehen für diese Vorlesung davon aus, dass die üblichen Zahlbereiche bereits an anderer Stelle grundlegend eingeführt worden sind. Wir geben hier darum nur einen kurzen Überblick über diese Thematik und legen bei dieser Gelegenheit unsere Notation fest:

- $\mathbb{N} := \{1, 2, 3, \ldots\}$ bezeichne die Menge der ***natürlichen Zahlen***. Letztere sind seit vorhistorischer Zeit bekannt und werden seit jeher dazu benutzt, Anzahlen als gleichartig betrachteter Objekte (etwa: Äpfel, Birnen, ...) zu beschreiben.
- $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$. Die Verwendung von Stellenwertsystemen (vgl. Abschnitt 3.2) machte die Einführung eines Symbols notwendig, das anzeigt, dass etwas *nicht* da ist. Dieses Symbol ist die ***Null*** – in Zeichen: 0. Zuerst erschien sie ca. 300 v. Chr. in Indien. Mit dem Einzug des Stellenwertsystems kam auch die Null im 12. Jahrhundert nach Europa.
- $\mathbb{Z} := \mathbb{N}_0 \cup \{-a : a \in \mathbb{N}\}$ bezeichne die Menge der ***ganzen Zahlen***. Im Zuge der Buchführung bei der Steuererhebung kam im China des 2. Jahrhunderts v. Chr. der Wunsch auf, nicht nur Guthaben sondern auch Ausstände notieren zu können. Mittel der Wahl war damals – und mancherorts auch noch heute – Guthaben in schwarz und Schulden in rot zu notieren. Nach Europa kamen die negativen Zahlen erst im 15. Jahrhundert, als in Florenz das moderne Bankwesen entstand.
- $\mathbb{Q} := \{\frac{a}{b} : a \in \mathbb{Z}, b \in \mathbb{N}\}$ bezeichne die Menge der ***rationalen Zahlen***. Diese wird algebraisch realisiert als Quotient

  $$\mathbb{Q} = (\mathbb{Z} \times \mathbb{N}) / \sim \quad \text{mit der Äquivalenzrelation } (a, b) \sim (c, d) :\Longleftrightarrow ad = bc.$$

  Während diese Beschreibung der rationalen Zahlen natürlich vergleichsweise rezent ist, lassen sich die ersten Beispiele für Bruchrechnung bereits ca. 1000 v. Chr. in Ägypten

nachweisen. Als Verhältnisse von Längen waren sie in der antiken Mathematik und ihren Anwendungen – etwa in der Architektur – weit verbreitet.

- $\mathbb{R} := \{\text{Cauchy-Folgen in } \mathbb{Q}\}/\{\text{Nullfolgen in } \mathbb{Q}\}$ bezeichne die ***reellen Zahlen***. Schon im 5. Jahrhundert v. Chr. fanden die Pythagoräer den ersten Beweis für irrationale Zahlenverhältnisse. Im 16. Jahrhundert schuf Simon Stevin die Voraussetzungen für die moderne Dezimalschreibweise und bestand darauf, hierbei zwischen rationalen und irrationalen Zahlen keinen Unterschied zu machen. Seit Einführung der modernen Analysis im 18. Jahrhundert nutzt man systematisch die komplette Menge der reellen Zahlen, zunächst jedoch ohne eine stringente Definition dieses Begriffs. Diese lieferte erst Georg Cantor im Jahr 1871. Drei Jahre später zeigte er mit seinem berühmten Diagonalargument, dass die Menge der reellen Zahlen nicht abzählbar – also echt mächtiger als die Menge der natürlichen Zahlen – ist.

- $\mathbb{C} := \mathbb{R}[X]/(X^2+1) = \{a+bi : a,b \in \mathbb{R}\}$ bezeichne die Menge der ***komplexen Zahlen***. Spätestens seit dem 16. Jahrhundert ist bekannt, dass beim Lösen algebraischer Gleichungen Wurzeln aus negativen Zahlen auftreten. Letztere wurden zunächst nicht als Zahlen akzeptiert, da sie keine Längen in der realen Welt darstellten, dann aber nach und nach als nützliches Hilfsmittel erkannt und als ***imaginäre Zahlen*** toleriert. Mit Aufkommen der modernen Algebra erkannte man schließlich die Bedeutung der komplexen Zahlen als algebraischem Abschluss der reellen Zahlen.

0.2 Über Zahlentheorie

Vereinfachend lässt sich sagen, die ***Zahlentheorie*** sei das Studium der natürlichen bzw. ganzen Zahlen. Untersuchungen verschiedener Eigenschaften natürlicher Zahlen gehören zu den ältesten Beschäftigungen mit mathematischen Problemen überhaupt. Bereits im antiken Griechenland entstanden Werke wie Euklids *Elemente* und Diophants *Arithmetika*, die sich teilweise oder ausschließlich mit der systematischen Behandlung ganzzahliger Fragestellungen befassten. Mit dem ausgehenden Altertum schwand jedoch weitgehend das Interesse an der Mathematik insgesamt und wirklich starke, neue Impulse erhielt die Lehre von den ganzen Zahlen erst wieder im 17. und 18. Jahrhundert, vor allem durch Fermat und Euler. Die ersten umfassenden und systematischen Darstellungen des (damals) aktuellen Wissensstandes der Zahlentheorie gaben dann um die Wende zum 19. Jahrhundert nahezu zeitgleich Legendre mit seinem *Essai sur la Théorie des Nombres* und Gauß mit seinen *Disquisitiones Arithmeticae*. Vor allem das fundamentale Werk von Gauß mit seiner Fülle von neuen und tiefliegenden Entdeckungen brachte die Zahlentheorie als selbständige Teildisziplin der Gesamtmathematik erst eigentlich auf den Weg. In den seither verflossenen fast zweihundert Jahren hat sich die Zahlentheorie gewaltig weiterentwickelt und in verschiedene Richtungen verzweigt. In Abhängigkeit von den eingesetzten Hilfsmitteln unterscheidet man dabei vor allem zwischen der Elementaren Zahlentheorie, der Analytischen Zahlentheorie und der Algebraischen Zahlentheorie. In dieser Vorlesung werden wir uns zumeist mit elementaren Fragestellungen beschäftigen.

KAPITEL 1

Teilbarkeit

1.1 Teiler und Vielfache

Definition 1.1. *Es seien $a, b \in \mathbb{Z}$. Die Zahl a heißt ein **Teiler** von b – wir schreiben: $a \mid b$ – wenn ein $q \in \mathbb{Z}$ mit $b = qa$ existiert. In diesem Fall nennt man die Zahl b auch ein **Vielfaches** von a.*

Die folgende Bemerkung beinhaltet einige sehr einfache Eigenschaften der Teilbarkeit, die sich unmittelbar aus der vorangegangenen Definition ergeben:

Proposition 1.2. *Es seien $a, b, c, d \in \mathbb{Z}$. Dann gilt:*

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

(b) *Aus $a \mid b$ folgt $a \mid bc$.*

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

(d) *Aus $a \mid c$ und $b \mid d$ folgt $ab \mid cd$.*

Beweis. Zum Nachweis von (a) gelte $a \mid b$ und $a \mid c$. Dann existieren $q_1, q_2 \in \mathbb{Z}$ mit $b = q_1 a$, $c = q_2 a$, somit ist $b + c = (q_1 + q_2)a$ und $a \mid (b + c)$. Für den Beweis von (b) setzen wir $a \mid b$ voraus, d.h. es existiert ein $q \in \mathbb{Z}$ mit $b = qa$. Dann ist $bc = qca$, und somit gilt $a \mid bc$. Zu (c) bemerken wir, dass aus $a \mid b$ und $b \mid c$ die Existenz von $q_1, q_2 \in \mathbb{Z}$ mit $b = q_1 a$, $c = q_2 b$ folgt, und damit $c = q_2 q_1 a$, was $a \mid c$ impliziert. Es verbleibt der Beweis von (d). Dazu gelte $a \mid c$ und $b \mid d$. Dann existieren $q_1, q_2 \in \mathbb{Z}$ mit $c = q_1 a$, $d = q_2 b$, weswegen $cd = q_1 q_2 ab$ und daraufhin $ab \mid cd$ folgt. □

Der nächste Satz beschreibt ein Verfahren, das letztlich schon aus aus der Grundschule bekannt sein dürfte: die Division mit Rest auf den ganzen Zahlen. Nichtsdestotrotz ist das Verfahren unglaublich nützlich und wir werden den Satz später in sehr vielen Beweisen anwenden:

Satz 1.3 (Division mit Rest)**.** *Seien $a, b \in \mathbb{Z}$ mit $b \neq 0$. Dann gilt: Es gibt eindeutig bestimmte Zahlen $q, r \in \mathbb{Z}$ mit*

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

*Die Zahl r heißt der **Rest**, die Zahl q heißt der **ganzzahlige Quotient** bei Division von a durch b.*

Beweis. Wir zeigen zunächst die Existenz von $q, r \in \mathbb{Z}$ mit obigen Eigenschaften. Dazu setzen wir

$$R := \{a - \tilde{q}b : \tilde{q} \in \mathbb{Z}\} \cap \mathbb{N}_0 \subseteq \mathbb{N}_0.$$

Offenbar ist R eine nichtleere Teilmenge von $\mathbb{N}_0$, insbesondere besitzt R ein eindeutig bestimmtes kleinstes Element, welches wir im Folgenden mit r bezeichnen wollen. Es sei q diejenige ganze Zahl mit $a - qb = r$, also mit $a = qb + r$. Wir behaupten, dass $0 \leq r < |b|$ ist, und nehmen dafür $r \geq |b|$ an. Hieraus ergäbe sich

$$0 \leq r - |b| = a - qb - \operatorname{sgn}(b)b = \underbrace{a - (q + \operatorname{sgn}(b))b}_{\in R} < r,$$

im Widerspruch zur Minimalität von r.

Es verbleibt der Beweis der Eindeutigkeit. Seien dazu $r, \tilde{r}, q, \tilde{q} \in \mathbb{Z}$ mit

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

Wir erhalten $(q - \tilde{q})b = \tilde{r} - r$ und also $b \mid (\tilde{r} - r)$. Nach Voraussetzung gilt $|\tilde{r} - r| < |b|$, weswegen sich $\tilde{r} - r = 0$, also $r = \tilde{r}$ und schließlich $q = \tilde{q}$ ergibt. □

Definition 1.4. *Seien $n \in \mathbb{N}$ und $a_1, \ldots, a_n \in \mathbb{Z}$. Dann bezeichnet*

$$\begin{aligned} T(a_1, \ldots, a_n) &:= \{t \in \mathbb{Z} \ : t \mid a_1, \ldots, t \mid a_n\} \\ &= T(a_1) \cap \ \ldots \ \cap T(a_n) \end{aligned}$$

*die Menge der **gemeinsamen Teiler** von $a_1, \ldots, a_n$. Eine Zahl $d \in \mathbb{Z}$ heißt ein **größter gemeinsamer Teiler** von $a_1, \ldots, a_n$, wenn Folgendes gilt:*

(a) $d \geq 0$,

(b) $d \in T(a_1, \ldots, a_n)$,

(c) *Ist $t \in T(a_1, \ldots, a_n)$, so gilt $t \mid d$.*

Aus dieser Definition geht nicht direkt hervor, ob ein größter gemeinsamer Teiler überhaupt existiert und inwieweit er eindeutig bestimmt ist. Natürlich könnten wir für $a_1, \ldots, a_n \in \mathbb{Z}$ mit $(a_1, \ldots, a_n) \neq (0, \ldots, 0)$ den größten gemeinsamen Teiler auch als das bzgl. „$\leq$“ größte Element von $T(a_1, \ldots, a_n)$ festsetzen. Unsere Definition ist jedoch für die meisten Verwendungszwecke tauglicher. Dafür müssen wir für Existenz und Eindeutigkeit allerdings etwas Arbeit investieren:

Proposition 1.5. *Seien $n \in \mathbb{N}$ und $a_1, \ldots, a_n \in \mathbb{Z}$. Dann besitzen $a_1, \ldots, a_n$ höchstens einen größten gemeinsamen Teiler.*

Beweis. Seien d_1, d_2 größte gemeinsame Teiler von $a_1, \ldots, a_n$. Da d_1 ein gemeinsamer Teiler von $a_1, \ldots, a_n$ ist und d_2 ein größter gemeinsamer Teiler, folgt $d_1 \mid d_2$ nach 1.4 (c). Analog erhalten wir $d_2 \mid d_1$. Somit existieren $q_1, q_2 \in \mathbb{Z}$ mit $d_2 = q_1 d_1, d_1 = q_2 d_2$ und also mit $d_1 = q_2 q_1 d_1$. Wir machen nun eine Fallunterscheidung: Ist $d_1 \neq 0$, so ist $q_2 q_1 = 1$. Es folgt $q_1 \in \{\pm 1\}$ und deshalb $d_2 = \pm d_1$. Aufgrund von $d_1, d_2 \geq 0$ – vgl. 1.4 (a) – folgt $d_2 = d_1$. Ist andererseits $d_1 = 0$, folgt $d_2 = q_1 \cdot 0 = 0 = d_1$. □

Der Beweis zeigt insbesondere: Lässt man in Definition 1.4 Bedingung (a) weg, so gibt es höchstens zwei größte gemeinsame Teiler von $a_1, \ldots, a_n$; mit d wäre dann stets auch $-d$ ein größter gemeinsamer Teiler von $a_1, \ldots, a_n$.

Die folgende einfache Bemerkung spielt eine Schlüsselrolle in der Konstruktion eines größten gemeinsamen Teilers zweier ganzer Zahlen:

Proposition 1.6. *Es seien $a, b \in \mathbb{Z}$. Dann gilt: Sind $q, r \in \mathbb{Z}$ mit $a = qb + r$, dann ist*

$$T(a, b) = T(b, r).$$

Beweis. Gilt $t \in T(a, b)$, so auch $t \mid (a - qb) = r$ und also $t \in T(b, r)$. Umgekehrt ergibt sich aus $t \in T(b, r)$ offensichtlich $t \mid (qb + r) = a$ und somit $t \in T(a, b)$. □

Gilt $a, b \in \mathbb{N}$ und ohne Einschränkung $a \geq b$, so folgt aus der obigen Bemerkung, dass man durch Division mit Rest – etwa in der Form $a = qb + r$ mit $0 \leq r < |b|$ – die Berechnung der Menge der gemeinsamen Teiler $T(a, b)$ auf die Berechnung der Menge der gemeinsamen Teiler $T(b, r)$ zurückführen kann - hierbei ist jetzt r kleiner als b und damit auch kleiner als a. Durch Iteration dieses Verfahrens kann man die Berechnung von $T(a, b)$ auf die Berechnung gemeinsamer Teilermengen immer kleiner werdender Zahlen zurückführen. Das ist die Grundidee des Euklidischen Algorithmus:

Satz 1.7 (Euklidischer Algorithmus)**.** *Seien $a \geq b \in \mathbb{Z}$. Dann gilt:*

(a) *a, b besitzen einen eindeutig bestimmten größten gemeinsamen Teiler. Dieser wird mit $\mathrm{ggT}(a, b)$ bezeichnet und **der größte gemeinsame Teiler** von a und b genannt.*

(b) *Der größte gemeinsame Teiler $\mathrm{ggT}(a, b)$ kann mit dem Euklidischen Algorithmus bestimmt werden: Ist $b \neq 0$, setze $z_1 := a,\ z_2 := |b|$ und erhalte $z_3, z_4, \ldots \in \mathbb{N}_0$ durch die Gleichungen*

$$\begin{aligned} &(G_1) \quad z_1 = q_1 z_2 + z_3 && \text{mit } 0 \leq z_3 < z_2, \\ &(G_2) \quad z_2 = q_2 z_3 + z_4 && \text{mit } 0 \leq z_4 < z_3, \end{aligned}$$

usw. Dieser Prozess bricht nach endlich vielen Schritten – etwa nach r Schritten – ab:

$$\begin{aligned} &(G_{r-1}) \quad z_{r-1} = q_{r-1} z_r + z_{r+1} && \text{mit } 0 \leq z_{r+1} < z_r \\ &(G_r) \quad z_r = q_r z_{r+1} + 0 \end{aligned}$$

und es gilt $\mathrm{ggT}(a,b) = z_{r+1}$. *Im Fall* $b = 0$ *ist* $\mathrm{ggT}(a,b) = \mathrm{ggT}(a,0) = |a|$.

(c) *Es gibt* $u, v \in \mathbb{Z}$ *mit*

$$\mathrm{ggT}(a,b) = ua + vb.$$

(„erweiterter Euklidischer Algorithmus“)

Beweis. Wir betrachten zunächst den Fall $b = 0$: Offenbar gilt $|a| \mid a$ sowie $|a| \mid 0$. Ist $t \in T(a,0) = T(a)$, so folgt $t \mid |a|$. Demnach ist $|a|$ ist ein größter gemeinsamer Teiler von a und 0; die Eindeutigkeit folgt mit Proposition 1.5. Außerdem gilt $|a| = \mathrm{ggT}(a,0) = \mathrm{sgn}(a) \cdot a + 0 \cdot 0$, was in diesem Spezialfall Behauptung (c) impliziert.

Im Folgenden sei $b \neq 0$. Für die Folge der Reste gilt $z_2 > z_3 > z_4 > \ldots$, so dass nach endlich vielen Schritten – etwa nach r Schritten – das Verfahren abbricht. Die letzten beiden Gleichungen sind dann von der Form

$$\begin{aligned} &(G_{r-1}) \quad z_{r-1} = q_{r-1} z_r + z_{r+1} && \text{mit } 0 \leq z_{r+1} < z_r, \\ &(G_r) \quad z_r = q_r z_{r+1} + 0 \end{aligned}$$

Nach Proposition 1.6 gilt nun

$$\begin{aligned} T(a,b) = T(a,|b|) = T(z_1,z_2) &\overset{1.6}{=} T(z_2,z_3) \\ &\overset{1.6}{=} \ldots \overset{1.6}{=} T(z_r,z_{r+1}) \overset{1.6}{=} T(z_{r+1},0) \\ &= T(z_{r+1}). \end{aligned}$$

Es folgt $z_{r+1} \in T(z_{r+1}) = T(a,b)$ und für alle $t \in T(a,b) = T(z_{r+1})$ auch $t \mid z_{r+1}$. Da nach Konstruktion $z_{r+1} > 0$ gilt, haben wir damit nachgewiesen, dass z_{r+1} ein größter gemeinsamer Teiler von a und b ist; die Eindeutigkeitsaussage ergibt sich mit Proposition 1.5. Hiermit sind die Behauptungen (a) und (b) gezeigt und es verbleibt der Nachweis von Behauptung (c). Aufgrund von

$$\begin{aligned} &(G_{r-2}) \quad z_{r-2} = q_{r-2} z_{r-1} + z_r, \\ &(G_{r-1}) \quad z_{r-1} = q_{r-1} z_r + \mathrm{ggT}(a,b) \end{aligned}$$

ergibt sich

$$\begin{aligned} \mathrm{ggT}(a,b) = z_{r-1} - q_{r-1} z_r &= z_{r-1} - q_{r-1}\big(z_{r-2} - q_{r-2} z_{r-1}\big) \\ &= v_{r-1} z_{r-1} + u_{r-1} z_{r-2} && \text{mit geeigneten } u_{r-1}, v_{r-1} \in \mathbb{Z}. \end{aligned}$$

Wir benutzen nun (G_{r-3}), um z_{r-1} über z_{r-3}, z_{r-2} auszudrücken, und so weiter. Aus (G_1) erhalten wir schließlich $u_2, v_2 \in \mathbb{Z}$ mit

$$\mathrm{ggT}(a,b) = v_2 z_2 + u_2 z_1 = v_2 |b| + u_2 a.$$

Wir setzen $u := u_2, v := v_2 \,\mathrm{sgn}(b)$ und erhalten $\mathrm{ggT}(a,b) = ua + vb$. □

Beispiel 1.8. *Wir bestimmen mithilfe des Euklidischen Algorithmus den größten gemeinsamen Teiler von* 6930 *und* 1098*:*

$$\begin{aligned}
6930 &= 6 \cdot 1098 + 342\\
1098 &= 3 \cdot 342 + 72\\
342 &= 4 \cdot 72 + 54\\
72 &= 1 \cdot 54 + 18\\
54 &= 3 \cdot 18 + 0
\end{aligned}$$

Wir erhalten $\mathrm{ggT}(6930, 1098) = 18$*. Das im obigen Beweis dafür gegebene Argument lautet hier konkret unter Verwendung von Proposition 1.6 konkret:*

$$\begin{aligned}
T(6930, 1098) &= T(1098, 342) = T(342, 72) = T(72, 54) = T(54, 18) = T(18, 0)\\
&= T(18).
\end{aligned}$$

Darüber hinaus ergibt sich

$$\begin{aligned}
\mathrm{ggT}(6930, 1098) &= 18 = 72 - 1 \cdot 54 = 72 - (342 - 4 \cdot 72) = 5 \cdot 72 - 342\\
&= 5 \cdot (1098 - 3 \cdot 342) - 342 = 5 \cdot 1098 - 16 \cdot 342\\
&= 5 \cdot 1098 - 16 \cdot (6930 - 6 \cdot 1098)\\
&= (-16) \cdot 6930 + 101 \cdot 1098.
\end{aligned}$$

Die lineare Kombinierbarkeit von $\mathrm{ggT}(a, b)$ aus a, b durch den erweiterten Euklidischen Algorithmus ist eine sehr wichtige Eigenschaft des größten gemeinsamen Teilers, die man sehr häufig in Beweisen benötigt. Als Beispiel hierfür dient der Beweis der folgenden Proposition:

Proposition 1.9. *Für beliebige ganze Zahlen* $a, b, c, d \in \mathbb{Z}$ *mit* $\mathrm{ggT}(a, b) = 1$ *gelten die folgenden beiden Aussagen:*

(a) *Aus* $a \mid bc$ *folgt* $a \mid c$

(b) *Aus* $a \mid d$ *und* $b \mid d$ *folgt* $ab \mid d$*.*

Beweis. Wir bemerken zunächst, dass es wegen $\mathrm{ggT}(a, b) = 1$ nach dem erweiterten Euklidischen Algorithmus ganze Zahlen $u, v \in \mathbb{Z}$ mit $ua + vb = 1$ gibt. Setzen wir $a \mid bc$ voraus, so existiert ein $q \in \mathbb{Z}$ mit $bc = qa$. Es folgt

$$c = c \cdot 1 = c(ua + vb) = cua + vbc = cua + vqa = a(cu + vq)$$

und also auch $a \mid c$, was Behauptung (a) impliziert.

Gilt weiter $a \mid d$ und $b \mid d$, so gibt es $q_1, q_2 \in \mathbb{Z}$ mit $d = q_1 a$ und $d = q_2 b$. Wir erhalten

$$d = d \cdot 1 = d(ua + vb) = dua + dvb = q_2 bua + q_1 avb = ab(q_2 u + q_1 v)$$

und deshalb $ab \mid d$. Es folgt Behauptung (b). □

Nachdem wir den Spezialfall des größten gemeinsamen Teilers zweier Zahlen abgehandelt haben, wenden wir uns nun dem allgemeinen Fall zu. Dafür ist es sehr nützlich, sich mit Idealen in $\mathbb{Z}$ zu beschäftigen:

Definition 1.10. *Eine Teilmenge $\mathfrak{a} \subseteq \mathbb{Z}$ heißt ein **Ideal** in $\mathbb{Z}$, wenn die folgenden Bedingungen erfüllt sind:*

(a) $0 \in \mathfrak{a}$.

(b) *Sind $a_1, a_2 \in \mathfrak{a}$, so auch $a_1 + a_2$.*

(c) *Sind $a \in \mathfrak{a}, r \in \mathbb{Z}$, so ist $ra \in \mathfrak{a}$.*

Die nächste Proposition zeigt, dass Ideale in $\mathbb{Z}$ von einer einfachen Form sind:

Proposition 1.11. *Für jedes Ideal $\mathfrak{a} \subseteq \mathbb{Z}$ gibt es ein eindeutig bestimmtes $m \in \mathbb{N}_0$ mit*

$$\mathfrak{a} = m\mathbb{Z} := \{mr : r \in \mathbb{Z}\}.$$

Beweis. Wir zeigen zunächst die Existenz eines $m \in \mathbb{N}_0$ mit $\mathfrak{a} = m\mathbb{Z}$. Im Fall $\mathfrak{a} = \{0\}$ gilt $\mathfrak{a} = 0 \cdot \mathbb{Z}$ und wir sind fertig. Im Folgenden sei daher $\mathfrak{a} \neq \{0\}$. Aufgrund von Definition 1.10 (c) folgt aus $n \in \mathfrak{a}$ stets auch $-n \in \mathfrak{a}$. Insbesondere ist $\mathfrak{a} \cap \mathbb{N}$ nicht leer und besitzt deshalb ein eindeutig bestimmtes kleinstes Element m. Dieses erfüllt $\mathfrak{a} = m\mathbb{Z}$,

denn: Jedes Element aus $m\mathbb{Z}$ ist von der Form rm mit einem $r \in \mathbb{Z}$. Wegen $m \in \mathfrak{a}$ folgt mit Definition 1.10 (c) hieraus $rm \in \mathfrak{a}$ und es gilt also die Inklusion $m\mathbb{Z} \subseteq \mathfrak{a}$.

Sei nun umgekehrt $a \in \mathfrak{a}$. Durch Division mit Rest erhalten wir $q, r \in \mathbb{Z}$ mit $a = qm + r$ und $0 \leq r < m$. Aufgrund von

$$r = a - qm = a + (-q)m \in \mathfrak{a}$$

und der Minimalität von m in $\mathfrak{a} \cap \mathbb{N}$ ergibt sich $r = 0$. Es folgt $a = qm \in m\mathbb{Z}$ und also auch die andere Inklusion $\mathfrak{a} \subseteq m\mathbb{Z}$. #

Zum Nachweis der Eindeutigkeit seien $m, n \in \mathbb{N}_0$ mit $m\mathbb{Z} = n\mathbb{Z}$. Dann gilt $n \in m\mathbb{Z}$ und $m \in n\mathbb{Z}$ und es existieren $r, \tilde{r} \in \mathbb{Z}$ mit $n = mr, m = n\tilde{r}$. Dies liefert $n = mr = n\tilde{r}r$. Im Fall $n = 0$ folgt hieraus $m = 0 \cdot \tilde{r} = 0$. Im Fall $n \neq 0$ erhalten wir $r = \tilde{r} = 1$ oder $r = \tilde{r} = -1$. Wegen $m, n \in \mathbb{N}_0$ ergibt sich $r = 1$, denn andernfalls wäre $m = -n < 0$. Wir erhalten $m = n$. □

Aus zwei Idealen in $\mathbb{Z}$ lässt sich auf einfache Weise ein weiteres Ideal erzeugen:

Definition 1.12. *Für je zwei Ideale $\mathfrak{a}, \mathfrak{b}$ Ideale in $\mathbb{Z}$ setzen wir*

$$\mathfrak{a} + \mathfrak{b} := \{a + b : a \in \mathfrak{a}, b \in \mathfrak{b}\}$$

*und nennen $\mathfrak{a} + \mathfrak{b}$ die **Summe** der Ideale $\mathfrak{a}$ und $\mathfrak{b}$.*

Proposition 1.13. *Für je zwei Ideale $\mathfrak{a}, \mathfrak{b}$ in $\mathbb{Z}$ ist die Summe $\mathfrak{a} + \mathfrak{b}$ wieder ein Ideal in $\mathbb{Z}$.*

Beweis. Aufgrund von $0 = 0 + 0$, $0 \in \mathfrak{a}$ und $0 \in \mathfrak{b}$ ist zunächst 0 in $\mathfrak{a} + \mathfrak{b}$ enthalten.

Sind $c_1, c_2 \in \mathfrak{a} + \mathfrak{b}$, so gibt es $a_1, a_2 \in \mathfrak{a}$ sowie $b_1, b_2 \in \mathfrak{b}$ mit $c_1 = a_1 + b_1$ und $c_2 = a_2 + b_2$. Es folgt

$$c_1 + c_2 = (a_1 + b_1) + (a_2 + b_2) = (a_1 + a_2) + (b_1 + b_2) \in \mathfrak{a} + \mathfrak{b}.$$

Sind schließlich $c \in \mathfrak{a} + \mathfrak{b}$ und $r \in \mathbb{Z}$, so gibt es Elemente $a \in \mathfrak{a}$ sowie $b \in \mathfrak{b}$ mit $c = a + b$. Das liefert

$$rc = r(a + b) = ra + rb \in \mathfrak{a} + \mathfrak{b}$$

und insgesamt die Proposition. □

Das folgende Beispiel legt nahe, dass ein sehr enger Zusammenhang zwischen Summen von Idealen in $\mathbb{Z}$ und größten gemeinsamen Teilern besteht:

Beispiel 1.14. *Es ist* $2\mathbb{Z} + 3\mathbb{Z} = \mathbb{Z}$,

denn: Es gilt

$$1 = \mathrm{ggT}(2, 3) = (-1) \cdot 2 + 1 \cdot 3 \in 2\mathbb{Z} + 3\mathbb{Z}$$

und für alle $r \in \mathbb{Z}$ *ist* $r = r \cdot 1 \in 2\mathbb{Z} + 3\mathbb{Z}$. #

Definition 1.12 und Proposition 1.13 verallgemeinern sich in naheliegender Weise auf Summen von Idealen $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ aus $\mathbb{Z}$. Offenbar ist Summenbildung von Idealen assoziativ. Wir erhalten mit dem folgenden Satz eine explizite Beschreibung von Summen von Idealen aus $\mathbb{Z}$ und damit gleichzeitig die Existenz des größten gemeinsamen Teilers ganzer Zahlen $a_1, \ldots, a_n$:

Satz 1.15. *Seien* $n \in \mathbb{N}$ *und* $a_1, \ldots, a_n \in \mathbb{Z}$. *Dann besitzen die Zahlen* $a_1, \ldots, a_n$ *einen eindeutig bestimmten größten gemeinsamen Teiler* $\mathrm{ggT}(a_1, \ldots, a_n)$ *und es gilt*

$$a_1\mathbb{Z} + \ldots + a_n\mathbb{Z} = \mathrm{ggT}(a_1, \ldots, a_n)\mathbb{Z}.$$

Insbesondere gibt es $u_1, \ldots, u_n \in \mathbb{Z}$ *mit* $\mathrm{ggT}(a_1, \ldots, a_n) = u_1a_1 + \ldots + u_na_n$.

Beweis. Nach den Propositionen 1.11 und 1.13 gibt es ein $d \in \mathbb{N}_0$ mit $a_1\mathbb{Z} + \ldots + a_n\mathbb{Z} = d\mathbb{Z}$. Dieses ist ein größter gemeinsamer Teiler von $a_1, \ldots, a_n$,

denn: Sei $i \in \{1, \ldots, n\}$. Aufgrund von

$$a_i = 0 \cdot a_1 + \ldots + 0 \cdot a_{i-1} + 1 \cdot a_i + 0 \cdot a_{i+1} + \cdots + 0 \cdot a_n \in a_1\mathbb{Z} + \ldots + a_n\mathbb{Z} = d\mathbb{Z}$$

gibt es ein $r_i \in \mathbb{Z}$ mit $a_i = dr_i$. Insbesondere ist d ein Teiler von a_i und es gilt $d \in T(a_1, \ldots, a_n)$. Sei nun $t \in T(a_1, \ldots, a_n)$. Wegen $d \in d\mathbb{Z} = a_1\mathbb{Z} + \ldots + a_n\mathbb{Z}$ existieren $u_1, \ldots, u_n \in \mathbb{Z}$ mit $d = u_1a_1 + \ldots + u_na_n$. Aufgrund von $t \mid a_1, \ldots, t \mid a_n$ folgt dann $t \mid d$. #

Die Eindeutigkeitsaussage ergibt sich unmittelbar aus Proposition 1.5. □

Der Beweis von Satz 1.15 lässt sich nicht für ein direktes Rechenverfahren zur Bestimmung von $\mathrm{ggT}(a_1, \ldots, a_n)$ verwenden. Allerdings zeigt eine genauere Betrachtung, dass der Euklidische Algorithmus auch hier zum Ziel führt:

Korollar 1.16. *Seien $n \in \mathbb{N}$ und $a_1, \ldots, a_n \in \mathbb{Z}$. Dann gilt*

$$\mathrm{ggT}(a_1, \ldots, a_n) = \mathrm{ggT}\big(a_1, \mathrm{ggT}(a_2, \ldots, a_n)\big).$$

Insbesondere kann $\mathrm{ggT}(a_1, \ldots, a_n)$ durch sukzessives Anwenden des Euklidischen Algorithmus 1.7 berechnet werden.

Beweis. Anwenden von Satz 1.15 liefert

$$\begin{aligned} \mathrm{ggT}(a_1, \ldots, a_n)\mathbb{Z} &= a_1\mathbb{Z} + a_2\mathbb{Z} + \ldots + a_n\mathbb{Z} \\ &= a_1\mathbb{Z} + \mathrm{ggT}(a_2, \ldots, a_n)\mathbb{Z} \\ &= \mathrm{ggT}(a_1, \mathrm{ggT}(a_2, \ldots, a_n))\mathbb{Z}. \end{aligned}$$

Das Korollar ergibt sich nun aus der Eindeutigkeitsaussage in 1.11. □

1.2 Der Fundamentalsatz der Arithmetik

In diesem Abschnitt werden uns mit einigen einfachen, aber für das Weitere sehr wichtigen Eigenschaften von Primzahlen beschäftigen. Zunächst wiederholen wir aber diesen Begriff:

Definition 1.17. *Ein natürliche Zahl $p > 1$ heißt eine **Primzahl**, wenn $T(p) = \{\pm 1, \pm p\}$ und also $T(p) \cap \mathbb{N} = \{1, p\}$ ist. Die Menge der Primzahlen bezeichnen wir mit $\mathbb{P}$.*

Proposition 1.18. *Sei $a \in \mathbb{N}$ größer als 1. Dann ist der kleinste positive, von 1 verschiedene Teiler von a eine Primzahl.*

Beweis. Wir setzen $T_+ := (T(a) \cap \mathbb{N}) \setminus \{1\} = \{t \in \mathbb{N} : t \mid a, t \neq 1\}$. Wegen $a \in T_+$ ist $T_+ \neq \emptyset$, insbesondere hat T_+ ein kleinstes Element p. Dieses ist eine Primzahl,

denn: Sei dazu $1 < t \in \mathbb{N}$ ein Teiler von p. Aufgrund von $p \mid a$ gilt dann nach Proposition 1.2 (c) auch $t \mid a$ und also $t \in T_+$. Da $t \mid p$ insbesondere $t \leq p$ nach sich zieht, folgt aus der Minimalität von p in T_+ bereits $t = p$ und damit die Primalität von p. #

□

Die nächste Aussage war bereits in der Antike bekannt und findet sich etwa in Euklids *Elementen*:

Satz 1.19 (Satz von Euklid)**.** *Es gibt unendlich viele Primzahlen.*

Beweis. Wir nehmen an, es gäbe es nur endlich viele Primzahlen $p_1, \ldots, p_n$, und setzen $N := p_1 \cdot \ldots \cdot p_n + 1$. Dann gälte $N > 1$ und nach Proposition 1.18 gäbe es eine Primzahl p mit $p \mid N$. Wegen $p \in \{p_1, \ldots, p_n\}$ folgte $p \mid p_1 \cdot \ldots \cdot p_n$ und somit auch $p \mid (N - p_1 \cdot \ldots \cdot p_n) = 1$, was nicht sein kann. □

Die nachfolgende Charakterisierung von Primzahlen ist sehr wichtig und in vielen Beweisen tauglicher als die direkte Verwendung der Definition von Primzahlen:

Proposition 1.20 (Primalitätskriterium)**.** *Sei $1 < p \in \mathbb{N}$. Dann sind äquivalent:*

(i) *p ist eine Primzahl.*

(ii) *Aus $p \mid ab$ für $a, b \in \mathbb{Z}$ folgt stets $p \mid a$ oder $p \mid b$.*

Beweis. Gelte zunächst Aussage (i). Seien dafür p eine Primzahl und $a, b \in \mathbb{Z}$ mit $p \mid ab$ und $p \nmid a$. Dann ist $\mathrm{ggT}(p, a) = 1$ und nach Proposition 1.9 (a) gilt $p \mid b$. Wir haben somit Aussage (ii) nachgewiesen.

Gelte nun umgekehrt Aussage (ii) und sei $a \in \mathbb{N}$ ein beliebiger Teiler von p. Dann gibt es ein $b \in \mathbb{Z}$ mit $p = ab$. Mit (ii) folgt hieraus $p \mid a$ oder $p \mid b$. Nach Konstruktion gelten andererseits offensichtlich $a \mid p$ und $b \mid p$. Zusammengenommen erhalten wir, dass eine der beiden Aussagen

$$\begin{aligned} p \mid a \quad &\text{und} \quad a \mid p, \\ \text{bzw. } p \mid b \quad &\text{und} \quad b \mid p \end{aligned}$$

zutrifft. Dies impliziert $a = p$ oder $b = p$, und demzufolge $a = p$ oder $a = 1$. Also ist p eine Primzahl. □

Als nächstes zeigen wir, dass die Primzahlen in gewissem Sinne die „Bausteine“ der natürlichen Zahlen darstellen. Wichtig für den Beweis ist das soeben gezeigte Primalitätskriterium 1.20:

Satz 1.21 (Fundamentalsatz der Arithmetik)**.** *Jede natürliche Zahl lässt sich bis auf die Reihenfolge der Faktoren eindeutig als Produkt von Primzahlen schreiben.*

Beweis. Wir zeigen die Aussage per Induktion nach $n \in \mathbb{N}$: Die Zahl $n = 1$ ist konventionsgemäß das leere Produkt und $n = 2$ ist selbst eine Primzahl. Sei ab sofort $n > 2$. Ist n eine Primzahl, dann haben wir bereits eine Primfaktorzerlegung erreicht. Ist n keine Primzahl, so ist $n = ab$ für geeignete $a, b \in \mathbb{N}$ mit $1 < a, b < n$. Nach Induktionsvoraussetzung besitzen a, b jeweils eine Primfaktorzerlegung, das gilt dann aber auch für deren Produkt $n = ab$. Damit ist die Existenz einer Primfaktorzerlegung gezeigt.

Zum Nachweis der Eindeutigkeit der Primfaktorzerlegung bis auf die Reihenfolge der Faktoren gelte

$$n = p_1 \cdot \ldots \cdot p_r = q_1 \cdot \ldots \cdot q_s$$

mit Primzahlen $p_1, \dots p_r$ und $q_1, \dots, q_s$. Insbesondere gilt dann $p_1 \mid q_1 \cdot \ldots \cdot q_s$. Weil p_1 eine Primzahl ist, gibt es nach dem Primalitätskriterium 1.20 ein $i \in \{1, \dots, s\}$ mit $p_1 \mid q_i$. Nach Umnummerieren können wir dabei ohne Einschränkung $i = 1$ annehmen. Da q_1 und p_1 Primzahlen sind, folgt $p_1 = q_1$. Durch Kürzen von p_1 erhalten wir aus der Ausgangsgleichung

$$p_2 \cdot \ldots \cdot p_r = q_2 \cdot \ldots \cdot q_s < n$$

Aus der Induktionsvoraussetzung erhalten wir nun $r = s$ und durch Vertauschen können wir $p_2 = q_2, \dots, p_r = q_r$ erreichen. □

Obwohl sich schon in Euklids *Elementen* dem Fundamentalsatz 1.21 verwandte Aussagen finden, scheint seine erste klare Formulierung von Carl Friedrich Gauß in seinen *Disquisitiones Arithmeticae* von 1801 gegeben worden zu sein.

Bemerkung 1.22. *Sei $n \in \mathbb{N}$. Fasst man in der im Fundamentalsatz 1.21 gegebenen Primfaktorzerlegung von n mehrfach vorkommende Primfaktoren in der Form $p \cdot \ldots \cdot p = p^\nu$ zusammen, so erhält man die Existenz einer* ***kanonischen Primfaktorzerlegung***

$$n = \prod_{p \in \mathbb{P}} p^{\nu_p(n)}$$

von n. Die Exponenten $\nu_p(n) \in \mathbb{N}_0$ sind hierbei durch n eindeutig bestimmt und heißen die ***Vielfachheiten*** *der Primzahlen p in n. Nach Konstruktion gilt dabei $\nu_p(n) \neq 0$ für nur endlich viele p.*

Wir können nun die Teiler einer gegebenen natürlichen Zahl präzise angeben und bereiten dies mit dem folgenden Lemma vor:

Lemma 1.23. *Für beliebige $n, m \in \mathbb{N}$ gilt:*

$$n \mid m \quad :\Longleftrightarrow \quad \nu_p(n) \leq \nu_p(m) \text{ für alle } p \in \mathbb{P}.$$

Beweis. Die Aussage $n \mid m$ ist gleichbedeutend mit der Existenz eines $a \in \mathbb{N}$ mit $m = an$. Mit der Existenz der eindeutigen kanonischen Primfaktorzerlegung aus Bemerkung 1.22 folgt hieraus

$$\nu_p(m) = \nu_p(a) + \nu_p(n) \qquad \text{für alle } p \in \mathbb{P}.$$

und wegen $\nu_p(a) \in \mathbb{N}_0$ insbesondere

$$\nu_p(m) \geq \nu_p(n) \qquad \text{für alle } p \in \mathbb{P}.$$

Gilt aber umgekehrt diese letzte Aussage, so sind die Differenzen $\delta_p := \nu_p(m) - \nu_p(n)$ für alle $p \in \mathbb{P}$ nichtnegative ganze Zahlen, aber höchstens endlich viele δ_p sind positiv. Es folgt $a := \prod_{p \in \mathbb{P}} p^{\delta_p} \in \mathbb{N}$ und konstruktionsgemäß auch $m = an$. □

Satz 1.24. *Für eine natürliche Zahl n mit kanonischer Primfaktorzerlegung $n = \prod_{p\in\mathbb{P}} p^{\nu_p(n)}$ gibt*

$$\tau(n) := \prod_{p\in\mathbb{P}} (1+\nu_p(n)) = \prod_{p\in\mathbb{P}} \tau(p^{\nu_p(n)}) \qquad \text{die Anzahl der Teiler von } n,$$

$$\sigma(n) := \prod_{p\in\mathbb{P}} \frac{p^{\nu_p(n)+1}-1}{p-1} = \prod_{p\in\mathbb{P}} \sigma(p^{\nu_p(n)}) \qquad \text{die Summe der Teiler von } n$$

*an. Die so definierten Funktionen $\tau\colon \mathbb{N}\to\mathbb{N}$ und $\sigma\colon \mathbb{N}\to\mathbb{N}$ nennen wir daher auch die **Teileranzahlfunktion** bzw. die **Teilersummenfunktion**. Wir werden in Kapitel 2 noch einmal auf diese Funktionen zurückkommen.*

Beweis. Nach Lemma 1.23 sind die Teiler von n genau diejenigen natürlichen Zahlen mit einer kanonischen Primfaktorzerlegung der Form

$$\prod_{p\in\mathbb{P}} p^{\nu_p(d)} \quad \text{mit } 0 \le \nu_p(d) \le \nu_p(n) \text{ für alle } p \in \mathbb{P}.$$

Da diese Zahlen nach dem Fundamentalsatz 1.21 paarweise verschieden sind, erhalten wir hieraus einerseits unmittelbar die behauptete Formel für τ und andererseits

$$\sigma(n) = \sum_{d|n}\Big(\prod_{p\in\mathbb{P}} p^{\nu_p(d)}\Big) = \prod_{p\in\mathbb{P}}\Big(\sum_{\nu=0}^{\nu_p(n)} p^{\nu}\Big) = \prod_{p\in\mathbb{P}} \frac{p^{\nu_p(n)+1}-1}{p-1}.$$

Insgesamt haben wir den Satz bewiesen. □

1.3 Vollkommene Zahlen

In der Zahlenmystik des Pythagoras (um 550 v. Chr.) spielten natürliche Zahlen, deren natürliche, echte Teiler sich zur gegebenen Zahl aufaddieren, eine wichtige Rolle. Pythagoras und seine Schule nannten derartige Zahlen vollkommen. Wir definieren:

Definition 1.25. *Für eine natürliche Zahl $n \in \mathbb{N}$ gilt:*

$$n \text{ heißt } \textbf{\textit{vollkommen}} \quad :\Longleftrightarrow \quad \sigma(n) = 2n.$$

Satz 1.26. *Für ein beliebiges $k \in \mathbb{N}$ heißt $M_k := 2^k - 1$ die **k-te Mersenne-Zahl**. Für eine beliebige gerade natürliche Zahl $n \in 2\mathbb{N}$ sind die folgenden beiden Aussagen äquivalent:*

(i) *n ist vollkommen.*

(ii) *$n = 2^{k-1}M_k$ mit ganzem $k \ge 2$ und M_k prim.*

Beweis. Gelte zunächst Aussage (ii). Nach Satz 1.24 und wegen $M_k \in \mathbb{P} \setminus \{2\}$ ist

$$\sigma(n) = \sigma(2^{k-1})\sigma(M_k) = \Big(\sum_{\nu=0}^{k-1} 2^\nu\Big)(1 + M_k) = (2^k - 1)2^k \overset{\text{(ii)}}{=} 2n,$$

also ist n vollkommen und es gilt Aussage (i).

Gelte nun umgekehrt (i), sei also n vollkommen. Wir schreiben die gerade Zahl n als

$$n = 2^{k-1}m \quad \text{mit ungeradem } m \in \mathbb{N} \text{ und ganzem } k \geq 2.$$

Wegen der Vollkommenheit von n und nach Satz 1.24 folgt

$$2^k m = 2n = \sigma(n) = \sigma(2^{k-1})\sigma(m) = (2^k - 1)\sigma(m).$$

Durch Vergleich der eindeutigen kanonischen Primfaktorzerlegungen auf beiden Seiten und wegen der Ungeradheit von $2^k - 1$ erhalten wir $2^k \mid \sigma(m)$. Es gibt also ein $\ell \in \mathbb{N}$ mit

$$\sigma(m) = 2^k \ell$$

und nach Einsetzen in die obige Gleichung erhalten wir

$$m = (2^k - 1)\ell.$$

Wäre hierbei $\ell > 1$, so hätte m mindestens 1, ℓ und $(2^k - 1)\ell$ als verschiedene, positive Teiler. Im Widerspruch zum bereits Bewiesenen folgte

$$\sigma(m) \geq 1 + \ell + (2^k - 1)\ell > 2^k \ell.$$

Es gilt also $\ell = 1$. Wir erhalten sofort

$$\sigma(m) = 2^k = (2^k - 1) + 1 = m + 1$$

und somit die Primalität von $m = 2^k - 1 = M_k$. Insgesamt haben wir Aussage (ii) hergeleitet. □

Bemerkung 1.27. (a) *Dass die in Aussage (ii) von Satz 1.26 beschriebenen Zahlen vollkommen sind, geht auf Euklid (ca. 350 v. Chr.) zurück. Die umgekehrte Implikation zeigte Leonhard Euler im Jahr 1747.*

(b) *Über ungerade vollkommene Zahlen weiß man viel weniger; man vermutet, dass es sie nicht gibt.*

(c) *Die kleinsten geraden vollkommenen Zahlen sind* 6, 28, 496, 8128.

Nach Satz 1.26 ist die Frage nach geraden vollkommenen Zahlen äquivalent mit derjenigen danach, welche Mersenne-Zahlen Primzahlen sind. Eine hierfür notwendige Bedingung liefert:

Proposition 1.28. *Für ein beliebiges $k \in \mathbb{N}$ gilt: Ist M_k prim, so notwendig auch k.*

Beweis. Für ein beliebiges $n \in \mathbb{N}$ gilt im Polynomring $\mathbb{R}[X, Y]$ die Gleichung

$$X^n - Y^n = (X - Y) \cdot \sum_{\nu=0}^{n-1} X^\nu Y^{n-1-\nu}.$$

Ist nun $k \in \mathbb{N}$ nicht prim, so gibt es natürliche Zahlen $1 < n, m < k$ mit $k = nm$. Setzen wir in der obigen Gleichung $X = 2^m$ und $Y = 1$ ein, so erhalten wir

$$M_k = 2^k - 1 = (2^m)^n - 1^n = (2^m - 1) \cdot \sum_{\nu=0}^{n-1} 2^{m\nu} = M_m \cdot \sum_{\nu=0}^{n-1} 2^{m\nu}$$

und insbesondere $M_m \mid M_k$. Mit $m \notin \{1, k\}$ folgt $M_m \notin \{1, M_k\}$, so dass M_k keine Primzahl ist. □

Bemerkung 1.29. *Umgekehrt zur Aussage von Proposition 1.28 gibt es sehr viele Primzahlen k, für die M_k keine Primzahl ist. Derzeit (Stand: Oktober 2024) sind genau 52 Mersenne-Primzahlen – und somit auch genau 52 gerade vollkommene Zahlen – bekannt, deren größte über 41 Millionen Stellen aufweist. Da es einen besonders effizienten Primzahltest für sie gibt, sind tatsächlich die größten derzeit bekannten Primzahlen Mersenne-Primzahlen.*

KAPITEL 2

Zahlentheoretische Funktionen

2.1 Der Ring der zahlentheoretischen Funktionen

Eine zahlentheoretische Funktion ist zunächst nichts anderes als eine Folge mit Werten in den komplexen Zahlen. Erst wenn eine arithmetische Komponente – wie etwa das Abzählen von Teilern – hinzukommt, wirkt der Begriff umfänglich motiviert. Diese subjektive Begriffsbildung kann jedoch nicht stringent mathematisch umgesetzt werden, so dass wir uns damit begnügen, die arithmetische Komponente durch die später aufgezeigte Ringstruktur auf der Menge der zahlentheoretischen Funktionen zu erklären.

Definition 2.1. *Eine beliebige Abbildung $a\colon \mathbb{N} \to \mathbb{C}$ nennen wir eine **zahlentheoretische Funktion**.*

Wir geben sogleich einige Beispiele wichtiger zahlentheoretischer Funktionen:

Beispiel 2.2. (a) *Für ein beliebiges $s \in \mathbb{C}$ nennen wir die durch $\iota^s(n) := n^s$ für alle $n \in \mathbb{N}$ definierte zahlentheoretische Funktion die **s-te Potenzfunktion**. Neben der Identität $\iota^1 =: \iota$ ist die konstante Einsfunktion ι^0 ein wichtiger Spezialfall.*

(b) *Für ein beliebiges $s \in \mathbb{C}$ definieren wir die **s-te Teilersummenfunktion** $\sigma_s\colon \mathbb{N} \to \mathbb{C}$ durch*

$$\sigma_s(n) := \sum_{d|n} d^s.$$

Summiert wird hierbei selbstverständlich nur über alle natürlichen Teiler d von n und nicht etwa auch über deren negative Gegenstücke in den ganzen Zahlen, was wir in diesem Kontext ohne weitere Erwähnung stets so handhaben wollen. Spezielle Teilersummenfunktionen sind uns mit den Funktionen $\tau = \sigma_0$ und $\sigma = \sigma_1$ bereits in Satz 1.24 begegnet. Genauer werden wir die Teilersummenfunktionen in Abschnitt 2.2 untersuchen.

(c) *Wir definieren die **Euler'sche φ-Funktion** $\varphi\colon \mathbb{N} \to \mathbb{N}$ durch*

$$\varphi(n) := \#\{k \in \mathbb{N}_0 : 0 \leq k < n \text{ und } \operatorname{ggT}(k,n) = 1\}.$$

Die φ-Funktion wurde zuerst 1763 *von Euler studiert. Die heute übliche Bezeichnung mit dem griechischen Buchstaben φ stammt von Gauß, der sie* 1801 *in seinen* Disquisitiones *einführte. Wir werden die φ-Funktion in Abschnitt 2.4 genauer studieren.*

(d) *Wir definieren die* ***Möbius-Funktion*** $\mu\colon \mathbb{N} \to \mathbb{C}$ *durch*

$$\mu(n) := \begin{cases} (-1)^k, & \text{für } n = p_1 \cdot p_2 \cdot \ldots \cdot p_k \text{ mit } k \in \mathbb{N}_0 \text{ und } p_1, \ldots, p_k \\ & \text{paarweise verschiedene Primzahlen,} \\ 0, & \text{sonst.} \end{cases}$$

Wegen der Eindeutigkeit der Primfaktorzerlegung bis auf Reihenfolge ist dies wohldefiniert. Es ist zum Beispiel

$$\begin{aligned} &\mu(1) = (-1)^0 = 1, && \\ &\mu(p) = (-1)^1 = -1 && \text{für jede Primzahl } p, \\ &\mu(pq) = (-1)^2 = 1, && \text{für Primzahlen } p \neq q, \\ &\mu(p^2) = 0, && \text{für jede Primzahl } p. \end{aligned}$$

Die Möbius-Funktion wurde zuerst 1832 *von Möbius studiert und spielt eine wichtige Rolle bei der Untersuchung der multiplikativen Struktur der Menge der zahlentheoretischen Funktionen, vergleiche auch Abschnitte 2.2 und 2.3.*

Wir können die Gesamtheit aller zahlentheoretischen Funktionen zur Menge

$$\mathcal{A} := \{a\colon \mathbb{N} \to \mathbb{C}\}$$

zusammenschließen. Offenbar besitzt diese durch komponentenweise Addition die Struktur einer abelschen Gruppe und wird ferner durch skalare Multiplikation zu einem $\mathbb{C}$-Vektorraum. Wir wollen $\mathcal{A}$ durch eine zusätzliche multiplikative Verknüpfung noch mehr Struktur verschaffen:

Definition 2.3. *Die Vorschrift*

$$*\colon \begin{cases} \mathcal{A} \times \mathcal{A} & \to \mathcal{A}, \\ (a, b) & \mapsto a * b \end{cases}$$

mit

$$(a * b)\colon \begin{cases} \mathbb{N} & \to \mathbb{C}, \\ n & \mapsto (a * b)(n) := \sum_{d|n} a(d) b\left(\frac{n}{d}\right) \end{cases}$$

wird auch als die ***Dirichlet-Faltung*** *der zahlentheoretischen Funktionen a und b bezeichnet.*

Beispiel 2.4. *Für ein beliebiges* $s \in \mathbb{C}$ *gilt offenbar* $\iota^0 * \iota^s = \sigma_s$.

Satz 2.5. *Das Tripel $(\mathcal{A}, +, *)$ mit komponentenweiser Addition $+$ und Dirichlet-Faltung $*$ ist ein kommutativer Ring mit Eins*

$$\mathbb{1}_{\mathcal{A}}(n) := \begin{cases} 1 & \text{für } n = 1, \\ 0 & \text{für } n > 1 \end{cases}$$

und Einheitengruppe

$$\mathcal{A}^{\times} = \{a \in \mathcal{A} : a(1) \neq 0\}.$$

Beweis. Die erste Behauptung lässt sich direkt nachrechnen und wird dem Leser überlassen. Wir zeigen aber die zweite Behauptung:

Sei zunächst a in der Einheitengruppe. Dann gibt es eine zahlentheoretische Funktion $b \in \mathcal{A}$ mit $a * b = \mathbb{1}_{\mathcal{A}}$ und also

$$1 = \mathbb{1}_{\mathcal{A}}(1) = (a * b)(1) = a(1)b(1).$$

Insbesondere kann $a(1)$ nicht Null sein.

Sei nun umgekehrt a eine zahlentheoretische Funktion mit $a(1) \neq 0$. Wir definieren induktiv eine zahlentheoretische Funktion b wie folgt: Zuerst setzen wir

$$b(1) := a(1)^{-1}.$$

Sind nun für ein beliebiges $n > 1$ die Werte $b(1), \ldots, b(n-1)$ bereits definiert, so setzen wir

$$b(n) := -a(1)^{-1} \sum_{\substack{d|n \\ d<n}} b(d) a\left(\frac{n}{d}\right).$$

Auf diese Weise erhalten wir eine Funktion b mit

$$\begin{aligned} (b * a)(1) &= b(1)a(1) = 1 = \mathbb{1}_{\mathcal{A}}(1), \\ (b * a)(n) &= b(n)a(1) + \sum_{\substack{d|n \\ d<n}} b(d) a\left(\frac{n}{d}\right) = 0 = \mathbb{1}_{\mathcal{A}}(n) \quad \text{für } n > 1 \end{aligned}$$

und also $b = a^{-1}$. Es folgt, dass a in der Einheitengruppe liegt. □

2.2 Multiplikativität

Wir benötigen nun den in der Zahlentheorie zentralen Begriff der Multiplikativität zahlentheoretischer Funktionen. Wir unterscheiden hierbei zwischen zwei Varianten:

Definition 2.6. *Sei a eine nicht konstant verschwindende zahlentheoretische Funktion.*

(a) *Wir bezeichnen a als **schwach multiplikativ**, falls für alle zueinander teilerfremden natürlichen n und m die Beziehung $a(nm) = a(n)a(m)$ gilt.*

(b) *Wir bezeichnen a als* ***stark multiplikativ****, falls für alle natürlichen n und m die Beziehung* $a(nm) = a(n)a(m)$ *gilt.*

Lemma 2.7. *Jede schwach multiplikative und somit auch jede stark multiplikative zahlentheoretische Funktion a erfüllt* $a(1) = 1$.

Beweis. Wegen $\mathrm{ggT}(n, 1) = 1$ für alle $n \in \mathbb{N}$ gilt mit der schwachen Multiplikativität

$$a(n) = a(n \cdot 1) = a(n) \cdot a(1) \quad \text{für alle } n \in \mathbb{N}.$$

Aufgrund von $a \not\equiv 0$ folgt hieraus zunächst $a(1) \neq 0$. Nutzen wir dies im Spezialfall $n = 1$ aus, so erhalten wir $a(1) = 1$ und also die Behauptung. □

Stark multiplikative Funktionen lassen sich offensichtlich leicht handhaben. Für die Zahlentheorie interessante Funktionen sind aber oft nur schwach multiplikativ:

Beispiel 2.8. *Die Möbius-Funktion* μ *ist schwach multiplikativ, aber nicht stark multiplikativ,*

denn: Wegen

$$\mu(4) = 0 \neq 1 = (-1)^2 = \mu(2)\mu(2)$$

ist μ *offenbar nicht stark multiplikativ. Wir zeigen nun die schwache Multiplikativität: Zunächst gilt* $\mu(1) = 1 \neq 0$. *Weiter betrachten wir* $\mu(nm)$ *für teilerfremde* $n, m \in \mathbb{N}$ *und unterscheiden hierbei die folgenden (nicht disjunkten) drei Fälle:*

Fall 1: $\mu(n) = 0$. *Dann gibt es eine Primzahl p mit* $p^2 \mid n$. *Es folgt unmittelbar* $p^2 \mid nm$ *und somit*

$$\mu(nm) = 0 = \mu(n)\mu(m).$$

Fall 2: $\mu(m) = 0$. *Analog zu Fall* 1.

Fall 3: $\mu(n) \neq 0 \neq \mu(m)$. *Dann gibt es* $k_n, k_m \in \mathbb{N}_0$, *so dass* n, m *und wegen der Teilerfremdheit auch* nm *Produkte von* k_n, k_m *bzw.* $k_n + k_m$ *paarweise verschiedenen Primzahlen sind, und es gilt*

$$\mu(nm) = (-1)^{k_n + k_m} = (-1)^{k_n}(-1)^{k_m} = \mu(n)\mu(m).$$

#

Eine Anleitung zur Handhabung schwach multiplikativer zahlentheoretischer Funktionen liefert das folgende Lemma:

Lemma 2.9. *Für eine nicht konstant verschwindende zahlentheoretische Funktion a sind äquivalent:*

(i) *a ist schwach multiplikativ.*

(ii) *Für jedes* $n \in \mathbb{N}$ *mit Primfaktorzerlegung* $n = \prod_{j=1}^{k_n} p_j^{\nu_{p_j}(n)}$ *gilt*

$$a(n) = \prod_{j=1}^{k_n} a\left(p_j^{\nu_{p_j}(n)}\right).$$

Bemerkung 2.10. *Nach Lemma 2.9 gibt uns Satz 1.24 bereits die schwache Multiplikativität der Teilersummenfunktionen $\tau = \sigma_0$ und $\sigma = \sigma_1$.*

Beweis von Lemma 2.9. Gelte zunächst Aussage (i), sei also a schwach multiplikativ. Zum Beweis von Aussage (ii) führen wir dann eine Induktion nach k_n durch, wobei der Fall $k_n = 0$ mit Lemma 2.7 folgt und der Fall $k_n = 1$ trivial ist. Sei also $k_n > 1$ und nehmen wir an, Aussage (ii) sei für $k_n - 1$ bereits bewiesen. Wegen der Eindeutigkeit der Primfaktorzerlegung gilt

$$\operatorname{ggT}\left(p_1^{\nu_{p_1}(n)}, \prod_{j=2}^{k_n} p_j^{\nu_{p_j}(n)}\right) = 1$$

und wegen der schwachen Multiplikativität somit

$$a(n) = a\left(p_1^{\nu_{p_1}(n)}\right) \cdot a\left(\prod_{j=2}^{k_n} p_j^{\nu_{p_j}(n)}\right) \overset{\text{Ind.vorauss.}}{=} \prod_{j=1}^{k_n} a\left(p_j^{\nu_{p_j}(n)}\right).$$

Es folgt Aussage (ii).

Gelte nun umgekehrt Aussage (ii). Für beliebige $n, m \in \mathbb{N}$ mit $\operatorname{ggT}(n,m) = 1$ und kanonischen Primfaktorzerlegungen

$$n = \prod_{j=1}^{k_n} p_j^{\nu_{p_j}(n)} \quad \text{und} \quad m = \prod_{k=1}^{k_m} q_k^{\nu_{q_k}(m)}$$

gilt

$$\begin{aligned} a(nm) &= a\left(\prod_{j=1}^{k_n} p_j^{\nu_{p_j}(n)} \cdot \prod_{k=1}^{k_m} q_k^{\nu_{q_k}(m)}\right) \\ &\overset{\text{(ii)}}{=} \prod_{j=1}^{k_n} a\left(p_j^{\nu_{p_j}(n)}\right) \cdot \prod_{k=1}^{k_m} a\left(q_k^{\nu_{q_k}(m)}\right) \\ &= a(n)a(m) \end{aligned}$$

und somit die schwache Multiplikativität (i). □

Hieraus folgt unmittelbar:

Korollar 2.11. *Stimmen zwei schwach multiplikative zahlentheoretische Funktionen auf allen Primpotenzen überein, so sind sie bereits als Funktionen identisch.*

Nach Satz 2.5 und Lemma 2.7 besitzt jede schwach multiplikative Funktion ein Inverses in $\mathcal{A}$. Es gilt sogar noch mehr:

Satz 2.12. *Die Teilmenge*

$$\mathcal{A}^* := \{a \in \mathcal{A} : a \text{ ist schwach multiplikativ}\} \subseteq \mathcal{A}^\times$$

ist eine Untergruppe von $\mathcal{A}^\times$.

Beweis. Wir weisen das Untergruppenkriterium nach. Da $\mathbb{1}_\mathcal{A}$ offenkundig schwach multiplikativ ist, ist die Teilmenge $\mathcal{A}^*$ nicht leer. Weiterhin gilt

$$(a * b) \in \mathcal{A}^* \quad \text{für je zwei zahlentheoretische Funktionen } a, b \in \mathcal{A}^*, \tag{2.1}$$

denn: Nach Lemma 2.7 gilt

$$(a * b)(1) \quad = a(1)b(1) = 1 \neq 0,$$

so dass $a * b$ nicht konstant verschwindet. Außerdem gilt nach Voraussetzung für alle zueinander teilerfremden natürlichen Zahlen n, m

$$\begin{aligned}(a * b)(nm) &= \sum_{d|nm} a(d)b\left(\frac{nm}{d}\right) \\ &= \sum_{d_n|n} \sum_{d_m|m} a(d_n d_m)b\left(\frac{n}{d_n}\frac{m}{d_m}\right) \\ &= \sum_{d_n|n} a(d_n)b\left(\frac{n}{d_n}\right) \sum_{d_m|m} a(d_m)b\left(\frac{m}{d_m}\right) \\ &= (a * b)(n)\,(a * b)(m).\end{aligned}$$

#

Schließlich gilt auch

$$a^{-1} \in \mathcal{A}^* \quad \text{für jede zahlentheoretische Funktion } a \in \mathcal{A}^*,$$

denn: Wir zeigen die Behauptung, indem wir eine schwach multiplikative zahlentheoretische Funktion $b \in \mathcal{A}$ konstruieren und nachweisen, dass diese mit a^{-1} übereinstimmt. Hierfür definieren wir

$$b(p^j) := a^{-1}(p^j) \quad \text{für alle Primzahlen } p \text{ und alle } j \in \mathbb{N}_0$$

und setzen dies (schwach) multiplikativ auf ganz $\mathbb{N}$ fort. Die Funktion b ist nach Konstruktion schwach multiplikativ, so dass wir den ersten Schritt unseres Beweises bereits bewältigt haben. Da nach Voraussetzung auch a schwach multiplikativ ist, gilt dies nach (2.1) auch für $a * b$. Da auch $\mathbb{1}_\mathcal{A}$ schwach multiplikativ ist, genügt es zum Beweis unserer Behauptung

$$(a * b)(p^j) = \mathbb{1}_\mathcal{A}(p^j) \quad \text{für alle Primzahlen } p \text{ und alle } j \in \mathbb{N}_0$$

zu zeigen. Tatsächlich gilt

$$\begin{aligned}(a * b)(p^j) &= \sum_{0\le k\le j} a(p^k)b(p^{j-k}) \\ &= \sum_{0\le k\le j} a(p^k)a^{-1}(p^{j-k}) \\ &= (a * a^{-1})(p^j) = \mathbb{1}_{\mathcal{A}}(p^j),\end{aligned}$$

wobei wir für die zweite Gleichheit ausgenutzt haben, dass nach Konstruktion von b die Funktionen b und a^{-1} auf Primpotenzen übereinstimmen. #

□

Indem wir die Resultate dieses Abschnitts auf die Teilersummenfunktionen σ_s für $s \in \mathbb{C}$ anwenden, können wir die in Satz 1.24 für die Spezialfälle $\tau = \sigma_0$ und $\sigma = \sigma_1$ gezeigten Resultate mühelos auch in Allgemeinheit zeigen:

Satz 2.13. *Für jedes beliebige $s \in \mathbb{C}$ ist die Teilersummenfunktion σ_s schwach multiplikativ, aber nicht stark multiplikativ.*

Beweis. Nach Beispiel 2.4 lässt sich für ein beliebiges $s \in \mathbb{C}$ die Teilersummenfunktion σ_s als Faltung

$$\iota^0 * \iota^s = \sigma_s.$$

zweier offensichtlich stark multiplikativer und also insbesondere schwach multiplikativer zahlentheoretischer Funktionen schreiben. Nach Satz 2.12 ist damit auch σ_s schwach multiplikativ.

Dass σ_s für kein $s \in \mathbb{C}$ stark multiplikativ ist, sieht man an

$$\sigma_s(4) = 1 + 2^s + 4^s \neq 1 + 2 \cdot 2^s + 4^s = (1 + 2^s)\,(1 + 2^s) = \sigma_s(2)\sigma_s(2).$$

Insbesondere haben wir gezeigt, dass die Faltung zweier stark multiplikativer Funktionen nicht wieder stark multiplikativ sein muss. □

Korollar 2.14. *Für jedes $s \in \mathbb{C}$ mit $\mathrm{Re}(s) \neq 0$ und jedes $n \in \mathbb{N}$ mit Primfaktorzerlegung $n = \prod_{\substack{p \text{ prim}\\ p|n}} p^{\nu_p(n)}$ gilt*

$$\sigma_s(n) = \prod_{\substack{p \text{ prim}\\ p|n}} \frac{p^{s(\nu_p(n)+1)} - 1}{p^s - 1}.$$

Beweis. Mit der endlichen geometrischen Summenformel gilt für jede Primzahl p und jedes $j \in \mathbb{N}$

$$\sigma_s(p^j) = \sum_{d|p^j} d^s = \sum_{k=0}^{j} p^{ks} = \sum_{k=0}^{j} (p^s)^k = \frac{(p^s)^{j+1} - 1}{p^s - 1}.$$

Das Korollar folgt mit Lemma 2.9 und Satz 2.13. □

2.3 Der Möbius'sche Umkehrsatz

In diesem Abschnitt werden wir ein Konzept einführen, um damit im Möbius'schen Umkehrsatz 2.20 das multiplikative Inverse der Möbius-Funktion zu bestimmen:

Definition 2.15. *Sei a eine zahlentheoretische Funktion. Unter der **summatorischen Funktion von** a versteht man die zahlentheoretische Funktion A, die durch*

$$A(n) := \sum_{d|n} a(d) \quad \text{für alle } n \in \mathbb{N}$$

definiert ist.

Beispiel 2.16. *Die summatorische Funktion der s-ten Potenzfunktion ι^s für ein festes $s \in \mathbb{C}$ ist offensichtlich die Teilersummenfunktion*

$$\sigma_s(n) = \sum_{d|n} d^s = \sum_{d|n} \iota^s(d) \quad \text{für alle } n \in \mathbb{N}.$$

Ein einfaches aber wichtiges Werkzeug ist nun das folgende Resultat:

Lemma 2.17. *Sei a eine zahlentheoretische Funktion und A die summatorische Funktion von a. Dann gilt $A = a * \iota^0$. Insbesondere gilt: Ist a schwach multiplikativ, so ist auch A schwach multiplikativ.*

Beweis. Nach Definition von Dirichlet-Faltung und summatorischer Funktion gilt

$$(a * \iota^0)(n) = \sum_{d|n} a(d) = A(n) \quad \text{für alle } n \in \mathbb{N}.$$

Da ι^0 offenbar schwach multiplikativ ist, folgt die Behauptung jetzt mit Satz 2.12. □

Beispiel 2.18. *Für ein festes $s \in \mathbb{C}$ ist die s-te Potenzfunktion ι^s offensichtlich stark und insbesondere auch schwach multiplikativ. Nach Beispiel 2.16 und Lemma 2.17 ist daher auch die Teilersummenfunktion σ_s schwach multiplikativ, was einen neuen Beweis für Satz 2.13 liefert.*

Proposition 2.19. *Die summatorische Funktion der Möbius-Funktion μ ist die Einsfunktion $\mathbb{1}_{\mathcal{A}}$ im Ring der zahlentheoretischen Funktionen.*

Beweis. Sei die summatorische Funktion der Möbius-Funktion μ zunächst mit M bezeichnet. Nach Lemma 2.17 ist M als summatorische Funktion der nach Beispiel 2.8 schwach multiplikativen Möbius-Funktion selbst wieder schwach multiplikativ. Zum Beweis der Proposition genügt es nach Korollar 2.11 also

$$M(p^j) = \mathbb{1}_{\mathcal{A}}(p^j) \quad \text{für alle primen } p \text{ und alle } j \in \mathbb{N}_0$$

zu zeigen. Tatsächlich gilt

$$M(p^0) = M(1) \overset{2.7}{=} 1 = \mathbb{1}_{\mathcal{A}}(1) = \mathbb{1}_{\mathcal{A}}(p^0),$$
$$M(p^j) = \sum_{k=0}^{j} \mu(p^k) = \mu(1) + \mu(p) = 1 - 1 = 0 = \mathbb{1}_{\mathcal{A}}(p^j) \qquad \text{für alle } j \geq 1.$$

□

Wir haben nun alle Vorüberlegungen angestellt, um den folgenden, 1832 von Möbius bewiesenen Satz zu beweisen:

Satz 2.20 (Möbius'scher Umkehrsatz)**.** *Für zwei zahlentheoretische Funktionen a und b gilt*

$$a(n) = \sum_{d|n} b(d) \qquad \text{für alle } n \in \mathbb{N}$$

genau dann, wenn

$$b(n) = \sum_{d|n} a(d)\mu\left(\frac{n}{d}\right) = \sum_{d|n} a\left(\frac{n}{d}\right)\mu(d) \qquad \text{für alle } n \in \mathbb{N}$$

erfüllt ist.

Beweis. Aus Proposition 2.19 und Lemma 2.17 folgt sofort

$$\mu * \iota^0 = \mathbb{1}_{\mathcal{A}}. \tag{2.2}$$

Hiermit gilt

$$a = a * \mathbb{1}_{\mathcal{A}} \overset{(2.2)}{=} a * (\mu * \iota^0) = (a * \mu) * \iota^0$$

und wegen der durch (2.2) gegebenen Invertierbarkeit der Funktion ι^0 im Ring $\mathcal{A}$

$$a = b * \iota^0 \quad \Longleftrightarrow \quad b = a * \mu,$$

also der Satz. □

Der Möbius'sche Umkehrsatz 2.20 ermöglicht eine unmittelbare Bestimmung von Relationen zwischen zahlentheoretischen Funktionen:

Beispiel 2.21. *Für die Teilersummenfunktion σ_s für ein $s \in \mathbb{C}$ gilt*

$$\sum_{d|n} \mu\left(\frac{n}{d}\right)\sigma_s(d) = n^s \qquad \text{für alle } n \in \mathbb{N}.$$

2.4 Die Euler'sche φ-Funktion

In diesem Abschnitt zeigen wir, dass die in Beispiel 2.2 (c) eingeführte Euler'sche φ-Funktion schwach multiplikativ ist und geben eine geschlossene Formel für ihre Funktionswerte an. In Hinsicht auf Lemma 2.9 bestimmen wir dafür zunächst die Werte auf den Primpotenzen:

Proposition 2.22. *Für eine Primzahl p und $j \in \mathbb{N}$ beliebig gilt:*

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

Beweis. Es gibt genau p^{j-1} Zahlen a mit $0 \leq a < p^j$, die *nicht* teilerfremd zu p^j sind, nämlich: $0 \cdot p, 1 \cdot p, 2 \cdot p, \ldots, (p^{j-1}-1) \cdot p$. Wir erhalten $\varphi(p^j) = p^j - p^{j-1} = p^{j-1}(p-1)$. □

Unser nächstes Ziel ist der Nachweis der schwachen Multiplikativität von φ. Zum Ausgangspunkt unserer Überlegungen hierzu machen wir die von Gauß in seinen 1801 erschienenen *Disquisitiones* gegebene

Satz 2.23 (Teilersummenformel)**.**

$$\sum_{d|n} \varphi(d) = n \quad \textit{für alle } n \in \mathbb{N}.$$

Beweis. Sei $n \in \mathbb{N}$ fest gewählt. Für einen beliebigen natürlichen Teiler $d \mid n$ setzen wir

$$\begin{aligned} G_d(n) &:= \{k \in \mathbb{N} : k \leq n \text{ und } \operatorname{ggT}(n,k) = d\} \\ &= \{k \in \mathbb{N} : \text{es gibt ein } c \in \mathbb{N} \text{ mit } k = cd,\ 1 \leq cd \leq n \text{ und } \operatorname{ggT}(n,cd) = d\}. \end{aligned}$$

Offensichtlich liegt dann jede Zahl $1 \leq k \leq n$ in genau einer der Mengen $G_d(n)$ mit $d \mid n$, nämlich in $G_{\operatorname{ggT}(n,k)}(n)$, und es folgt

$$n = \#\{1, \ldots, n\} = \# \left(\bigcup_{d|n} G_d(n) \right) = \sum_{d|n} \# G_d(n). \tag{2.3}$$

Wir bestimmen nun die einzelnen Summanden rechts genauer. Es gilt

$$\operatorname{ggT}(n,cd) = d \quad \Longrightarrow \quad \operatorname{ggT}\left(\frac{n}{d}, c\right) = 1 \qquad \text{für alle } d \mid n \text{ und alle } c \in \mathbb{N},$$

denn: Gelte $\operatorname{ggT}(n,cd) = d$. Nach dem erweiterten Euklidischen Algorithmus gibt es dann $u, v \in \mathbb{Z}$ mit $un + vcd = d$ und also mit $u\frac{n}{d} + vc = 1$. #

Es folgt

$$\begin{aligned} \# G_d(n) &= \# \left\{ k \in \mathbb{N} : \exists c \in \mathbb{N} \text{ mit } k = cd,\ 1 \leq c \leq \frac{n}{d} \text{ und } \operatorname{ggT}\left(\frac{n}{d}, c\right) = 1 \right\} \\ &= \varphi\left(\frac{n}{d}\right). \end{aligned}$$

Insgesamt erhalten wir

$$n \overset{(2.3)}{=} \sum_{d|n} \#G_d(n) = \sum_{d|n} \varphi\left(\frac{n}{d}\right) = \sum_{d|n} \varphi(d).$$

□

Beispiel 2.24. *Für $n = 12$ besagt die Teilersummenformel 2.23*

$$\begin{aligned}\sum_{d|12} \varphi(d) &= \varphi(1) + \varphi(2) + \varphi(3) + \varphi(4) + \varphi(6) + \varphi(12)\\ &= 1 + 1 + 2 + 2 + 2 + 4\\ &= 12.\end{aligned}$$

Wir erhalten nun die schwache Multiplikativität von φ:

Satz 2.25. *Die Euler'sche φ-Funktion ist schwach multiplikativ.*

Beweis. Nach der Teilersummenformel 2.23 gilt $\iota^1 = \varphi * \iota^0$. Nach dem Möbius'schen Umkehrsatz 2.20 gilt damit $\varphi = \iota^1 * \mu$. Da offenbar ι^1 und mit Beispiel 2.8 auch μ schwach multiplikativ ist, folgt die Behauptung mit Satz 2.12. □

Aus Proposition 2.22 und Satz 2.25 ergibt sich nun unmittelbar eine geschlossene Formel für die Werte der Euler'schen φ-Funktion:

Korollar 2.26. *Die Euler'sche φ-Funktion erfüllt*

$$\varphi(n) = n \cdot \prod_{\substack{p \text{ prim}\\ p|n}} \left(1 - \frac{1}{p}\right) \qquad \text{für alle } n \in \mathbb{N}.$$

Beweis. Für ein beliebiges $n \in \mathbb{N}$ mit Primfaktorzerlegung

$$n = \prod_{\substack{p \text{ prim}\\ p|n}} p^{\nu_p(n)}$$

folgt mit Lemma 2.9 und der schwachen Multiplikativität 2.25 der Euler'schen φ-Funktion

$$\begin{aligned}\varphi(n) &= \prod_{\substack{p \text{ prim}\\ p|n}} \varphi(p^{\nu_p(n)}) \overset{2.22}{=} \prod_{\substack{p \text{ prim}\\ p|n}} p^{\nu_p(n)-1}(p-1)\\ &= \prod_{\substack{p \text{ prim}\\ p|n}} p^{\nu_p(n)} \left(1 - \frac{1}{p}\right) = n \cdot \prod_{\substack{p \text{ prim}\\ p|n}} \left(1 - \frac{1}{p}\right)\end{aligned}$$

und somit die geschlossene Formel für φ. □

Beispiel 2.27. *In der Praxis berechnet man Werte der Euler'schen φ-Funktion meist nicht mit der Formel aus Korollar 2.26 sondern einfacher direkt mit schwacher Multiplikativität und Proposition 2.22:*

$$\varphi(140) = \varphi(4 \cdot 5 \cdot 7) = \varphi(4) \cdot \varphi(5) \cdot \varphi(7) = 2 \cdot (5-1) \cdot (7-1) = 2 \cdot 4 \cdot 6 = 48.$$

KAPITEL 3

Rechnen mit Restklassen

3.1 Restklassenringe

Die nachfolgende Definition sollte hinlänglich aus der Linearen Algebra bekannt sein:

Definition 3.1. *Ein **Ring (mit Eins)** ist eine Menge R zusammen mit zwei Verknüpfungen $+\colon R \times R \to R$ und $\cdot\colon R \times R \to R$ mit:*

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

(b) $(R, \cdot)$ *ist eine Halbgruppe (es gilt also das Assoziativgesetz) mit neutralem Element.*

(c) *Es gelten die Distributivgesetze*

$$(a + b)c = ac + bc \quad \text{sowie} \quad a(b + c) = ab + ac$$

für alle $a, b, c \in R$.

*Das neutrale Element bezüglich „+“ bezeichnen wir mit 0, das neutrale Element bezüglich „$\cdot$“ mit 1. Der Ring heißt **kommutativ**, wenn die Multiplikation kommutativ ist, wenn also $ab = ba$ für alle $a, b \in R$ gilt.*

Die Verknüpfungen lassen wir im Folgenden aus der Notation heraus und schreiben kurz: „R ist ein Ring“ anstelle von „$(R, +, \cdot)$ ist ein Ring“. Außerdem betrachten wir nur noch kommutative Ringe, der Ausdruck „Ring“ soll daher bis zum Ende des Skriptes stets für „kommutativer Ring“ stehen.

Beispiel 3.2. (a) *Die ganzen Zahlen $\mathbb{Z}$ bilden zusammen mit der üblichen Addition und Multiplikation einen Ring.*

(b) *Die **ganzen Gauß'schen Zahlen** $\mathbb{Z}[i] := \{a + bi : a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ bilden mit der eingeschränkten Addition und Multiplikation von $\mathbb{C}$ einen Ring.*

(c) *Ist R ein Ring, so ist*

$$R[X] := \{a_n X^n + \ldots + a_1 X + a_0 : n \in \mathbb{N}_0, a_0, \ldots, a_n \in R\}$$

*zusammen mit der üblichen Addition und Multiplikation von Polynomen ein Ring, der **Polynomring** in einer Variablen über R.*

Definition 3.3. *Eine Äquivalenzrelation „$\equiv$“ auf einem Ring R heißt eine **Kongruenzrelation**, wenn für alle $a_1, a_2, b_1, b_2 \in R$ gilt:*

$$a_1 \equiv a_2 \text{ und } b_1 \equiv b_2 \quad \Longrightarrow \quad a_1 + b_1 \equiv a_2 + b_2 \text{ und } a_1 b_1 \equiv a_2 b_2.$$

Wir führen an dieser Stelle den Begriff des Ideals in einem Ring R ein, den wir schon aus Definition 1.10 vom Ring der ganzen Zahlen kennen.

Definition 3.4. *Eine Teilmenge $\mathfrak{a}$ eines Rings R heißt ein **Ideal** in R, wenn gilt:*

(a) $0 \in \mathfrak{a}$

(b) *Sind $a, b \in \mathfrak{a}$, dann ist auch $a + b \in \mathfrak{a}$*

(c) *Sind $a \in \mathfrak{a}$ und $r \in R$, dann ist auch $ra \in \mathfrak{a}$.*

Ideale in einem Ring R und Kongruenzrelationen auf R stehen in einem sehr engen Zusammenhang:

Proposition 3.5. *Sei R ein Ring. Dann gelten die folgenden beiden Aussagen:*

(a) *Ist „$\equiv$“ eine Kongruenzrelation auf R, so ist*

$$\mathfrak{a} := \{a \in R : a \equiv 0\}$$

ein Ideal in R und es gilt

$$a \equiv b \iff a - b \in \mathfrak{a}.$$

(b) *Ist $\mathfrak{a} \subseteq R$ ein Ideal, so ist durch*

$$a \equiv b \ :\Longleftrightarrow \ a - b \in \mathfrak{a}$$

eine Kongruenzrelation „$\equiv$“ auf R gegeben und es gilt

$$\mathfrak{a} = \{a \in R : a \equiv 0\}.$$

Die Äquivalenzklasse von $b \in R$ bezüglich „$\equiv$“ ist jeweils durch

$$\overline{b} := b + \mathfrak{a} := \{b + a : a \in \mathfrak{a}\}$$

*gegeben und heißt auch die **Restklasse** von b modulo „$\equiv$“ bzw. modulo $\mathfrak{a}$.*

Beweis. Wir zeigen zunächst Aussage (a). Sei dazu „$\equiv$“ eine Kongruenzrelation auf R. Wir rechnen nach, dass $\mathfrak{a} := \{a \in R : a \equiv 0\}$ die Eigenschaften eines Ideals aus Definition 3.4 hat. Weil „$\equiv$“ als Äquivalenzrelation reflexiv ist, gilt $0 \equiv 0$ und also $0 \in \mathfrak{a}$. Für $a, b \in \mathfrak{a}$ folgt weiter $a \equiv 0$ sowie $b \equiv 0$. Da „$\equiv$“ eine Kongruenzrelation ist, erhalten wir $a + b \equiv 0 + 0 = 0$ und somit $a + b \in \mathfrak{a}$. Ist schließlich $a \in \mathfrak{a}$ und $r \in R$, so gilt $a \equiv 0$, und weil „$\equiv$“ eine Kongruenzrelation ist, ergibt sich $ra \equiv r \cdot 0 = 0$ und also $ra \in \mathfrak{a}$. Damit ist $\mathfrak{a}$ ein Ideal in R und es gilt $a \equiv b \iff a - b \equiv 0 \iff a - b \in \mathfrak{a}$.

Zum Beweis von Aussage (b) sei $\mathfrak{a}$ ein Ideal in R und wir setzen $a \equiv b :\iff a - b \in \mathfrak{a}$. Zunächst zeigen wir, dass „$\equiv$“ eine Äquivalenzrelation ist. Zum Nachweis der Reflexivität sei $a \in R$. Dann ist $a - a = 0 \in \mathfrak{a}$, denn $\mathfrak{a}$ ist ein Ideal. Wir erhalten $a \equiv a$. Für den Beweis der Symmetrie seien $a, b \in R$ mit $a \equiv b$. Wir finden $a - b \in \mathfrak{a}$, was aufgrund der Idealeigenschaft von a auch $b - a = (-1)(a - b) \in \mathfrak{a}$ liefert, also $b \equiv a$. Die Transitivität erkennen wir wie folgt: Sind $a, b, c \in R$ mit $a \equiv b$ und $b \equiv c$, so ergeben sich $a - b \in \mathfrak{a}$ und $b - c \in \mathfrak{a}$. Weil $\mathfrak{a}$ ein Ideal ist, erhalten wir $a - c = (a - b) + (b - c) \in \mathfrak{a}$ und deshalb $a \equiv c$. Somit ist „$\equiv$“ eine Äquivalenzrelation. Wir weisen nun noch die restlichen Eigenschaften einer Kongruenzrelation nach. Dazu seien $a_1, a_2, b_1, b_2 \in R$ mit $a_1 \equiv a_2$ und $b_1 \equiv b_2$. Dann folgt $a_1 - a_2 \in \mathfrak{a}$ und $b_1 - b_2 \in \mathfrak{a}$. Da $\mathfrak{a}$ ein Ideal ist, ergibt sich $(a_1 + b_1) - (a_2 + b_2) = (a_1 - a_2) + (b_1 - b_2) \in \mathfrak{a}$ und deher auch $a_1 + b_1 \equiv a_2 + b_2$. Außerdem erhalten wir $b_1(a_1 - a_2) \in \mathfrak{a}$ sowie $a_2(b_1 - b_2) \in \mathfrak{a}$. Das liefert $a_1 b_1 - a_2 b_2 = b_1(a_1 - a_2) + a_2(b_1 - b_2) \in \mathfrak{a}$, also $a_1 b_1 \equiv a_2 b_2$. Wir haben somit gesehen, dass „$\equiv$“ eine Kongruenzrelation auf R ist.

Schließlich ist jeweils die Äquivalenzklasse eines Elementes $b \in R$ bezüglich „$\equiv$“ durch

$$\begin{aligned}\{x \in R : x \equiv b\} &= \{x \in R : x - b \in \mathfrak{a}\} = \{x \in R : \text{Es gibt ein } a \in \mathfrak{a} \text{ mit } x - b = a\} \\ &= \{b + a : a \in \mathfrak{a}\} \\ &= b + \mathfrak{a}\end{aligned}$$

gegeben. □

Es lohnt sich, diese Proposition im besonders wichtigen Spezialfall $R = \mathbb{Z}$ noch einmal gesondert zu formulieren und Notationen für diesen festzulegen:

Korollar 3.6. *Ist „$\equiv$“ eine Kongruenzrelation auf $\mathbb{Z}$, so gibt es ein eindeutig bestimmtes $n \in \mathbb{N}_0$ mit*

$$a \equiv b \iff a - b \in n\mathbb{Z} \iff n \mid (a - b).$$

Umgekehrt ist für jedes $n \in \mathbb{N}_0$ durch

$$a \equiv b :\iff a - b \in n\mathbb{Z} \iff n \mid (a - b)$$

eine Kongruenzrelation auf $\mathbb{Z}$ gegeben. Für $a \equiv b$ schreiben wir in diesem Fall $a \equiv b \bmod (n)$. Die Äquivalenzklasse von $a \in \mathbb{Z}$ bezüglich „$\equiv \bmod (n)$“ ist durch

$$\overline{a} := a + n\mathbb{Z} = \{a + nr : r \in \mathbb{Z}\}$$

gegeben.

Beweis. Das Korollar folgt unmittelbar aus Proposition 3.5, da die Ideale in $\mathbb{Z}$ nach Proposition 1.11 von der Form $n\mathbb{Z}$ mit $n \in \mathbb{N}_0$ sind. □

Beispiel 3.7. *Für $a, b \in \mathbb{Z}$ ist*

$$a \equiv b \bmod (3) \iff a - b \in 3\mathbb{Z} \iff 3 \mid (a - b).$$

Als Restklassen erhalten wir $\overline{0} = 3\mathbb{Z}$, $\overline{1} = 1 + 3\mathbb{Z}$, $\overline{2} = 2 + 3\mathbb{Z}$. Weitere, davon verschiedene Restklassen erhalten wir nicht, denn es ist $\overline{3} = \overline{0}$, da $3 \equiv 0 \bmod (3)$, $\overline{4} = \overline{1}$, $\overline{-1} = \overline{2}$ usw. Die Menge der Restklassen modulo 3 ist also durch $\{\overline{0}, \overline{1}, \overline{2}\}$ gegeben.

Proposition 3.8. *Seien R ein Ring, „$\equiv$“ eine Kongruenzrelation auf R und $\mathfrak{a}$ das nach Proposition 3.5 zu „$\equiv$“ gehörige Ideal in R. Dann ist die Menge $R/\equiv$ bzw. $R/\mathfrak{a}$ aller Restklassen bezüglich „$\equiv$“ zusammen mit den Verknüpfungen*

$$\overline{a} + \overline{b} := \overline{a + b} \quad \textit{und} \quad \overline{a} \cdot \overline{b} := \overline{a \cdot b}$$

*ein Ring und heißt der **Restklassenring** („R modulo $\mathfrak{a}$“).*

Beweis. Wir müssen zeigen, dass die Verknüpfungen wohldefiniert sind. Seien dazu $a_1, a_2 \in \overline{a}$ sowie $b_1, b_2 \in \overline{b}$. Dann gelten $a_1 \equiv a_2$ sowie $b_1 \equiv b_2$ und, weil „$\equiv$“ eine Kongruenzrelation ist, ergibt sich $a_1 + b_1 \equiv a_2 + b_2$ und somit $\overline{a_1 + b_1} = \overline{a_2 + b_2}$. Analog folgt $a_1 b_1 \equiv a_2 b_2$ und deshalb $\overline{a_1 b_1} = \overline{a_2 b_2}$. Addition und Multiplikation von Restklassen sind damit wohldefiniert. Die Ringeigenschaften übertragen sich von R auf $R/\mathfrak{a}$, da Addition und Multiplikation vertreterweise definiert sind. □

Beispiel 3.9. *Die Restklassenringe von $\mathbb{Z}$ sind nach Korollar 3.6 durch $\mathbb{Z}/n\mathbb{Z}$ mit $n \in \mathbb{N}_0$ gegeben. Explizit sehen diese wie folgt aus:*

- *$n = 0$: Dann gilt $\mathbb{Z}/0\mathbb{Z} = \mathbb{Z}$, denn für $a \in \mathbb{Z}$ ist $a + 0 \cdot \mathbb{Z} = \{a\}$, wobei wir $\mathbb{Z}$ mit $\{\{a\} : a \in \mathbb{Z}\}$ identifizieren.*
- *$n = 1$: Dann ist $\mathbb{Z}/\mathbb{Z} = 0$ der Nullring – hier sind Eins- und Nullelement gleich – denn für $a \in \mathbb{Z}$ ist $a + \mathbb{Z} = \mathbb{Z} = 0 + \mathbb{Z}$.*
- *$n > 1$: Dann ist $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$, denn für jedes $a \in \mathbb{Z}$ existieren $q, r \in \mathbb{Z}$ mit $0 \leq r \leq n - 1$ und $a = qn + r$. Hieraus folgt $\overline{a} = \overline{qn + r} = \overline{qn} + \overline{r} = \overline{r}$. Weiter gilt $a \not\equiv b \bmod (n)$ und also $\overline{a} \neq \overline{b}$ für $a, b \in \mathbb{Z}$ mit $0 \leq a \neq b \leq n - 1$.*

Beispiel 3.10. *Für die Ringe $\mathbb{Z}/3\mathbb{Z}$ und $\mathbb{Z}/4\mathbb{Z}$ gelten nach Proposition 3.8 die folgenden Verknüp-*

fungstafeln:

$\mathbb{Z}/3\mathbb{Z}$:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

$\mathbb{Z}/4\mathbb{Z}$:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Im Ring $\mathbb{Z}/3\mathbb{Z}$ besitzt jede von $\overline{0}$ verschiedene Restklasse ein Inverses bezüglich der Multiplikation, während das im Ring $\mathbb{Z}/4\mathbb{Z}$ nicht gilt. Darüber hinaus treten im Falle des Ringes $\mathbb{Z}/4\mathbb{Z}$ sogenannte Nullteiler auf: Es ist $\overline{2}\cdot\overline{2} = \overline{0}$, obwohl $\overline{2} \neq \overline{0}$ ist. Damit werden wir uns in Abschnitt 3.3 gründlicher beschäftigen.

3.2 Teilbarkeitsregeln

Eine leichte, aber nette Anwendung der bisherigen Kongruenzrechnung ist die Herleitung der aus der Schule bekannten Teilbarkeitsregeln in den natürlichen Zahlen. Wir können diese verallgemeinern, wenn wir neben dem Dezimalsystem auch andere Stellenwertsysteme zulassen: Sei dafür in diesem Abschnitt $g \geq 2$ stets eine feste natürliche Zahl und S_g das kleinste nichtnegative Restesystem $\{0, 1, \ldots, g-1\}$ modulo g. Es gilt:

Proposition 3.11. *Jedes $n \in \mathbb{N}$ hat eine eindeutige Darstellung der Form*

$$n = \sum_{i=0}^{r} a_i g^i \quad \text{mit } a_0, \ldots, a_r \in S_g \text{ und } a_r \neq 0.$$

*Diese heißt die **g-adische Darstellung** von n, die a_i ihre **Ziffern** und $1 + r = 1 + \lfloor \frac{\log n}{\log g} \rfloor$ ihre **Stellenzahl**. Die Zahl g, nach der entwickelt wird, heißt die **Basis** der Darstellung. Weiter heißen*

$$\sum_{i=0}^{r} a_i \quad \text{bzw.} \quad \sum_{i=0}^{r} (-1)^i a_i$$

*die **g-adische Quersumme** bzw. die **alternierende g-adische Quersumme** von n.*

Beweis. Um die Existenz einer g-adischen Darstellung für n zu zeigen, setzen wir zunächst $\nu_0 := n$ und gehen dann schrittweise vor: Sei $j \in \mathbb{N}_0$ und seien $\nu_0, \ldots, \nu_j$ und $a_0, \ldots, a_{j-1}$ mit

$$\nu_i = \nu_{i+1} g + a_i \quad \text{und} \quad 0 \leq a_i < g \leq \nu_i \qquad \text{für alle } i \in \{0, \ldots, j-1\} \tag{3.1}$$

gegeben. Dann gilt

$$\frac{\nu_i}{g} \geq \nu_{i+1} > 0 \qquad \text{für alle } i \in \{0, \ldots, j-1\}$$

und also

$$\nu_0 g^{-j} \geq \nu_1 g^{1-j} \geq \ldots \geq \nu_j > 0.$$

Wir unterscheiden nun zwei Fälle:

Fall 1: $\nu_j \geq g$**.** Dann führen wir mit dem Paar (ν_j, g) eine Division mit Rest durch und erhalten (3.1) für $i = j$ mit ganzen Zahlen ν_{j+1} und a_j.

Fall 2: $\nu_j < g$**.** Dann setzen wir $a_j := \nu_j$ und hören auf; in diesem Fall ist $0 < a_j < g$.

Wegen $\nu_0 g^{-j} \geq \nu_j$ tritt Fall 2 ein, sobald j größer als $\frac{\log n}{\log g}$ ist. Sei dies nach genau r Schritten der Fall. Dann gilt (3.1) für $i \in \{0, \ldots, r-1\}$ und $0 < a_r := \nu_r < g$. Induktiv erhalten wir

$$\nu_0 = \nu_j g^j + \sum_{i=0}^{j-1} a_i g^i \quad \text{für alle } j \in \{0, \ldots, r\}$$

und somit die Existenz einer g-adischen Darstellung für n, insbesondere haben die Koeffizienten a_i die behaupteten Eigenschaften.

Zum Beweis der Eindeutigkeit der g-adischen Darstellung beachten wir, dass nach Konstruktion $g^r \leq n < g^{r+1}$ und also $r = \lfloor \frac{\log n}{\log g} \rfloor$ gilt, so dass die Stellenzahl der g-adischen Entwicklung eindeutig bestimmt ist. Seien nun

$$\sum_{i=0}^{r} a_i g^i = n = \sum_{i=0}^{r} \tilde{a}_i g^i$$

zwei g-adische Darstellungen von n. Dann folgt

$$\sum_{i=0}^{r} (a_i - \tilde{a}_i) g^i = 0 \tag{3.2}$$

und insbesondere $g \mid (a_0 - \tilde{a}_0)$. Wegen $a_0, \tilde{a}_0 \in S_g$ impliziert das bereits $a_0 = \tilde{a}_0$. Berücksichtigen wir dies in (3.2), so erhalten wir $g^2 \mid (a_1 - \tilde{a}_1)g$ und schließen analog auf $a_1 = \tilde{a}_1$. Induktiv folgt $a_i = \tilde{a}_i$ für alle $i \in \{0, \ldots, r\}$. □

Proposition 3.12 (Teilbarkeitsregeln)**.** *Für eine beliebige natürliche Zahl n mit g-adischer Darstellung $n = \sum_{i=0}^{r} a_i g^i$ gelten die folgenden Aussagen:*

(a) *Ein beliebiger Teiler d von $g-1$ teilt n genau dann, wenn d die g-adische Quersumme von n teilt.*

(b) *Ein beliebiger Teiler d von g teilt n genau dann, wenn d die Ziffer a_0 teilt.*

(c) *Ein beliebiger Teiler d von $g+1$ teilt n genau dann, wenn d die alternierende g-adische Quersumme von n teilt.*

Beweis. Die Behauptungen ergeben sich unmittelbar aus

$$\begin{aligned} n &= \sum_{i=0}^{r} a_i\big((g-1)+1\big)^i \equiv \sum_{i=0}^{r} a_i && \mod (g-1),\\ n &= \sum_{i=0}^{r} a_i g^i \equiv a_0 && \mod (g),\\ n &= \sum_{i=0}^{r} a_i\big((g+1)-1\big)^i \equiv \sum_{i=0}^{r} (-1)^i a_i && \mod (g+1). \end{aligned}$$

□

Als Spezialfälle dieses Ergebnisses sind die Teilbarkeitsregeln durch 2, 3, 5, 9 und 11 in der Dezimaldarstellung bereits aus der Schule bekannt. Offensichtlich lässt sich diese Methode auf jedes zu g teilerfremde d verallgemeinern – die so erhaltenen Teilbarkeitsregeln sind dann aber in aller Regel komplizierter und ihr praktischer Nutzen daher geringer.

3.3 Prime Restklassen und der Satz von Euler-Fermat

Wir greifen nun die am Ende von Abschnitt 3.1 thematisierte Fragestellung nach Nullteilern in den Restklassenringen $\mathbb{Z}/n\mathbb{Z}$ auf. Wir wiederholen hierfür zunächst einige Begriffe, die bereits aus der Linearen Algebra bekannt sein sollten:

Definition 3.13. *Es sei R ein Ring. Ein Element $x \in R$ heißt ein **Nullteiler**, wenn es ein $y \in R$, $y \neq 0$ mit $xy = 0$ gibt. Der Ring R heißt **nullteilerfrei**, wenn $R \neq 0$ ist und 0 der einzige Nullteiler in R ist.*

Beispiel 3.14. *Wie bereits in Beispiel 3.10 untersucht gilt:*

- *Nullteiler in $\mathbb{Z}/3\mathbb{Z}$: $\overline{0}$, also ist $\mathbb{Z}/3\mathbb{Z}$ nullteilerfrei.*
- *Nullteiler in $\mathbb{Z}/4\mathbb{Z}$: $\overline{0}, \overline{2}$ – denn es gilt $\overline{2} \cdot \overline{2} = \overline{0}$ – also ist $\mathbb{Z}/4\mathbb{Z}$ nicht nullteilerfrei.*

Definition 3.15. *Ein Element x in einem Ring R heißt eine **Einheit**, wenn es ein $y \in R$ mit $xy = 1$ gibt.*

Beispiel 3.16. *Wie bereits in Beispiel 3.10 untersucht gilt:*

- *Einheiten in $\mathbb{Z}/3\mathbb{Z}$: $\overline{1}, \overline{2}$.*
- *Einheiten in $\mathbb{Z}/4\mathbb{Z}$: $\overline{1}, \overline{3}$.*

Proposition 3.17. *Sei R ein Ring. Dann gilt:*

(a) *Die Menge* $R^\times := \{x \in R : x \text{ ist eine Einheit}\}$ *bildet zusammen mit der Multiplikation eine abelsche Gruppe, die sogenannte* ***Einheitengruppe*** *von* R*. Insbesondere gibt es für jedes* $x \in R^\times$ *genau ein* $y \in R^\times$ *mit* $xy = 1$*. Dieses Element bezeichnen wir mit* x^{-1} *und nennen es das* ***(multiplikativ) Inverse*** *zu* x*.*

(b) *Ist* $x \in R^\times$*, so ist* x *kein Nullteiler.*

(c) *Falls* R *endlich ist, dann gilt auch die Umkehrung von (b): Ist* $x \in R$ *kein Nullteiler, so ist* x *eine Einheit.*

Beweis. Sind $a, b \in R^\times$, so auch ab, denn in diesem Fall existieren $c, d \in R$ mit $ac = 1$ sowie $bd = 1$ und es folgt $(ab)(cd) = (ac)(bd) = 1$. Das Assoziativgesetz und die Kommutativität folgen aus den entsprechenden Eigenschaften der Multiplikation in R, das neutrale Element ist durch das Element 1 gegeben, welches wegen $1 \cdot 1 = 1$ in $R^\times$ liegt. Ist $a \in R^\times$, so existiert nach Definition ein $b \in R$ mit $ab = 1$. Das impliziert $ba = 1$ und somit $b \in R^\times$. Wir haben damit gezeigt, dass $R^\times$ eine abelsche Gruppe bezüglich der Multiplikation ist. Daraus folgt insbesondere die Eindeutigkeit des Inversen. Das ist Behauptung (a).

Zum Beweis von Behauptung (b) betrachten wir zunächst den Fall $R \neq 0$. Sei $x \in R^\times$ und $y \in R$ mit $xy = 0$. Wir erhalten $y = x^{-1}xy = 0$, so dass x kein Nullteiler ist. Im Fall $R = 0$ ist das Element 0 eine Einheit, aber kein Nullteiler.

Im Beweis von Behauptung (c) setzen wir nun R als endlich voraus. Sei $x \in R$ kein Nullteiler. Wir betrachten die Abbildung

$$\tau_x \colon \begin{cases} R & \to R, \\ a & \mapsto xa. \end{cases}$$

Diese ist injektiv, denn aus $\tau_x(a) = \tau_x(b)$ folgt $xa = xb$ und also $x(a - b) = 0$. Da x kein Nullteiler ist, ergibt sich hieraus $a - b = 0$ und somit $a = b$. Als injektive Selbstabbildung der endlichen Menge R ist τ_x auch surjektiv, insbesondere gibt es ein $y \in R$ mit $\tau_x(y) = 1$, was $xy = 1$ und deshalb $x \in R^\times$ impliziert. □

Beispiel 3.18. *Im Fall des (endlichen) Restklassenrings* $R = \mathbb{Z}/n\mathbb{Z}$ *für ein* $n \in \mathbb{N}$ *gilt speziell, dass ein* $\overline{x} \in R$ *genau dann eine Einheit ist, wenn* $\overline{x}$ *kein Nullteiler ist. Die Einheiten im Ring* $\mathbb{Z}/n\mathbb{Z}$ *nennt man die* ***primen Restklassen*** *modulo* n*, die Gruppe* $(\mathbb{Z}/n\mathbb{Z})^\times$ *entsprechend die* ***Gruppe der primen Restklassen*** *modulo* n*.*

Definition 3.19. *Ein Ring* R *heißt ein* ***Körper****, falls* $R^\times = R \setminus \{0\}$ *gilt.*

Beispiel 3.20. *Nach Beispiel 3.16 ist* $\mathbb{Z}/3\mathbb{Z}$ *ein Körper,* $\mathbb{Z}/4\mathbb{Z}$ *aber nicht. Zudem ist der Nullring* $R = 0$ *nach Definition* kein *Körper.*

Satz 3.21. *Es sei* $n \in \mathbb{N}$*. Dann sind äquivalent:*

(i) n *ist eine Primzahl.*

(ii) $\mathbb{Z}/n\mathbb{Z}$ *ist ein Körper.*

(iii) $\mathbb{Z}/n\mathbb{Z}$ *ist nullteilerfrei.*

Für Primzahlen p schreiben wir auch $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.

Beweis. Gelte zunächst Aussage (i), sei also n eine Primzahl. Wir betrachten ein beliebiges $\overline{0} \neq \overline{a} \in \mathbb{Z}/n\mathbb{Z}$. Für dieses gilt $n \nmid a$ und, da n eine Primzahl ist, auch $\mathrm{ggT}(n,a) = 1$. Nach dem erweiterten Euklidischen Algorithmus 1.7 (c) gibt es $u, v \in \mathbb{Z}$ mit $un + va = 1$. Das impliziert $\overline{un} + \overline{va} = \overline{1}$ und also $\overline{v} \cdot \overline{a} = \overline{1}$. Es folgt $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$ und wegen der beliebigen Wahl von $\overline{a}$ somit Aussage (ii).

Gelte nun Aussage (ii), sei also $\mathbb{Z}/n\mathbb{Z}$ ein Körper. Damit ist $\mathbb{Z}/n\mathbb{Z} \neq 0$ und $(\mathbb{Z}/n\mathbb{Z})^\times = \mathbb{Z}/n\mathbb{Z} \setminus \{\overline{0}\}$. Nach Proposition 3.17 (b) ist dann $\overline{0}$ der einzige Nullteiler in $\mathbb{Z}/n\mathbb{Z}$ und $\mathbb{Z}/n\mathbb{Z}$ ist nullteilerfrei. Das ist Aussage (iii).

Dass Aussage (iii) auch Aussage (i) impliziert, zeigen wir schließlich indirekt: Gelte also *nicht* Aussage (i) und sei also n *keine* Primzahl. Im Fall $n = 1$ erhalten wir so den nicht nullteilerfreien Nullring $\mathbb{Z}/n\mathbb{Z} = 0$. Im Fall $n > 1$ gibt es dann $a, b \in \mathbb{N}$ mit $1 < a, b < n$ und $n = ab$. Es ergibt sich $\overline{0} = \overline{n} = \overline{ab} = \overline{a}\overline{b}$ mit $\overline{a}, \overline{b} \neq \overline{0}$, so dass $\overline{a}, \overline{b}$ Nullteiler sind. Insbesondere ist $\mathbb{Z}/n\mathbb{Z}$ nicht nullteilerfrei. In beiden Fällen haben wir gezeigt, dass Aussage (iii) *nicht* gilt. □

Der Beweis der Implikation „(i)$\Longrightarrow$(ii)“ hat gezeigt, dass man für eine Primzahl p durch den erweiterten Euklidischen Algorithmus Inverse in $(\mathbb{Z}/p\mathbb{Z})^\times$ bestimmen kann. Es sei ferner angemerkt, dass es für Primzahlen p auch für $r > 1$ Körper mit p^r Elementen gibt. Diese sind aber von $\mathbb{Z}/p^r\mathbb{Z}$ verschieden, denn letztere sind nach Satz 3.21 keine Körper.

Wir greifen die Idee aus dem obigen Beweis der Implikation „(i) $\Longrightarrow$(ii)“ noch einmal auf und verwenden diese, um die Einheiten im Ring $\mathbb{Z}/n\mathbb{Z}$ zu charakterisieren:

Proposition 3.22. *Sei $n \in \mathbb{N}$. Dann sind für ein beliebiges $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ die folgenden beiden Aussagen äquivalent:*

(i) $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$,

(ii) $\mathrm{ggT}(a,n) = 1$.

Beweis. Gelte zunächst Aussage (i) und sei also $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$. Dann gibt es ein $\overline{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$ mit $\overline{a}\overline{b} = \overline{1}$ und somit ein $k \in \mathbb{Z}$ mit $ab = 1 + kn$. Sei nun $d \in \mathbb{Z}$ mit $d \mid a$ und $d \mid n$ ein gemeinsamer Teiler von a und n. Für diesen gilt $d \mid (ab - kn) = 1$ und es folgt $\mathrm{ggT}(a,n) = 1$.

Gelte nun umgekehrt Aussage (ii) und sei also $\mathrm{ggT}(a,n) = 1$. Dann gibt es nach dem erweiterten Euklidischen Algorithmus 1.7 (c) Zahlen $u, v \in \mathbb{Z}$ mit $au + vn = 1$. Wir erhalten $\overline{a} \cdot \overline{u} = \overline{1}$ und also $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$. □

Der Beweis hat gezeigt, dass Inverse in $(\mathbb{Z}/n\mathbb{Z})^\times$ durch den erweiterten Euklidischen Algorithmus bestimmt werden können:

Korollar 3.23. *Sei $n \in \mathbb{N}$. Dann sind für ein beliebiges $a \in \mathbb{Z}$ die folgenden beiden Aussagen äquivalent:*

(i) *Die Kongruenz* $ax \equiv 1 \bmod (n)$ *besitzt eine Lösung in* $\mathbb{Z}$.

(ii) $\mathrm{ggT}(a,n) = 1$.

Beweis. Die Kongruenz $ax \equiv 1 \bmod (n)$ entspricht der Gleichung $\overline{a} \cdot \overline{x} = \overline{1}$ in $\mathbb{Z}/n\mathbb{Z}$, welche genau dann lösbar ist, wenn $\overline{x}$ eine Einheit in $\mathbb{Z}/n\mathbb{Z}$ ist. □

Beispiel 3.24. *Gesucht ist eine Lösung der Kongruenz*

$$3x \equiv 1 \bmod (37).$$

Es ist $\mathrm{ggT}(3,37) = 1 = (-12) \cdot 3 + 37$ *und also* $\overline{1} = \overline{-12} \cdot \overline{3} = \overline{25} \cdot \overline{3}$. *Es folgt, dass* $x = 25$ *eine Lösung der Kongruenz ist. Die Menge* L *aller Lösungen ist gegeben durch* $L = 25 + 37\mathbb{Z}$.

Proposition 3.25. *Es seien* $a, b \in \mathbb{Z},\ n \in \mathbb{N}$. *Dann sind äquivalent:*

(i) *Die Kongruenz* $ax \equiv b \bmod (n)$ *besitzt eine Lösung in* $\mathbb{Z}$.

(ii) $\mathrm{ggT}(a,n) \mid b$.

Beweis. Gelte zunächst Aussage (i), sei also $x \in \mathbb{Z}$ mit $ax \equiv b \bmod (n)$. Dann gibt es ein $k \in \mathbb{Z}$ mit $ax = b + kn$ und also mit $b = ax - kn$. Wegen $\mathrm{ggT}(a,n) \mid a$ und $\mathrm{ggT}(a,n) \mid n$ folgt hieraus bereits $\mathrm{ggT}(a,n) \mid b$, also Aussage (ii).

Gelte nun umgekehrt Aussage (ii) und also $\mathrm{ggT}(a,n) \mid b$. Nach dem erweiterten Euklidischen Algorithmus 1.7 (c) gibt es dann $u, v \in \mathbb{Z}$ mit

$$ua + vn = \mathrm{ggT}(a,n).$$

Durch Multiplikation mit der nach Voraussetzung ganzen Zahl $\frac{b}{\mathrm{ggT}(a,n)}$ erhalten wir

$$ua\frac{b}{\mathrm{ggT}(a,n)} + vn\frac{b}{\mathrm{ggT}(a,n)} = b,$$

was die Kongruenz

$$a \cdot \frac{bu}{\mathrm{ggT}(a,n)} \equiv b \bmod (n)$$

und damit die Behauptung nach sich zieht. □

Beispiel 3.26. (a) *Die Kongruenz* $15x \equiv 7 \bmod (21)$ *hat wegen* $\mathrm{ggT}(15,21) = 3 \nmid 7$ *keine Lösung.*

(b) *Gesucht ist eine Lösung der Kongruenz* $15x \equiv 6 \bmod (21)$. *Es ist* $\mathrm{ggT}(15,21) = 3 \mid 6$, *so dass die Kongruenz lösbar ist. Der erweiterte Euklidische Algorithmus liefert*

$$\mathrm{ggT}(15,21) = 3 = 3 \cdot 15 + (-2) \cdot 21.$$

Wie im obigen Beweis ergibt sich daraus

$$6 = 6 \cdot 15 + (-4) \cdot 21 \equiv 15 \cdot 6 \bmod (21),$$

so dass $x = 6$ *eine Lösung der Kongruenz ist.*

Definition 3.27. *Sei G eine endliche Gruppe. Die **Ordnung** $|G|$ von G ist definiert als die Anzahl der Elemente von G.*[1]

Beispiel 3.28. *Nach Proposition 3.22 gilt*

$$\left|(\mathbb{Z}/n\mathbb{Z})^\times\right| = \#\{a \in \mathbb{N}_0 : 0 \leq a < n \text{ und } \operatorname{ggT}(a,n) = 1\} = \varphi(n).$$

Im Folgenden werden wir öfters abstrakte Gruppen betrachten. Hierbei werden wir die Verknüpfung stets multiplikativ schreiben und das neutrale Element mit 1 bezeichnen (sofern nicht anders angegeben):

Proposition 3.29. *Sei G eine endliche abelsche Gruppe und $g \in G$. Dann gilt*[2]

$$g^{|G|} = 1.$$

Beweis. Wir betrachten die Abbildung

$$\tau_g \colon \begin{cases} G & \to G, \\ x & \mapsto gx. \end{cases}$$

Diese ist injektiv, denn aus $\tau_g(x) = \tau_g(y)$ für $x, y \in G$ folgt $gx = gy$ und somit $x = g^{-1}gx = g^{-1}gy = y$. Die Abbildung τ_g ist auch surjektiv, denn für $y \in G$ gilt $\tau_g(g^{-1}y) = gg^{-1}y = y$. Also ist τ_g bijektiv und, weil die Gruppe G endlich und abelsch ist, ergibt sich

$$\prod_{x\in G} x = \prod_{x\in G} \tau_g(x) = \prod_{x\in G} gx = g^{|G|} \prod_{x\in G} x,$$

woraus $g^{|G|} = 1$ folgt. □

Satz 3.30 (Satz von Euler-Fermat)**.** *Sei $n \in \mathbb{N}$. Dann gilt für ein beliebiges $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$ die Identität*

$$\bar{a}^{\varphi(n)} = \bar{1}.$$

Beweis. Nach Beispiel 3.28 gilt $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$. Die Behauptung folgt nun direkt aus Proposition 3.29, angewandt auf $G = (\mathbb{Z}/n\mathbb{Z})^\times$. □

Beispiel 3.31. *Es ist* $3^{19} \equiv 10 \bmod (17)$,

denn: Nach dem Satz von Euler-Fermat 3.30 gilt

$$3^{16} = 3^{\varphi(17)} \equiv 1 \bmod (17).$$

Es folgt

$$3^{19} = 3^3 \cdot 3^{16} \equiv 27 \cdot 1 \equiv 10 \bmod (17).$$

#

[1] Für die Anzahl der Elemente einer beliebigen Menge M werden wir im Unterschied dazu die Notation $\#M \in \mathbb{N}_0 \cup \{\infty\}$ verwenden.

[2] In der Algebra lernt man, dass diese Aussage auch für beliebige endliche Gruppen korrekt ist.

Korollar 3.32 (Kleiner Satz von Fermat)**.** *Sei p eine Primzahl. Dann gelten die folgenden beiden Aussagen:*

(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. Nach Proposition 2.22 gilt $\varphi(p) = p - 1$, so dass sich Behauptung (a) direkt aus dem Satz von Euler-Fermat 3.30 ergibt. Behauptung (b) folgt hieraus nach Multiplikation mit $\overline{a}$ und, da für $\overline{a} = \overline{0}$ zusätzlich $\overline{a}^p = \overline{0}^p = \overline{0} = \overline{a}$ gilt. □

3.4 Zyklische Gruppen

Unser nächstes wichtiges Ziel ist es, die Gruppen $(\mathbb{Z}/n\mathbb{Z})^\times$ strukturell genauer zu untersuchen. Insbesondere werden wir später in Abschnitt 3.7 in Satz 3.86 beschreiben, wann genau diese von nur einem Element erzeugt werden. In diesem Abschnitt führen wir diese Eigenschaft einer Gruppe – die Zyklizität – ein und gewinnen eine Reihe von Sätzen zur Beschreibung zyklischer Gruppen anhand des Verhaltens ihrer Elemente:

Definition 3.33. *Eine Gruppe G heißt **zyklisch**, wenn es ein $g \in G$ mit*

$$G = \{g^n : n \in \mathbb{Z}\} =: \langle g \rangle$$

*gibt. In diesem Fall nennen wir g einen **Erzeuger** von G.*

Bemerkung 3.34. *Jede zyklische Gruppe G ist offenbar abelsch, denn für einen Erzeuger g von G und beliebige $a, b \in \mathbb{Z}$ gilt*

$$g^a g^b = g^{a+b} = g^{b+a} = g^b g^a.$$

Beispiel 3.35. (a) *Die Gruppe $(\mathbb{Z}/5\mathbb{Z})^\times = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$ ist zyklisch,*

denn: Es gilt $\overline{2}^0 = \overline{1}$, $\overline{2}^1 = \overline{2}$, $\overline{2}^2 = \overline{4}$ und $\overline{2}^3 = \overline{8} = \overline{3}$. Wir erhalten $(\mathbb{Z}/5\mathbb{Z})^\times = \langle \overline{2} \rangle$ und also die Behauptung. #

(b) *Die Gruppe $(\mathbb{Z}/8\mathbb{Z})^\times = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$ ist nicht zyklisch,*

denn: Wir bestimmen $\langle g \rangle$ für alle $g \in (\mathbb{Z}/8\mathbb{Z})^\times$ und erhalten wie in Teil (a): $\langle \overline{1} \rangle = \{\overline{1}\}$, $\langle \overline{3} \rangle = \{\overline{1}, \overline{3}\}$, $\langle \overline{5} \rangle = \{\overline{1}, \overline{5}\}$ sowie $\langle \overline{7} \rangle = \{\overline{1}, \overline{7}\}$. Somit ist $(\mathbb{Z}/8\mathbb{Z})^\times$ nicht zyklisch. #

(c) *Die additive Gruppe $\mathbb{Z}$ ist zyklisch,*

denn: Es ist $\mathbb{Z} = \{n \cdot 1 : n \in \mathbb{Z}\} = \langle 1 \rangle$. Man beachte, dass die Verknüpfung hier durch „+“gegeben ist, so dass g^n im Sinne der obigen Definition hier als das n-fache Aufsummieren von g, falls $n \in \mathbb{N}_0$ ist, bzw. als das $(-n)$-fache Aufsummieren von $-g$, falls $-n \in \mathbb{N}_0$ ist, zu verstehen ist. Also ist $\mathbb{Z}$ zyklisch. #

(d) *Die additive Gruppe $\mathbb{Z}/m\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$ ist zyklisch,*

denn: Für jedes Element $a \in \{0, \ldots, m-1\}$ ist $\overline{a}$ durch das a-fache Aufsummieren von $\overline{1}$ gegeben, woraus folgt, dass $\mathbb{Z}/m\mathbb{Z}$ zyklisch ist. #

Definition 3.36. *Sei G eine endliche abelsche Gruppe und $g \in G$. Dann ist die **Ordnung** von g definiert als*

$$\operatorname{ord}(g) := \min\{n \in \mathbb{N} : g^n = 1\}.$$

Nach Proposition 3.29 ist $g^{|G|} = 1$, so dass $\operatorname{ord}(g)$ wohldefiniert ist und stets $\operatorname{ord}(g) \leq |G|$ gilt.

Beispiel 3.37. *Sei $G = (\mathbb{Z}/5\mathbb{Z})^\times$. Dann gilt:*

(a) $\operatorname{ord}(\overline{2}) = 4$,
denn: $\overline{2}^1 = \overline{2}, \overline{2}^2 = \overline{4}, \overline{2}^3 = \overline{3}, \overline{2}^4 = \overline{1}$. #

(b) $\operatorname{ord}(\overline{4}) = 2$,
denn: $\overline{4}^1 = \overline{4}, \overline{4}^2 = \overline{1}$. #

Proposition 3.38. *Sei G eine endliche abelsche Gruppe. Dann sind die folgenden Aussagen äquivalent:*

(i) *G ist zyklisch.*
(ii) *Es gibt ein $g \in G$ mit $\operatorname{ord}(g) = |G|$.*

Ist dies der Fall, so ist jedes Element $g \in G$ mit $\operatorname{ord}(g) = |G|$ ein Erzeuger von G, und für jeden Erzeuger g von G gilt $\operatorname{ord}(g) = |G|$.

Beweis. Gelte zunächst Aussage (i) und sei also G zyklisch. Dann existiert ein $g \in G$ mit $G = \langle g \rangle = \{g^k : k \in \mathbb{Z}\}$. Wir behaupten, dass dann $n := \operatorname{ord}(g) = |G|$ gilt. Für ein beliebiges $k \in \mathbb{Z}$ gibt es $q, r \in \mathbb{Z}$ mit $0 \leq r < n$ und $k = qn + r$, insbesondere gilt $g^k = g^{qn+r} = (g^n)^q g^r = g^r$. Für $r_1, r_2 \in \mathbb{Z}$ mit $0 \leq r_1 < r_2 < n$ ist $g^{r_1} \neq g^{r_2}$, sonst wäre $g^{r_2 - r_1} = 1$ im Widerspruch zur Minimalität von $\operatorname{ord}(g)$. Es ergibt sich $G = \langle g \rangle = \{g^0, g^1, \ldots, g^{n-1}\}$ und deshalb $|G| = n = \operatorname{ord}(g)$.

Gelte nun umgekehrt Aussage (ii) und sei $g \in G$ mit $\operatorname{ord}(g) = |G| =: n$. Wie im Beweis der anderen Implikation erhalten wir $\langle g \rangle = \{g^0, g^1, \ldots, g^{n-1}\}$, also $|\langle g \rangle| = n = |G|$ und somit $\langle g \rangle = G$. Das ist die Zyklizität von G. □

Der Beweis hat insbesondere gezeigt: $\langle g \rangle = \{1, g, \ldots, g^{\operatorname{ord}(g)-1}\}$.

Proposition 3.39. *Seien G eine endliche abelsche Gruppe, $g \in G$ und $m \in \mathbb{Z}$. Dann sind die folgenden beiden Aussagen äquivalent:*

(i) *$\operatorname{ord}(g) \mid m$.*
(ii) *$g^m = 1$.*

Beweis. Gelte zunächst Aussage (i) und also $\operatorname{ord}(g) \mid m$. Dann ist $m = q \operatorname{ord}(g)$ für ein $q \in \mathbb{Z}$ und wir erhalten $g^m = (g^{\operatorname{ord}(g)})^q = 1$, also Aussage (ii).

Gelte nun umgekehrt Aussage (ii) und also $g^m = 1$. Wir schreiben $m = q \operatorname{ord}(g) + r$ mit $q, r \in \mathbb{Z}$ und $0 \leq r < \operatorname{ord}(g)$. Es ergibt sich $1 = g^m = (g^{\operatorname{ord}(g)})^q g^r = g^r$. Aus der Minimalität von $\operatorname{ord}(g)$ erhalten wir $r = 0$, was $\operatorname{ord}(g) \mid m$ und also Aussage (i) impliziert. □

Korollar 3.40. *Sei G eine endliche abelsche Gruppe und $g \in G$. Dann gilt* $\operatorname{ord}(g) \mid |G|$.

Beweis. Das ergibt sich direkt aus Proposition 3.39, da nach Proposition 3.29 bereits $g^{|G|} = 1$ gilt. □

Definition 3.41. *Sei G eine endliche abelsche Gruppe. Dann ist der **Exponent** von G definiert als*

$$\exp(G) := \min\{n \in \mathbb{N} : g^n = 1 \text{ für alle } g \in G\}.$$

Beispiel 3.42. (a) *Es ist* $\exp((\mathbb{Z}/5\mathbb{Z})^\times) = 4$,

denn: Es ist $\overline{a}^4 = \overline{1}$ für alle $\overline{a} \in (\mathbb{Z}/5\mathbb{Z})^\times$ und $\operatorname{ord}(\overline{2}) = 4$. #

(b) *Es ist* $\exp((\mathbb{Z}/8\mathbb{Z})^\times) = 2$,

denn: Es ist $\operatorname{ord}(\overline{3}) = \operatorname{ord}(\overline{5}) = \operatorname{ord}(\overline{7}) = 2$. #

Proposition 3.43. *Sei G eine endliche abelsche Gruppe. Dann gelten die folgenden beiden Aussagen:*

(a) $\exp(G) \mid |G|$.

(b) $\exp(G) = \operatorname{kgV}\{\operatorname{ord}(g) : g \in G\}$.

Beweis. Wir schreiben $|G| = q\exp(G) + r$ mit $0 \leq r < \exp(G)$ und $q \in \mathbb{Z}$. Für alle $g \in G$ gilt dann

$$1 = g^{|G|} = (g^{\exp(G)})^q g^r = g^r$$

und aufgrund der Minimalität von $\exp(G)$ ist $r = 0$, was $\exp(G) \mid |G|$ impliziert. Das ist Behauptung (a).

Zum Beweis von Behauptung (b) rechnen wir nach, dass $\exp(G)$ die definierenden Eigenschaften von $\operatorname{kgV}\{\operatorname{ord}(g) : g \in G\}$ erfüllt: Zunächst ist $\exp(G)$ ein gemeinsames Vielfaches aller Ordnungen von Elementen von G, denn für $g \in G$ gilt $g^{\exp(G)} = 1$, was nach Proposition 3.39 bereits $\operatorname{ord}(g) \mid \exp(G)$ impliziert. Sei nun $m \in \mathbb{Z}$ mit $\operatorname{ord}(g) \mid m$ für alle $g \in G$. Wir behaupten, dass dann $\exp(G) \mid m$ gilt, und schreiben dazu $m = q\exp(G) + r$ mit $q, r \in \mathbb{Z}$ und $0 \leq r < \exp(G)$. Wegen $\operatorname{ord}(g) \mid m$ gilt für alle $g \in G$:

$$1 = g^m = (g^{\exp(G)})^q g^r = g^r,$$

was wegen der Minimalität von $\exp(G)$ bereits $r = 0$ zur Folge hat, was unsere Behauptung impliziert. □

Definition 3.44. *Eine Abbildung $\psi\colon G \to H$ zwischen zwei Gruppen G, H heißt ein **(Gruppen-)Homomorphismus**, wenn für alle Elemente $a, b \in G$ die Beziehung $\psi(ab) = \psi(a)\psi(b)$ gilt. Ist ψ zusätzlich bijektiv, so heißt ψ ein **(Gruppen-)Isomorphismus**. Existiert ein Isomorphismus zwischen G und H, so nennen wir G und H **isomorph** und schreiben $G \cong H$.*

Beispiel 3.45. *Sei K ein Körper. Dann ist* $\det\colon \mathrm{GL}_n(K) \to K^\times$ *ein Homomorphismus, denn es gilt* $\det(AB) = \det(A)\det(B)$ *für alle $A, B \in \mathrm{GL}_n(K)$.*

Proposition 3.46. *Seien G, H Gruppen und $\psi\colon G \to H$ ein Homomorphismus. Dann gelten die folgenden beiden Aussagen:*

(a) *ψ ist genau dann injektiv, wenn* $\mathrm{Kern}(\psi) := \{g \in G : \psi(g) = 1\} = \{1\}$ *gilt.*

(b) *Ist ψ ein Isomorphismus, so ist $\psi^{-1}\colon H \to G$ ebenfalls ein Isomorphismus.*

Beweis. Wir bemerken zunächst $\psi(1) = \psi(1 \cdot 1) = \psi(1)\psi(1)$ und folgern $\psi(1) = 1$. Sei nun ψ injektiv und $g \in \mathrm{Kern}(\psi)$. Dann gilt $\psi(g) = 1 = \psi(1)$, was wegen der Injektivität von ψ bereits $g = 1$ und also $\mathrm{Kern}(\psi) = \{1\}$ impliziert. Gelte nun umgekehrt $\mathrm{Kern}(\psi) = \{1\}$ und seien $g_1, g_2 \in G$ mit $\psi(g_1) = \psi(g_2)$ gegeben. Wegen

$$1 = \psi(1) = \psi(g_2 g_2^{-1}) = \psi(g_2)\psi(g_2^{-1})$$

gilt dann $\psi(g_2^{-1}) = \psi(g_2)^{-1}$. Wir erhalten

$$\psi(g_1 g_2^{-1}) = \psi(g_1)\psi(g_2^{-1}) = \psi(g_1)\psi(g_2)^{-1} = 1$$

und also $g_1 g_2^{-1} \in \mathrm{Kern}(\psi) = \{1\}$. Das ergibt $g_1 = g_2$ und somit die Injektivität von ψ. Insgesamt haben wir so Behauptung (a) bewiesen.

Wir zeigen nun Behauptung (b): Aufgrund der Bijektivität von ψ existiert das Inverse ψ^{-1} und ist selbst bijektiv. Wir müssen zeigen, dass ψ^{-1} ein Homomorphismus ist. Dazu seien $h_1, h_2 \in H$. Für $g_1 := \psi^{-1}(h_1)$ und $g_2 := \psi^{-1}(h_2)$ ergibt sich dann $\psi(g_1 g_2) = \psi(g_1)\psi(g_2) = h_1 h_2$ und also $\psi^{-1}(h_1 h_2) = g_1 g_2 = \psi^{-1}(h_1)\psi^{-1}(h_2)$, was zu zeigen war. □

Der nächste Satz liefert eine Klassifikation zyklischer Gruppen bis auf Isomorphie:

Satz 3.47. *Für eine beliebige zyklische Gruppe G gilt:*

$$G \cong \begin{cases} \mathbb{Z} & \text{für } G \text{ unendlich,} \\ \mathbb{Z}/|G|\mathbb{Z} & \text{für } G \text{ endlich.} \end{cases}$$

Beweis. Wir setzen $n := |G|$, falls G endlich ist, und $n := 0$, falls G unendlich ist. Sei $g \in G$ ein Erzeuger von G. Wir definieren

$$\psi\colon \begin{cases} \mathbb{Z}/n\mathbb{Z} & \to G, \\ \overline{a} & \mapsto g^a. \end{cases}$$

Der Satz folgt, wenn wir zeigen können, dass ψ ein Isomorphismus ist. Tatsächlich ist ψ wohldefiniert,

denn: Für je zwei $a_1, a_2 \in \overline{a}$ gilt $a_1 - a_2 \in n\mathbb{Z}$. Es gibt also ein $k \in \mathbb{Z}$ mit $a_1 - a_2 = nk$ und wir erhalten

$$g^{a_1 - a_2} = g^{nk} = \begin{cases} (g^{|G|})^k & \text{für } G \text{ endlich,} \\ g^0 & \text{für } G \text{ unendlich} \end{cases} = 1,$$

also $g^{a_1} = g^{a_2}$. #

Die Abbildung ψ ist ein Homomorphismus,

denn: Für je zwei $\overline{a}, \overline{b} \in \mathbb{Z}/n\mathbb{Z}$ ist

$$\psi(\overline{a} + \overline{b}) = \psi(\overline{a+b}) = g^{a+b} = g^a g^b = \psi(\overline{a})\psi(\overline{b}).$$

#

Weiter ist ψ auch injektiv und es gilt also $\mathrm{Kern}(\psi) = \{\overline{0}\}$,

denn: Sei $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ mit $\psi(\overline{a}) = g^a = 1$. Falls G endlich ist, so folgt $n = |G| \overset{3.38}{=} \mathrm{ord}(g) \mid a$ nach Proposition 3.39. Damit ist $\overline{a} = \overline{0}$. Ist G unendlich, so nehmen wir an, dass $a \neq 0$ ist. Wir können dann ohne Einschränkung $a > 0$ annehmen, denn $g^a = 1$ ist äquivalent zu $g^{-a} = 1$. Aus $g^a = 1$ folgt dann $\langle g \rangle = \{1, g, \ldots, g^{a-1}\}$ wie im Beweis zu Proposition 3.38. Wegen $G = \langle g \rangle$ ist das ein Widerspruch zur Unendlichkeit von G. Also ist $a = 0$ und ψ injektiv. #

Schließlich ist die Abbildung ψ auch surjektiv, denn für endliches G ist $G = \{1, g, \ldots, g^{n-1}\} = \psi(\mathbb{Z}/n\mathbb{Z})$ und für unendliches G gilt $G = \{g^k : k \in \mathbb{Z}\} = \psi(\mathbb{Z})$. Somit ist ψ ein Isomorphismus. □

Beispiel 3.48. *In Beispiel 3.35 haben wir gesehen, dass $(\mathbb{Z}/5\mathbb{Z})^\times$ zyklisch ist. Nach Satz 3.47 gilt genauer $(\mathbb{Z}/5\mathbb{Z})^\times \cong \mathbb{Z}/4\mathbb{Z}$. Explizit ist ein Isomorphismus durch*

$$\psi\colon \begin{cases} \mathbb{Z}/4\mathbb{Z} & \to (\mathbb{Z}/5\mathbb{Z})^\times, \\ a & \mapsto \overline{2}^a \end{cases}$$

gegeben, also $\psi(\overline{0}) = \overline{2}^0 = \overline{1}$, $\psi(\overline{1}) = \overline{2}^1 = \overline{2}$, $\psi(\overline{2}) = \overline{2}^2 = \overline{4}$, $\psi(\overline{3}) = \overline{2}^3 = \overline{3}$.

Satz 3.49. *Sei G eine endliche abelsche Gruppe. Dann sind die folgenden beiden Aussagen äquivalent:*

(i) *G ist zyklisch.*
(ii) $\exp(G) = |G|$.

Beweis. Gelte zunächst Aussage (i) und sei also G zyklisch. Nach Proposition 3.43 gilt $\exp(G) \mid |G|$. Für einen beliebigen Erzeuger $g \in G$ von G folgt dann

$$|G| \overset{3.38}{=} \mathrm{ord}(g) \mid \mathrm{kgV}\{\mathrm{ord}(\tilde{g}) : \tilde{g} \in G\} = \exp(G)$$

und deshalb $\exp(G) = |G|$, also Aussage (ii).

Gelte nun umgekehrt Aussage (ii). Wir setzen $n := \exp(G) = |G|$ und schreiben $n = \prod_{p \in \mathbb{P}} p^{\nu_p(n)}$ für die kanonische Primfaktorzerlegung von n. Im ersten Beweisschritt zeigen wir, dass es für jedes $p \in \mathbb{P}$ ein Element $g_p \in G$ mit $\mathrm{ord}(g_p) = p^{\nu_p(n)}$ gibt. Sei dazu $p \in \mathbb{P}$ fixiert. Im Fall $p^{\nu_p(n)} \nmid \mathrm{ord}(g)$ für alle $g \in G$ folgt

$$p^{\nu_p(n)} \nmid \mathrm{kgV}\{\mathrm{ord}(g) : g \in G\} = \exp(G) = n,$$

was ein Widerspruch ist. Also gibt es ein $\tilde{g}_p \in G$ mit $p^{\nu_p(n)} \mid \operatorname{ord}(\tilde{g}_p)$. Wir setzen

$$g_p := \tilde{g}_p^{\frac{\operatorname{ord}(\tilde{g}_p)}{p^{\nu_p(n)}}}.$$

Es ergibt sich

$$g_p^{p^{\nu_p(n)}} = \tilde{g}_p^{\operatorname{ord}(\tilde{g}_p)} = 1$$

und deshalb $\operatorname{ord}(g_p) \mid p_p^{\nu_p(n)}$ nach Proposition 3.39. Wäre $\operatorname{ord}(g_p) < p^{\nu_p(n)}$, etwa $\operatorname{ord}(g_p) = p^f$ mit $f < \nu_p(n)$, so gälte

$$1 = g_p^{p^f} = \tilde{g}_p^{\frac{\operatorname{ord}(\tilde{g}_p)}{p^{\nu_p(n)-f}}}$$

und also wegen $\frac{\operatorname{ord}(\tilde{g}_p)}{p^{\nu_p(n)-f}} < \operatorname{ord}(\tilde{g}_p)$ ein Widerspruch. Deshalb ist $\operatorname{ord}(g_p) = p^{\nu_p(n)}$.

Im zweiten Beweisschritt zeigen wir, dass $g := \prod_{p\in\mathbb{P}} g_p$ ein Erzeuger von G ist und dass also $\operatorname{ord}(g) = |G| = n$ gilt. Wir nehmen an, es gälte $\operatorname{ord}(g) =: d < n$. Nach Proposition 3.39 ergäbe sich daraus $d \mid n$. Wegen $d < n$ gäbe es ein $\tilde{p} \in \mathbb{P}$ mit $d \mid \frac{n}{\tilde{p}}$ und insbesondere mit $g^{\frac{n}{\tilde{p}}} = 1$. Es folgte

$$1 = g^{\frac{n}{\tilde{p}}} = \prod_{p\in\mathbb{P}} g_p^{\frac{n}{\tilde{p}}}.$$

Für $p \neq \tilde{p}$ gälte $p^{\nu_p(n)} \mid \frac{n}{\tilde{p}}$ und somit $g_p^{\frac{n}{\tilde{p}}} = 1$. Wir erhielten $g_{\tilde{p}}^{\frac{n}{\tilde{p}}} = 1$, also

$$\operatorname{ord}(g_{\tilde{p}}) = \tilde{p}^{\nu_{\tilde{p}}(n)} \mid \frac{n}{\tilde{p}} = \frac{1}{\tilde{p}} \cdot \prod_{p\in\mathbb{P}} p^{\nu_p(n)},$$

was ein Widerspruch ist. Aufgrund dessen ist $\operatorname{ord}(g) = n = |G|$, also ist G zyklisch. □

3.5 Die Zyklizität von $\mathbb{F}_p^\times$

In diesem Abschnitt zeigen wir, dass für eine Primzahl p die Gruppe $\mathbb{F}_p^\times = (\mathbb{Z}/p\mathbb{Z})^\times$ zyklisch ist, und somit einen ersten Spezialfall der von uns angestrebten Untersuchung der Zyklizität von $(\mathbb{Z}/n\mathbb{Z})^\times$. Dazu werden wir das Kriterium aus Satz 3.49 verwenden, benötigen aber zunächst noch einige Vorbereitungen aus der Theorie der Polynomringe:

Definition 3.50. *Seien R ein Ring und $f = a_nX^n + \ldots + a_1X + a_0 \in R[X]$ mit $a_n \neq 0$. Dann ist der **Grad** von f definiert als $\deg(f) := n$ und der **Leitkoeffizient** von f als $\ell(f) := a_n$. Wir setzen $\deg(0) := -\infty$ und $\ell(0) := 0$.*

Proposition 3.51. *Seien R ein Ring und $f, g \in R[X]$, wobei $\ell(f)$ oder $\ell(g)$ kein Nullteiler sei. Dann gilt $\deg(fg) = \deg(f) + \deg(g)$.*

Beweis. Im Fall $f = 0$ oder $g = 0$ gilt $\deg(fg) = \deg(0) = -\infty = \deg(f) + \deg(g)$. Sei ab sofort $f := a_n X^n + \ldots + a_0 \neq 0 \neq b_m X^m + \ldots + b_0 =: g$ mit $a_n, b_m \neq 0$. Wir erhalten $fg = a_n b_m X^{n+m} +$ Terme kleineren Grades. Da $\ell(f) = a_n$ oder $\ell(g) = b_m$ kein Nullteiler ist, folgt $a_n b_m \neq 0$ und somit $\deg(fg) = n + m = \deg(f) + \deg(g)$. □

Proposition 3.52 (Polynomdivision mit Rest)**.** *Seien $R \neq 0$ ein Ring und $f, g \in R[X]$ mit $\ell(g) \in R^\times$. Dann gibt es eindeutig bestimmte Polynome $q, r \in R[X]$ mit $f = qg + r$ und $\deg(r) < \deg(g)$.*

Beweis. Wir zeigen zuerst die Existenzaussage per Induktion nach $\deg(f)$. Im Fall $\deg(f) < \deg(g)$ setzen wir $q := 0$ und $r := f$. Sei nun $\deg(f) \geq \deg(g)$ und schreiben wir

$$f = aX^{n+k} + \text{ Terme kleineren Grades}, \quad g = bX^n + \text{ Terme kleineren Grades}$$

mit $a \in R \setminus \{0\}, b \in R^\times, n, k \in \mathbb{N}_0$. Es ist

$$\deg(f - \frac{a}{b} X^k g) < \deg(f),$$

so dass es nach Induktionsvoraussetzung $q_1, r_1 \in R[X]$ gibt mit

$$f - \frac{a}{b} X^k g = q_1 g + r_1 \quad \text{und} \quad \deg(r_1) < \deg(g).$$

Daraus erhalten wir

$$f = \left(q_1 + \frac{a}{b} X^k\right) g + r_1.$$

Wir setzen $q := q_1 + \frac{a}{b} X^k$ sowie $r := r_1$ und der Existenzbeweis ist beendet.

Zum Nachweis der Eindeutigkeit sei $f = q_1 g + r_1 = q_2 g + r_2$ mit $\deg(r_1), \deg(r_2) < \deg(g)$. Es ergibt sich

$$(q_1 - q_2) g = r_2 - r_1.$$

Wäre $q_1 \neq q_2$, dann folgte aus Proposition 3.51

$$\deg((q_1 - q_2) g) = \deg(q_1 - q_2) + \deg(g) \geq \deg(g),$$

da $\ell(g) \in R^\times$ und damit nach Proposition 3.17 kein Nullteiler ist. Andererseits ist

$$\deg((q_1 - q_2) g) = \deg(r_2 - r_1) < \deg(g),$$

was zum Widerspruch führt. Deshalb ist $q_1 = q_2$ und somit auch $r_1 = r_2$. □

Proposition 3.53. *Seien R ein Ring, $f \in R[X]$ und $a \in R$ eine Nullstelle von f. Dann gibt es ein $q \in R[X]$ mit $f = (X - a)q$.*

Beweis. Nach Proposition 3.52 existieren $q, r \in R[X]$ mit $f = q(X - a) + r$ und $\deg(r) < \deg(X - a) = 1$. Also ist r ein konstantes Polynom und es gilt

$$0 = f(a) = q(a)(a - a) + r(a) = r(a),$$

weswegen $r = 0$ ist. □

Korollar 3.54. *Seien R ein nullteilerfreier Ring und $f \in R[X] \setminus \{0\}$ mit $\deg(f) = n$. Dann besitzt f in R höchstens n Nullstellen.*

Beweis. Wir zeigen die Aussage per Induktion nach n. Für $n = 0$ ist die Behauptung wahr, denn ein konstantes, von Null verschiedenes Polynom besitzt keine Nullstelle. Sei nun $n > 0$. Falls f keine Nullstelle besitzt, so sind wir fertig. Wir nehmen im Folgenden daher an, dass f eine Nullstelle $a \in R$ besitzt. Nach Proposition 3.53 gibt es dann ein $q \in R[X]$ mit $f = (X - a)q$. Aufgrund von

$$n = \deg(f) = \deg((X - a)q) = 1 + \deg(q)$$

ist $\deg(q) = n - 1$. Ist nun $b \in R$ eine weitere Nullstelle von f, so gilt $0 = f(b) = (b - a)q(b)$. Da R nullteilerfrei ist, folgt $b = a$ oder b ist eine Nullstelle von q. Nach Induktionsvoraussetzung hat q aber höchstens $n - 1$ Nullstellen, weshalb f höchstens n Nullstellen haben kann. □

Beispiel 3.55. *Lässt man in Korollar 3.54 die Voraussetzung, dass R ein nullteilerfreier Ring ist, weg, so kann man leicht Gegenbeispiele finden: So hat etwa im Ring $R = \mathbb{Z}/8\mathbb{Z}$ das Polynom $f = X^2 - \overline{1}$ die vier verschiedenen Nullstellen $\overline{1}, \overline{3}, \overline{5}, \overline{7}$.*

Proposition 3.56. *Für eine beliebige Primzahl p gilt in $\mathbb{F}_p[X]$ die Identität*

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

Beweis. Wir setzen

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

Division mit Rest im Polynomring $\mathbb{F}_p[X]$ liefert

$$X^{p-1} - \overline{1} = qf + r \quad \text{mit } q, r \in \mathbb{F}_p[X] \text{ und } \deg(r) < \deg(f) = p - 1.$$

Für jedes $\overline{a} \in \mathbb{F}_p^\times$ gilt nach dem Kleinen Satz von Fermat 3.32 die Gleichung $\overline{a}^{p-1} = \overline{1}$, so dass $\overline{a}$ eine Nullstelle von $X^{p-1} - \overline{1}$ ist. Weil auch $f(\overline{a}) = \overline{0}$ gilt, erhalten wir $r(\overline{a}) = \overline{0}$. Das Polynom r hat somit $p - 1$ Nullstellen. Aufgrund von $\deg(r) < p - 1$ ergibt sich aus Korollar 3.54 somit $r = \overline{0}$. Wegen $\deg(X^{p-1} - \overline{1}) = p - 1 = \deg(f)$ ist q ein konstantes Polynom und aus $\ell(X^{p-1} - \overline{1}) = \overline{1} = \ell(f)$ erhalten wir $q = \overline{1}$ und insgesamt die Behauptung. □

Korollar 3.57 (Satz von Wilson)**.** *Für eine beliebige natürliche Zahl $n \in \mathbb{N}$ mit $n > 1$ sind die folgenden beiden Aussagen äquivalent:*

(i) *n ist eine Primzahl.*

(ii) $(n - 1)! \equiv -1 \bmod (n)$.

Beweis. Gelte zunächst Aussage (i) und sei also $n = p$ eine Primzahl. Aus Proposition 3.56 ergibt sich

$$(X - \overline{1})(X - \overline{2}) \cdot \ldots \cdot (X - \overline{p-1}) = X^{p-1} - \overline{1}$$

in $\mathbb{F}_p[X]$. Setzen wir $X = \overline{0} = \overline{p}$, so erhalten wir

$$\overline{p-1} \cdot \overline{p-2} \cdot \ldots \cdot \overline{1} = -\overline{1}.$$

und somit $(p-1)! \equiv -1 \bmod (p)$. Das ist Aussage (ii).

Die andere Implikation zeigen wir indirekt: Gelte Aussage (i) nicht und sei also $1 < n$ keine Primzahl. Dann gibt es eine Primzahl $p < n$ mit $p \mid n$. Insbesondere folgt $p \mid (n-1)!$ und also $\mathrm{ggT}((n-1)!, n) \neq 1$. Es ist daher $\overline{(n-1)!}$ keine prime Restklasse modulo n. Weil $\overline{-1}$ aber eine prime Restklasse modulo n ist, erhalten wir $(n-1)! \not\equiv -1 \bmod (n)$, so dass Aussage (ii) nicht gilt. □

Satz 3.58. *Seien R ein nullteilerfreier Ring und $G \subseteq R^\times$ eine endliche Gruppe mit der eingeschränkten Multiplikation als Verknüpfung. Dann ist G zyklisch.*

Beweis. Wir setzen $n := \exp(G)$. Dann gilt $g^n = 1$ für alle $g \in G$, alle $g \in G$ sind also Nullstellen des Polynoms $X^n - 1 \in R[X]$. Nach Korollar 3.54 hat dieses Polynom höchstens n Nullstellen und wir erhalten $|G| \leq n = \exp(G)$. Nach Proposition 3.43 gilt andererseits aber $\exp(G) \mid |G|$. Es folgt $\exp(G) = |G|$, was nach Satz 3.49 die Zyklizität von G impliziert. □

Korollar 3.59. *Für jede beliebige Primzahl p ist $\mathbb{F}_p^\times$ eine zyklische Gruppe und es gilt insbesondere*

$$\mathbb{F}_p^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}.$$

Beweis. Das ergibt sich direkt aus Satz 3.58, wenn man dort $R = \mathbb{F}_p$ und $G = \mathbb{F}_p^\times$ setzt. □

Definition 3.60. *Sei p eine Primzahl. Eine ganze Zahl $w \in \mathbb{Z}$ heißt eine **primitive Wurzel** modulo p, wenn $\overline{w}$ ein Erzeuger von $\mathbb{F}_p^\times$ ist, wenn also $\mathbb{F}_p^\times = \langle \overline{w} \rangle$ gilt.*

Beispiel 3.61. (a) *Nach Beispiel 3.35 (a) gilt $\mathbb{F}_5^\times = \langle \overline{2} \rangle$, so dass 2 eine primitive Wurzel modulo 5 ist.*

(b) *Wir betrachten den Fall $p = 7$. Hier gilt zunächst $\mathbb{F}_7^\times = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}$. Ordnungen von Elementen aus $\mathbb{F}_7^\times$ müssen Teiler von $|\mathbb{F}_7^\times| = 6$ sein, so dass als Elementordnungen nur $1, 2, 3, 6$ infrage kommen. Wegen $\overline{2}^3 = \overline{1}$ gilt $\mathrm{ord}(\overline{2}) = 3$, so dass 2 keine primitive Wurzel modulo 7 ist. Aber wegen $\overline{3}^2 = \overline{2} \neq \overline{1}$ und $\overline{3}^3 = \overline{6} \neq \overline{1}$ ist $\mathrm{ord}(\overline{3}) = 6$ und 3 ist eine primitive Wurzel modulo 7. Explizit erhalten wir:*

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

Es ist keine allgemeingültige Formel bekannt, die für jede Primzahl p eine primitive Wurzel modulo p liefert.

3.6 Die Struktur der primen Restklassengruppen für Primpotenzen

In diesem Abschnitt studieren wir die Struktur der primen Restklassengruppe $(\mathbb{Z}/n\mathbb{Z})^\times$ im Fall, dass n eine Primpotenz ist. Zunächst betrachten wir den Fall $n = p^r$ mit einer ungeraden Primzahl p. Eine Vorüberlegung hierzu ist:

Proposition 3.62. *Seien G eine endliche abelsche Gruppe und $m, n \in \mathbb{N}$ mit $\mathrm{ggT}(m,n) = 1$ und $|G| = mn$. Existieren dann Elemente $g, h \in G$ mit $\mathrm{ord}(g) = m$ und $\mathrm{ord}(h) = n$, so ist G zyklisch und gh ist ein Erzeuger von G.*

Beweis. Wir zeigen $\mathrm{ord}(gh) = mn$, was die Behauptung dann impliziert. Sei dafür $d \in \mathbb{N}$ mit $(gh)^d = 1$. Für dieses gilt

$$1 = 1^m = \big((gh)^d\big)^m = (g^m)^d h^{dm} = h^{dm}$$

und deswegen $\mathrm{ord}(h) = n \mid dm$, was aufgrund von $\mathrm{ggT}(m,n) = 1$ schließlich $n \mid d$ zur Folge hat. Analog ergibt sich $m \mid d$ und unter erneuter Verwendung von $\mathrm{ggT}(m,n) = 1$ somit $mn \mid d$. Es folgt $\mathrm{ord}(gh) \geq mn$ und wegen $\mathrm{ord}(gh) \leq |G| = mn$ insgesamt $\mathrm{ord}(gh) = mn$. □

Dass die Gruppe G unter den obigen Voraussetzungen zyklisch ist, folgt direkt aus Satz 3.49, denn aus den Voraussetzungen folgt $m \mid \exp(G)$ sowie $n \mid \exp(G)$ und wegen $\mathrm{ggT}(m,n) = 1$ also $|G| = mn \mid \exp(G)$. Der Sinn von Proposition 3.62 ist vor allem darin zu sehen, dass explizit ein Erzeuger angegeben wird.

Wir nutzen nun Proposition 3.62, um die Zyklizität von $(\mathbb{Z}/p^r\mathbb{Z})^\times$ für ungerade Primzahlen p und $r \in \mathbb{N}$ nachzuweisen. Aufgrund von

$$|(\mathbb{Z}/p^r\mathbb{Z})^\times| = \varphi(p^r) \overset{2.22}{=} p^{r-1}(p-1)$$

genügt es dabei, Elemente der Ordnung p^{r-1} bzw. $p-1$ zu konstruieren. Dies bereiten wir mit einem technischen Lemma vor:

Lemma 3.63. *Seien p eine Primzahl und $r, m \in \mathbb{N}$ mit $1 \leq m \leq p^r$. Dann gilt:*

$$v_p\Big(\binom{p^r}{m}\Big) = r - v_p(m).$$

Beweis. Es ist

$$\binom{p^r}{m} = \frac{(p^r)!}{(p^r-m)!m!} = \frac{p^r(p^r-1)\cdot\ldots\cdot(p^r-(m-1))}{1\cdot 2\cdot\ldots\cdot(m-1)\cdot m}$$

und deshalb

$$\begin{aligned} v_p\Big(\binom{p^r}{m}\Big) &= v_p(p^r) + v_p(p^r-1) + \ldots + v_p\big(p^r-(m-1)\big) \\ &\quad - v_p(1) - \ldots - v_p(m-1) - v_p(m) \\ &= r + \big(v_p(p^r-1) - v_p(1)\big) + \ldots + \big(v_p(p^r-(m-1)) - v_p(m-1)\big) - v_p(m) \end{aligned}$$

Sei $a \in \{1, \ldots, m-1\}$ mit $v_p(a) = k$ und also mit $a = p^k b$ mit $p \nmid b$. Es ergibt sich

$$p^r - a = p^r - p^k b = p^k(p^{r-k} - b)$$

mit $p \nmid (p^{r-k} - b)$ und somit $v_p(p^r - a) = v_p(a)$. Das impliziert

$$v_p\left(\binom{p^r}{m}\right) = r - v_p(m).$$

□

Wir nutzen nun Lemma 3.63, um ein Element von Ordnung p^{r-1} zu finden:

Proposition 3.64. *Seien p eine Primzahl und $r \in \mathbb{N}$ mit $r > 1$. Dann gilt:*

(a) $(1+p)^{p^{r-1}} \equiv 1 \bmod (p^r)$,
(b) $(1+p)^{p^{r-2}} \not\equiv 1 \bmod (p^r)$, *falls* $p \neq 2$.

Beweis. Nach dem Binomischen Lehrsatz gilt

$$(1+p)^{p^{r-1}} = 1 + \binom{p^{r-1}}{1} p + \binom{p^{r-1}}{2} p^2 + \ldots + \binom{p^{r-1}}{p^{r-1}} p^{(p^{r-1})}.$$

Für ein beliebiges $m \in \mathbb{N}$ mit $1 \leq m \leq p^{r-1}$ erhalten wir dabei

$$v_p\left(\binom{p^{r-1}}{m} p^m\right) \overset{3.63}{=} r - 1 - v_p(m) + m = r + \big(m - (v_p(m) + 1)\big).$$

Durch einen einfachen Induktionsbeweis sieht man, dass für $k \in \mathbb{N}_0$ stets $p^k \geq k + 1$ gilt. Daraus ergibt sich

$$m \geq p^{v_p(m)} \geq v_p(m) + 1$$

und deshalb

$$v_p\left(\binom{p^{r-1}}{m} p^m\right) \geq r.$$

Oben eingesetzt erhalten wir sofort

$$(1+p)^{p^{r-1}} \equiv 1 \bmod (p^r)$$

und somit Behauptung (a).

Zum Beweis von Behauptung (b) wenden wir wieder den Binomischen Lehrsatz an und erhalten

$$\begin{aligned}(1+p)^{p^{r-2}} &= 1 + \binom{p^{r-2}}{1} p + \binom{p^{r-2}}{2} p^2 + \ldots + \binom{p^{r-2}}{p^{r-2}} p^{(p^{r-2})} \\ &= 1 + p^{r-1} + \binom{p^{r-2}}{2} p^2 + \ldots + \binom{p^{r-2}}{p^{r-2}} p^{(p^{r-2})}.\end{aligned}$$

Sei $m \in \mathbb{N}$ mit $2 \leq m \leq p^{r-2}$. Es ergibt sich

$$v_p\left(\binom{p^{r-2}}{m} p^m\right) \overset{3.63}{=} r - 2 - v_p(m) + m = r + \big(m - (v_p(m) + 2)\big).$$

Ist $v_p(m) = 0$, so ist $m \geq 2 = v_p(m) + 2$. Wir betrachten nun den Fall $v_p(m) \neq 0$. Durch eine einfache Induktion sieht man, dass für $k \in \mathbb{N}$ stets $p^k \geq k + 2$ gilt. An dieser Stelle geht $p \neq 2$ ein, denn für $p = 2$ und $k = 1$ ist die Aussage falsch. Wir erhalten

$$m \geq p^{v_p(m)} \geq v_p(m) + 2,$$

also

$$v_p\left(\binom{p^{r-2}}{m} p^m\right) \geq r$$

und somit

$$(1 + p)^{p^{r-2}} \equiv 1 + p^{r-1} \not\equiv 1 \bmod (p^r).$$

Das ist Behauptung (b). □

Wir können nun die Zyklizität von $(\mathbb{Z}/p^r\mathbb{Z})^\times$ für ungerade Primzahlen p zeigen:

Satz 3.65. *Für eine beliebige Primzahl $p \neq 2$ und ein beliebiges $r \in \mathbb{N}$ gilt:*

(a) *$(\mathbb{Z}/p^r\mathbb{Z})^\times$ ist eine zyklische Gruppe.*

(b) *Ist $w \in \mathbb{Z}$ eine primitive Wurzel modulo p, so ist $\overline{w^{p^{r-1}}(1+p)}$ ein Erzeuger von $(\mathbb{Z}/p^r\mathbb{Z})^\times$.*

Beweis. Es genügt offenbar, Behauptung (b) zu beweisen, da diese (a) impliziert. Sei also $w \in \mathbb{Z}$ eine primitive Wurzel modulo p. Wir setzen $u := w^{p^{r-1}}$. Dann gilt $\operatorname{ord}(\overline{u}) = p - 1$,

denn: Nach dem Kleinen Satz von Fermat 3.32 gilt $w^p \equiv w \bmod (p)$. Induktiv erhalten wir $u = w^{p^{r-1}} \equiv w \bmod (p)$, so dass u eine primitive Wurzel modulo p ist. Damit sind $1, u, \ldots, u^{p-2}$ paarweise inkongruent modulo p, und also auch paarweise inkongruent modulo p^r. Hieraus folgt $\operatorname{ord}(\overline{u}) \geq p - 1$. Andererseits gilt aber auch

$$u^{p-1} = w^{p^{r-1}(p-1)} = w^{\varphi(p^r)} \equiv 1 \bmod (p^r),$$

was $\operatorname{ord}(\overline{u}) \mid (p - 1)$ impliziert. Zusammengenommen erhalten wir die Behauptung. #

Weiter gilt aber auch $\operatorname{ord}(\overline{1+p}) = p^{r-1}$,

denn: Nach Proposition 3.64 (a) gilt

$$(1 + p)^{p^{r-1}} \equiv 1 \bmod (p^r),$$

woraus $\operatorname{ord}(\overline{1+p}) \mid p^{r-1}$ folgt. Deshalb ist $\operatorname{ord}(\overline{1+p}) = p^k$ für ein $k \in \mathbb{N}$ mit $1 < k \leq r-1$. Nach Proposition 3.64 (b) ist jedoch

$$(1+p)^{p^{r-2}} \not\equiv 1 \bmod (p^r).$$

Die Behauptung folgt. #

Mit Proposition 3.62 erhalten wir wegen $|(\mathbb{Z}/p^r\mathbb{Z})^\times| = \varphi(p^r) = (p-1)p^{r-1}$ und $\operatorname{ord}(\overline{u}) = p-1$ sowie $\operatorname{ord}(\overline{1+p}) = p^{r-1}$, dass $\overline{u} \cdot \overline{1+p}$ ein Erzeuger von $(\mathbb{Z}/p^r\mathbb{Z})^\times$ ist. □

Der Beweis hat gezeigt: Ist $w \in \mathbb{Z}$ eine primitive Wurzel modulo p mit $\operatorname{ord}(\overline{w}) = p-1$ in $(\mathbb{Z}/p^r\mathbb{Z})^\times$, dann ist $\overline{w(1+p)}$ ein Erzeuger von $(\mathbb{Z}/p^r\mathbb{Z})^\times$.

Definition 3.66. *Seien p eine ungerade Primzahl und $r \in \mathbb{N}$. Eine Zahl $w \in \mathbb{Z}$ heißt eine **primitive Wurzel** modulo p^r, wenn $\overline{w}$ ein Erzeuger von $(\mathbb{Z}/p^r\mathbb{Z})^\times$ ist.*

Beispiel 3.67. *In Beispiel 3.61 haben wir gesehen, dass 3 eine primitive Wurzel modulo 7 ist. Gesucht ist nun eine primitive Wurzel modulo 49. Nach Satz 3.65 ist $\overline{3^7(1+7)} = \overline{31} \cdot \overline{8} = \overline{3}$ ein Erzeuger von $(\mathbb{Z}/49\mathbb{Z})^\times$, so dass 3 auch eine primitive Wurzel modulo 49 ist.*

In Ergänzung zu Satz 3.65 verbleibt in diesem Abschnitt die Struktur der Gruppen $(\mathbb{Z}/2^r\mathbb{Z})^\times$ zu studieren. Die Gruppen $(\mathbb{Z}/2\mathbb{Z})^\times$ und $(\mathbb{Z}/4\mathbb{Z})^\times$ sind beide offenbar zyklisch. In Beispiel 3.35 haben wir jedoch gesehen, dass dies für die Gruppe $(\mathbb{Z}/8\mathbb{Z})^\times$ nicht mehr gilt. Wir müssen also etwas genauer hinschauen. In Analogie zu Proposition 3.64 erhalten wir zunächst:

Proposition 3.68. *Für ein beliebiges $r \in \mathbb{N}$ mit $r > 1$ gilt:*

(a) $5^{2^{r-2}} \equiv 1 \bmod (2^r)$,

(b) $5^{2^{r-3}} \not\equiv 1 \bmod (2^r)$.

Beweis. Nach dem Binomischen Lehrsatz gilt

$$5^{2^{r-2}} = (1+2^2)^{2^{r-2}} = 1 + \binom{2^{r-2}}{1}2^2 + \binom{2^{r-2}}{2}2^4 + \ldots + \binom{2^{r-2}}{2^{r-2}}2^{2\cdot 2^{r-2}}.$$

Sei $m \in \mathbb{N}$ mit $1 \leq m \leq 2^{r-2}$. Wir erhalten

$$v_2\left(\binom{2^{r-2}}{m}2^{2m}\right) \overset{3.63}{=} r - 2 - v_2(m) + 2m = r + \big(m - (v_2(m)+1)\big) + m - 1.$$

Wie im Beweis von Proposition 3.64 ist $m - (v_2(m)+1) \geq 0$ und deshalb

$$v_2\left(\binom{2^{r-2}}{m}2^{2m}\right) \geq r,$$

woraus

$$5^{2^{r-2}} \equiv 1 \bmod (2^r)$$

und also Behauptung (a) folgt.

Zum Beweis von Behauptung (b) verwenden wir wieder den Binomischen Lehrsatz und erhalten

$$\begin{aligned} 5^{2^{r-3}} &= (1+2^2)^{2^{r-3}} = 1 + \binom{2^{r-3}}{1}2^2 + \binom{2^{r-3}}{2}2^4 + \ldots + \binom{2^{r-3}}{2^{r-3}}2^{2\cdot 2^{r-3}} \\ &= 1 + 2^{r-1} + \binom{2^{r-3}}{2}2^4 + \ldots + \binom{2^{r-3}}{2^{r-3}}2^{2\cdot 2^{r-3}}. \end{aligned}$$

Sei $m \in \mathbb{N}$ mit $2 \leq m \leq 2^{r-3}$. Es ergibt sich

$$v_2\left(\binom{2^{r-3}}{m}2^{2m}\right) \overset{3.63}{=} r - 3 - v_2(m) + 2m = r + \big(m - (v_2(m)+1)\big) + m - 2,$$

was mit analoger Argumentation wie im Beweis von Proposition 3.64 zu

$$v_2\left(\binom{2^{r-3}}{m}2^{2m}\right) \geq r$$

und so schließlich

$$5^{2^{r-3}} \equiv 1 + 2^{r-1} \not\equiv 1 \bmod (2^r).$$

impliziert. □

Es folgt, dass $(\mathbb{Z}/2^r\mathbb{Z})^\times$ für $r > 2$ niemals zyklisch ist:

Proposition 3.69. *Für $r \in \mathbb{N}$ mit $r > 2$ gilt:*

(a) *In $(\mathbb{Z}/2^r\mathbb{Z})^\times$ ist $\operatorname{ord}(\overline{5}) = 2^{r-2}$.*

(b) *Für jedes $\overline{a} \in (\mathbb{Z}/2^r\mathbb{Z})^\times$ gibt es eindeutig bestimmte Zahlen $i \in \{0,1\}$, $j \in \{0,\ldots,2^{r-2}-1\}$ mit*

$$\overline{a} = \overline{-1}^i\overline{5}^j.$$

(c) $\exp((\mathbb{Z}/2^r\mathbb{Z})^\times) = 2^{r-2} < |(\mathbb{Z}/2^r\mathbb{Z})^\times| = 2^{r-1}$, *insbesondere ist $(\mathbb{Z}/2^r\mathbb{Z})^\times$ nicht zyklisch.*

Beweis. Nach Proposition 3.68 gilt einerseits $\overline{5}^{2^{r-2}} = \overline{1}$ und somit $\operatorname{ord}(\overline{5}) \mid 2^{r-2}$. Daher gilt $\operatorname{ord}(\overline{5}) = 2^k$ für ein k mit $1 \leq k \leq r-2$. Andererseits gilt nach Proposition 3.68 auch

$$\overline{5}^{2^{r-3}} \neq \overline{1}.$$

Das hat $\operatorname{ord}(\overline{5}) = 2^{r-2}$ und also Behauptung (a) zur Folge.

Beim Beweis von Behauptung (b) bemerken wir zunächst, dass es offenbar $2 \cdot 2^{r-2} = 2^{r-1} = \varphi(2^r) = |(\mathbb{Z}/2^r\mathbb{Z})^\times|$ Paare (i,j) mit $i \in \{0,1\}$ und $j \in \{0,\ldots,2^{r-2}-1\}$ gibt. Seien nun $i, i' \in \{0,1\}$ und $j, j' \in \{0,\ldots,2^{r-2}-1\}$ mit

$$\overline{-1}^i\overline{5}^j = \overline{-1}^{i'}\overline{5}^{j'}.$$

Dann erhalten wir $\overline{-1}^{i-i'} = \overline{5}^{j'-j}$. Wäre nun $i \neq i'$, so folgte $\overline{-1} = \overline{5}^{j'-j}$ und somit $-1 \equiv 5^{j'-j} \bmod (2^r)$. Wegen $r > 2$ wäre dann $-1 \equiv 1 \bmod (4)$, was nicht stimmt. Also ist $i = i'$ und folglich $\overline{5}^{j'-j} = \overline{1}$. Das liefert $2^{r-2} = \operatorname{ord}(\overline{5}) \mid (j' - j)$. Da $-(2^{r-2} - 1) \leq j' - j \leq 2^{n-2} - 1$ ist, erhalten wir $j' - j = 0$ und also $j = j'$. Damit gibt es genau $|(\mathbb{Z}/2^r\mathbb{Z})^\times|$ verschiedene Produkte der Form $\overline{-1}^i\overline{5}^j$ mit $i \in \{0,1\}$, $j \in \{0,\ldots,2^{r-2}-1\}$. Dies impliziert Behauptung (b).

Es verbleibt Behauptung (c) zu zeigen. Aus $\operatorname{ord}(\overline{5}) = 2^{r-2}$ und Proposition 3.43 ergibt sich $2^{r-2} \mid \exp((\mathbb{Z}/2^r\mathbb{Z})^\times)$. Ist $\overline{a} \in (\mathbb{Z}/2^r\mathbb{Z})^\times$, so gibt es nach Aussage (b) Zahlen $i \in \{0,1\}$ und $j \in \{0,\ldots,2^{r-2}-1\}$ mit $\overline{a} = \overline{-1}^i\overline{5}^j$. Insbesondere ist

$$\overline{a}^{2^{r-2}} = \overline{-1}^{2^{r-2}i}\overline{5}^{2^{r-2}j} = (\overline{-1}^2)^{2^{r-3}i}(\overline{5}^{2^{r-2}})^j = \overline{1},$$

also ist $\exp((\mathbb{Z}/2^r\mathbb{Z})^\times) \leq 2^{r-2}$. Insgesamt erhalten wir $\exp((\mathbb{Z}/2^r\mathbb{Z})^\times) = 2^{r-2}$. Aufgrund von

$$|(\mathbb{Z}/2^r\mathbb{Z})^\times| = \varphi(2^r) = 2^{r-1} \neq 2^{r-2} = \exp((\mathbb{Z}/2^r\mathbb{Z})^\times)$$

und Satz 3.49 ist die Gruppe $(\mathbb{Z}/2^r\mathbb{Z})^\times$ nicht zyklisch. □

Nachdem wir festgestellt haben, dass die Gruppen $(\mathbb{Z}/2^r\mathbb{Z})^\times$ für $r > 2$ nicht zyklisch sind, würden wir natürlich trotzdem gerne ihre Struktur beschreiben. Dazu führen wir das direkte Produkt von Gruppen ein.

Proposition 3.70. *Seien $n \in \mathbb{N}$ und $G_1,\ldots,G_n$ Gruppen. Dann ist die Menge*

$$G_1 \times \ldots \times G_n := \{(g_1,\ldots,g_n) : g_1 \in G_1,\ldots,g_n \in G_n\}$$

zusammen mit der komponentenweisen Verknüpfung

$$(g_1,\ldots,g_n)\cdot(g_1',\ldots,g_n') := (g_1g_1',\ldots,g_ng_n')$$

*eine Gruppe, das sogenannte **direkte Produkt** der Gruppen $G_1,\ldots,G_n$. Sind alle Gruppen $G_1,\ldots,G_n$ abelsch, so ist auch $G_1 \times \ldots \times G_n$ abelsch.*

Beweis. Die Behauptung ergibt sich unmittelbar aus der Definition: Das Assoziativgesetz folgt aus dem Assoziativgesetz auf jeder Komponente, das neutrale Element ist durch $(1_{G_1},\ldots,1_{G_n})$ gegeben, wobei 1_{G_i} das neutrale Element in G_i bezeichne, und das zu $(g_1,\ldots,g_n)$ inverse Element ist durch $(g_1^{-1},\ldots,g_n^{-1})$ gegeben. □

Satz 3.71. *Sei $r \in \mathbb{N}$ mit $r > 1$. Dann ist die Abbildung*

$$\psi\colon \begin{cases} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{r-2}\mathbb{Z} & \to (\mathbb{Z}/2^r\mathbb{Z})^\times \\ (i+2\mathbb{Z}, j+2^{r-2}\mathbb{Z}) & \mapsto \overline{-1}^i\overline{5}^j \end{cases}$$

ein Isomorphismus und es gilt daher

$$(\mathbb{Z}/2^r\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{r-2}\mathbb{Z}.$$

Beweis. Die Abbildung ψ ist wohldefiniert,

denn: Seien $i_1, i_2 \in i + 2\mathbb{Z}$ und $j_1, j_2 \in j + 2^{r-2}\mathbb{Z}$. Dann ist $i_1 - i_2 \in 2\mathbb{Z}$ und $j_1 - j_2 \in 2^{r-2}\mathbb{Z}$. Wegen $\operatorname{ord}(\overline{-1}) = 2$ und $\operatorname{ord}(\overline{5}) = 2^{r-2}$ erhalten wir $\overline{-1}^{i_1-i_2} = \overline{1}$ und $\overline{5}^{j_1-j_2} = \overline{1}$. Das liefert $\overline{-1}^{i_1} = \overline{-1}^{i_2}$ und $\overline{5}^{j_1} = \overline{5}^{j_2}$ und deshalb $\psi(i_1 + 2\mathbb{Z}, j_1 + 2^{r-2}\mathbb{Z}) = \psi(i_2 + 2\mathbb{Z}, j_2 + 2^{r-2}\mathbb{Z})$. #

Die Abbildung ψ ist ein Homomorphismus,

denn: Seien $i + 2\mathbb{Z}, i' + 2\mathbb{Z} \in \mathbb{Z}/2\mathbb{Z}$ und $j + 2^{r-2}\mathbb{Z}, j' + 2^{r-2}\mathbb{Z} \in \mathbb{Z}/2^{r-2}\mathbb{Z}$. Wir erhalten

$$\begin{aligned}&\psi\big((i + 2\mathbb{Z}, j + 2^{r-2}\mathbb{Z}) + (i' + 2\mathbb{Z}, j' + 2^{r-2}\mathbb{Z})\big) = \psi(i + i' + 2\mathbb{Z}, j + j' + 2^{r-2}\mathbb{Z})\\ &= \overline{-1}^{i+i'}\overline{5}^{j+j'} = \overline{-1}^{i}\overline{5}^{j}\overline{-1}^{i'}\overline{5}^{j'} = \psi(i + 2\mathbb{Z}, j + 2^{r-2}\mathbb{Z}) \cdot \psi(i' + 2\mathbb{Z}, j' + 2^{r-2}\mathbb{Z}).\end{aligned}$$

#

Die Bijektivität von ψ ergibt sich unmittelbar aus Proposition 3.69. □

3.7 Der Chinesische Restsatz

Aus Abschnitt 3.6 kennen wir bereits die Struktur der primen Restklassengruppen $(\mathbb{Z}/n\mathbb{Z})^\times$ für den Fall, dass n eine Primpotenz ist. Die Idee im Fall eines allgemeinen n ist nun, die Gruppen $(\mathbb{Z}/n\mathbb{Z})^\times$ gemäß der kanonischen Primfaktorzerlegung von n in ein direktes Produkt von primen Restklassengruppen zu Primpotenzen zu zerlegen. Aufgrund der bereits in Satz 2.25 bewiesenen schwachen Multiplikativität der Euler'schen φ-Funktion ist dies plausibel. Wir betrachten die Situation zunächst auf den kompletten Restklassenringen und führen dafür zuerst einige Begriffe der Ringtheorie ein:

Proposition 3.72. *Seien $n \in \mathbb{N}$ und $R_1, \ldots, R_n$ Ringe. Dann ist*

$$R_1 \times \ldots \times R_n := \{(r_1, \ldots, r_n) : r_1 \in R_1, \ldots, r_n \in R_n\}$$

zusammen mit den komponentenweisen Verknüpfungen

$$\begin{aligned}(r_1, \ldots, r_n) + (r'_1, \ldots, r'_n) &:= (r_1 + r'_1, \ldots, r_n + r'_n),\\ (r_1, \ldots, r_n) \cdot (r'_1, \ldots, r'_n) &:= (r_1 r'_1, \ldots, r_n r'_n).\end{aligned}$$

*ein Ring, das sogenannte **direkte Produkt** von $R_1, \ldots, R_n$.*

Beweis. Nach Proposition 3.70 ist $R_1 \times \ldots \times R_n$ eine additive Gruppe mit neutralem Element $(0_{R_1}, \ldots, 0_{R_n})$. Das Assoziativgesetz der Multiplikation und die Distributivgesetze werden von den Komponenten vererbt. Das neutrales Element der Multiplikation ist durch $(1_{R_1}, \ldots, 1_{R_n})$ gegeben. □

Definition 3.73. *Eine Abbildung $\psi\colon R \to S$ zwischen zwei Ringen R, S heißt ein **(Ring-)Homomorphismus**, wenn für alle $a, b \in R$ die folgenden Rechenregeln gelten:*

$$\begin{aligned}\psi(a+b) &= \psi(a) + \psi(b),\\ \psi(ab) &= \psi(a)\psi(b),\\ \psi(1_R) &= 1_S.\end{aligned}$$

*Ein Ringhomomorphismus ψ heißt ein **(Ring-)Isomorphismus**, wenn er bijektiv ist.*

Die folgende Aussage ergibt sich analog zu Proposition 3.46:

Proposition 3.74. *Seien R, S Ringe und $\psi\colon R \to S$ ein Ringhomomorphismus. Dann gilt:*

(a) *Genau dann ist ψ injektiv, wenn* $\operatorname{Kern}\psi := \{a \in R : \psi(a) = 0_S\} = \{0_R\}$ *gilt.*
(b) *Ist ψ ein Ringisomorphismus, so ist auch $\psi^{-1}\colon S \to R$ ein Ringisomorphismus.*

*Existiert ein Isomorphismus zwischen R und S, so nennen wir R und S **isomorph** und schreiben $R \cong S$.*

Wir können nun den Restklassenring $\mathbb{Z}/n\mathbb{Z}$ schwach multiplikativ zerlegen. Genauer gilt:

Satz 3.75 (Chinesischer Restsatz)**.** *Seien $r \in \mathbb{N}$ und $m_1, \ldots, m_r \in \mathbb{N}$ paarweise teilerfremd mit $m := m_1 \cdot \ldots \cdot m_r$. Dann ist die Abbildung*

$$\Psi := \Psi_{m_1,\ldots,m_r}\colon \begin{cases}\mathbb{Z}/m\mathbb{Z} & \to \mathbb{Z}/m_1\mathbb{Z} \times \ldots \times \mathbb{Z}/m_r\mathbb{Z},\\ a + m\mathbb{Z} & \mapsto (a + m_1\mathbb{Z}, \ldots, a + m_r\mathbb{Z})\end{cases}$$

ein Ringisomorphismus mit Umkehrabbildung

$$\Psi^{-1} =: \Phi_{m_1,\ldots,m_r}\colon \begin{cases}\mathbb{Z}/m_1\mathbb{Z} \times \ldots \times \mathbb{Z}/m_r\mathbb{Z} & \to \mathbb{Z}/m\mathbb{Z},\\ (a_1 + m_1\mathbb{Z}, \ldots, a_r + m_r\mathbb{Z}) & \mapsto a_1e_1 + \ldots + a_re_r + m\mathbb{Z}.\end{cases}$$

Hierbei ist

$$e_i := \left(\frac{m}{m_i}\right)^{\varphi(m_i)} \quad \text{für } i = 1, \ldots, r.$$

Beweis. Die Abbildung Ψ ist wohldefiniert,

denn: Seien $a, b \in \mathbb{Z}$ mit $a + m\mathbb{Z} = b + m\mathbb{Z}$. Dann ist $a - b \in m\mathbb{Z} \subseteq m_i\mathbb{Z}$ für alle $i \in \{1, \ldots, r\}$, denn $m_i \mid m$. Wir erhalten $a + m_i\mathbb{Z} = b + m_i\mathbb{Z}$ für alle $i \in \{1, \ldots, r\}$. #

Die Abbildung Ψ ist ein Ringhomomorphismus,

denn: Seien $a, b \in \mathbb{Z}$. Dann ist

$$\begin{aligned}\Psi\big((a + m\mathbb{Z}) + (b + m\mathbb{Z})\big) &= \Psi(a + b + m\mathbb{Z})\\ &= (a + b + m_1\mathbb{Z}, \ldots, a + b + m_r\mathbb{Z})\\ &= (a + m_1\mathbb{Z}, \ldots, a + m_r\mathbb{Z}) + (b + m_1\mathbb{Z}, \ldots, b + m_r\mathbb{Z})\\ &= \Psi(a + m\mathbb{Z}) + \Psi(b + m\mathbb{Z}).\end{aligned}$$

Die Rechnung für die für die Multiplikation verläuft analog. Darüber hinaus ist

$$\Psi(1 + m\mathbb{Z}) = (1 + m_1\mathbb{Z}, \ldots, 1 + m_r\mathbb{Z}).$$

#

Die Abbildung Ψ ist injektiv,

denn: Sei $a \in \mathbb{Z}$ mit $\Psi(a + m\mathbb{Z}) = (a + m_1\mathbb{Z}, \ldots, a + m_r\mathbb{Z}) = (0 + m_1\mathbb{Z}, \ldots, 0 + m_r\mathbb{Z})$. Hieraus folgt $m_1 \mid a, \ldots, m_r \mid a$. Da die m_i paarweise teilerfremd sind, erhalten wir mit Proposition 1.9, dass auch $m_1 \cdot \ldots \cdot m_r \mid a$ gilt. Somit ist $a + m\mathbb{Z} = 0 + m\mathbb{Z}$. #

Schließlich ist die Abbildung Ψ auch surjektiv, denn aufgrund von

$$|\mathbb{Z}/m\mathbb{Z}| = m = m_1 \cdot \ldots \cdot m_r = |\mathbb{Z}/m_1\mathbb{Z} \times \ldots \times \mathbb{Z}/m_r\mathbb{Z}|$$

folgt die Surjektivität von Ψ aus seiner Injektivität. Damit ist die Abbildung Ψ ein Ringisomorphismus und wir müssen nur noch nachrechnen, dass die Umkehrabbildung von Ψ tatsächlich so aussieht, wie oben behauptet wird.

Die wie in der Formulierung des Satzes definierte Abbildung $\Phi := \Phi_{m_1,\ldots,m_r}$ ist wohldefiniert,

denn: Seien $a_1, \ldots, a_r, b_1, \ldots, b_r \in \mathbb{Z}$ mit $a_i + m_i\mathbb{Z} = b_i + m_i\mathbb{Z}$ für $i = 1, \ldots, r$. Das liefert $a_i - b_i \in m_i\mathbb{Z}$, also ist

$$(a_i - b_i)e_i = (\underbrace{a_i - b_i}_{\in m_i\mathbb{Z}}) \underbrace{\left(\frac{m}{m_i}\right)^{\varphi(m_i)}}_{\in \frac{m}{m_i}\mathbb{Z}} \in m\mathbb{Z} \quad \text{für } i = 1, \ldots, r.$$

Es ergibt sich

$$(a_1 - b_1)e_1 + \ldots + (a_r - b_r)e_r \in m\mathbb{Z},$$

und deshalb ist

$$a_1e_1 + \ldots + a_re_r + m\mathbb{Z} = b_1e_1 + \ldots + b_re_r + m\mathbb{Z}.$$

#

Es gilt $\Psi \circ \Phi = id_{\mathbb{Z}/m_1\mathbb{Z}\times\ldots\times\mathbb{Z}/m_r\mathbb{Z}}$,

denn: Für $a_1, \ldots, a_r \in \mathbb{Z}$ ist

$$\Psi\big(\Phi(a_1 + m_1\mathbb{Z}, \ldots, a_r + m_r\mathbb{Z})\big) = \Psi(a_1e_1 + \ldots + a_re_r + m\mathbb{Z}).$$

Wegen $e_i = (\frac{m}{m_i})^{\varphi(m_i)}$ und $m_j \mid \frac{m}{m_i}$ für $j \neq i$ folgt $e_i \in m_j\mathbb{Z}$ für $j \neq i$. Daraus ergibt sich

$$\begin{aligned}\Psi(a_1e_1 + \ldots a_re_r + m\mathbb{Z}) &= (a_1e_1 + \ldots + a_re_r + m_1\mathbb{Z}, \ldots, a_1e_1 + \ldots + a_re_r + m_r\mathbb{Z}) \\ &= (a_1e_1 + m_1\mathbb{Z}, \ldots, a_re_r + m_r\mathbb{Z}).\end{aligned}$$

Es ist $\frac{m}{m_i} = m_1 \cdot \ldots \cdot m_{i-1} m_{i+1} \cdot \ldots \cdot m_r$. Da die m_j nach Voraussetzung paarweise teilerfremd sind, gilt $\mathrm{ggT}(\frac{m}{m_i}, m_i) = 1$. Der Satz von Euler-Fermat 3.30 liefert

$$e_i = \left(\frac{m}{m_i}\right)^{\varphi(m_i)} \equiv 1 \bmod (m_i).$$

Wir erhalten

$$\begin{aligned}\Psi\big(\Phi(a_1 + m_1\mathbb{Z}, \ldots, a_r + m_r\mathbb{Z})\big) &= (a_1 e_1 + m_1\mathbb{Z}, \ldots, a_r e_r + m_r\mathbb{Z}) \\ &= (a_1 + m_1\mathbb{Z}, \ldots, a_r + m_r\mathbb{Z}),\end{aligned}$$

was die Behauptung zeigt. #

Da die Abbildung Ψ bijektiv ist, ist hiermit Φ die Umkehrabbildung von Ψ. □

Eine unmittelbare und nützliche Anwendung des Chinesischen Restsatzes 3.75 ist das Lösen von Systemen simultaner Kongruenzen:

Korollar 3.76. *Seien $r \in \mathbb{N}$ und $m_1, \ldots, m_r \in \mathbb{N}$ paarweise teilerfremd sowie $a_1, \ldots, a_r \in \mathbb{Z}$. Dann besitzt das System von Kongruenzen*

$$\begin{aligned} x &\equiv a_1 \bmod (m_1), \\ x &\equiv a_2 \bmod (m_2), \\ &\vdots \\ x &\equiv a_r \bmod (m_r) \end{aligned}$$

eine Lösung $x \in \mathbb{Z}$. Diese Lösung ist eindeutig bestimmt modulo $m_1 \cdot \ldots \cdot m_r$.

Beweis. Aufgrund der Surjektivität der Abbildung $\Psi = \Psi_{m_1,\ldots,m_r}$ existiert ein $x \in \mathbb{Z}$ mit

$$\Psi(x + m_1 \cdot \ldots \cdot m_r\mathbb{Z}) = (x + m_1\mathbb{Z}, \ldots, x + m_r\mathbb{Z}) = (a_1 + m_1\mathbb{Z}, \ldots, a_r + m_r\mathbb{Z}),$$

und also mit

$$x \equiv a_1 \bmod (m_1), \quad \ldots \quad , x \equiv a_r \bmod (m_r).$$

Ist $y \in \mathbb{Z}$ mit $y \equiv a_1 \bmod (m_1), \ldots, y \equiv a_r \bmod (m_r)$, dann folgt

$$\Psi(x + m_1 \cdot \ldots \cdot m_r\mathbb{Z}) = \Psi(y + m_1 \cdot \ldots \cdot m_r\mathbb{Z})$$

und wegen der Injektivität von Ψ somit

$$x + m_1 \cdot \ldots \cdot m_r\mathbb{Z} = y + m_1 \cdot \ldots \cdot m_r\mathbb{Z},$$

also $y \equiv x \bmod (m_1 \cdot \ldots \cdot m_r)$. □

Beispiel 3.77. *Heute ist Montag. Angenommen, heute ist Neumond. In wie vielen Tagen fällt der Vollmond auf einen Mittwoch?*

Wir gehen davon aus, dass die Mondphasen eine Periode von 29 Tagen haben und nummerieren die Wochentage mit $0, \ldots, 6$, beginnend bei Montag. Zu lösen ist also das folgende System von Kongruenzen:

$$\begin{aligned} x &\equiv 2 \bmod (7), \\ x &\equiv 15 \bmod (29) \end{aligned}$$

Aufgrund des Chinesischen Restsatzes 3.75 haben wir einen Ringisomorphismus

$$\Phi_{7,29}\colon \begin{cases} \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/29\mathbb{Z} & \to \mathbb{Z}/(7\cdot 29)\mathbb{Z} = \mathbb{Z}/203\mathbb{Z}, \\ (a_1 + 7\mathbb{Z}, a_2 + 29\mathbb{Z}) & \mapsto a_1 e_1 + a_2 e_2 + 203\mathbb{Z} \end{cases}$$

mit

$$\begin{aligned} e_1 &= \left(\frac{7\cdot 29}{7}\right)^{\varphi(7)} = 29^6 \equiv 29 \bmod (203), \\ e_2 &= \left(\frac{7\cdot 29}{29}\right)^{\varphi(29)} = 7^{28} \equiv 175 \bmod (203). \end{aligned}$$

Es ist also

$$\Phi_{7,29}(a_1 + 7\mathbb{Z}, a_2 + 29\mathbb{Z}) = 29a_1 + 175a_2 + 203\mathbb{Z}$$

und speziell

$$\Phi_{7,29}(2 + 7\mathbb{Z}, 15 + 29\mathbb{Z}) = 29\cdot 2 + 175\cdot 15 + 203\mathbb{Z} = 44 + 203\mathbb{Z}.$$

Insgesamt erhalten wir als Lösung

$$\{x \in \mathbb{Z} : x \equiv 2 \bmod (7), x \equiv 15 \bmod (29)\} = \{44 + 203k : k \in \mathbb{Z}\}.$$

Die Elemente e_i aus dem Chinesischen Restsatz 3.75 haben bemerkenswerte Eigenschaften:

Proposition 3.78. *Seien $r \in \mathbb{N}$ und $m_1, \ldots, m_r \in \mathbb{N}$ paarweise teilerfremd mit $m := m_1 \cdot \ldots \cdot m_r$. Ferner sei*

$$e_i := \left(\frac{m}{m_i}\right)^{\varphi(m_i)} \quad \text{für } i = 1, \ldots, r.$$

Dann gelten die folgenden Aussagen:

(a) $\Psi_{m_1,\ldots,m_r}(e_i + m\mathbb{Z}) = (0 + m_1\mathbb{Z}, \ldots, 1 + m_i\mathbb{Z}, \ldots, 0 + m_r\mathbb{Z})$.

(b) *In $\mathbb{Z}/m\mathbb{Z}$ gilt*

- $\overline{e_i} \cdot \overline{e_j} = \overline{0}$ *für $i \neq j$.*
- $\overline{e_i} \cdot \overline{e_i} = \overline{e_i}$ *für $i = 1, \ldots, r$.*

- $\overline{e_1} + \ldots + \overline{e_r} = \overline{1}$.

*Man sagt auch: Die $\overline{e_i}$ bilden eine **Zerlegung der Eins in paarweise orthogonale Idempotente**.*

Beweis. Im Beweis des Chinesischen Restsatzes 3.75 haben wir gesehen:

$$e_i \in m_j\mathbb{Z} \quad \text{für alle } j \neq i,$$
$$e_i \equiv 1 \bmod (m_i).$$

Hieraus ergibt sich unmittelbar Behauptung (a).

Wir zeigen nun Behauptung (b). Aus Aussage (a) für $i \neq j$ folgt

$$\Psi_{m_1,\ldots,m_r}(\overline{e_i} \cdot \overline{e_j}) = \Psi_{m_1,\ldots,m_r}(\overline{e_i})\Psi_{m_1,\ldots,m_r}(\overline{e_j}) = (0 + m_1\mathbb{Z}, \ldots, 0 + m_r\mathbb{Z}) = \Psi_{m_1,\ldots,m_r}(\overline{0}),$$

was wegen der Injektivität von $\Psi_{m_1,\ldots,m_r}$ zu $\overline{e_i} \cdot \overline{e_j} = \overline{0}$ führt. Die anderen Aussagen folgen analog unter Verwendung von

$$\Psi_{m_1,\ldots,m_r}(\overline{e_i})\Psi_{m_1,\ldots,m_r}(\overline{e_i}) = (0 + m_1\mathbb{Z}, \ldots, 1 + m_i\mathbb{Z}, \ldots, 0 + m_r\mathbb{Z}) = \Psi_{m_1,\ldots,m_r}(\overline{e_i}),$$
$$\Psi_{m_1,\ldots,m_r}(\overline{e_1}) + \ldots + \Psi_{m_1,\ldots,m_r}(\overline{e_r}) = (1 + m_1\mathbb{Z}, \ldots, 1 + m_r\mathbb{Z}) = \Psi_{m_1,\ldots,m_r}(\overline{1}).$$

□

Proposition 3.79. *Seien $r \in \mathbb{N}$ und $m_1, \ldots, m_r \in \mathbb{N}$ paarweise teilerfremd mit $m := m_1 \cdot \ldots \cdot m_r$. Ferner seien*

$$e_i := \left(\frac{m}{m_i}\right)^{\varphi(m_i)} \quad \text{für } i = 1, \ldots, r.$$

und $u_1, \ldots, u_r \in \mathbb{Z}$ mit

$$u_1\frac{m}{m_1} + \ldots + u_r\frac{m}{m_r} = 1.$$

Dann gilt in $\mathbb{Z}/m\mathbb{Z}$

$$\overline{e_i} = \overline{u_i\frac{m}{m_i}} \quad \text{für alle } i = 1, \ldots, r.$$

Beweis. Da die Zahlen $m_1, \ldots, m_r$ paarweise teilerfremd sind, gilt $\mathrm{ggT}(\frac{m}{m_1}, \ldots, \frac{m}{m_r}) = 1$, so dass tatsächlich ganze Zahlen $u_1, \ldots, u_r$ wie in der Formulierung der Proposition existieren. Offenbar gilt dann $u_i\frac{m}{m_i} \equiv 0 \bmod (m_j)$ für alle $j \neq i$ und es ist

$$u_i\frac{m}{m_i} = 1 - u_1\frac{m}{m_1} - \ldots - u_{i-1}\frac{m}{m_{i-1}} - u_{i+1}\frac{m}{m_{i+1}} - \ldots - u_r\frac{m}{m_r} \equiv 1 \bmod (m_i).$$

Es folgt

$$\Psi_{m_1,\ldots,m_r}(\overline{u_i\frac{m}{m_i}}) = \Psi_{m_1,\ldots,m_r}(\overline{e_i}).$$

Aufgrund der Injektivität von $\Psi_{m_1,\ldots,m_r}$ folgt schließlich $\overline{e_i} = \overline{u_i\frac{m}{m_i}}$. □

Beispiel 3.80. *Wir berechnen nun in der Situation von Beispiel 3.77 die Größen $\overline{e_1}, \overline{e_2}$ für $m_1 = 7$ und $m_2 = 29$ vermöge Proposition 3.79: Aufgrund von*

$$\mathrm{ggT}(7, 29) = 1 = (-4) \cdot 7 + 1 \cdot 29$$

gilt

$$\begin{aligned} \overline{e_1} &= \overline{1 \cdot 29} = \overline{29}, \\ \overline{e_2} &= \overline{(-4) \cdot 7} = \overline{-28} = \overline{175}. \end{aligned}$$

Wir nutzen den Chinesischen Restsatz 3.75 nun, um einen Strukturatz für die primen Restklassengruppen zu erhalten. Dazu brauchen wir noch eine kleine algebraische Vorüberlegung:

Proposition 3.81. *Seien R, S Ringe und $\psi \colon R \to S$ ein Ringisomorphismus. Dann induziert ψ einen Gruppenisomorphismus*

$$\psi^\times := \psi|_{R^\times} \colon R^\times \to S^\times.$$

Beweis. Die Abbildung $\psi^\times$ ist wohldefiniert, denn zu jedem $a \in R^\times$ existiert ein $b \in R^\times$ mit $ab = 1$. Das liefert

$$\psi^\times(a)\psi^\times(b) = \psi^\times(ab) = \psi^\times(1) = 1$$

udn also $\psi^\times(a) \in S^\times$. Da ψ ein Ringhomomorphismus ist, ist die Abbildung $\psi^\times$ ein Gruppenhomomorphismus. Die Injektivität von ψ vererbt sich auf $\psi^\times$. Zum Nachweis der Surjektivität sei $\tilde{a} \in S^\times$. Dann gibt es ein $\tilde{b} \in S^\times$ mit $\tilde{a}\tilde{b} = 1$. Aufgrund der Surjektivität von ψ existieren $a, b \in R$ mit $\psi(a) = \tilde{a}$ und $\psi(b) = \tilde{b}$. Damit erhalten wir

$$\psi(ab) = \psi(a)\psi(b) = \tilde{a}\tilde{b} = 1 = \psi(1),$$

was $ab = 1$ und damit $a \in R^\times$ zur Folge hat. □

Die nächste Aussage ergibt sich direkt aus der komponentenweisen Erklärung der Multiplikation in direkten Produkten von Ringen:

Proposition 3.82. *Seien $R_1, \ldots, R_n$ Ringe. Dann gilt:*

$$(R_1 \times \ldots \times R_n)^\times = R_1^\times \times \ldots \times R_n^\times.$$

Aus diesen Vorüberlegungen und dem Chinesischen Restsatz ergibt sich unmittelbar:

Korollar 3.83. *Seien $r \in \mathbb{N}$ und $m_1, \ldots, m_r \in \mathbb{N}$ paarweise teilerfremd mit $m := m_1 \cdot \ldots \cdot m_r$. Dann ist die Abbildung*

$$\Psi^\times_{m_1,\ldots,m_r} \colon \begin{cases} (\mathbb{Z}/m\mathbb{Z})^\times & \to (\mathbb{Z}/m_1\mathbb{Z})^\times \times \ldots \times (\mathbb{Z}/m_r\mathbb{Z})^\times, \\ a + m\mathbb{Z} & \mapsto (a + m_1\mathbb{Z}, \ldots, a + m_r\mathbb{Z}) \end{cases}$$

ein Gruppenisomorphismus.

Bemerkung 3.84. *Korollar 3.83 liefert einen neuen Beweis für die bereits in Satz 2.25 gezeigte schwache Multiplikativität der Euler'schen φ-Funktion,*

denn: Seien $r \in \mathbb{N}$ und $m_1, \ldots, m_r \in \mathbb{N}$ paarweise teilerfremd mit $m := m_1 \cdot \ldots \cdot m_r$. Dann gilt

$$\begin{aligned}\varphi(m_1 \cdot \ldots \cdot m_r) &= \left|(\mathbb{Z}/m_1 \cdot \ldots \cdot m_r\mathbb{Z})^\times\right| \\ &\overset{3.83}{=} \left|(\mathbb{Z}/m_1\mathbb{Z})^\times \times \ldots \times (\mathbb{Z}/m_r\mathbb{Z})^\times\right| \\ &= \left|(\mathbb{Z}/m_1\mathbb{Z})^\times\right| \cdot \ldots \cdot \left|(\mathbb{Z}/m_r\mathbb{Z})^\times\right| \\ &= \varphi(m_1) \cdot \ldots \cdot \varphi(m_r).\end{aligned}$$

#

Wir wollen uns nun der Frage zuwenden, für welche Werte von n die primen Restklassengruppen $(\mathbb{Z}/n\mathbb{Z})^\times$ zyklisch sind:

Proposition 3.85. *Seien $r \in \mathbb{N}$ und $G_1, \ldots, G_r$ endliche zyklische Gruppen mit $G := G_1 \times \ldots \times G_r$. Dann gilt:*

$$\exp(G) = \mathrm{kgV}\big(|G_1|, \ldots, |G_r|\big).$$

Insbesondere ist die Gruppe G genau dann zyklisch, wenn die Ordnungen $|G_1|, \ldots, |G_r|$ paarweise teilerfremd sind.

Beweis. Wir rechnen nach, dass $\exp(G)$ die definierenden Eigenschaften des kleinsten gemeinsamen Vielfachen $\mathrm{kgV}(|G_1|, \ldots, |G_r|)$ erfüllt: Offenbar gilt $|G_i| \mid \exp(G)$ für alle $i = 1, \ldots, r$,

denn: Es gilt

$$\exp(G) = \mathrm{kgV}\big(\mathrm{ord}(g) : g \in G\big)$$

und für das Element $\tilde{g}_i := (1, \ldots, 1, g_i, 1, \ldots, 1) \in G$ mit einem Erzeuger g_i von G_i ist $\mathrm{ord}(\tilde{g}_i) = |G_i|$. #

Sei nun $m \in \mathbb{Z}$ mit $|G_1| \mid m, \ldots, |G_r| \mid m$. Dann folgt $\exp(G) \mid m$,

denn: Für alle $i \in \{1, \ldots, r\}$ existiert ein $q_i \in \mathbb{Z}$ mit $m = q_i|G_i|$. Für $x = (x_1, \ldots, x_r) \in G$ ist dann

$$x^m = (x_1^m, \ldots, x_r^m) = (x_1^{q_1|G_1|}, \ldots, x_r^{q_r|G_r|}) = (1, \ldots, 1).$$

Wir schreiben m in der Form $m = q\exp(G) + s$ mit $0 \leq s < \exp(G)$ und erhalten

$$1 = x^m = x^{q\exp(G)}x^s = x^s \quad \text{für alle } x \in G.$$

Aufgrund der Minimalität von $\exp(G)$ ergibt sich $s = 0$. Das impliziert $\exp(G) \mid m$. #

Die Gruppe G ist nach Satz 3.49 genau dann zyklisch, wenn $\exp(G) = |G| = |G_1| \cdot \ldots \cdot |G_r|$ gilt. Das ist nach dem eben Gezeigten genau dann der Fall, wenn $\mathrm{kgV}(|G_1|, \ldots, |G_r|) = |G_1| \cdot \ldots \cdot |G_r|$ ist. Dies ist wiederum äquivalent dazu, dass die Ordnungen $|G_1|, \ldots, |G_r|$ paarweise teilerfremd sind (vgl. Übungen). □

Satz 3.86. *Für ein beliebiges $n \in \mathbb{N}$ mit $n > 1$ sind die folgenden Aussagen äquivalent:*

(i) *Die Gruppe* $(\mathbb{Z}/n\mathbb{Z})^\times$ *ist zyklisch.*

(ii) *Einer der folgenden Fälle liegt vor:*

$$n = \begin{cases} 2, & \\ 4, & \\ p^e & \text{für eine ungerade Primzahl } p \text{ und } e \in \mathbb{N}, \\ 2p^e & \text{für eine ungerade Primzahl } p \text{ und } e \in \mathbb{N}. \end{cases}$$

Beweis. Gelte zunächst Aussage (i) und sei also $(\mathbb{Z}/n\mathbb{Z})^\times$ zyklisch. Wir schreiben n in der Form $n = 2^a p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$ mit paarweise verschiedenen ungeraden Primzahlen $p_1, \ldots, p_r$ und $e_1, \ldots, e_r \in \mathbb{N}$ sowie $a, r \in \mathbb{N}_0$. Nach dem Chinesischen Restsatz 3.83 gilt

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/2^a\mathbb{Z})^\times \times (\mathbb{Z}/p_1^{e_1}\mathbb{Z})^\times \times \ldots \times (\mathbb{Z}/p_r^{e_r}\mathbb{Z})^\times,$$

wobei die Gruppen $(\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times$ hierbei nach Satz 3.65 zyklisch der Ordnung

$$|(\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times| = \varphi(p_i^{e_i}) = (p_i - 1)p_i^{e_i - 1}$$

sind. Wäre $a > 2$, so folgte nach Satz 3.71 bereits

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{a-2}\mathbb{Z} \times (\mathbb{Z}/p_1^{e_1}\mathbb{Z})^\times \times \ldots \times (\mathbb{Z}/p_r^{e_r}\mathbb{Z})^\times.$$

Da die Gruppen $\mathbb{Z}/2\mathbb{Z}$ und $\mathbb{Z}/2^{a-2}\mathbb{Z}$ beide gerade Ordnung haben, stünde dies nach Proposition 3.85 im Widerspruch zur Zyklizität von $(\mathbb{Z}/n\mathbb{Z})^\times$. Somit ist $a \leq 2$ und insbesondere die Gruppe $(\mathbb{Z}/2^a\mathbb{Z})^\times$ zyklisch. Da die Primzahlen p_i alle ungerade sind, sind die Ordnungen der Gruppen $(\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times$ für alle $i = 1, \ldots, r$ gerade. Wiederum mittels Proposition 3.85 folgt $r \in \{0, 1\}$. Ist $r = 0$, so erhalten wir die Fälle $n = 2$ und $n = 4$. Ist $r = 1$, so ergeben sich die Fälle $n = p_1^{e_1}$, $n = 2p_1^{e_1}$ und $n = 4p_1^{e_1}$. Der Fall $n = 4p_1^{e_1}$ scheidet wegen Proposition 3.85 aus, da die Gruppen $(\mathbb{Z}/4\mathbb{Z})^\times$ und $(\mathbb{Z}/p_1^{e_1}\mathbb{Z})^\times$ beide gerade Ordnung haben. Somit verbleiben genau die in Aussage (ii) angegebenen Fälle.

Gelte nun umgekehrt Aussage (ii). Die Gruppen $(\mathbb{Z}/2\mathbb{Z})^\times$ sowie $(\mathbb{Z}/4\mathbb{Z})^\times$ sind offenbar zyklisch. Gruppen der Form $(\mathbb{Z}/p^e\mathbb{Z})^\times$ sind zyklisch nach Satz 3.65. Darüber hinaus ist

$$(\mathbb{Z}/2p^e\mathbb{Z})^\times \cong (\mathbb{Z}/2\mathbb{Z})^\times \times (\mathbb{Z}/p^e\mathbb{Z})^\times = \{\overline{1}\} \times (\mathbb{Z}/p^e\mathbb{Z})^\times \cong (\mathbb{Z}/p^e\mathbb{Z})^\times$$

und somit ebenfalls zyklisch. □

Beispiel 3.87. (a) *Die Gruppe* $(\mathbb{Z}/35\mathbb{Z})^\times$ *ist wegen* $35 = 5 \cdot 7$ *und Satz 3.86 nicht zyklisch. In der Tat ist*

$$(\mathbb{Z}/35\mathbb{Z})^\times \cong (\mathbb{Z}/5\mathbb{Z})^\times \times (\mathbb{Z}/7\mathbb{Z})^\times \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$$

und somit $\exp((\mathbb{Z}/35\mathbb{Z})^\times) = \mathrm{kgV}(4, 6) = 12 < \varphi(35) = 4 \cdot 6 = 24$.

(b) *Die Gruppe* $(\mathbb{Z}/18\mathbb{Z})^\times$ *ist wegen* $18 = 2 \cdot 3^2$ *nach Satz 3.86 zyklisch. In der Tat ist*

$$(\mathbb{Z}/18\mathbb{Z})^\times \cong (\mathbb{Z}/2\mathbb{Z})^\times \times (\mathbb{Z}/3^2\mathbb{Z})^\times \cong \{\overline{1}\} \times \mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z}.$$

Definition 3.88. *Sei $n \in \mathbb{N}$ mit $n > 1$ von der Form wie in Satz 3.86 (ii). Ist dann $w \in \mathbb{Z}$ ein Erzeuger von $(\mathbb{Z}/n\mathbb{Z})^\times$, so heißt w eine **primitive Wurzel modulo** n.*

Beispiel 3.89. *Nach Satz 3.86 ist die Gruppe $(\mathbb{Z}/10\mathbb{Z})^\times$ zyklisch. Offenbar ist 3 eine primitive Wurzel modulo 10, denn es gilt*

$$\langle\overline{3}\rangle = \{\overline{1},\overline{3},\overline{9},\overline{7}\} = (\mathbb{Z}/10\mathbb{Z})^\times.$$

3.8 Das RSA-Verfahren

In diesem Abschnitt lernen wir eine Anwendung des bisher behandelten Stoffes kennen, das sogenannte RSA-Verschlüsselungsverfahren. Wir beschränken uns dabei auf die wesentlichen mathematischen Grundlagen; für alles Weitere sei auf die entsprechende Literatur zur Kryptographie verwiesen.

Problemstellung: Man möchte eine Nachricht verschlüsselt übertragen, ohne dass der Absender A und der Empfänger E vorher gemeinsam auf sichere Weise einen Schlüssel austauschen.

Idee: Der Empfänger E erzeugt einen öffentlichen Schlüssel (zur Verschlüsselung) und einen privaten Schlüssel (zur Entschlüsselung). Der öffentliche Schlüssel wird öffentlich bekanntgegeben, den privaten Schlüssel behält E für sich. Der Absender A verwendet den öffentlichen Schlüssel, um die Nachricht zu verschlüsseln und sendet die Nachricht an E. Der Empfänger E benutzt den privaten Schlüssel, um die Nachricht zu entschlüsseln.

Problem: Das Erzeugen des öffentlichen und privaten Schlüssels muss schnell gehen, ebenso das Verschlüsseln mit dem öffentlichen Schlüssel und das Entschlüsseln, wenn der private Schlüssel bekannt ist. Das Bestimmen des privaten Schlüssels aus dem öffentlichen Schlüssel darf in angemessener Zeit nicht machbar sein.

Das ***RSA-Verfahren*** (nach Rivest, Shamir und Adleman, 1977) basiert auf dem aktuellen Wissensstand, dass das Faktorisieren einer Zahl in ihre Primfaktoren sehr aufwändig ist, wo hingegen das Erzeugen einer Zahl durch Multiplikation von Primzahlen sehr einfach ist.

Algorithmus 3.90 (Schlüsselerzeugung beim RSA-Verfahren)**.** *Person E möchte ein Paar von Schlüsseln erzeugen, um künftig als Empfänger von verschlüsselten Nachrichten infrage zu kommen.*

(1) E bestimmt zufällig zwei große (mehrere Hundert Stellen), voneinander verschiedene Primzahlen p, q, indem er/sie etwa so lange zufällig natürliche Zahlen auswählt und auf Primalität testet, bis zwei Primzahlen gefunden sind. Einen effizienten Primzahltest werden wir in Abschnitt 5.4 kennenlernen.

(2) E berechnet den RSA-Modul $n = pq$.

(3) E berechnet $\varphi(n) = (p-1)(q-1)$.

(4) E wählt zufällig eine Zahl $e \in \mathbb{N}$ mit $1 < e < \varphi(n)$ und $\mathrm{ggT}(e, \varphi(n)) = 1$.

(5) E bestimmt die eindeutig bestimmte Lösung $d \in \mathbb{N}$ mit $1 < d < \varphi(n)$ der Kongruenz $ed \equiv 1 \bmod (\varphi(n))$. Das kann etwa mit dem erweiterten Euklidischen Algorithmus geschehen.

(6) E setzt

$$\begin{aligned} &\textit{öffentlicher Schlüssel} := (n, e),\\ &\textit{privater Schlüssel} := (n, d). \end{aligned}$$

Den öffentlichen Schlüssel gibt E bekannt, den privaten Schlüssel behält er/sie für sich.

Beispiel 3.91. *Zur Veranschaulichung der Schlüsselerzeugung betrachten wir ein Beispiel mit – natürlich für die Praxis viel zu kleinen – Primzahlen $p = 17$ und $q = 19$. Es gelten*

$$n = 17 \cdot 19 = 323 \quad \textit{und} \quad \varphi(n) = (17-1) \cdot (19-1) = 16 \cdot 18 = 288.$$

Wir wählen $e = 95$. Es ist $\mathrm{ggT}(95, 288) = 1 = 32 \cdot 288 - 97 \cdot 95$. *Insbesondere gilt* $(-97) \cdot 95 \equiv 1 \bmod (288)$ *und also* $191 \cdot 95 \equiv 1 \bmod (288)$. *Somit ist $d = 191$ und es gilt:*

$$\begin{aligned} &\textit{öffentlicher Schlüssel} \;= (323, 95),\\ &\textit{privater Schlüssel} \;= (323, 191). \end{aligned}$$

Ist der öffentliche Schlüssel durch (n, e) gegeben, so geht das weitere Verfahren davon aus, dass die zu übermittelnde Nachricht als eine Folge von Elementen aus $\mathbb{Z}/n\mathbb{Z}$ vorliegt. Wie man eine übliche Nachricht – etwa einen Text – in eine Folge von Elementen von $\mathbb{Z}/n\mathbb{Z}$ und zurück umwandelt, werden wir an dieser Stelle nicht thematisieren (vgl. Übungen). Es sollte jedoch klar sein, dass man auch hier geschickt vorgehen muss, sonst ist das ganze Verfahren angreifbar.

Algorithmus 3.92 (Verschlüsselung mit dem RSA-Verfahren)**.** *Person A möchte eine Nachricht verschlüsselt an E senden.*

(1) A besorgt sich den öffentlichen Schlüssel (n, e) von E.

(2) A schreibt seine/ihre Nachricht als Folge von Elementen $\overline{x_1}, \ldots, \overline{x_r} \in \mathbb{Z}/n\mathbb{Z}$.

(3) Mithilfe der Verschlüsselungsfunktion

$$V\colon \begin{cases} \mathbb{Z}/n\mathbb{Z} & \to \mathbb{Z}/n\mathbb{Z},\\ \overline{x} & \mapsto \overline{x}^e \end{cases}$$

verschlüsselt A die Nachricht zu $V(\overline{x_1}), \ldots, V(\overline{x_r})$.

(4) A übermittelt $V(\overline{x_1}), \ldots, V(\overline{x_r})$.

Algorithmus 3.93 (Entschlüsselung mit dem RSA-Verfahren)**.** *Der Empfänger E möchte eine empfangene Nachricht entschlüsseln.*

(1) E empfängt eine Folge von Elementen $\overline{y_1}, \ldots, \overline{y_r}$ aus $\mathbb{Z}/n\mathbb{Z}$ als verschlüsselte Nachricht.

(2) Mithilfe des privaten Schlüssels (n, d) und der Entschlüsselungsfunktion

$$E\colon \begin{cases} \mathbb{Z}/n\mathbb{Z} & \to \mathbb{Z}/n\mathbb{Z},\\ \overline{y} & \mapsto \overline{y}^d \end{cases}$$

entschlüsselt E die Nachricht als $E(\overline{y_1}), \ldots, E(\overline{y_r})$.

Wir müssen uns an dieser Stelle überlegen, dass die Entschlüsselung tatsächlich funktioniert, dass also für alle $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$ tatsächlich $E(V(\overline{x})) = \overline{x}$ gilt. Dies folgt jedoch recht schnell aus der folgenden Überlegung:

Proposition 3.94. *Seien $n \in \mathbb{N}$ quadratfrei, $k \in \mathbb{N}$ und $a \in \mathbb{Z}$. Dann gilt:*

$$a^{k\varphi(n)+1} \equiv a \bmod (n).$$

Beweis. Sei $n = p_1 \cdot \ldots \cdot p_r$ mit paarweise verschiedenen Primzahlen $p_1, \ldots, p_r$. Dann gilt bekanntlich

$$\varphi(n) = (p_1 - 1) \cdot \ldots \cdot (p_r - 1).$$

Sei $i \in \{1, \ldots, r\}$ beliebig. Im Fall $p_i \nmid a$ gilt dann $a^{p_i - 1} \equiv 1 \bmod (p_i)$. Es folgt $a^{k\varphi(n)} \equiv 1 \bmod (p_i)$ und also auch $a^{k\varphi(n)+1} \equiv a \bmod (p_i)$. Im Fall $p_i \mid a$ gilt offenbar $a^{k\varphi(n)+1} \equiv 0 \equiv a \bmod (p_i)$. Somit ergibt sich $a^{k\varphi(n)+1} \equiv a \bmod (p_1 \cdot \ldots \cdot p_r)$ und damit die Behauptung. □

Es ist nun

$$E(V(\overline{x})) = E(\overline{x}^e) = \overline{x}^{ed}.$$

Nach Konstruktion von e, d ist $ed \equiv 1 \bmod (\varphi(n))$. Wegen $ed > 1$ existiert also ein $k \in \mathbb{N}$ mit $ed = k\varphi(n) + 1$. Mit Proposition 3.94 ergibt sich

$$E(V(\overline{x})) = \overline{x}^{k\varphi(n)+1} = \overline{x}.$$

Damit ist gezeigt, dass das RSA-Verfahren korrekt arbeitet.

Wieso sieht man das RSA-Verfahren als sicher an? Ein „naives“ Argument hierfür ist:

> Um zu entschlüsseln, muss man den privaten Schlüssel (n, d) aus dem öffentlichen Schlüssel (n, e) bestimmen. Dazu muss man die Kongruenz $ed \equiv 1 \bmod (\varphi(n))$ lösen. Dafür benötigt man $\varphi(n) = (p-1) \cdot (q-1)$ und dafür wiederum p und q, also die Primfaktoren von n. Für große Zahlen n ist die Faktorisierung jedoch mit den heute gängigen Verfahren praktisch nicht durchführbar.

Leider ist diese Überlegung nicht wirklich tragfähig, denn es könnte ja möglich sein, den privaten Schlüssel auf andere Weise aus dem öffentlichen Schlüssel zu bestimmen oder auch ohne Kenntnis des privaten Schlüssels eine Entschlüsselung durchzuführen. Wir schauen daher doch noch einmal etwas genauer hin – wobei für eine wirklich ernsthafte Betrachtung auf die entsprechende Literatur zur Kryptographie verwiesen sei – und betrachten im Weiteren die folgenden Probleme:

- *RSA*: Gegeben ist der öffentliche Schlüssel (n, e) sowie eine verschlüsselte Nachricht $\overline{y} \in \mathbb{Z}/n\mathbb{Z}$. Gesucht wird die Ausgangsnachricht, also ein $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$ mit $V(\overline{x}) = \overline{x}^e = \overline{y}$.
- *RSA-Schlüssel*: Gegeben ist der öffentliche Schlüssel (n, e). Gesucht wird der private Schüssel (n, d), also dasjenige $d \in \mathbb{N}$ mit $1 < d < \varphi(n)$ und $ed \equiv 1 \bmod (\varphi(n))$.

- *Faktorisierung*: Gegeben ist eine Zahl $n \in \mathbb{N}$, welche genau zwei Primfaktoren p, q hat. Gesucht sind p und q.

Wir vergleichen, wie schwierig diese Probleme sind. Hierbei schreiben wir „Problem $A \leq_p$ Problem B“, falls nach Lösung von Problem B Problem A durch einen Algorithmus mit polynomialer Laufzeit gelöst werden kann. Anschaulich heißt das in diesem Kontext, dass Problem A leichter als oder gleich schwer wie Problem B ist. Für die oben aufgeführten Probleme gilt nun

$$\textit{RSA} \leq_p \textit{RSA-Schlüssel} \leq_p \textit{Faktorisierung},$$

denn: Ist die *Faktorisierung* von n in Primzahlen p, q mit $n = pq$ bekannt, so kann man $\varphi(n) = (p-1) \cdot (q-1)$ berechnen. Über den erweiterten Euklidischen Algorithmus bestimmt man dann (n, d) aus (n, e) und kann also *RSA-Schlüssel* lösen. Dies liefert $\overline{x} = E(\overline{y}) = \overline{y}^d$ und somit die Lösung von *RSA*. #

Man kann zeigen, dass umgekehrt auch

$$\textit{Faktorisierung} \leq_p \textit{RSA-Schlüssel}$$

gilt. Momentan ist kein effizienter Algorithmus bekannt, der das Faktorisierungsproblem löst. Dasselbe gilt somit auch für *RSA-Schlüssel*. Es ist allerdings unbekannt, ob auch *RSA-Schlüssel* $\leq_p$ *RSA* ist. Es könnte also effiziente Möglichkeiten geben, Nachrichten zu entschlüsseln, ohne den privaten Schlüssel zu finden. Da das Verfahren in der realen Welt auf real existierenden Computern durchgeführt wird, gibt es auch darüber hinaus eine nicht unbeträchtliche Zahl von Angriffsmöglichkeiten auf das RSA-Verfahren.

KAPITEL 4

Diophantische Gleichungen

4.1 Pythagoräische Tripel und der Große Satz von Fermat

Definition 4.1. *Eine **diophantische Gleichung** ist eine Gleichung der Form*

$$F(X_1, \ldots, X_n) = 0 \quad \text{mit } F \in \mathbb{Z}[X_1, \ldots, X_n] \text{ für ein } n \in \mathbb{N}. \tag{4.1}$$

*Eine **Lösung** der diophantischen Gleichung (4.1) ist ein Tupel*

$$P = (a_1, \ldots, a_n) \in \mathbb{Z}^n \qquad \text{mit } F(P) = 0.$$

*Eine **rationale** bzw. **reelle** bzw. **komplexe Lösung** von (4.1) ist ein Tupel*

$$P = (a_1, \ldots, a_n) \in \mathbb{Q}^n \text{ bzw. } \mathbb{R}^n \text{ bzw. } \mathbb{C}^n \qquad \text{mit } F(P) = 0.$$

*Eine Lösung $P = (a_1, \ldots, a_n)$ einer diophantischen Gleichung heißt eine **primitive Lösung**, wenn $\mathrm{ggT}(a_1, \ldots, a_n) = 1$ gilt.*

*Analog definiert man **Systeme diophantischer Gleichungen** und ihre Lösungen.*

Diophantos lebte vermutlich um das Jahr 250 herum in Alexandria. Sein 13-bändiges Hauptwerk, die *Arithmetika*, galt lange Jahre als verschollen. Im 15. Jahrhundert wurden die Bücher 1 – 3 und 8 – 10 wiederentdeckt, 1968 zudem die Bücher 4 – 7 in arabischer Übersetzung. Diophantos gilt als Begründer der Theorie der nach ihm benannten diophantischen Gleichungen.

Ein klassisches Beispiel einer diophantischen Gleichung ist

$$X_1^2 + X_2^2 - X_3^2 = 0. \tag{4.2}$$

Nach dem Satz des Pythagoras beschreiben ihre Lösungen gerade alle Möglichkeiten, ein rechtwinkliges Dreieck mit ganzzahligen Seitenlängen zu konstruieren. Bekannte Lösungen sind etwa $(3, 4, 5)$ und $(5, 12, 13)$.

Weil die Lösungen (a_1, a_2, a_3) von (4.2) mit $a_1a_2a_3 = 0$ ungeometrisch und leicht zu beschreiben sind, betrachten wir nur Lösungen mit $a_1a_2a_3 \neq 0$. Da weiter mit (a_1, a_2, a_3) auch jedes der acht Tripel $(\pm a_1, \pm a_2, \pm a_3)$ eine Lösung ist, genügt es zur Beschreibung der Lösungsmenge, die Lösungen in $\mathbb{N}^3$ anzugeben, die sogenannten ***pythagoräische Tripel***. Mit jedem pythagoräischen Tripel (a_1, a_2, a_3) und jedem $c \in \mathbb{Z}$ ist auch $\frac{c}{\mathrm{ggT}(a_1,a_2,a_3)} \cdot (a_1, a_2, a_3)$ pythagoräisch und es genügt sogar, diejenigen Tripel zu beschreiben, die primitive Lösungen im Sinne von Definition 4.1 sind, die ***primitiven pythagoräischen Tripel***.

Die Einträge eines primitiven pythagoräischen Tripels sind paarweise teilerfremd,

denn: Hätten zwei der drei Einträge eines gegebenen primitiven pythagoräischen Tripels (a_1, a_2, a_3) einen gemeinsamen Primteiler p, so wäre wegen (4.2) auch der dritte Eintrag durch p teilbar, was ein Widerspruch zur Primitivität des Tripels wäre. #

Folglich ist in einem primitiven pythagoräischen Tripel (a_1, a_2, a_3) genau eine der Zahlen a_1, a_2 gerade,

denn: Wegen der paarweisen Teilerfremdheit sind nicht beide gerade. Wären beide ungerade, so gälte $a_1^2 \equiv a_2^2 \equiv 1 \bmod (4)$ und nach (4.2) also $a_3^2 \equiv 2 \bmod (4)$, was nicht sein kann. #

Der folgende Satz war bereits Euklid bekannt:

Satz 4.2. *Die Menge der primitiven pythagoräischen Tripel (a_1, a_2, a_3) mit geradem a_2 stimmt überein mit der Menge der Tripel*

$$\{(a^2 - b^2, 2ab, a^2 + b^2) : a, b \in \mathbb{N}, \mathrm{ggT}(a, b) = 1, a - b \text{ positiv und ungerade}\}.$$

Beweis. Die im Satz angegebenen Tripel sind tatsächlich pythagoräisch und primitiv,

denn: Offensichtlich erfüllt jedes dieser Tripel (a_1, a_2, a_3) die Bedingungen

$$\begin{aligned} a_1^2 + a_2^2 - a_3^2 &= (a^2 - b^2)^2 + 4a^2b^2 - (a^2 + b^2)^2 = 0, \\ a_1 &= a^2 - b^2 = (a + b)(a - b) > 0, \\ a_2 &= 2ab > 0, \\ a_3 &= a^2 + b^2 > 0. \end{aligned}$$

und ist also ein pythagoräisches Tripel.

Zum Beweis der Primitivität nehmen wir nun an, a_1 und a_3 hätten einen gemeinsamen Primteiler p. Nach Voraussetzung wäre dieser ungerade und erfüllte

$$\begin{aligned} p \mid (a_1 + a_3) &= (a^2 - b^2) + (a^2 + b^2) = 2a^2, \\ p \mid (a_1 - a_3) &= (a^2 + b^2) - (a^2 - b^2) = 2b^2. \end{aligned}$$

Im Widerspruch zur vorausgesetzten Teilerfremdheit von a und b folgte $p \mid a$ und $p \mid b$. #

Sei nun umgekehrt (a_1, a_2, a_3) ein primitives pythagoräisches Tripel mit geradem a_2. Wegen (4.2) und $a_3 > 0$ sind $a_3 - a_1$ und $a_3 + a_1$ natürliche Zahlen und wegen $2 \nmid a_1$ sowie $2 \nmid a_3$ auch

beide gerade. Wir erhalten natürliche Zahlen

$$a_1' := \frac{a_3 - a_1}{2}, \quad a_2' := \frac{a_2}{2}, \quad a_3' := \frac{a_3 + a_1}{2}$$

und nach Einsetzen in (4.2) den Zusammenhang

$$(a_2')^2 = \frac{a_2^2}{4} = \frac{a_3^2 - a_1^2}{4} = \frac{a_3 - a_1}{2} \cdot \frac{a_3 + a_1}{2} = a_1' \cdot a_3'. \tag{4.3}$$

Es gilt $\mathrm{ggT}(a_1', a_3') = 1$,

denn: Wäre p ein gemeinsamer Primfaktor der natürlichen Zahlen a_1' und a_3', so gälten

$$p \mid (a_3' - a_1') = a_1 \quad \text{und} \quad p \mid (a_3' + a_1') = a_3,$$

was wegen der vorausgesetzten Teilerfremdheit von a_1 und a_3 nicht sein kann. #

Führen wir auf beiden Seiten von (4.3) die kanonische Primfaktorzerlegung 1.22 durch, so folgt mit der Teilerfremdheit von a_1' und a_3' sofort die Existenz von teilerfremden natürlichen Zahlen $a, b \in \mathbb{N}$ mit $a_3' = a^2$ und $a_1' = b^2$. Wir erhalten

$$a_1 = a_3' - a_1' = a^2 - b^2 \quad \text{und} \quad a_3 = a_3' + a_1' = a^2 + b^2$$

sowie

$$a_2^2 = 4(a_2')^2 \overset{(4.3)}{=} 4a_1'a_3' = (2ab)^2 \quad \text{und also} \quad a_2 = 2ab.$$

Weiter gelten

$$\begin{aligned} &a_1 > 0 \quad \Longrightarrow \quad a_3' > a_1' \quad \Longrightarrow \quad a > b, \\ &2 \nmid a_1 = a^2 - b^2 = (a+b)(a-b) \quad \Longrightarrow \quad 2 \nmid (a-b). \end{aligned}$$

Das gegebene Tripel (a_1, a_2, a_3) ist also tatsächlich von der behaupteten Gestalt. □

An diesem recht übersichtlichen Beispiel können wir bereits erkennen, dass das Bestimmen aller Lösungen einer diophantischen Gleichung im Allgemeinen nicht leicht ist. Tatsächlich war eine harmlos aussehende Verallgemeinerung der gerade gelösten Frage über 350 Jahre lang ungelöst und eines der berühmtesten mathematischen Probleme schlechthin:

Satz 4.3 (Großer Satz von Fermat). *Für kein $2 < n \in \mathbb{N}$ hat die diophantische Gleichung*

$$X_1^n + X_2^n - X_3^n = 0$$

Lösungen (a_1, a_2, a_3), deren Einträge a_1, a_2, a_3 sämtlich natürliche Zahlen sind.

Formuliert wurde dieser Satz zuerst um 1640 von Pierre de Fermat, als dieser ihn als Randnotiz in seine Ausgabe des zweiten Buches der *Arithmetika* schrieb, versehen mit dem Hinweis, er habe eine gar wundervolle Lösung für dieses Problem, der Platz auf dem Rand reiche aber

nicht aus, sie zu fassen. Das Problem wurde schnell als ***Fermat'sche Vermutung*** bekannt. Man glaubt heute, dass Fermat auf eine Lösung im Fall $n = 4$ und vielleicht auch im Fall $n = 3$ gekommen war und fälschlich annahm, diese analog auf ein allgemeines n ausdehnen zu können. Tatsächlich lässt sich der Fall $n = 4$ mit dem elementaren ***Prinzip des unendlichen Abstiegs*** beweisen, das Fermat an anderer Stelle bereits eingesetzt hatte, vergleiche hierzu auch Proposition 4.9.

In den folgenden Jahrhunderten konnte der Große Satz von Fermat 4.3 nach und nach für immer mehr Fälle nachgewiesen werden. Zahlreiche Mathematiker versuchten sich an einem Beweis und entwickelten im Zuge dessen fruchtbare neue Theorien, vor allem in der Algebraischen Zahlentheorie. Besonders zu erwähnen ist hier Ernst Kummer, der 1846 das Konzept der (gebrochenen) Ideale einführte, um in endlichen Körpererweiterungen der rationalen Zahlen $\mathbb{Q}$ ein Pendant zum Fundamentalsatz der Arithmetik 1.21 zur Verfügung zu haben. Kummer konnte den Satz in dem Fall zeigen, dass n eine sogenannte ***reguläre Primzahl*** ist.

Endgültig bewiesen wurde der Große Satz von Fermat 4.3 erst 1994 durch Andrew Wiles. In Wirklichkeit zeigte dieser die im Jahr 1958 formulierte ***Taniyama-Shimura-Vermutung*** über elliptische Kurven, von der man bereits seit 1990 wusste, dass sie den Großen Satz von Fermat impliziert. Seine Arbeit stellt einen wichtigen Baustein des ambitionierten ***Langlands-Programms*** dar, in dem aktuell versucht wird, bestimmte Objekte der Algebraischen und der Analytischen Zahlentheorie miteinander zu identifizieren, um für künftige Resultate simultanen Zugriff auf beide Methoden zu haben.

4.2 Lösungsstrategien

Da diophantische Gleichungen aus beliebig vielen Termen in mehreren Veränderlichen bestehen können, bildet ihr Studium ein komplexes Teilgebiet der Zahlentheorie, für das es unmöglich ist, ein Kochrezept zum Lösen dieser Gleichungen anzugeben. Es gilt sogar noch mehr: Im Jahr 1900 stellte David Hilbert das Problem der Entscheidbarkeit der Lösbarkeit einer diophantischen Gleichung als zehntes Problem seiner berühmten Liste von 23 mathematischen Problemen vor. 1970 bewies Juri Wladimirowitsch Matijassewitsch, dass die Lösbarkeit diophantischer Gleichungen unentscheidbar ist, es also keinen allgemeinen Algorithmus geben kann, der zu einer beliebigen diophantischen Gleichung feststellt, ob sie lösbar oder unlösbar ist. Das Lösen diophantischer Gleichungen erfordert daher eine Vielzahl an die jeweils untersuchte Gleichung angepassten Vorgehensweisen, von denen wir einige klassische in diesem Abschnitt vorstellen wollen. Weitere Klassen diophantischer Gleichungen werden wir in den Abschnitten 5.3 und 6.3 studieren.

Modulare Arithmetik

Oftmals helfen Überlegungen über die Teilbarkeit von Termen einer diophantischen Gleichung, deren Lösbarkeit zu zeigen oder zu widerlegen. Ein einfaches Kriterium für die Nicht-Lösbarkeit ist:

Proposition 4.4 (Lösbarkeitskriterium für diophantische Gleichungen)**.** *Ist $P = (a_1, \ldots, a_n)$ eine Lösung einer diophantischen Gleichung*

$$F(X_1, \ldots, X_n) = 0 \quad \textit{mit } n \in \mathbb{N} \textit{ und } F \in \mathbb{Z}[X_1, \ldots, X_n],$$

so ist für jedes $m \in \mathbb{N}$ durch $(a_1 + m\mathbb{Z}, \ldots, a_n + m\mathbb{Z})$ eine Lösung der Gleichung $F(X_1, \ldots, X_n) = 0$ im Restklassenring $\mathbb{Z}/m\mathbb{Z}$.

Beweis. Die Zuordnung

$$\begin{aligned} \mathbb{Z} &\to \mathbb{Z}/m\mathbb{Z}, \\ a &\mapsto a + m\mathbb{Z} \end{aligned}$$

ist ein Ringhomomorphismus. Es gilt daher

$$0 = F(a_1, \ldots, a_n) + m\mathbb{Z} = F(a_1 + m\mathbb{Z}, \ldots, a_n + m\mathbb{Z}).$$

□

Ein einfaches Beispiel hierzu ist:

Beispiel 4.5. *Die diophantische Gleichung $X_1^2 - 3X_2^2 + 4 = 0$ hat keine Lösung,*

denn: Reduzieren wir die diophantische Gleichung modulo 3, so erhalten wir die Gleichung $X_1^2 + 1 = 0$, welche keine Lösung in $\mathbb{Z}/3\mathbb{Z}$ aufweist. Nach dem Lösbarkeitskriterium 4.4 hat somit auch die ursprüngliche diophantische Gleichung keine Lösung. #

Manchmal muss man aber auch aufwändiger argumentieren:

Beispiel 4.6. *Die diophantische Gleichung $X_1^5 - X_2^2 - 4 = 0$ hat keine Lösung,*

denn: Nach dem Kleinen Satz von Fermat 3.32 gilt $X_1^{10} \equiv 0, 1 \bmod (11)$ und also

$$X_1^5 \equiv -1, 0, 1 \bmod (11).$$

Reduzieren wir die diophantische Gleichung modulo 11 und lösen sie nach X_2^2 auf, erhalten wir so

$$X_2^2 = X_1^5 - 4 \equiv 6, 7, 8 \bmod (11).$$

Durch eine einfache Fallunterscheidung zeigt man andererseits

$$X_2^2 \equiv 0, 1, 3, 4, 5, 9 \bmod (11),$$

so dass die modulo 11 reduzierte Gleichung $X_1^5 - X_2^2 - 4 = 0$ keine Lösung in $\mathbb{Z}/11\mathbb{Z}$ aufweist. Nach dem Lösbarkeitskriterium 4.4 hat somit auch die ursprüngliche diophantische Gleichung keine Lösung. #

Faktorisierung

Gegeben seien eine diophantische Gleichung

$$F(X_1, \ldots, X_n) = 0$$

und eine ganze Zahl $a \in \mathbb{Z}$ mit einer Faktorisierung

$$F(X_1, \ldots, X_n) - a = \prod_{i=1}^{r} F_i(X_1, \ldots, X_n)$$

im Ring $\mathbb{Z}[X_1, \ldots, X_n]$ für ein geeignetes $r \in \mathbb{N}$. Schreiben wir nun a anhand ihrer kanonischen Primfaktorzerlegung als ein Produkt $a = \prod_{i=1}^{r} a_i$ ganzer Zahlen, so erhalten wir auf diese Weise ein System diophantischer Gleichungen

$$\begin{aligned} F_1(X_1, \ldots, X_n) &= a_1, \\ &\vdots \\ F_r(X_1, \ldots, X_n) &= a_r, \end{aligned}$$

aus deren simultanen, ganzzahligen Lösungen wir Lösungen der ursprünglichen Gleichung bestimmen können. Das ist besonders effektiv, wenn wir durch die Faktorisierung von $F - a$ die Variablen trennen können. Die Methode veranschaulichen wir am besten an einem Beispiel:

Beispiel 4.7. *Die Gleichung*

$$X_1^2X_2^2 + (X_1^2 + 1)(2X_2 + 1) + X_2^2(1 - 2X_1) - 2X_1(2X_2 + 1) - 9 = 0$$

hat die Lösungen

$$(-2, -2), (-2, 0), (0, -4), (0, 2), (2, -4), (2, 2), (4, -2), (4, 0),$$

denn: Wir können die Gleichung zunächst äquivalent umformen zu

$$\begin{aligned} & X_1^2X_2^2 + (X_1^2 + 1)(2X_2 + 1) + X_2^2(1 - 2X_1) - 2X_1(2X_2 + 1) - 9 = 0 \\ \iff & X_1^2X_2^2 + X_1^2(2X_2 + 1) + X_2^2(1 - 2X_1) - 2X_1(2X_2 + 1) + 2X_2 + 1 = 9 \\ \iff & X_1^2X_2^2 + 2X_1^2X_2 + X_1^2 + X_2^2 - 2X_1X_2^2 - 2X_1 - 4X_1X_2 + 2X_2 + 1 = 9 \\ \iff & (X_1^2 - 2X_1 + 1)(X_2^2 + 2X_2 + 1) = 9 \\ \iff & (X_1 - 1)^2(X_2 + 1)^2 = 9 \\ \iff & (X_1 - 1)(X_2 + 1) = \pm 3. \end{aligned}$$

Aufgrund der Primalität von 3 ist ± 3 nicht in das Produkt zweier Nicht-Einheiten in $\mathbb{Z}$ zerlegbar und wir folgern, dass einer der Faktoren auf der linken Seite ± 1 und der entsprechend andere ± 3 sein muss. Wir unterscheiden zwei Fälle:

Fall 1: $(X_1 - 1)(X_2 + 1) = 3$. *In diesem Fall erhalten wir vier Systeme diophantischer Gleichungen:*

$$\begin{cases} X_1 - 1 = 1, \\ X_2 + 1 = 3 \end{cases}, \quad \begin{cases} X_1 - 1 = 3, \\ X_2 + 1 = 1 \end{cases}, \quad \begin{cases} X_1 - 1 = -1, \\ X_2 + 1 = -3 \end{cases}, \quad \begin{cases} X_1 - 1 = -3, \\ X_2 + 1 = -1 \end{cases}$$

mit zugehörigen Lösungen $(2,2), (4,0), (0,-4), (-2,-2)$.

Fall 2: $(X_1 - 1)(X_2 + 1) = -3$. *In diesem Fall erhalten wir vier Systeme diophantischer Gleichungen:*

$$\begin{cases} X_1 - 1 = -1, \\ X_2 + 1 = 3 \end{cases}, \quad \begin{cases} X_1 - 1 = 3, \\ X_2 + 1 = -1 \end{cases}, \quad \begin{cases} X_1 - 1 = 1, \\ X_2 + 1 = -3 \end{cases}, \quad \begin{cases} X_1 - 1 = -3, \\ X_2 + 1 = 1 \end{cases}$$

mit zugehörigen Lösungen $(0,2), (4,-2), (2,-4), (-2,0)$. #

In Beispiel 4.7 haben wir zentral die Eindeutigkeit der kanonischen Primfaktorzerlegung ausgenutzt, um die betrachtete Fallunterscheidung zu erhalten. In Abschnitt 6.4 werden wir mit den Ganzheitsringen quadratischer Zahlkörper Ringerweiterungen der ganzen Zahlen $\mathbb{Z}$ kennenlernen, die in manchen Fällen ebenfalls eine eindeutige Primfaktorzerlegung aufweisen. Die Methode der Faktorisierung zur Lösung von diophantischen Gleichungen lässt sich so auf weitere Fälle ausdehnen. In dieser Vorlesung verfolgen wir dies allerdings nicht weiter.

Unendlicher Abstieg

Diese Beweismethode geht auf Pierre de Fermat zurück und benutzt das Prinzip des Widerspruchsbeweises. Die Idee dahinter ist ein gezielt herbeigeführter Widerspruch zur Existenz einer kleinsten natürlichen Zahl, indem man von einer Lösung $F(X_1, \ldots, X_n) = 0$ in den natürlichen Zahlen ausgeht und versucht, eine weitere Lösung mit kleineren Werten zu konstruieren. Gelingt dies, so lässt sich diese Konstruktion aufbauend auf der neuen Lösung wiederholen. Iterativ erhält man so eine unendliche absteigende Kette von Lösungen in den natürlichen Zahlen, was nicht sein kann. Wir können dieses Beweisprinzip auf eine diophantische Gleichung anwenden, um zu zeigen, dass diese keine Lösung in den natürlichen Zahlen hat. Gehen mit ganzzahligen Lösungen automatisch Lösungen in den natürlichen Zahlen einher, so lassen sich mit dieser Methode sogar ganzzahlige Lösungen ausschließen.

Beispiel 4.8. *Die Gleichung*

$$X_1^3 + 2X_2^3 = 4X_3^3$$

hat keine Lösungen in den natürlichen Zahlen,

denn: Nehmen wir an, es gäbe eine Lösung $\left(x_1^{(1)}, x_2^{(1)}, x_3^{(1)}\right) \in \mathbb{N}^3$. *Setzten wir diese in die Gleichung ein und isolierten* $x_1^{(1)}$, *so gälte*

$$(x_1^1)^3 = 2\big(2(x_3^{(1)})^3 - (x_2^{(1)})^3\big),$$

also $2 \mid (x_1^1)^3$ *und schließlich* $2 \mid x_1^{(1)}$*. Es gäbe daher ein* $x_1^{(2)} \in \mathbb{N}$ *mit* $x_1^{(1)} = 2x_1^{(2)}$ *und – da* $x_1^{(1)}$ *als natürliche Zahl nicht Null ist – insbesondere mit* $x_1^{(2)} < x_1^{(1)}$*. Eingesetzt erhalten wir*

$$\begin{aligned} & 8(x_1^{(2)})^3 = 4(x_3^{(1)})^3 - 2(x_2^{(1)})^3 \\ \iff & (x_2^{(1)})^3 = 2(x_3^{(1)})^3 - 4(x_1^{(2)})^3. \end{aligned}$$

Mit analoger Argumentation erhalten wir nun $2 \mid x_2^{(1)}$ *und also die Existenz eines* $x_2^{(2)} \in \mathbb{N}$ *mit* $x_2^{(1)} = 2x_2^{(2)}$ *und insbesondere mit* $x_2^{(2)} < x_2^{(1)}$*. Eingesetzt erhalten wir*

$$\begin{aligned} & 8(x_2^{(2)})^3 = 2(x_3^{(1)})^3 - 4(x_1^{(2)})^3 \\ \iff & (x_3^{(1)})^3 = 4(x_2^{(2)})^3 + 2(x_1^{(2)})^3. \end{aligned}$$

Mit analoger Argumentation erhalten wir nun $2 \mid x_3^{(1)}$ *und also die Existenz eines* $x_3^{(2)} \in \mathbb{N}$ *mit* $x_3^{(1)} = 2x_3^{(2)}$ *und insbesondere mit* $x_3^{(2)} < x_3^{(1)}$*. Eingesetzt erhalten wir schließlich*

$$\begin{aligned} & 8(x_3^{(2)})^3 = 4(x_2^{(2)})^3 + 2(x_1^{(2)})^3 \\ \iff & (x_1^{(2)})^3 + 2(x_2^{(2)})^3 = 4(x_3^{(2)})^3 \end{aligned}$$

und also eine weitere Lösung $(x_1^{(2)}, x_2^{(2)}, x_3^{(2)}) \in \mathbb{N}^3$ *mit echt kleineren Einträgen. Iterativ erhalten wir so eine unendliche Folge von Lösungen in* $\mathbb{N}^3$ *mit streng monoton fallenden Einträgen. Das steht im Widerspruch zur Existenz einer kleinsten natürlichen Zahl und kann also nicht sein. Es folgt, dass die gegebene diophantische Gleichung keine natürlichen Lösungen haben kann.* #

In der folgenden Proposition untersuchen wir ein berühmtes Beispiel einer diophantischen Gleichung:

Proposition 4.9. *Die Gleichung*

$$X_1^4 + X_2^4 = X_3^2$$

hat außer den trivialen Lösungen mit $X_1X_2X_3 = 0$ *keine Lösungen in den ganzen Zahlen. Offensichtlich folgt hieraus sofort dieselbe Aussage für die Gleichung*

$$X_1^4 + X_2^4 = X_3^4,$$

was die ***Fermat'sche Vermutung*** *im Fall* $n = 4$ *zeigt.*

Beweis. Da offensichtlich für eine gegebene Lösung $(x_1, x_2, x_3) \in \mathbb{Z}^3$ auch jedes der Tripel $(\pm x_1, \pm x_2, \pm x_3) \in \mathbb{Z}^3$ eine Lösung ist, reicht es zum Beweis der Behauptung aus zu zeigen, dass keine Lösungen mit Einträgen in den natürlichen Zahlen existieren. Nehmen wir dafür an, es existierte eine Lösung $(x_1, x_2, x_3) \in \mathbb{N}^3$. Ohne Einschränkung könnten wir dann annehmen, die Einträge x_1, x_2, x_3 wären paarweise teilerfremd,

denn: Man überlegt sich leicht: Hätten zwei dieser Einträge einen nichttrivialen Teiler d, so teilte dieser in geeigneter Potenz auch den dritten Eintrag und es wäre auch $\left(\frac{x_1}{d}, \frac{x_2}{d}, \frac{x_3}{d^2}\right)$ eine Lösung. #

Weiter wären die Einträge x_1 und x_2 nicht beide gerade oder beide ungerade, so dass wir ohne Einschränkung annehmen könnten, x_1 wäre ungerade und x_2 gerade,

denn: Andernfalls gälte für die linke Seite der Gleichung

$$x_1^4 + x_2^4 \equiv \begin{cases} 0 \bmod (4) & \text{für } x_1, x_2 \text{ beide gerade,} \\ 2 \bmod (4) & \text{für } x_1, x_2 \text{ beide ungerade} \end{cases}$$

und für die rechte Seite

$$x_3^2 \equiv \begin{cases} 0 \bmod (4) & \text{für } x_3 \text{ gerade,} \\ 1 \bmod (4) & \text{für } x_3 \text{ ungerade.} \end{cases}$$

Dies könnte nur übereinstimmen, wenn x_1, x_2, x_3 allesamt gerade wären, was gegen die bereits vorausgesetzte paarweise Teilerfremdheit verstieße. #

Der Eintrag x_3 wäre dann ungerade,

denn: Das ergibt sich unmittelbar aus einer Reduktion modulo 4. #

In der faktorisierten Gleichung

$$x_2^4 = (x_3 - x_1^2)(x_3 + x_1^2) \tag{4.4}$$

gälte weiter sogar $1 < g := \mathrm{ggT}(x_3 - x_1^2, x_3 + x_1^2) = 2$,

denn: Für einen ungeraden Primteiler $p \mid g$ gälte

$$\begin{aligned} p \mid \big((x_3 - x_1^2) + (x_3 + x_1^2)\big) &= 2x_3, \\ p \mid \big((x_3 - x_1^2) - (x_3 + x_1^2)\big) &= 2x_1^2. \end{aligned}$$

Aufgrund von $p \nmid 2$, dem Primalitätskriterium 1.20 und der vorausgesetzten Teilerfremdheit von x_1 und x_3 erhielten wir hieraus

$$p \mid \mathrm{ggT}(x_3, x_1) = 1,$$

was nicht sein kann. Es folgt, dass g keinen ungeraden Primteiler haben kann. Andererseits gälte mit derselben Argumentation wie oben bereits $g \mid 2x_3$. Aufgrund der Ungeradheit von x_3 kann somit der Primfaktor 2 höchstens einmal in der Primfaktorzerlegung von g auftauchen. Die Behauptung folgt, da nach Konstruktion $(x_3 - x_1^2)$ und $(x_3 + x_1^2)$ beide gerade sind. #

Es folgte die Existenz von teilerfremden natürlichen Zahlen $a, b \in \mathbb{N}$ mit

$$x_3 - x_1^2 = 8a^4 \quad \text{und} \quad x_3 + x_1^2 = 2b^4 \quad \text{mit ungeradem } b \tag{4.5}$$

denn: Durch Vergleich der kanonischen Primfaktorzerlegung auf beiden Seiten von (4.4) erhielten wir, dass die Potenzen der ungeraden Primfaktoren der teilerfremden natürlichen Zahlen

$$\frac{x_3 - x_1^2}{2} \quad \text{und} \quad \frac{x_3 + x_1^2}{2}$$

allesamt durch vier teilbar wären und dass außerdem genau eine der Zahlen gerade wäre. Bei genauerer Betrachtung der Beiträge der Primzahl 2 erhielten wir im Fall $2 \mid \frac{x_3 - x_1^2}{2}$ die Existenz teilerfremder $a, b \in \mathbb{N}$ mit

$$\begin{aligned} x_3 - x_1^2 &= \frac{(2a)^4}{2} = 8a^4, \\ x_3 + x_1^2 &= 2b^4 \end{aligned}$$

und also die Behauptung. Der Fall $2 \mid \frac{x_3 + x_1^2}{2}$ ginge genauso und führte auf die Existenz von teilerfremden natürlichen Zahlen $a, b \in \mathbb{N}$ mit

$$x_3 - x_1^2 = 2a^4 \quad \text{und} \quad x_3 + x_1^2 = 8b^4 \quad \text{mit ungeradem } a.$$

Es verbleibt zu zeigen, dass diese zweite Möglichkeit nicht auftreten kann. In der Tat erhielten wir hier als Differenz der beiden gegebenen Gleichungen die Identität $x_1^2 = 4b^4 - a^4$ und nach Reduktion modulo 4 die Kongruenz $x_1^2 \equiv -a^4 \bmod (4)$, was wegen der Ungeradheit von x_1 und a nicht möglich wäre. #

Durch Differenzbilden und Umordnen der Terme aus (4.5) erhielten wir

$$4a^4 = b^4 - x_1^2 = (b^2 - x_1)(b^2 + x_1).$$

Hierbei gälte

$$g := \mathrm{ggT}(x_1, b) = 1,$$

denn: Mit $x_1 = g\tilde{x}_1$ und $b = g\tilde{b}$ für $\tilde{x}_1, \tilde{b} \in \mathbb{N}$ gälte

$$4a^4 = g^2(\tilde{b}^4 - \tilde{x}_1^2).$$

Wegen der Ungeradheit von b folgte hieraus $g^2 \mid a^4$ und also auch $g \mid a^2$. Das stünde im Widerspruch zur Teilerfremdheit von a und b und könnte daher nicht sein. #

Analog zum größten gemeinsamen Teiler der Faktoren von (4.4) erhielten wir nun $\mathrm{ggT}(b^2 - x_1, b^2 + x_1) = 2$ und analog zu (4.5) folgte hieraus die Existenz von $c, d \in \mathbb{N}$ mit

$$b^2 - x_1 = 2c^4 \quad \text{und} \quad b^2 + x_1 = 2d^4.$$

Summierten wir die letzten beiden Gleichungen auf, ergäbe sich $b^2 = c^4 + d^4$, so dass $(c, d, b) \in \mathbb{N}^3$ eine weitere Lösung der ursprünglichen diophantischen Gleichung wäre. Hierbei gälte $b < x_3$,

denn: Nach (4.5) und wegen der Gültigkeit der ursprünglichen Gleichung wäre

$$2b^4 = x_3 + x_1^2 \leq x_3^2 + x_1^4 < x_3^2 + (x_1^4 + x_2^4) = 2x_3^2$$

und also

$$b^2 < x_3.$$

#

Durch Wiederholen dieser Konstruktion erhielten wir eine unendliche Folge von Lösungen, deren dritte Einträge von Folgeglied zu Folgeglied stets echt kleiner würden. Das steht im Widerspruch zur Existenz einer kleinsten natürlichen Zahl und kann also nicht sein. Es folgt, dass die gegebene diophantische Gleichung keine natürlichen Lösungen haben kann. □

4.3 Lineare diophantische Gleichungen

Im Fall linearer diophantischer Gleichungen können wir mit Methoden der Linearen Algebra sogar Charakterisierungen der Lösbarkeit angeben. Das ist das Ziel dieses Abschnitts. Zunächst studieren wir den Fall einer einzelnen linearen diophantischen Gleichung:

Proposition 4.10 (Lösbarkeitskriterium für lineare diophantische Gleichungen)**.** *Seien die ganzen Zahlen $c_0, c_1, \ldots, c_n \in \mathbb{Z}$ nicht alle gleich Null. Dann gilt:*

$$\begin{aligned} & \textit{Die lineare diophantische Gleichung } c_1X_1 + \ldots + c_nX_n = c_0 \textit{ hat eine Lösung} \\ \iff \quad & \operatorname{ggT}(c_1, \ldots, c_n) \mid c_0. \end{aligned}$$

Beweis. Nehmen wir zunächst an, die diophantische Gleichung habe eine Lösung $(a_1, \ldots, a_n)$. Trivialerweise gilt

$$\operatorname{ggT}(c_1, \ldots, c_n) \mid c_i \qquad \text{für alle } i \in \{1, \ldots, n\}$$

und es folgt

$$\operatorname{ggT}(c_1, \ldots, c_n) \mid (c_1a_1 + \ldots + c_na_n) = c_0.$$

Gelte nun umgekehrt $\operatorname{ggT}(c_1, \ldots, c_n) \mid c_0$. Nach dem erweiterten Euklidischen Algorithmus gibt es ganze Zahlen u_1 und v mit

$$\operatorname{ggT}(c_1, \ldots, c_n) \overset{1.16}{=} \operatorname{ggT}(c_1, \operatorname{ggT}(c_2, \ldots, c_n)) = u_1c_1 + v \operatorname{ggT}(c_2, \ldots, c_n).$$

Iterativ erhalten wir ganze Zahlen $u_1, \ldots, u_n \in \mathbb{Z}$ mit

$$\operatorname{ggT}(c_1, \ldots, c_n) = u_1c_1 + \ldots + u_nc_n.$$

Setzen wir nun

$$a_i := du_i \quad \text{mit } d := \frac{c_0}{\operatorname{ggT}(c_1, \ldots, c_n)} \in \mathbb{Z},$$

so folgt

$$a_1c_1 + \ldots + a_nc_n = d\big(u_1c_1 + \ldots + u_nc_n\big) = c_0,$$

so dass $(a_1, \ldots, a_n)$ eine Lösung der diophantischen Gleichung ist. □

Beispiel 4.11. *Das Lösbarkeitskriterium 4.10 kann bei kleinen Alltagsproblemen nützlich sein:*

- *Ein Automat verkauft Snacks für* $1,20€$, $1,50€$, *sowie* $2,70€$*und gibt kein Rückgeld. Ich habe* $7€$. *Kann ich mein ganzes Geld für Snacks ausgeben, ohne zuviel zu zahlen?*

  Wir müssen die diophantische Gleichung

  $$120X_1 + 150X_2 + 270X_3 = 700$$

  lösen. Wegen $\operatorname{ggT}(120, 150, 270) = 30 \nmid 700$ *ist das nicht möglich.*

Man sollte die Anwendungsmöglichkeiten aber nicht überbewerten, wie das folgende Beispiel zeigt:

- *Ein Automat verkauft Briefmarken für* $0,80€$, $0,95€$, $1,55€$*sowie* $2,70€$*und gibt kein Rückgeld. Ich habe* $7€$. *Kann ich mein ganzes Geld für Briefmarken ausgeben, ohne zuviel zu zahlen?*

  Es gilt die diophantische Gleichung

  $$80X_1 + 95X_2 + 155X_3 + 270X_4 = 700$$

  zu lösen. Es gilt $\operatorname{ggT}(80, 95, 155, 270) = 5 \mid 700$. *Tatsächlich ist etwa* $(280, 0, -140, 0)$ *eine Lösung der diophantischen Gleichung, die uns aber nicht weiterbringt, weil wir in Wirklichkeit nach einer Lösung in* $\mathbb{N}_0^4$ *gesucht haben.*

Um ein ganzes System linearer diophantischer Gleichungen simultan zu lösen, ziehen wir einen Satz aus der Linearen Algebra zu Rate:

Satz 4.12 (Elementarteilersatz)**.** *Für alle* $m, n \in \mathbb{N}$ *und jede Matrix* $A = (a_{ij})_{i,j} \in \mathbb{Z}^{m \times n}$ *gibt es eindeutige Zahlen*

$$e_1 \mid e_2 \mid \ldots \mid e_{\min\{m,n\}} \in \mathbb{N}_0,$$

die ***Elementarteiler*** *von* A*, sowie Matrizen* $M \in \mathrm{GL}_n(\mathbb{Z})$ *und* $N \in \mathrm{GL}_m(\mathbb{Z})$ *mit*

$$(MAN)_{i,j} = \begin{cases} e_i & \text{für } i = j, \\ 0 & \text{für } i \neq j. \end{cases}$$

Beweis. Wir beweisen den Satz durch Angabe eines zielführenden Algorithmus.

Da sonst nichts zu zeigen ist, können wir ohne Einschränkung $A \neq 0$ annehmen. Nach eventuellem Vertauschen von Zeilen und Spalten über Links- bzw. Rechtsmultiplikation mit geeigneten Matrizen aus $\mathrm{GL}_m(\mathbb{Z})$ bzw. $\mathrm{GL}_n(\mathbb{Z})$ gilt dann ohne Einschränkung sogar $a_{11} \neq 0$.

Solange es in der ersten Zeile oder Spalte einen Eintrag a gibt, der nicht durch a_{11} teilbar ist, bestimme mit dem erweiterten Euklidischen Algorithmus ganze Zahlen $u, v \in \mathbb{Z}$ mit

$\mathrm{ggT}(a_{11}, a) = ua_{11} + va$. Im Fall $a = a_{1j}$ mit einem $j \in \{1, \dots, n\}$ multiplizieren wir von rechts mit der Matrix

$$\begin{pmatrix} u & 0 & \cdots & 0 & -\frac{a_{1j}}{\mathrm{ggT}(a_{11}, a_{1j})} & 0 & \cdots & 0 \\ 0 & 1 & & & 0 & & & \\ \vdots & & \ddots & & \vdots & & & \\ 0 & & & 1 & 0 & & & \\ v & & & & \frac{a_{11}}{\mathrm{ggT}(a_{11}, a_{1j})} & & & \\ 0 & & & & & 1 & & \\ \vdots & & & & & & \ddots & \\ 0 & & & & & & & 1 \end{pmatrix} \in \mathrm{GL}_n(\mathbb{Z})$$

und ersetzen so

$$\begin{aligned} &1.\ \text{Spalte} \ \mapsto u \cdot (1.\ \text{Spalte}) + v \cdot (j.\ \text{Spalte}), \\ &j.\ \text{Spalte} \ \mapsto -\frac{a_{1j}}{\mathrm{ggT}(a_{11}, a_{1j})} \cdot (1.\ \text{Spalte}) + \frac{a_{11}}{\mathrm{ggT}(a_{11}, a_{1j})} \cdot (j.\ \text{Spalte}). \end{aligned}$$

Im Fall $a = a_{i1}$ gehen wir analog vor. Nach jedem solchen Schritt erreichen wir auf diese Weise einen echt kleineren Wert von a_{11}, so dass wir nach eventueller Anwendung endlich vieler solcher Schritte ohne Einschränkung annehmen können, alle Einträge der ersten Zeile und der ersten Spalte seien durch a_{11} teilbar.

Durch Addition von ganzzahligen Vielfachen der ersten Zeile bzw. Spalte zu den anderen Zeilen bzw. Spalten von A können wir nun ohne Einschränkung erreichen, dass a_{11} sowohl in der ersten Zeile als auch in der ersten Spalte der einzige nicht verschwindende Eintrag ist.

Der Satz folgt, wenn wir nun den bisherigen Algorithmus auf die Matrix anwenden, die wir nach Streichen der ersten Zeile und der ersten Spalte von A erhalten, und dann so weiter, bis wir nach $\min\{m, n\}$ Schritten terminieren. □

Korollar 4.13 (Lösbarkeitskriterium für Systeme linearer diophantischer Gleichungen)**.** *Für alle $m, n \in \mathbb{N}$, jede Matrix $A = (a_{ij})_{i,j} \in \mathbb{Z}^{m \times n}$ und jeden Vektor $b \in \mathbb{Z}^m$ gilt in der Notation von Satz 4.12:*

$$\begin{aligned} &\textit{Das System } A \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix} = b \textit{ linearer diophantischer Gleichungen hat eine Lösung} \\ \iff \quad &e_i \mid (Mb)_i \textit{ für alle } i \in \{1, \dots, n\} \textit{ und } (Mb)_i = 0 \textit{ für alle } i > n. \end{aligned}$$

Beweis. Ein $a \in \mathbb{Z}^n$ ist genau dann eine Lösung des gegebenen Systems linearer diophantischer Gleichungen, wenn $N^{-1}a$ eine Lösung von

$$MAN \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix} = Mb$$

ist. Nach dem Elementarteilersatz 4.12 ist letzteres Gleichungssystem von der Form

$$\begin{aligned} e_1 X_1 &= (Mb)_1, \\ &\vdots \\ e_n X_n &= (Mb)_n, \\ 0 &= (Mb)_{n+1}, \\ &\vdots \\ 0 &= (Mb)_m. \end{aligned}$$

□

Beispiel 4.14. *Das System*

$$A \begin{pmatrix} X_1 \\ X_2 \end{pmatrix} = b \quad \textit{mit } A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \in \mathbb{Z}^{2\times 2} \textit{ und } b = \begin{pmatrix} 2 \\ 2 \end{pmatrix} \in \mathbb{Z}^2$$

linearer diophantischer Gleichungen ist lösbar, das gegebene Lineare Gleichungssystem hat also eine Lösung mit ganzen Koeffizienten,

denn: In der Notation des Elementarteilersatzes 4.12 berechnet man

$$M = \begin{pmatrix} -2 & 1 \\ 3 & -1 \end{pmatrix}, \quad N = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad MAN = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \quad \textit{und} \quad Mb = \begin{pmatrix} -2 \\ 4 \end{pmatrix}.$$

Wir überprüfen

$$e_1 = 1 \mid -2 = (Mb)_1 \quad \textit{und} \quad e_2 = 2 \mid 4 = (Mb)_2.$$

Nach dem Lösbarkeitskriterium 4.13 ist das gegebene System linearer diophantischer Gleichungen also lösbar. #

Tatsächlich ist

$$\begin{pmatrix} -2 \\ 2 \end{pmatrix} \in \mathbb{Z}^2$$

eine Lösung.

KAPITEL 5

Das Quadratische Reziprozitätsgesetz und seine Anwendungen

5.1 Das Reziprozitätsgesetz

Definition 5.1. *Seien p eine ungerade Primzahl und $a \in \mathbb{Z}$. Die Zahl a (bzw. die Restklasse $\overline{a} \in \mathbb{Z}/p\mathbb{Z}$) heißt ein **quadratischer Rest** modulo p, falls $p \nmid a$ gilt und es ein $x \in \mathbb{Z}$ mit $x^2 \equiv a \bmod (p)$ gibt. Die Zahl a (bzw. die Restklasse $\overline{a} \in \mathbb{Z}/p\mathbb{Z}$) heißt ein **quadratischer Nichtrest** modulo p, falls $p \nmid a$ gilt und es kein $x \in \mathbb{Z}$ mit $x^2 \equiv a \bmod (p)$ gibt. Wir setzen*

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{für } a \text{ quadratischer Rest modulo } p, \\ 0 & \text{für } p \mid a, \\ -1 & \text{für } a \text{ quadratischer Nichtrest modulo } p. \end{cases}$$

*Die Abbildung $\left(\frac{\cdot}{p}\right) : \mathbb{Z} \to \{-1, 0, 1\}$ heißt hierbei das **Legendre-Symbol** modulo p.*

Offenbar hängt das Legendre-Symbol $\left(\frac{a}{p}\right)$ nur von der Restklasse von a modulo p ab.

Beispiel 5.2. *In $(\mathbb{Z}/5\mathbb{Z})^\times$ gilt $\overline{1}^2 = \overline{1}, \overline{2}^2 = \overline{4}, \overline{3}^2 = \overline{4}$ und $\overline{4}^2 = \overline{1}$. Dementsprechend erhalten wir als*

- *quadratische Reste modulo 5: $\overline{1}, \overline{4}$,*
- *quadratische Nichtreste modulo 5: $\overline{2}, \overline{3}$*

und für $a \in \mathbb{Z}$ gilt

$$\left(\frac{a}{5}\right) = \begin{cases} 1 & \text{für } a \equiv 1, 4 \bmod (5), \\ 0 & \text{für } a \equiv 0 \bmod (5), \\ -1 & \text{für } a \equiv 2, 3 \bmod (5). \end{cases}$$

Proposition 5.3. *Seien p eine ungerade Primzahl, w eine primitive Wurzel modulo p und $r \in \mathbb{N}_0$. Dann gilt:*

$$\left(\frac{w^r}{p}\right) = (-1)^r.$$

Beweis. Die Behauptung ist offenbar äquivalent zur Aussage, dass w^r genau dann quadratischer Rest modulo p ist, wenn r gerade ist. Dies zeigen wir nun. Sei dafür zunächst w^r ein quadratischer Rest modulo p. Dann gibt es ein $x \in \mathbb{Z}$ mit $\overline{w}^r = \overline{x}^2$ in $\mathbb{Z}/p\mathbb{Z}$. Da w eine primitive Wurzel modulo p ist, existiert ein $n \in \mathbb{N}_0$ mit $\overline{x} = \overline{w}^n$. Wir erhalten $\overline{w}^r = \overline{w}^{2n}$ und somit $\overline{w}^{r-2n} = \overline{1}$. Nach Proposition 3.39 folgt hieraus $p-1 = \operatorname{ord}(\overline{w}) \mid (r-2n)$. Wegen $2 \mid (p-1)$ folgt hieraus $2 \mid (r-2n)$ und somit $2 \mid r$.

Gelte nun umgekehrt $2 \mid r$. Dann gibt es ein $q \in \mathbb{N}_0$ mit $r = 2q$. Das liefert $\overline{w}^r = (\overline{w}^q)^2$, weswegen $\overline{w}^r$ ein quadratischer Rest modulo p ist. □

Es gilt $(\mathbb{Z}/p\mathbb{Z})^\times = \{\overline{1}, \overline{w}, \ldots, \overline{w}^{p-2}\}$. In dieser Darstellung sind die quadratischen Reste modulo p also genau diejenigen Restklassen mit geradem Exponenten, die quadratischen Nichtreste diejenigen mit ungeradem Exponenten.

Satz 5.4. *Seien p eine ungerade Primzahl und $a, b \in \mathbb{Z}$. Dann ist das Legendre-Symbol modulo p stark multiplikativ, es gilt also*

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

Insbesondere induziert das Legendre-Symbol einen Gruppenhomomorphismus

$$\left(\frac{\cdot}{p}\right) : \begin{cases} (\mathbb{Z}/p\mathbb{Z})^\times & \to \{\pm 1\}, \\ \overline{a} & \mapsto \left(\frac{a}{p}\right). \end{cases}$$

Beweis. Da p eine Primzahl ist, gilt die Äquivalenz $p \mid ab \iff p \mid a$ oder $p \mid b$. Damit ist die linke Seite genau dann Null, wenn die rechte Seite Null ist. Im Folgenden seien a, b und somit auch ab nicht durch p teilbar. Sei w eine primitive Wurzel modulo p. Dann existieren $r, s \in \mathbb{N}_0$ mit $\overline{a} = \overline{w}^r$ und $\overline{b} = \overline{w}^s$. Es ergibt sich

$$\left(\frac{ab}{p}\right) = \left(\frac{w^{r+s}}{p}\right) = (-1)^{r+s} = (-1)^r(-1)^s = \left(\frac{w^r}{p}\right)\left(\frac{w^s}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

□

Satz 5.5 (Satz von Euler)**.** *Seien p eine ungerade Primzahl und $a \in \mathbb{Z}$. Dann gilt*

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

Beweis. Falls $p \mid a$ gilt, so ist

$$\left(\frac{a}{p}\right) = 0 \equiv a^{\frac{p-1}{2}} \bmod (p).$$

Im Folgenden gelte $p \nmid a$. Nach dem Kleinen Satz von Fermat 3.32 gilt in $\mathbb{F}_p$ die Gleichung

$$(\overline{a}^{\frac{p-1}{2}})^2 = \overline{a}^{p-1} = \overline{1}.$$

Das Polynom $X^2 - \overline{1} \in \mathbb{F}_p[X]$ hat nach Korollar 3.54 höchstens zwei Nullstellen. Somit sind $\overline{1}, \overline{-1}$ die einzigen Nullstellen dieses Polynoms und es gilt $\overline{a}^{\frac{p-1}{2}} \in \{\overline{1}, \overline{-1}\}$. Zu zeigen ist damit die Aussage

$$\left(\frac{a}{p}\right) = 1 \quad \Longleftrightarrow \quad \overline{a}^{\frac{p-1}{2}} = \overline{1}.$$

Gelte dafür zunächst $\left(\frac{a}{p}\right) = 1$. Dann gibt es ein $\overline{x} \in (\mathbb{Z}/p\mathbb{Z})^\times$ mit $\overline{a} = \overline{x}^2$, woraus unmittelbar

$$\overline{a}^{\frac{p-1}{2}} = \overline{x}^{p-1} = \overline{1}$$

folgt.

Sei umgekehrt $w \in \mathbb{Z}$ eine primitive Wurzel modulo p und sei $r \in \mathbb{N}_0$ mit $\overline{a} = \overline{w}^r$. Wir erhalten

$$(\overline{w}^r)^{\frac{p-1}{2}} = \overline{a}^{\frac{p-1}{2}} = \overline{1}.$$

Mittels Proposition 3.39 ergibt sich $(p-1) \mid r\frac{p-1}{2}$, weswegen r gerade ist. Somit ist

$$\left(\frac{a}{p}\right) = (-1)^r = 1.$$

□

Wegen $p > 2$ sind die Restklassen von $-1, 0, 1$ modulo p paarweise verschieden. Daher ist das Legendre-Symbol durch seine Restklasse modulo p eindeutig bestimmt.

Proposition 5.6 (Lemma von Gauß)**.** *Seien p eine ungerade Primzahl und $a \in \mathbb{Z}$ mit $p \nmid a$. Wir setzen*

$$H := \{\overline{1}, \overline{2}, \ldots, \overline{\frac{p-1}{2}}\} \subseteq \mathbb{Z}/p\mathbb{Z}.$$

Seien $\overline{h_1}, \ldots, \overline{h_{\frac{p-1}{2}}} \in H$ und $\varepsilon_1, \ldots, \varepsilon_{\frac{p-1}{2}} \in \{\pm 1\}$ mit

$$\overline{a} \cdot \overline{1} = \overline{\varepsilon_1} \cdot \overline{h_1},\ \ldots,\ \overline{a} \cdot \overline{\frac{p-1}{2}} = \overline{\varepsilon_{\frac{p-1}{2}}} \cdot \overline{h_{\frac{p-1}{2}}}.$$

Dann gilt

$$\left(\frac{a}{p}\right) = \varepsilon_1 \cdot \ldots \cdot \varepsilon_{\frac{p-1}{2}}.$$

Beweis. Die Restklassen $\overline{h_1}, \ldots, \overline{h_{\frac{p-1}{2}}}$ sind paarweise verschieden,

denn: Seien $i, j \in \{1, \ldots, \frac{p-1}{2}\}$ mit $\overline{h_i} = \overline{h_j}$. Dann ist $\overline{h_i}^2 = \overline{h_j}^2$ und deshalb $\bar{a}^2\bar{i}^2 = \bar{a}^2\bar{j}^2$. Das liefert $\bar{i}^2 = \bar{j}^2$ und deshalb $(\bar{i} \cdot \bar{j}^{-1})^2 = \bar{1}$. Da wir in $\mathbb{Z}/p\mathbb{Z}$ rechnen, folgt $\bar{i} \cdot \bar{j}^{-1} \in \{\bar{1}, \overline{-1}\}$ und somit $\bar{i} = \pm\bar{j}$. Wegen $\bar{i}, \bar{j} \in H$ folgt $\bar{i} = \bar{j}$. #

Aufgrund der eben getätigten Überlegung taucht jedes Element aus H genau einmal als ein Element der Form $\overline{h_i}$ auf. Wir erhalten

$$\bar{a}^{\frac{p-1}{2}} \prod_{i=1}^{\frac{p-1}{2}} \bar{i} = \prod_{i=1}^{\frac{p-1}{2}} (\bar{a} \cdot \bar{i}) = \prod_{i=1}^{\frac{p-1}{2}} (\overline{\varepsilon_i} \cdot \overline{h_i}) = \overline{\varepsilon_1 \cdot \ldots \cdot \varepsilon_{\frac{p-1}{2}}} \prod_{i=1}^{\frac{p-1}{2}} \overline{h_i} = \overline{\varepsilon_1 \cdot \ldots \cdot \varepsilon_{\frac{p-1}{2}}} \prod_{i=1}^{\frac{p-1}{2}} \bar{i}$$

und deshalb

$$\bar{a}^{\frac{p-1}{2}} = \overline{\varepsilon_1 \cdot \ldots \cdot \varepsilon_{\frac{p-1}{2}}}.$$

Nach Satz 5.5 gilt

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \equiv \varepsilon_1 \cdot \ldots \cdot \varepsilon_{\frac{p-1}{2}} \bmod (p).$$

Da das Produkt auf der rechten Seite in der Menge $\{\pm 1\}$ liegt, folgt sogar

$$\left(\frac{a}{p}\right) = \varepsilon_1 \cdot \ldots \cdot \varepsilon_{\frac{p-1}{2}}.$$

□

Beispiel 5.7. *Für $p = 5$ und $a = 2$ gilt $H = \{\bar{1}, \bar{2}\}$ und wir erhalten*

- $\bar{a} \cdot \bar{1} = \bar{2} \cdot \bar{1} = \bar{1} \cdot \bar{2}$, *also ist* $\varepsilon_1 = 1$, $\overline{h_1} = \bar{2}$.
- $\bar{a} \cdot \bar{2} = \bar{2} \cdot \bar{2} = \bar{4} = \overline{-1} = \overline{-1} \cdot \bar{1}$, *also ist* $\varepsilon_2 = -1$, $\overline{h_2} = \bar{1}$.

Es ergibt sich

$$\left(\frac{2}{5}\right) = \varepsilon_1 \cdot \varepsilon_2 = 1 \cdot (-1) = -1.$$

Satz 5.8 (Quadratisches Reziprozitätsgesetz)**.** *Seien p, q ungerade Primzahlen. Dann gilt*

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

Ist also eine der beiden Primzahlen p, q kongruent 1 modulo 4, so ist

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right),$$

andernfalls

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right).$$

Satz 5.9 (Erster Ergänzungssatz zum Reziprozitätsgesetz)**.** *Sei p eine ungerade Primzahl. Dann gilt*

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

Die Zahl -1 ist also genau dann quadratischer Rest modulo p, wenn $p \equiv 1 \bmod (4)$ gilt.

Satz 5.10 (Zweiter Ergänzungssatz zum Reziprozitätsgesetz)**.** *Sei p eine ungerade Primzahl. Dann gilt*

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

Die Zahl 2 ist also genau dann quadratischer Rest modulo p, wenn $p \equiv \pm 1 \bmod (8)$ gilt.

Beweis von Satz 5.8, Satz 5.9 und Satz 5.10. Wir bemerken zunächst, dass der Satz von Euler 5.5 für $a = -1$ den Ersten Ergänzungssatz 5.9 liefert.

Im Folgenden sei $a \in \mathbb{Z}$ mit $p \nmid a$. Für alle $1 \leq i \leq \frac{p-1}{2}$ schreiben wir

$$a \cdot i = \varepsilon_i \cdot h_i + e_i \cdot p \quad \text{mit } h_i \in \{1, \ldots, \frac{p-1}{2}\}, \varepsilon_i \in \{\pm 1\}, e_i \in \mathbb{Z}.$$

Sei $i \in \{1, \ldots, \frac{p-1}{2}\}$. Dann ist

$$\varepsilon_i = (-1)^{\left\lfloor \frac{2ai}{p} \right\rfloor},$$

denn: Wir unterscheiden zwei Fälle:

Fall 1: $\varepsilon_i = 1$**.** Dann ist $ai = h_i + e_i p$ und somit

$$\frac{2ai}{p} = \frac{2h_i}{p} + 2e_i.$$

Es gilt $0 < \frac{2h_i}{p} < 1$ und somit $\left\lfloor \frac{2ai}{p} \right\rfloor = 2e_i$, insbesondere ist $\left\lfloor \frac{2ai}{p} \right\rfloor$ gerade.

Fall 2: $\varepsilon_i = -1$**.** Dann ist $ai = -h_i + e_i p$ und somit

$$\frac{2ai}{p} = \frac{p - 2h_i}{p} + 2e_i - 1.$$

Wegen $0 < \frac{p-2h_i}{p} < 1$ ist $\left\lfloor \frac{2ai}{p} \right\rfloor = 2e_i - 1$, insbesondere ist $\left\lfloor \frac{2ai}{p} \right\rfloor$ ungerade. #

Nach dem Lemma von Gauß 5.6 gilt

$$\left(\frac{a}{p}\right) = \varepsilon_1 \cdot \ldots \cdot \varepsilon_{\frac{p-1}{2}} = (-1)^{\sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{2ai}{p} \right\rfloor}.$$

Als zusätzliche Voraussetzung an a fordern wir ab jetzt, dass a ungerade ist. Dann ist $a+p$ gerade und wir erhalten

$$\left(\frac{2a}{p}\right) = \left(\frac{2a+2p}{p}\right) = \left(\frac{4\frac{a+p}{2}}{p}\right) = \left(\frac{4}{p}\right)\left(\frac{\frac{a+p}{2}}{p}\right) = \left(\frac{\frac{a+p}{2}}{p}\right).$$

Hierbei haben wir verwendet, dass 4 offensichtlich ein Quadrat modulo p ist. Es ergibt sich

$$\begin{aligned}\left(\frac{2a}{p}\right) &= (-1)^{\sum_{i=1}^{\frac{p-1}{2}}\left\lfloor\frac{(a+p)i}{p}\right\rfloor} = (-1)^{\sum_{i=1}^{\frac{p-1}{2}}\left\lfloor\frac{ai}{p}+i\right\rfloor} = (-1)^{\sum_{i=1}^{\frac{p-1}{2}} i+\sum_{i=1}^{\frac{p-1}{2}}\left\lfloor\frac{ai}{p}\right\rfloor}\\ &= (-1)^{\frac{1}{2}\cdot\frac{p-1}{2}\cdot(\frac{p-1}{2}+1)}(-1)^{\sum_{i=1}^{\frac{p-1}{2}}\left\lfloor\frac{ai}{p}\right\rfloor}\\ &= (-1)^{\frac{p^2-1}{8}}(-1)^{\sum_{i=1}^{\frac{p-1}{2}}\left\lfloor\frac{ai}{p}\right\rfloor}.\end{aligned}$$

Für $a=1$ ist $\sum_{i=1}^{\frac{p-1}{2}}\left\lfloor\frac{ai}{p}\right\rfloor = 0$ und deshalb

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}},$$

womit wir den Zweiten Ergänzungssatz 5.10 gezeigt haben.

Es verbleibt der Beweis des Reziprozitätsgesetzes 5.8. Wir bemerken dafür zunächst, dass nach der obigen Rechnung

$$\left(\frac{2}{p}\right)\left(\frac{a}{p}\right) = \left(\frac{2a}{p}\right) = (-1)^{\frac{p^2-1}{8}}(-1)^{\sum_{i=1}^{\frac{p-1}{2}}\left\lfloor\frac{ai}{p}\right\rfloor} = \left(\frac{2}{p}\right)(-1)^{\sum_{i=1}^{\frac{p-1}{2}}\left\lfloor\frac{ai}{p}\right\rfloor},$$

gilt, woraus sich

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{i=1}^{\frac{p-1}{2}}\left\lfloor\frac{ai}{p}\right\rfloor}$$

ergibt. Diese Beschreibung des Legendre-Symbols werden wir im weiteren Verlauf benutzen, um die gewünschte Identität zu zeigen. Sei q eine ungerade Primzahl. Im Fall $p=q$ ist die Behauptung des Reziprozitätsgesetzes 5.8 offensichtlich, da dann beide Seiten den Wert 0 annehmen. Im Folgenden sei daher $q \neq p$. Wir setzen

$$\begin{aligned}\ell_1 &:= \#\{(i,j) \in \{1,\dots,\frac{p-1}{2}\} \times \{1,\dots,\frac{q-1}{2}\} : qi > pj\},\\ \ell_2 &:= \#\{(i,j) \in \{1,\dots,\frac{p-1}{2}\} \times \{1,\dots,\frac{q-1}{2}\} : qi < pj\}.\end{aligned}$$

Wegen $qi \neq pj$ für $(i,j) \in \{1,\dots,\frac{p-1}{2}\} \times \{1,\dots,\frac{q-1}{2}\}$ folgt für festes $i \in \{1,\dots,\frac{p-1}{2}\}$

$$qi > pj \quad\Longleftrightarrow\quad j < \frac{qi}{p} \quad\Longleftrightarrow\quad j \leq \left\lfloor\frac{qi}{p}\right\rfloor.$$

Das liefert

$$\ell_1 = \sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{qi}{p} \right\rfloor$$

und analog

$$\ell_2 = \sum_{j=1}^{\frac{q-1}{2}} \left\lfloor \frac{pj}{q} \right\rfloor.$$

Außerdem ist

$$\ell_1 + \ell_2 = \#(\{1, \ldots, \frac{p-1}{2}\} \times \{1, \ldots, \frac{q-1}{2}\}) = \frac{p-1}{2}\frac{q-1}{2}.$$

Wir erhalten

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\sum_{j=1}^{\frac{q-1}{2}} \left\lfloor \frac{pj}{q} \right\rfloor} (-1)^{\sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{qi}{p} \right\rfloor} = (-1)^{\ell_2+\ell_1} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Wegen $\left(\frac{q}{p}\right)^2 = 1$ ergibt sich

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

und somit das Reziprozitätsgesetz 5.8. □

Beispiel 5.11. *Das Reziprozitätsgesetz kann benutzt werden, um Legendre-Symbole auszurechnen: Wir wollen das Legendre-Symbol* $\left(\frac{273}{307}\right)$ *bestimmen. Unter Verwendung der starken Multiplikativität 5.4 des Legendre-Symbols erhalten wir zunächst*

$$\left(\frac{273}{307}\right) = \left(\frac{3 \cdot 7 \cdot 13}{307}\right) = \left(\frac{3}{307}\right)\left(\frac{7}{307}\right)\left(\frac{13}{307}\right).$$

Wegen $3 \equiv 3 \bmod (4)$, $7 \equiv 3 \bmod (4)$, $13 \equiv 1 \bmod (4)$ *und* $307 \equiv 3 \bmod (4)$ *ergibt sich bei Anwendung des Quadratischen Reziprozitätsgesetzes 5.8*

$$\left(\frac{273}{307}\right) = (-1)\left(\frac{307}{3}\right)(-1)\left(\frac{307}{7}\right)\left(\frac{307}{13}\right) = \left(\frac{307}{3}\right)\left(\frac{307}{7}\right)\left(\frac{307}{13}\right).$$

Aufgrund von $307 \equiv 1 \bmod (3)$, $307 \equiv -1 \bmod (7)$ *und* $307 \equiv 8 \bmod (13)$ *können wir die Legendre-Symbole rechts vereinfachen zu*

$$\left(\frac{273}{307}\right) = \left(\frac{1}{3}\right)\left(\frac{-1}{7}\right)\left(\frac{8}{13}\right).$$

Der erste Faktor ist offenbar 1*, der zweite Faktor ist wegen* $7 \equiv 3 \bmod (4)$ *nach dem Ersten Ergänzungssatz 5.9 durch* -1 *gegeben. Somit ist*

$$\left(\frac{273}{307}\right) = -\left(\frac{8}{13}\right) = -\left(\frac{2}{13}\right)^3 = -\left(\frac{2}{13}\right),$$

wobei wir für die letzte Gleichung verwendet haben, dass das Legendre-Symbol den Wert 1 *oder* -1 *hat. Aus dem Zweiten Ergänzungssatz 5.10 erhalten wir wegen* $13 \equiv 5 \bmod (8)$ *als Ergebnis schließlich*

$$\left(\frac{273}{307}\right) = (-1) \cdot (-1) = 1.$$

Eine Verallgemeinerung des Legendre-Symbols ist durch das Jacobi-Symbol gegeben, welches wir im Folgenden studieren werden:

Definition 5.12. *Seien* $a \in \mathbb{Z}$ *und* $n \in \mathbb{N}$ *ungerade mit Primfaktorzerlegung* $n = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$*. Wir setzen*

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

und nennen $\left(\frac{\cdot}{n}\right)$ *das* ***Jacobi-Symbol*** *modulo* n*.*

Ist n eine Primzahl, so stimmen das Jacobi- und das Legendre-Symbol modulo n offenbar überein, unsere Notation ist also konsistent. Ist a ein quadratischer Rest modulo $n = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$, so ist a auch quadratischer Rest modulo $p_1, \ldots, p_r$, es gilt also

$$\left(\frac{a}{p_1}\right) = \ldots = \left(\frac{a}{p_r}\right) = 1.$$

Es folgt $\left(\frac{a}{n}\right) = 1$. Die Umkehrung ist jedoch falsch: So ist beispielsweise

$$\left(\frac{5}{9}\right) = \left(\frac{5}{3^2}\right) = \left(\frac{5}{3}\right)^2 = (-1)^2 = 1,$$

aber 5 ist kein quadratischer Rest modulo 9 – sonst wäre 2 quadratischer Rest modulo 3!

Wir merken an, dass das Jacobi-Symbol offenbar multiplikativ in beiden Argumenten ist. Darüber hinaus ist genau dann $\left(\frac{a}{n}\right) = 0$, wenn a und n nicht teilerfremd sind.

Wir wollen im Folgenden ein Reziprozitätsgesetz für das Jacobi-Symbol zeigen. Wir starten dazu mit einer Vorbemerkung:

Proposition 5.13. *Seien* $n_1, n_2 \in \mathbb{N}$ *ungerade. Dann gelten*

$$\frac{n_1 - 1}{2} + \frac{n_2 - 1}{2} \equiv \frac{n_1 n_2 - 1}{2} \bmod (2),$$
$$\frac{n_1^2 - 1}{8} + \frac{n_2^2 - 1}{8} \equiv \frac{(n_1 n_2)^2 - 1}{8} \bmod (2).$$

Beweis. Es ist $n_1 - 1 \equiv 0 \equiv n_2 - 1 \bmod (2)$ und deshalb ist $(n_1 - 1)(n_2 - 1) \equiv 0 \bmod (4)$. Das liefert $n_1 n_2 - n_1 - n_2 + 1 \equiv 0 \bmod (4)$ und somit $n_1 n_2 - 1 \equiv n_1 - 1 + n_2 - 1 \bmod (4)$. Wir erhalten

$$\frac{n_1 - 1}{2} + \frac{n_2 - 1}{2} \equiv \frac{n_1 n_2 - 1}{2} \bmod (2)$$

und also die erste Teilbehauptung.

Weiter ist $n_1 - 1 \equiv n_1 + 1 \equiv n_2 - 1 \equiv n_2 + 1 \bmod (2)$. Es folgt

$$(n_1^2 - 1)(n_2^2 - 1) = (n_1 - 1)(n_1 + 1)(n_2 - 1)(n_2 + 1) \equiv 0 \bmod (16).$$

Es ergibt sich

$$n_1^2 n_2^2 - 1 \equiv n_1^2 - 1 + n_2^2 - 1 \bmod (16)$$

und schließlich

$$\frac{n_1^2 - 1}{8} + \frac{n_2^2 - 1}{8} \equiv \frac{(n_1 n_2)^2 - 1}{8} \bmod (2)$$

und somit auch die zweite Teilbehauptung. □

Satz 5.14 (Reziprozitätsgesetz für das Jacobi-Symbol)**.** *Seien m, n ungerade natürliche Zahlen mit $m, n \geq 3$. Dann gelten die folgenden drei Aussagen:*

$$\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}, \tag{5.1}$$

$$\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}, \tag{5.2}$$

$$\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}} \left(\frac{n}{m}\right). \tag{5.3}$$

Beweis. Die Primfaktorzerlegungen von n bzw. m seien durch $n = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$ bzw. $m = q_1^{f_1} \cdot \ldots \cdot q_s^{f_s}$ gegeben. Es gilt dann zunächst

$$\begin{aligned}\left(\frac{-1}{n}\right) &= \left(\frac{-1}{p_1}\right)^{e_1} \cdot \ldots \cdot \left(\frac{-1}{p_r}\right)^{e_r} = (-1)^{\frac{p_1-1}{2}e_1} \cdot \ldots \cdot (-1)^{\frac{p_r-1}{2}e_r} \\ &\overset{5.13}{=} (-1)^{\frac{p_1^{e_1}-1}{2}} \cdot \ldots \cdot (-1)^{\frac{p_r^{e_r}-1}{2}} \overset{5.13}{=} (-1)^{\frac{p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}-1}{2}} \\ &= (-1)^{\frac{n-1}{2}}\end{aligned}$$

und also (5.1).

Weiter gilt

$$\begin{aligned}\left(\frac{2}{n}\right) &= \left(\frac{2}{p_1}\right)^{e_1} \cdot \ldots \cdot \left(\frac{2}{p_r}\right)^{e_r} = (-1)^{\frac{p_1^2-1}{8}e_1} \cdot \ldots \cdot (-1)^{\frac{p_r^2-1}{8}e_r} \\ &\overset{5.13}{=} (-1)^{\frac{p_1^{2e_1}-1}{8}} \cdot \ldots \cdot (-1)^{\frac{p_r^{2e_r}-1}{8}} \overset{5.13}{=} (-1)^{\frac{p_1^{2e_1} \cdot \ldots \cdot p_r^{2e_r}-1}{8}} \\ &= (-1)^{\frac{n^2-1}{8}}\end{aligned}$$

und also (5.2).

Es verbleibt (5.3) zu zeigen. Ist hierbei $\operatorname{ggT}(m,n) \neq 1$, so ist $\left(\frac{m}{n}\right) = 0 = \left(\frac{n}{m}\right)$. Im Folgenden sei daher $\operatorname{ggT}(m,n) = 1$ und also $\{p_1,\dots,p_r\} \cap \{q_1,\dots,q_s\} = \emptyset$. Wir erhalten

$$\begin{aligned}\left(\frac{m}{n}\right) &= \left(\frac{m}{p_1}\right)^{e_1} \cdot \ldots \cdot \left(\frac{m}{p_r}\right)^{e_r} = \prod_{i,j} \left(\frac{q_i}{p_j}\right)^{f_i e_j} \overset{5.8}{=} \prod_{i,j} ((-1)^{\frac{q_i-1}{2}\frac{p_j-1}{2}} \left(\frac{p_j}{q_i}\right))^{f_i e_j} \\ &\overset{5.13}{=} \prod_{i,j} (-1)^{\frac{q_i^{f_i}-1}{2}\frac{p_j^{e_j}-1}{2}} \left(\frac{p_j}{q_i}\right)^{e_j f_i} \\ &\overset{5.13}{=} (-1)^{\frac{m-1}{2}\frac{n-1}{2}} \left(\frac{n}{m}\right).\end{aligned}$$

□

Beispiel 5.15. *Wir wollen das Legendre-Symbol* $\left(\frac{273}{307}\right)$ *aus Beispiel 5.11 erneut berechnen, diesmal unter Verwendung des Reziprozitätsgesetzes für das Jacobi-Symbol 5.14. Wegen* $273 \equiv 1 \bmod (4)$ *erhalten wir zunächst*

$$\left(\frac{273}{307}\right) \overset{(5.3)}{=} \left(\frac{307}{273}\right) = \left(\frac{34}{273}\right) = \left(\frac{2}{273}\right)\left(\frac{17}{273}\right).$$

Wegen $273 \equiv 1 \bmod (8)$ *liefert der Zweite Ergänzungssatz (5.2)*

$$\left(\frac{273}{307}\right) = \left(\frac{17}{273}\right).$$

Unter Beachtung von $17 \equiv 1 \bmod (4)$ *erhalten wir*

$$\left(\frac{273}{307}\right) \overset{(5.3)}{=} \left(\frac{273}{17}\right) = \left(\frac{1}{17}\right) = 1.$$

Im Gegensatz zur Rechnung in Beispiel 5.15 brauchten wir hier nicht die Primfaktorzerlegung von 273 *zu bestimmen.*

5.2 Primzahlen mit vorgegebener Restklasse

In diesem Abschnitt untersuchen wir unter Verwendung des Quadratischen Reziprozitätsgesetzes 5.8 und seiner Ergänzungssätze, ob es in einer vorgegebenen Restklasse modulo einer geeigneten ganzen Zahl unendlich viele Primzahlen gibt. Die hier bewiesenen Sätze sind dabei sämtlich Spezialfälle des Primzahlsatzes in arithmetischen Progressionen, den man in der Analytischen Zahlentheorie beweist.

Proposition 5.16. (a) *Es gibt unendlich viele Primzahlen* p *mit* $p \equiv -1 \bmod (3)$.

(b) *Es gibt unendlich viele Primzahlen* p *mit* $p \equiv -1 \bmod (4)$.

Beweis. Nehmen wir zunächst an, es gäbe nur endlich viele Primzahlen p mit $p \equiv -1 \bmod (3)$, etwa $p_1, \ldots, p_n$. Dann ließe sich auch die natürliche Zahl

$$m := 3p_1 \cdot \ldots \cdot p_n - 1$$

definieren. Für diese gälte $3 \nmid m$, $p_1 \nmid m, \ldots, p_n \nmid m$. Für jeden Primteiler q von m wäre somit $q \equiv 1 \bmod (3)$. Im Widerspruch zur Konstruktion von m folgte $m \equiv 1 \bmod (3)$. Es muss also unendlich viele Primzahlen p mit $p \equiv -1 \bmod (3)$ geben und wir haben Behauptung (a) gezeigt. Der Beweis von Behauptung (b) geht komplett analog. □

Proposition 5.17. *Es gibt unendlich viele Primzahlen p mit $p \equiv 1 \bmod (4)$.*

Beweis. Wir nehmen an, es gäbe nur endlich viele Primzahlen p mit $p \equiv 1 \bmod (4)$, etwa $p_1, \ldots, p_n$. Dann ließe sich die natürliche Zahl

$$m := (2p_1 \cdot \ldots \cdot p_n)^2 + 1$$

definieren. Jeder Primteiler q von m wäre ungerade und erfüllte $(2p_1 \cdot \ldots \cdot p_n)^2 \equiv -1 \bmod (q)$. Es gälte also

$$\left(\frac{-1}{q}\right) = 1$$

und nach dem Ersten Ergänzungssatz 5.9 folgte $q \equiv 1 \bmod (4)$. Nach Annahme erhielten wir so $q \in \{p_1, \ldots, p_n\}$. Aufgrund von $q \mid m$ und der Konstruktion von m folgte hieraus $q \mid 1$, was ein Widerspruch zur Primalität von q ist. □

Satz 5.18. *Sei $0 \neq a \in \mathbb{Z}$. Dann gibt es unendlich viele (ungerade) Primzahlen p mit $\left(\frac{a}{p}\right) = 1$.*

Beweis. Wir nehmen an, es gäbe nur endlich viele (ungerade) Primzahlen p mit $\left(\frac{a}{p}\right) = 1$, etwa $p_1, \ldots, p_n$. Dann gäbe es offensichtlich eine ganze Zahl $A \in \mathbb{Z}$ mit den Eigenschaften:

- $\mathrm{ggT}(a, A) = 1$,
- A gerade $\Longleftrightarrow$ a ungerade,
- $N := (p_1 \cdot \ldots \cdot p_n A)^2 - a > 1$.

Da N nach Konstruktion ungerade wäre, träfe dies auch auf jeden Primteiler q von N zu und wegen $p_i \nmid a$ für alle $i = 1, \ldots, n$ wäre $q \notin \{p_1, \ldots, p_n\}$. Wir unterscheiden nun zwei Fälle:

Fall 1: $q \mid a$**.** Dann ergäbe sich $q \mid (N + a) = (p_1 \cdot \ldots \cdot p_n A)^2$ und deshalb $q \mid A^2$. Aufgrund der Primalität von q folgte $q \mid A$, im Widerspruch zu $\mathrm{ggT}(a, A) = 1$.

Fall 2: $q \nmid a$**.** Aufgrund von $(p_1 \cdot \ldots \cdot p_n A)^2 \equiv a \bmod (q)$ folgte dann $\left(\frac{a}{q}\right) = 1$. Somit wäre $q \in \{p_1, \ldots, p_n\}$, was ein Widerspruch ist. □

Proposition 5.19. *Es gibt unendlich viele Primzahlen p mit $p \equiv 1 \bmod (3)$.*

Beweis. Für eine beliebige ungerade Primzahl p gilt

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}\frac{3-1}{2}}\left(\frac{p}{3}\right) = (-1)^{p-1}\left(\frac{p}{3}\right) = \left(\frac{p}{3}\right).$$

Insbesondere gilt für ungerade Primzahlen p die Äquivalenz

$$p \equiv 1 \bmod (3) \iff \left(\frac{p}{3}\right) = 1 \iff \left(\frac{-3}{p}\right) = 1.$$

Die Proposition folgt, da es nach Satz 5.18 unendlich viele Primzahlen p mit $\left(\frac{-3}{p}\right) = 1$ gibt. □

Satz 5.20. *Es sei $a \in \mathbb{Z}$ kein Quadrat. Dann gibt es unendlich viele (ungerade) Primzahlen p mit $\left(\frac{a}{p}\right) = -1$.*

Beweis. Wir unterscheiden für den Beweis des Satzes vier Fälle:

Fall 1: $a = -1$**.** Nach dem Ersten Ergänzungssatz 5.9 ist

$$\left(\frac{-1}{p}\right) = -1 \iff p \equiv -1 \bmod (4).$$

Die Behauptung in diesem Fall ergibt sich somit, da es nach Proposition 5.16 unendlich viele Primzahlen p mit $p \equiv -1 \bmod (4)$ gibt.

Fall 2: $a = 2$**.** Nach dem Zweiten Ergänzungssatz 5.10 ist

$$\left(\frac{2}{p}\right) = -1 \iff p \equiv \pm 3 \bmod (8).$$

Wir nehmen an, es gäbe nur endlich viele Primzahlen p mit $p \equiv \pm 3 \bmod (8)$, etwa $p_1 = 3, p_2, \ldots, p_n$. Dann ließe sich auch die natürliche Zahl

$$N := 8p_2 \cdot \ldots \cdot p_n + 3$$

definieren. Diese wäre nach Konstruktion größer als 1, ungerade und durch keine der Primzahlen $p_1, \ldots, p_n$ teilbar. Insbesondere hätte N nur Primteiler, welche modulo 8 kongruent zu ± 1 wären. Hieraus folgte jedoch $N \equiv \pm 1 \bmod (8)$, was im Widerspruch zu $N \equiv 3 \bmod (8)$ stünde. Es folgt, dass es unendlich viele Primzahlen p mit $p \equiv 3 \bmod (8)$ und also die Behauptung in diesem Fall.

Fall 3: $a = -2$**.** Mit den Ergänzungssätzen 5.9 und 5.10 gilt

$$\begin{aligned}
&\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = -1 \\
\iff &\left(p \equiv 1 \bmod (4) \text{ und } p \equiv \pm 3 \bmod (8)\right) \text{ oder } \left(p \equiv 3 \bmod (4) \text{ und } p \equiv \pm 1 \bmod (8)\right) \\
\iff &p \equiv 5 \bmod (8) \text{ oder } p \equiv 7 \bmod (8).
\end{aligned}$$

Wir nehmen an, es gäbe nur endlich viele Primzahlen p mit $p \equiv 5 \bmod (8)$ oder $p \equiv 7 \bmod (8)$, etwa $p_1 = 5, p_2, \ldots, p_n$. Dann ließe sich auch die natürliche Zahl

$$N := 8p_2 \ldots p_n + 5.$$

definieren. Diese wäre nach Konstruktion größer als 1, ungerade und durch keine der Primzahlen $p_1, \ldots, p_n$ teilbar. Insbesondere hätte N nur Primteiler, welche modulo 8 kongruent zu 1 oder 3 wären. Hieraus folgte jedoch $N \equiv 1 \bmod (8)$ oder $N \equiv 3 \bmod (8)$, im Widerspruch zu $N \equiv 5 \bmod (8)$. Damit gibt es unendlich viele Primzahlen p mit $p \equiv 3 \bmod (8)$ oder $p \equiv 7 \bmod (8)$, was die Behauptung in diesem Fall liefert.

Fall 4: $a \notin \{-1, \pm 2\}$**.** Da sich $(\frac{a}{p})$ sich bei Abänderung von a um Quadrate höchstens bei endlich vielen Primzahlen p ändert – nämlich bei den Primteilern von a – können wir ohne Einschränkung annehmen, es gelte

$$a = (-1)^{\varepsilon} 2^{e} q_1 \cdot \ldots \cdot q_n$$

mit paarweise verschiedenen ungeraden Primzahlen $q_1, \ldots, q_n$, $n \geq 1$ sowie $e, \varepsilon \in \{0, 1\}$. Wir nehmen an, es gäbe nur endlich viele Primzahlen p mit $(\frac{a}{p}) = -1$, etwa $p_1, \ldots, p_m$. Für diese gälte insbesondere $\{q_1, \ldots, q_n\} \cap \{p_1, \ldots, p_m\} = \emptyset$. Zu jedem quadratischen Nichtrest $\alpha \in \mathbb{Z}$ modulo q_n existierte nach dem Chinesischen Restsatz 3.75 ein $N \in \mathbb{N}$ mit

$$\begin{aligned} &N \equiv 1 \bmod (8), N \equiv 1 \bmod (p_1), \ldots, N \equiv 1 \bmod (p_m), \\ &N \equiv 1 \bmod (q_1), \ldots, N \equiv 1 \bmod (q_{n-1}), N \equiv \alpha \bmod (q_n). \end{aligned}$$

Schreiben wir N in der Form $N = \ell_1 \cdot \ldots \cdot \ell_r$ mit ungeraden, nicht notwendig paarweise verschiedenen Primzahlen $\ell_1, \ldots, \ell_r$, so gälte offenbar $\{\ell_1, \ldots, \ell_r\} \cap \{2, p_1, \ldots, p_m, q_1, \ldots, q_n\} = \emptyset$. Unter Verwendung von $N \equiv 1 \bmod (8)$ erhielten wir aus dem Reziprozitätsgesetz für das Jacobi-Symbol 5.14:

$$\begin{aligned} \prod_{i=1}^{r} \left(\frac{a}{\ell_i}\right) = \left(\frac{a}{N}\right) &= \left(\frac{-1}{N}\right)^{\varepsilon} \left(\frac{2}{N}\right)^{e} \left(\frac{q_1 \cdot \ldots \cdot q_n}{N}\right) = (-1)^{\frac{N-1}{2}\varepsilon} (-1)^{\frac{N^2-1}{8}e} \left(\frac{N}{q_1 \cdot \ldots \cdot q_n}\right) \\ &= \left(\frac{N}{q_1}\right) \cdot \ldots \cdot \left(\frac{N}{q_n}\right) = \left(\frac{1}{q_n}\right) \cdot \ldots \cdot \left(\frac{1}{q_{n-1}}\right) \left(\frac{\alpha}{q_n}\right) = \left(\frac{\alpha}{q_n}\right) = -1 \end{aligned}$$

Aus diesem Grund existierte ein $i \in \{1, \ldots, r\}$ mit $\left(\frac{a}{\ell_i}\right) = -1$. Wegen $\ell_i \notin \{p_1, \ldots, p_m\}$ ist das ein Widerspruch. □

5.3 Summen von Quadraten

In diesem Abschnitt beschäftigen wir uns mit der Frage, welche natürlichen Zahlen sich als Summe von zwei bzw. vier Quadratzahlen schreiben lassen, und lösen also für alle $n \in \mathbb{N}$ die – schon in der Antike untersuchten – diophantischen Gleichungen

$$\begin{aligned} n &= X_1^2 + X_2^2, \\ n &= X_1^2 + X_2^2 + X_3^2 + X_4^2. \end{aligned}$$

Dass diese Fragen interessant sind, zeigt bereits das folgende Beispiel:

Beispiel 5.21. *Aufgrund von* $2 = 1^2 + 1^2$, $4 = 2^2 + 0^2$ *und* $5 = 1^2 + 2^2$ *lassen sich* 2, 4 *und* 5 *als Summe zweier Quadrate schreiben, während das für die Zahl* 3 *nicht möglich ist.*

Proposition 5.22 (Lemma von Thue)**.** *Seien p eine Primzahl und $e, f \in \mathbb{N}$ mit $ef > p$. Dann gibt es für jedes $r \in \mathbb{Z}$ ganze Zahlen $x, y \in \mathbb{Z}$ mit $0 \leq x < e$, $1 \leq y < f$, $p \nmid y$ und*

$$r \equiv \pm\frac{x}{y} \bmod (p).$$

Beweis. Sei $r \in \mathbb{Z}$. Wir unterscheiden drei Fälle:

Fall 1: $e \geq p$**.** Wir setzen $y := 1$ und x als den Rest, den r bei Division durch p lässt. Dann gilt

$$r \equiv x = \frac{x}{y} \bmod (p)$$

und wir haben die Proposition in diesem Fall gezeigt.

Fall 2: $f \geq p$**.** Gilt $p \mid r$, so setzen wir $x := 0$ und $y := 1$. Dann gilt

$$r \equiv 0 = \frac{x}{y} \bmod (p).$$

Gilt $p \nmid r$, so setzen wir $x := 1$ und y sei ein Vertreter aus $\{1, \ldots, p-1\}$ der Restklasse $\overline{r}^{-1}$. Dann gilt

$$r \equiv \frac{1}{\frac{1}{r}} \equiv \frac{x}{y} \bmod (p),$$

was die Proposition in diesem Fall zeigt.

Fall 3: $e, f < p$**.** Wir betrachten die Menge

$$M := \{1, \ldots, e\} \times \{1, \ldots, f\}.$$

Für diese gilt $\#M = ef > p$, so dass es nach dem Schubfachprinzip $(x_1, y_1) \neq (x_2, y_2) \in M$ mit

$$y_1 r - x_1 \equiv y_2 r - x_2 \bmod (p)$$

gibt. Wäre $y_1 \equiv y_2 \bmod (p)$, so folgte $x_1 - x_2 \equiv r(y_1 - y_2) \equiv 0 \bmod (p)$. Wegen $e, f < p$ ergäbe sich dann $x_1 = x_2$ und $y_1 = y_2$, was ein Widerspruch ist. Also ist $y_1 - y_2 \not\equiv 0 \bmod (p)$ und deshalb

$$r \equiv \frac{x_1 - x_2}{y_1 - y_2} \equiv \pm\frac{|x_1 - x_2|}{|y_1 - y_2|} \bmod (p).$$

Mit $x := |x_1 - x_2|$ und $y := |y_1 - y_2|$ folgt die Proposition auch in diesem letzten Fall. □

Satz 5.23 (Fermat'scher Quadratesatz)**.** *Für eine ungerade Primzahl p sind die folgenden beiden Aussagen äquivalent:*

(i) *Die Zahl p lässt sich als Summe von zwei Quadraten schreiben.*

(ii) $p \equiv 1 \bmod (4)$.

Beweis. Gelte zunächst Aussage (i) und sei also $p = x^2 + y^2$ mit $x, y \in \mathbb{Z}$. Insbesondere gilt dann $p \equiv x^2 + y^2 \bmod (4)$. Wegen $x^2 \equiv 0, 1 \bmod (4)$ und $y^2 \equiv 0, 1 \bmod (4)$ folgt hieraus $p \equiv 0, 1, 2 \bmod (4)$. Da p ungerade ist, ergibt sich $p \equiv 1 \bmod (4)$ und also Aussage (ii).

Gelte nun umgekehrt Aussage (ii) und sei also $p \equiv 1 \bmod (4)$. Nach dem Ersten Ergänzungssatz 5.9 ist dann -1 ein quadratischer Rest modulo p, so dass es ein $r \in \mathbb{Z}$ mit $r^2 \equiv -1 \bmod (p)$ gibt. Wir setzen

$$e := f := \lfloor \sqrt{p} \rfloor + 1.$$

Offenbar ist dann $ef > p$ und nach dem Lemma von Thue 5.22 existieren $x, y \in \mathbb{Z}$ mit $0 \leq x < e$, $1 \leq y < f$, $p \nmid y$ und

$$r \equiv \pm \frac{x}{y} \bmod (p).$$

Das liefert

$$-1 \equiv r^2 \equiv \frac{x^2}{y^2} \bmod (p)$$

und also $x^2 + y^2 \equiv 0 \bmod (p)$. Aufgrund von $x < e = \lfloor \sqrt{p} \rfloor + 1$ folgt $x < \sqrt{p}$ und also $x^2 < p$. Analog gilt $y^2 < p$. Wegen $0 < x^2 + y^2 < 2p$ folgt $x^2 + y^2 = p$ und somit Aussage (i). □

Satz 5.24 (Zwei-Quadrate-Satz)**.** *Für eine natürliche Zahl n sind die folgenden beiden Aussagen äquivalent:*

(i) *Die Zahl n lässt sich als Summe von zwei Quadraten schreiben.*

(ii) *In der Primfaktorzerlegung von n kommen die Primzahlen p mit $p \equiv 3 \bmod (4)$ nur mit geradem Exponenten vor.*

Beweis. Dass Aussage (i) Aussage (ii) impliziert, zeigen wir indirekt. Wir gehen also davon aus, dass Aussage (ii) verletzt ist, und dass gleichzeitig $n = x^2 + y^2$ für geeignete $x, y \in \mathbb{Z}$ ist. Insbesondere gibt es eine Primzahl p mit $p \equiv 3 \bmod (4)$ und ein $k \in \mathbb{N}_0$, so dass $n = mp^{2k+1}$ mit $p \nmid m$ ist. Aus $x^2 + y^2 = mp^{2k+1}$ ergibt sich $x^2 \equiv -y^2 \bmod (p)$. Gilt $p \mid y$, so folgt $p \mid x^2 = mp^{2k+1} - y^2$, und weil p eine Primzahl ist, folgt $p \mid x$. Es ergibt sich $p^2 \mid (x^2 + y^2) = n$ und

$$\left(\frac{x}{p}\right)^2 + \left(\frac{y}{p}\right)^2 = \frac{n}{p^2} = mp^{2(k-1)+1}.$$

Wir ersetzen dann x durch $\frac{x}{p}$, y durch $\frac{y}{p}$, n durch $\frac{n}{p^2}$ und k durch $k - 1$. Indem wir dieses Argument gegebenfalls mehrfach anwenden, können wir schließlich erreichen, dass zuätzlich $p \mid y$ gilt – das Verfahren bricht ab, weil spätestens bei $k = 0$ der Fall $p \mid y$ zum Widerspruch $p^2 \mid n$ führt. Aus $x^2 \equiv -y^2 \bmod (p)$ folgt dann

$$\left(\frac{x}{y}\right)^2 \equiv -1 \bmod (p),$$

was einen Widerspruch zu $p \equiv 3 \bmod (4)$ darstellt.

Wir zeigen nun umgekehrt, dass Aussage (ii) auch Aussage (i) impliziert. Wir bemerken dafür zunächst, dass sich mit zwei Zahlen $m_1 = a^2 + b^2$, $m_2 = c^2 + d^2$ mit $a, b, c, d \in \mathbb{Z}$ auch deren Produkt $m_1 m_2$ als Summe von zwei Quadraten darstellen lässt:

$$m_1 m_2 = (a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2.$$

Nach Voraussetzung ist

$$n = 2^e p_1^{2f_1} \cdot \ldots \cdot p_r^{2f_r} q_1^{g_1} \cdot \ldots \cdot q_s^{g_s},$$

wobei $p_1, \ldots, p_r$ paarweise verschiedene Primzahlen mit $p_i \equiv 3 \bmod (4)$ sind, und $q_1, \ldots, q_s$ sind paarweise verschiedene Primzahlen mit $q_i \equiv 1 \bmod (4)$. Wir setzen $n_1 := 2^e q_1^{g_1} \cdot \ldots \cdot q_s^{e_s}$. Wegen $2 = 1^2 + 1^2$ und dem Fermat'schen Quadratesatz 5.23, zusammen mit unserer Vorüberlegung, ist $n_1 = a^2 + b^2$ für geeignete $a, b \in \mathbb{Z}$. Wir setzen $n_2 := p_1^{f_1} \cdot \ldots \cdot p_r^{f_r}$. Es ergibt sich

$$n = n_1 n_2^2 = (a^2 + b^2) n_2^2 = (n_2 a)^2 + (n_2 b)^2.$$

□

Satz 5.25 (Satz von Lagrange)**.** *Jede natürliche Zahl lässt sich als Summe von vier Quadraten schreiben.*

Beweis. Wir bemerken zunächst, dass für $x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4 \in \mathbb{Z}$ die Gleichung

$$\begin{aligned}(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) =& (x_1 y_1 - x_2 y_2 + x_3 y_3 - x_4 y_4)^2 \\ &+ (x_1 y_2 + x_2 y_1 + x_3 y_4 - x_4 y_3)^2 \\ &+ (x_1 y_3 + x_3 y_1 - x_2 y_4 + x_4 y_2)^2 \\ &+ (x_1 y_4 + x_4 y_1 + x_2 y_3 - x_3 y_2)^2\end{aligned}$$

gilt. Aufgrunddessen und wegen $2 = 1^2 + 1^2 + 0^2 + 0^2$ genügt es zu zeigen, dass sich jede ungerade Primzahl als Summe von vier Quadraten schreiben lässt.

Die Gleichung $x^2 + y^2 \equiv -1 \bmod (p)$ besitzt eine Lösung,

denn: Es ist

$$x^2 + y^2 \equiv -1 \bmod (p) \quad \Longleftrightarrow \quad y^2 \equiv -1 - x^2 \bmod (p).$$

Nach Proposition 5.3 gibt es zusammen mit 0 genau $\frac{p+1}{2}$ Quadrate modulo p und genauso viele Restklassen der Form $-1 - x^2$ modulo p. Da es nur $\frac{p-1}{2}$ Nichtquadrate modulo p gibt, ist unter den $\frac{p+1}{2}$ Restklassen der Form $-1 - x^2$ modulo p mindestens ein Quadrat modulo p. Somit existieren $x, y \in \mathbb{Z}$ mit $y^2 \equiv -1 - x^2 \bmod (p)$. #

Es folgt, dass die Gleichung

$$X_1^2 + X_2^2 + X_3^2 + X_4^2 \equiv 0 \bmod (p)$$

eine Lösung des Typs $(x, y, 1, 0)$ mit $x, y \in \mathbb{Z}$ besitzt. Hierbei können x, y so gewählt werden, dass $|x|, |y| \leq \frac{p}{2}$ sind. Dann ist

$$x^2 + y^2 + 1^2 + 0^2 \leq \frac{p^2}{4} + \frac{p^2}{4} + 1 < p^2.$$

Zusammenfassend stellen wir fest, dass es $x_1, x_2, x_3, x_4 \in \mathbb{Z}$ und $k \in \mathbb{N}$ mit $k < p$ gibt, so dass

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = kp$$

ist. Ist $k = 1$, so sind wir fertig. Ist $k > 1$, so werden wir zeigen, dass man $x_1, \ldots, x_4$ so verändern kann, dass die Gleichung auch mit kleinerem k gilt. Durch endliche Wiederholung dieses Schrittes kann man schließlich $k = 1$ erreichen, was die Behauptung liefert. Wir unterscheiden hierbei zwei Fälle:

Fall 1: k ist gerade. Dann ist auch $kp = x_1^2 + x_2^2 + x_3^2 + x_4^2$ und somit eine gerade Anzahl der x_i gerade. Wir nummerieren die x_i so um, dass x_1 und x_2 sowie x_3 und x_4 jeweils dieselbe Parität haben. Dann ist

$$\left(\frac{x_1 + x_2}{2}\right)^2 + \left(\frac{x_1 - x_2}{2}\right)^2 + \left(\frac{x_3 + x_4}{2}\right)^2 + \left(\frac{x_3 - x_4}{2}\right)^2 = \frac{k}{2}p.$$

Fall 2: k ist ungerade. Wir wählen $y_1, \ldots, y_4 \in \mathbb{Z}$ mit

$$y_1 \equiv -x_1 \bmod (k),\ y_2 \equiv x_2 \bmod (k),\ y_3 \equiv x_3 \bmod (k),\ y_4 \equiv x_4 \bmod (k)$$

und $|y_i| < \frac{k}{2}$ für $i = 1, \ldots, 4$. Dann gilt

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 < 4\frac{k^2}{4} = k^2.$$

Darüber hinaus ist

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \bmod (k),$$

weswegen ein $\tilde{k} \in \mathbb{N}_0$ mit $0 \leq \tilde{k} < k$ und

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 = \tilde{k}k$$

existiert. Hierbei ist $\tilde{k} \neq 0$,

denn: Wir nehmen an, es gälte $\tilde{k} = 0$. Dann folgte $y_1 = y_2 = y_3 = y_4 = 0$ und also $x_i \equiv 0 \bmod (k)$ für alle $i = 1, \ldots, 4$. Das lieferte $x_i^2 \equiv 0 \bmod (k^2)$ für alle $i = 1, \ldots, 4$ und also

$$0 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv kp \bmod (k^2).$$

Im Widerspruch zu $1 < k < p$ folgte hieraus $k \mid p$. #

Aufgrund unserer Vorüberlegung ist nun

$$k^2\tilde{k}p = kp\tilde{k}k = \left(x_1^2 + x_2^2 + x_3^2 + x_4^2\right)\left(y_1^2 + y_2^2 + y_3^2 + y_4^2\right) = a_1^2 + a_2^2 + a_3^2 + a_4^2$$

mit

$$\begin{aligned}
a_1 &= x_1y_1 - x_2y_2 + x_3y_3 - x_4y_4,\\
a_2 &= x_1y_2 + x_2y_1 + x_3y_4 - x_4y_3 \equiv x_1x_2 + x_2(-x_1) + x_3x_4 - x_4x_3 \equiv 0 \bmod (k),\\
a_3 &= x_1y_3 + x_3y_1 - x_2y_4 + x_4y_2 \equiv x_1x_3 + x_3(-x_1) - x_2x_4 + x_4x_2 \equiv 0 \bmod (k),\\
a_4 &= x_1y_4 + x_4y_1 + x_2y_3 - x_3y_2 \equiv x_1x_4 + x_4(-x_1) + x_2x_3 - x_3x_2 \equiv 0 \bmod (k).
\end{aligned}$$

Hieraus ergibt sich $k^2 \mid \left(k^2\tilde{k}p - a_2^2 - a_3^2 - a_4^2\right) = a_1^2$. Wir erhalten

$$\left(\frac{a_1}{k}\right)^2 + \left(\frac{a_2}{k}\right)^2 + \left(\frac{a_3}{k}\right)^2 + \left(\frac{a_4}{k}\right)^2 = \tilde{k}p$$

mit $1 \leq \tilde{k} < k$. □

5.4 Der Primzahltest von Solovay-Strassen

In diesem Abschnitt suchen wir einen Algorithmus, der testet, ob eine vorgegebene Zahl eine Primzahl ist. Die naive Methode – die Methode der Probedivisionen – geht von der Definition einer Primzahl aus und testet bei Vorgabe einer Zahl n für alle (Prim-) Zahlen $x \leq \sqrt{n}$, ob $x \mid n$ gilt. Es ist offensichtlich, dass diese Methode für große Zahlen n nicht praktikabel ist. Um effizientere Verfahren zu erhalten, benötigen wir geeignete Primzahlkriterien. Hierfür betrachten wir die bisher bewiesenen Sätze über Primzahlen und fragen, ob sich diese in geeigneter Weise umkehren und zur Charakterisierung von Primzahlen verwenden lassen.

Der erste Satz, mit dessen Umkehrung wir uns beschäftigen werden, ist der Kleine Satz von Fermat 3.32: Ist p eine Primzahl, so gilt $\overline{a}^{p-1} = \overline{1}$ für alle $\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^\times$. Es stellt sich leider heraus, dass man diese Eigenschaft nicht zur Charakterisierung von Primzahlen verwenden kann. Es ist allerdings von Interesse, für welche Zahlen die Umkehrung schiefgeht:

Definition 5.26. *Eine natürliche Zahl n mit $n > 1$ heißt eine **Carmichael-Zahl**, wenn n keine Primzahl ist und für alle $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$ die Gleichung $\overline{a}^{n-1} = \overline{1}$ gilt.*

Proposition 5.27. *Für ein beliebiges $n \in \mathbb{N}$ mit $n > 1$ sind die folgenden Aussagen äquivalent:*

(i) *Die Zahl n ist eine Carmichael-Zahl.*

(ii) *Die Zahl n ist von der Form $n = p_1 \cdot \ldots \cdot p_r$ mit einem $r \geq 3$ und paarweise verschiedenen ungeraden Primzahlen $p_1, \ldots, p_r$ mit $(p_i - 1) \mid (n-1)$ für alle $i = 1, \ldots, r$.*

Beweis. Gelte zunächst Aussage (i), sei also n eine Carmichael-Zahl und gelte $\overline{a}^{n-1} = \overline{1}$ für alle $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$. Insbesondere gilt dann $\operatorname{ord}(\overline{a}) \mid (n-1)$ für alle $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$. Das liefert

$$\exp((\mathbb{Z}/n\mathbb{Z})^\times) = \operatorname{kgV}\big(\operatorname{ord}(\overline{a}) : \overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times\big) \mid (n-1).$$

Wir schreiben n in der Form $n = 2^a p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$ mit paarweise verschiedenen ungeraden Primzahlen $p_1, \ldots, p_r$ für ein geeignetes $r \in \mathbb{N}_0$ und mit $e_1, \ldots, e_r \in \mathbb{N}$ sowie $a \in \mathbb{N}_0$. Dann ist

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong \begin{cases} \mathbb{Z}/\big(p_1^{e_1-1}(p_1-1)\big)\mathbb{Z} \times \ldots \times \mathbb{Z}/\big(p_r^{e_r-1}(p_r-1)\big)\mathbb{Z} & \text{für } a = 0, 1, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{a-2}\mathbb{Z} \times \mathbb{Z}/\big(p_1^{e_1-1}(p_1-1)\big)\mathbb{Z} \times \ldots \times \mathbb{Z}/\big(p_r^{e_r-1}(p_r-1)\big)\mathbb{Z} & \text{für } a \geq 2. \end{cases}$$

Die Zahl n ist ungerade,

denn: Im Fall $a = 1$ gilt $r \geq 1$, denn $n = 2$ ist keine Carmichael-Zahl. Nach Proposition 3.43 gilt $p_1^{e_1-1}(p_1-1) \mid \exp((\mathbb{Z}/n\mathbb{Z})^\times)$ und deshalb auch $p_1^{e_1-1}(p_1-1) \mid (n-1)$. Weil p_1 ungerade ist, muss somit auch n ungerade sein. Im Fall $a \geq 2$ ergibt sich mittels Proposition 3.43 die Teilbarkeitsbeziehung $2 \mid \exp((\mathbb{Z}/n\mathbb{Z})^\times)$ und hieraus auch $2 \mid (n-1)$. Wieder folgt, dass n ungerade ist. #

Für alle $i = 1, \ldots, r$ gilt $e_i = 1$ und $(p_i - 1) \mid (n-1)$,

denn: Sei $i \in \{1, \ldots, r\}$. Nach Proposition 3.43 gilt dann $p_i^{e_i-1}(p_i-1) \mid (n-1)$. Wäre $e_i > 1$, so folgte $p_i \mid (n-1)$, was wegen $p_i \mid n$ zu $p_i \mid 1$ führen würde. #

Es ist $r \geq 3$,

denn: Da n als Carmichael-Zahl keine Primzahl ist, gilt $r \geq 2$. Nehmen wir an, es gälte $r = 2$, so dass n von der Form $n = p_1 p_2$ mit ungeraden Primzahlen p_1, p_2 wäre, wobei wir ohne Einschränkung $p_1 < p_2$ annehmen. Wie wir uns bereits überlegt haben, gilt $n - 1 \equiv 0 \bmod (p_2 - 1)$. Darüber hinaus ist

$$n - 1 = p_1 p_2 - 1 = p_1(p_2 - 1) + p_1 - 1 \equiv p_1 - 1 \bmod (p_2 - 1).$$

Das liefert $p_1 - 1 \equiv 0 \bmod (p_2 - 1)$, also $(p_2 - 1) \mid (p_1 - 1)$, im Widerspruch zu $1 < p_1 - 1 < p_2 - 1$. #

Es ergibt sich Aussage (ii).

Gelte nun umgekehrt Aussage (ii) und sei also $n = p_1 \cdot \ldots \cdot p_r$ mit einem $r \geq 3$ und paarweise verschiedenen ungeraden Primzahlen $p_1, \ldots, p_r$ mit $(p_i - 1) \mid (n-1)$ für alle $i = 1, \ldots, r$. Dann gilt

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1\mathbb{Z})^\times \times \ldots \times (\mathbb{Z}/p_r\mathbb{Z})^\times \cong \mathbb{Z}/(p_1-1)\mathbb{Z} \times \ldots \times \mathbb{Z}/(p_r-1)\mathbb{Z}.$$

Mittels Proposition 3.43 erhalten wir

$$\exp((\mathbb{Z}/n\mathbb{Z})^\times) = \operatorname{kgV}\big(p_i - 1 : i = 1, \ldots, r\big) \mid (n-1).$$

Das liefert $\overline{a}^{n-1} = \overline{1}$ für alle $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$, weshalb n eine Carmichael-Zahl ist. □

Beispiel 5.28. *Die kleinsten Carmichael-Zahlen sind* $561 = 3 \cdot 11 \cdot 17$, $1105 = 5 \cdot 13 \cdot 17$ *sowie* $1729 = 7 \cdot 13 \cdot 19$.

Nach dem erst 1994 bewiesenen Satz von Alford-Granville-Pomerance gibt es unendlich viele Carmichael-Zahlen. Genauer gilt: Für $x \gg 0$ ist

$$\#\{n \in \mathbb{N} : n \leq x, n \text{ ist Carmichael-Zahl}\} > x^{\frac{2}{7}}.$$

Der nächste Satz, mit dessen Umkehrung wir uns beschäftigen, ist der Satz von Euler 5.5. Wie sich herausstellt, kann dieser tatsächlich zur Charakterisierung von Primzahlen verwendet werden:

Satz 5.29. *Für ein beliebiges ungerades $n \in \mathbb{N}$ mit $n > 1$ sind die folgenden beiden Aussagen äquivalent:*

(i) *n ist eine Primzahl.*

(ii) *Für alle $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$ gilt*
$$\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \bmod (n).$$

Beweis. Dass Aussage (i) Aussage (ii) impliziert, ist gerade der Satz von Euler 5.5.

Zum Beweis der umgekehrten Implikation nehmen wir nun an, es gelte Aussage (ii) und also

$$\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \bmod (n) \qquad \text{für alle } \overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times.$$

Durch Quadrieren ergibt sich hieraus

$$\overline{a}^{n-1} = \overline{1} \qquad \text{für alle } \overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times.$$

Somit ist n eine Primzahl oder eine Carmichael-Zahl. Die Zahl n ist jedoch keine Carmichael-Zahl,

denn: Angenommen, n wäre eine Carmichael-Zahl. Nach Proposition 5.27 wäre n dann von der Form

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

mit einem $r \geq 3$ und paarweise verschiedenen ungeraden Primzahlen $p_1, \ldots, p_r$. Für ein beliebiges Nichtquadrat $\alpha \in \mathbb{Z}$ modulo p_1 existierte dann nach dem Chinesischen Restsatz 3.75 ein $b \in \mathbb{Z}$ mit

$$b \equiv \alpha \bmod (p_1),\ b \equiv 1 \bmod (p_2),\ \ldots,\ b \equiv 1 \bmod (p_r).$$

Es folgte

$$\left(\frac{b}{n}\right) = \left(\frac{b}{p_1}\right)\left(\frac{b}{p_2}\right) \cdot \ldots \cdot \left(\frac{b}{p_n}\right) = (-1) \cdot 1 \cdot \ldots \cdot 1 = -1.$$

Nach Konstruktion wäre $\overline{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$ und nach Voraussetzung gälte

$$\left(\frac{b}{n}\right) \equiv b^{\frac{n-1}{2}} \bmod (n).$$

Das lieferte

$$b^{\frac{n-1}{2}} \equiv -1 \bmod (n)$$

und somit insbesondere

$$b^{\frac{n-1}{2}} \equiv -1 \bmod (p_2),$$

was im Widerspruch zu

$$b^{\frac{n-1}{2}} \equiv 1 \bmod (p_2)$$

steht. #

Damit haben wir gezeigt, dass n eine Primzahl ist. □

Definition 5.30. *Seien $n \in \mathbb{N}$ ungerade mit $n > 1$ und $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$. Die Zahl a heißt ein **Euler'scher Zeuge für die Zerlegbarkeit** von n, wenn*

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

ist. Wir setzen

$$E_n := \{\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times : a \text{ ist Eulerscher Zeuge für die Zerlegbarkeit von } n\}.$$

Nach Satz 5.29 ist eine ungerade Zahl $n \in \mathbb{N}$ mit $n > 1$ genau dann eine Primzahl, wenn $E_n = \emptyset$ gilt, es also keine Euler'schen Zeugen für die Zerlegbarkeit von n gibt.

Proposition 5.31. *Sei $1 < n \in \mathbb{N}$ ungerade keine Primzahl. Dann gilt:*

$$|E_n| \geq \frac{1}{2}|(\mathbb{Z}/n\mathbb{Z})^\times| = \frac{\varphi(n)}{2}.$$

Mindestens die Hälfte aller Restklassen aus $(\mathbb{Z}/n\mathbb{Z})^\times$ liefert also Euler'sche Zeugen für die Zerlegbarkeit von n.

Beweis. Da n keine Primzahl ist, existiert nach Satz 5.29 ein $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$ mit $\overline{a} \in E_n$. Wir setzen

$$\widehat{E_n} := (\mathbb{Z}/n\mathbb{Z})^\times \setminus E_n.$$

und

$$M := \{\overline{a}\overline{b} : \overline{b} \in \widehat{E_n}\}.$$

Es gilt $\#M = \#\widehat{E_n}$, denn für $\overline{b_1}, \overline{b_2} \in \widehat{E_n}$ gilt $\overline{a}\overline{b_1} = \overline{a}\overline{b_2}$ genau dann, wenn $\overline{b_1} = \overline{b_2}$ ist. Darüber hinaus gilt $M \cap \widehat{E_n} = \emptyset$,

denn: Angenommen, es gäbe ein $\overline{c} \in M \cap \widehat{E_n}$. Dann wäre $\overline{c}$ von der Form $\overline{c} = \overline{a}\overline{b}$ für ein $\overline{b} \in \widehat{E_n}$. Das lieferte

$$\overline{a} = \overline{c}\overline{b}^{-1} = \overline{c}\overline{b}^{\varphi(n)-1} = \overline{cb^{\varphi(n)-1}}$$

und deshalb wegen $\overline{c}, \overline{b} \in \widehat{E_n}$

$$\left(\frac{a}{n}\right) = \left(\frac{cb^{\varphi(n)-1}}{n}\right) = \left(\frac{c}{n}\right)\left(\frac{b}{n}\right)^{\varphi(n)-1} \equiv c^{\frac{n-1}{2}}(b^{\frac{n-1}{2}})^{\varphi(n)-1} \equiv (cb^{\varphi(n)-1})^{\frac{n-1}{2}} \equiv a^{\frac{n-1}{2}} \bmod (n),$$

was $a \in \widehat{E_n}$ zur Folge hätte, was ein Widerspruch ist. #

Wir erhalten

$$\#\widehat{E_n} = \frac{1}{2}\#(\widehat{E_n} \cup M) \leq \frac{1}{2}|(\mathbb{Z}/n\mathbb{Z})^\times| = \frac{\varphi(n)}{2}$$

und somit

$$\#E_n \geq \frac{1}{2}|(\mathbb{Z}/n\mathbb{Z})^\times| = \frac{\varphi(n)}{2}.$$

□

Algorithmus 5.32 (Primzahltest von Solovay-Strassen, 1977)**.** *Es soll getestet werden, ob die ungerade natürliche Zahl $n > 1$ eine Primzahl ist.*

(1) Wähle zufällig Zahlen $a_1, \ldots, a_r$ mit $\mathrm{ggT}(a_i, n) = 1$ für alle $i = 1, \ldots, r$.

(2) Bestimme für $i = 1, \ldots, r$, ob a_i ein Eulerscher Zeuge für die Zerlegbarkeit von n ist.

(3) Falls eines der a_i ein Eulerscher Zeuge für die Zerlegbarkeit von n ist, so gib aus: „n ist keine Primzahl“. Andernfalls gib aus: „n ist vermutlich eine Primzahl“.

Ist n keine Primzahl, so gilt für die Wahrscheinlichkeit W, dass die Ausgabe „n ist vermutlich eine Primzahl“ lautet, die Abschätzung $W \leq \frac{1}{2^r}$.

Die Korrektheit des Algorithmus, falls die Ausgabe „n ist keine Primzahl“ lautet, ergibt sich aus Satz 5.29; die Abschätzung für die Wahrscheinlichkeit W folgt unmittelbar aus Proposition 5.31.

Beim Primzahltest von Solovay-Strassen handelt es sich um einen *probabilistischen* Primzahltest. Für die Praxis ist das durchaus akzeptabel, denn selbst ein deterministischer Primzahltest wird, wenn er auf einem Computer implementiert ist, aufgrund der Möglichkeit von Hardware- und Softwarefehlern eine gewisse Fehlerwahrscheinlichkeit aufweisen. In der Praxis wählt man den Parameter r „hinreichend groß“.

Beispiel 5.33. *Es sei $n = 73$. Wir wählen $r = 2$, $a_1 = 3$, $a_2 = 5$. Dann gilt*

$$a_1^{\frac{n-1}{2}} = 3^{36} \equiv 1 \bmod (73), \qquad \left(\frac{a_1}{n}\right) = \left(\frac{3}{73}\right) = \left(\frac{73}{3}\right) = \left(\frac{1}{3}\right) = 1,$$

$$a_2^{\frac{n-1}{2}} = 5^{36} \equiv -1 \bmod (73), \qquad \left(\frac{a_2}{n}\right) = \left(\frac{5}{73}\right) = \left(\frac{73}{5}\right) = \left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{-1}{3}\right) = -1.$$

Somit sind $a_1 = 3$, $a_2 = 5$ keine Euler'schen Zeugen für die Zerlegbarkeit von n. Die Ausgabe des Solovay-Strassen-Tests lautet: $n = 73$ ist vermutlich eine Primzahl.

Ganz ähnlich wie den Primzahltest von Solovay-Strassen 5.32 lässt sich auch der Miller-Rabin-Test herleiten, der in der Durchführung etwas aufwändiger ist, dafür aber eine geringere Fehlerwahrscheinlichkeit aufweist. Unter Annahme der (unbewiesenen) erweiterten Riemannschen Vermutung kann man zeigen: Ist $1 < n \in \mathbb{N}$ ungerade und keine Primzahl, dann gibt es einen Zeugen a für die Zerlegbarkeit von n mit $0 < a < 2(\log n)^2$ und a Primzahl, das ist der Satz von Ankeny-Montgomery-Bach, 1980-1994. Das liefert einen deterministischen Primzahltest, der in polynomialer Zeit läuft. Im Jahr 2002 haben Agrawal, Kayal und Saxena einen deterministischen Algorithmus gefunden, der ohne Annahme von zusätzlichen Hypothesen in polynomialer Zeit testet, ob eine Zahl eine Primzahl ist. In der Praxis ist dieser jedoch langsamer als der Miller-Rabin-Test.

KAPITEL 6

Kettenbrüche und quadratische Zahlkörper

6.1 Die Kettenbruchentwicklung reeller Zahlen

Die Darstellung reeller Zahlen im Dezimalsystem ist aus mathematischer Sicht insofern unkanonisch, als dass in diese die Wahl der Basis 10 eingeht. In diesem Abschnitt werden wir die Kettenbruchentwicklung reeller Zahlen behandeln. Diese kommt ohne Basiswahl aus und weist darüber hinaus zahlreiche weitere bemerkenswerte Eigenschaften auf:

Definition 6.1. *Für $a_0, \ldots, a_m \in \mathbb{R}$ mit $a_1 \ldots, a_m > 0$ setzen wir*

$$[a_0, a_1, \ldots, a_m] := a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ldots + \cfrac{1}{a_{m-1} + \cfrac{1}{a_m}}}}$$

*und nennen das Tupel $((a_0, \ldots, a_m), [a_0, \ldots, a_m])$ einen **endlichen Kettenbruch** mit Wert $[a_0, \ldots, a_m]$. Ist $(a_n)_{n\in\mathbb{N}_0}$ eine Folge reeller Zahlen mit $a_n > 0$ für $n \in \mathbb{N}$ und existiert der Grenzwert $\lim_{n\to\infty}[a_0, \ldots, a_n]$, dann setzen wir*

$$[a_0, a_1, \ldots] := \lim_{n\to\infty}[a_0, \ldots, a_n]$$

*und nennen das Tupel $((a_n)_{n\in\mathbb{N}_0}, [a_0, a_1, \ldots])$ einen **unendlichen Kettenbruch** mit Wert $[a_0, a_1, \ldots]$.*

*Unter einer **Kettenbruchdarstellung** einer reellen Zahl x verstehen wir einen Kettenbruch, dessen Wert durch x gegeben ist, also einen Kettenbruch der Form $((a_0, \ldots, a_m), x)$ oder $((a_n)_{n\in\mathbb{N}_0}, x)$. Eine solche Kettenbruchdarstellung von x heißt eine **Kettenbruchentwicklung** von x, wenn $a_0 \in \mathbb{Z}$ ist und $a_n \in \mathbb{N}$ für alle $n \in \mathbb{N}$, sowie $a_m \neq 1$, falls die Kettenbruchdarstellung endlich ist.*

Bemerkung 6.2. *Die obige Definition des Wertes endlicher Kettenbrüche lässt sich auch induktiv formulieren: Es ist dann* $[a_0] := a_0$ *sowie*

$$[a_0, \ldots, a_i, a_{i+1}] := [a_0, \ldots, a_{i-1}, a_i + \frac{1}{a_{i+1}}] \quad \text{für alle } i \in \mathbb{N}.$$

Beispiel 6.3. (a) *Es ist*

$$\frac{65}{27} = 2 + \frac{11}{27} = 2 + \frac{1}{\frac{27}{11}} = 2 + \frac{1}{2 + \frac{5}{11}} = 2 + \frac{1}{2 + \frac{1}{\frac{11}{5}}} = 2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{5}}} = [2,2,2,5]$$

und also $((2,2,2,5), \frac{65}{27})$ *eine endliche Kettenbruchentwicklung von* $\frac{65}{27}$.

(b) *Falls der Grenzwert* $\phi = \lim_{n\to\infty}[\underbrace{1,1,\ldots,1}_{n-\text{mal}}]$ *existiert, dann gilt offensichtlich*

$$\phi = 1 + \frac{1}{1 + \frac{1}{1 + \ldots}} = 1 + \frac{1}{\phi},$$

also $\phi^2 - \phi - 1 = 0$. *Die einzige positive Lösung dieser Gleichung ist* $\phi = \frac{1+\sqrt{5}}{2}$, *der* ***Goldene Schnitt****. Somit ist vorbehaltlich der Existenz des obigen Grenzwertes* $([1,1,\ldots], \phi)$ *eine unendliche Kettenbruchentwicklung des Goldenen Schnittes.*

Ziel dieses Abschnitts wird es sein, zu zeigen, dass jede reelle Zahl eine eindeutig bestimmte Kettenbruchentwicklung hat. Im Folgenden geben wir den Kettenbruchalgorithmus an. Dieser dient dazu, zu einer gegebenen reellen Zahl x die Kettenbruchentwicklung zu bestimmen:

Algorithmus 6.4 (Kettenbruchalgorithmus)**.** *Es soll die Kettenbruchentwicklung von* $x \in \mathbb{R}$ *bestimmt werden.*

(1) $a_0 := \lfloor x \rfloor \in \mathbb{Z}$, $t_0 := x - a_0 \in [0,1)$ *und* $m := 0$.

(2) Solange $t_m \neq 0$ *ist, wiederhole* (3) – (6)*:*

(3) $\xi_m := \frac{1}{t_m}$

(4) $a_{m+1} := \lfloor \xi_m \rfloor \in \mathbb{N}$

(5) $t_{m+1} := \xi_m - a_{m+1} \in [0,1)$

(6) $m := m + 1$

Falls die Schleife (2) – (6) *terminiert, falls also nach endlich vielen Schritten* $t_m = 0$ *erreicht wird, so ist* $((a_0, \ldots, a_m), x)$ *die Kettenbruchentwicklung von* x. *Falls die Schleife nicht terminiert, so ist* $((a_n)_{n\in\mathbb{N}_0}, x)$ *die Kettenbruchentwicklung von* x.

Wir werden im Laufe dieses Abschnittes sehen, dass der Kettenbruchalgorithmus ein korrektes Ergebnis liefert. Er terminiert nur für rationales x und gibt in diesem Fall eine endliche Kettenbruchentwicklung als Ergebnis aus; für irrationales x erhalten wir eine unendliche Kettenbruchentwicklung.

Satz 6.5. *Sei $x \in \mathbb{R}$. Dann gilt:*

(a) *Die Zahl x besitzt eine eindeutig bestimmte Kettenbruchentwicklung. Diese wird durch den Kettenbruchalgorithmus geliefert.*

(b) *Ist x rational, dann ist die Kettenbruchentwicklung von x endlich. Ist x irrational, dann ist die Kettenbruchentwicklung von x unendlich.*

Ist die Kettenbruchentwicklung von x durch $((a_0, \ldots, a_m), x)$ bzw. $((a_n)_{n\in\mathbb{N}_0}, x)$ gegeben, dann heißen die rationalen Zahlen $[a_0, \ldots, a_n]$ mit $n \in \mathbb{N}_0$ – und $n \leq m$, falls $x \in \mathbb{Q}$ ist – die ***Näherungsbrüche*** *von x.*

Den Beweis schieben wir an dieser Stelle auf, er benötigt einige Hilfsresultate, die wir im Laufe dieses Abschnitts bereitstellen werden. Wir studieren zunächst einige Beispiele zur Anwendung des Kettenbruchalgorithmus 6.4 auf rationale Zahlen:

Beispiel 6.6. *Mit den Bezeichnungen aus dem Kettenbruchalgorithmus 6.4 stellt sich die Rechnung in Beispiel 6.3 (a) wie folgt dar:*

$$\begin{aligned} a_0 &= 2, \quad t_0 = \tfrac{11}{27}, \quad \xi_0 = \tfrac{27}{11}, \\ a_1 &= 2, \quad t_1 = \tfrac{5}{11}, \quad \xi_1 = \tfrac{11}{5}, \\ a_2 &= 2, \quad t_2 = \tfrac{1}{5}, \quad \xi_2 = 5, \\ a_3 &= 5, \quad t_3 = 0. \end{aligned}$$

Beispiel 6.7. *Kettenbruchentwicklungen treten auch in einigen Anwendungen auf:*

(a) *Die Umlaufzeit der Erde um die Sonne beträgt in guter Näherung*

$$365\,\mathrm{d}\ 5\,\mathrm{h}\ 48\,\mathrm{min}\ 45{,}8\mathrm{s} = \left(365 + \frac{104.629}{432.000}\right)\ \mathrm{d}.$$

Der Kettenbruchalgorithmus liefert

$$\frac{104.629}{432.000} = [0, 4, 7, 1, 3, 6, 2, 1, 170].$$

Näherungsbrüche dafür lassen sich in klassischen Kalendersystemen finden:

- *Der nullte Näherungsbruch für $\frac{104.629}{432.000}$ ist $[0] = 0$. Diese Näherung wurde beispielsweise im alten Ägypten vorgenommen: Es gibt keine Schaltjahre, dafür wird gelegentlich ein Jahr um einige Tage verlängert.*
- *Der erste Näherungsbruch für $\frac{104.629}{432.000}$ lautet $[0, 4] = \frac{1}{4}$. Dies entspricht dem Vorgehen im julianischen Kalender: Alle 4 Jahre wird ein Schaltjahr eingefügt.*

- *Der fünfte Näherungsbruch für* $\frac{104.629}{432.000}$ *ist durch* $[0,4,7,1,3,6] = \frac{194}{801}$ *gegeben. Das kommt der Gestaltung des gregorianischen Kalenders sehr nahe: In Modifikation des julianischen Kalenders fallen hier in* 800 *Jahren* 6 *Schaltjahre weg, nämlich diejenigen Jahre, deren Jahreszahl durch* 100*, aber nicht durch* 400 *teilbar ist.*

(b) *Bei der Einteilung des Jahres in Monate muss man das Verhältnis einer Mondperiode zur Jahreslänge berechnen. Dieses ist ziemlich genau*

$$x = \frac{2.953.059}{36.524.220}.$$

Über den Kettenbruchalgorithmus erhält man

$$x = [0,12,2,1,2,1,1,17,3,6,2,1,2,1,1,7].$$

Auch hier lassen sich Näherungsbrüche in klassischen Kalendersystemen finden:

- *Der erste Näherungsbruch für* x *lautet* $[0,12] = \frac{1}{12}$*. Das entspricht der Kalendereinteilung im alten Ägypten: Ein Jahr besteht aus* 12 *Monaten mit je* 30 *Tagen, dazu kommen* 5 *Feiertage.*
- *Der sechste Näherungsbruch für* x *ist durch* $[0,12,2,1,2,1,1] = \frac{19}{235}$ *gegeben. Dieses Verhältnis wird im* Meton-Zyklus *des jüdischen Kalenders verwendet:* 19 *Jahre werden zu einer Zeitperiode von* 235 *Monaten zusammengefasst.*

Lemma 6.8. *Mit den Notationen aus dem Kettenbruchalgorithmus 6.4 gilt für ein beliebiges* $x \in \mathbb{R}$*:*

(a) *Ist* $m \in \mathbb{N}_0$ *mit* $t_m \neq 0$*, dann ist* $x = [a_0, \ldots, a_m, \xi_m]$*.*

(b) *Ist* $m \in \mathbb{N}_0$ *mit* $t_m = 0$*, dann ist* $x = [a_0, \ldots, a_m]$*. Im Falle* $m \geq 1$ *ist dabei* $a_m > 1$*.*

Es folgt, dass der Kettenbruchalgorithmus, falls er nach endlich vielen Schritten terminiert, eine endliche Kettenbruchentwicklung von x *von der Form* $((a_0, \ldots, a_m), x)$ *ausgibt.*

Beweis. Wir zeigen zunächst Behauptung (a) per Induktion nach m und setzen dafür $m = 0$ und $t_0 \neq 0$. Dann ist

$$\xi_0 = \frac{1}{t_0} = \frac{1}{x - a_0}$$

und deshalb

$$x = a_0 + \frac{1}{\xi_0} = [a_0, \xi_0].$$

Das zeigt den Induktionsanfang. Für den Induktionsschritt nehmen wir nun an, wir hätten bereits $x = [a_0, \ldots, a_m, \xi_m]$ für ein $m \in \mathbb{N}_0$ gezeigt und es gelte $t_{m+1} \neq 0$. Wir erhalten

$$\begin{aligned} x &= [a_0, \ldots, a_m, \xi_m] = [a_0, \ldots, a_m, a_{m+1} + t_{m+1}] = [a_0, \ldots, a_m, a_{m+1} + \frac{1}{\xi_{m+1}}] \\ &= [a_0, \ldots, a_m, a_{m+1}, \xi_{m+1}] \end{aligned}$$

und somit Behauptung (a).

Wir zeigen nun Behauptung (b). Ist hierbei einerseits $t_0 = 0$, so gilt offenbar $x = [a_0]$. Ist andererseits $m \geq 1$ mit $t_m = 0$, so ist $t_{m-1} \neq 0$, weshalb sich aus Aussage (a) unmittelbar $x = [a_0, \ldots, a_{m-1}, \xi_{m-1}]$ ergibt. Mit $0 = t_m = \xi_{m-1} - a_m$ folgt $x = [a_0, \ldots, a_m]$. In diesem Fall ist $a_m = \xi_{m-1} = \frac{1}{t_{m-1}} > 1$ wegen $t_{m-1} \in (0,1)$. □

Lemma 6.9. *Für ein beliebiges $x \in \mathbb{R}$ sind die folgenden beiden Aussagen äquivalent:*

(i) *Der Kettenbruchalgorithmus 6.4 terminiert bei Eingabe von x nach endlich vielen Schritten.*

(ii) $x \in \mathbb{Q}$.

Insbesondere gibt Algorithmus 6.4 für rationale Eingaben endliche Kettenbruchentwicklungen aus.

Beweis. Nehmen wir zunächst (i) an, der Kettenbruchalgorithmus 6.4 terminiere nach Eingabe von x also nach endlich vielen Schritten. Ist hierbei $t_0 = 0$, so gilt $x = [a_0] \in \mathbb{Z}$. Ist sonst $m \in \mathbb{N}_0$ maximal mit $t_m \neq 0$, so zeigt man anhand von 6.4 in einem leichten Induktionsbeweis

$$x = [a_0, \ldots, a_m, \xi_m] = [a_0, \ldots, a_m, a_{m+1}]$$

mit $a_0 \in \mathbb{Z}$ sowie $a_1, \ldots, a_{m+1} \in \mathbb{N}$. Hiermit erhalten wir $x \in \mathbb{Q}$, also Aussage (ii).

Gelte nun umgekehrt Aussage (ii), sei also $x \in \mathbb{Q}$, etwa $x = \frac{p}{q}$ mit $p \in \mathbb{Z}$ und $q \in \mathbb{N}$. Da für $x = 0$ nichts zu zeigen ist, können wir im Folgenden ohne Einschränkung $x \neq 0$ annehmen. Wir setzen $r_0 := p$ sowie $r_1 := q$ und führen den Euklidischen Algorithmus 1.7 aus:

$$\begin{array}{lll}
r_0 = a_0' r_1 + r_2 & \text{mit } a_0' \in \mathbb{Z} & \text{und } 0 < r_2 < r_1, \\
r_1 = a_1' r_2 + r_3 & \text{mit } a_1' \in \mathbb{N} & \text{und } 0 < r_3 < r_2, \\
\vdots & & \\
r_i = a_i' r_{i+1} + r_{i+2} & \text{mit } a_i' \in \mathbb{N} & \text{und } 0 < r_{i+2} < r_{i+1}, \\
\vdots & & \\
r_{m-1} = a_{m-1}' r_m + r_{m+1} & \text{mit } a_{m-1}' \in \mathbb{N} & \text{und } 0 < r_{m+1} < r_m, \\
r_m = a_m' r_{m+1} & \text{mit } a_m' \in \mathbb{N}. &
\end{array}$$

Wir erhalten

$$\begin{aligned}
&\frac{r_i}{r_{i+1}} = a_i' + \frac{r_{i+2}}{r_{i+1}} \quad \text{mit } \frac{r_{i+2}}{r_{i+1}} \in (0,1) \text{ für alle } i \in \{0, \ldots, m-1\}, \\
&\frac{r_m}{r_{m+1}} = a_m'.
\end{aligned}$$

Wir setzen

$$t_i' := \frac{r_{i+2}}{r_{i+1}} \qquad \text{für } i \in \{-1, \ldots, m-1\} \quad \text{sowie} \quad t_m' := 0,$$

und erhalten

$$\frac{1}{t'_{i-1}} = a'_i + t'_i \qquad \text{für } i \in \{0, \dots, m\},$$

wobei $t'_i \in (0,1)$ für $i = 0, \dots, m-1$ ist. Wir vergleichen dies mit den Formeln aus dem Kettenbruchalgorithmus 6.4: Es bezeichne $((a_i)_{i\in I}, x)$ das Resultat des Kettenbruchalgorithmus bei Eingabe von x, wobei $I = \{0, \dots, n\}$ sei, falls der Algorithmus nach $n \in \mathbb{N}_0$ Schritten abbricht, und $I = \mathbb{N}_0$ sonst. Die Folge $(t_i)_{i\in I}$ sei wie im Kettenbruchalgorithmus definiert. Wir zeigen induktiv $a_i = a'_i$ und $t_i = t'_i$ für $i \in \{0, \dots, m\}$. Insbesondere ist dann $t_m = t'_m = 0$, so dass der Kettenbruchalgorithmus nach endlich vielen Schritten abbricht. Sei zunächst $i = 0$. Dann ist

$$a_0 = \lfloor x \rfloor = \lfloor \frac{r_0}{r_1} \rfloor = \lfloor \frac{1}{t'_{-1}} \rfloor = a'_0 \qquad \text{und} \quad t_0 = x - a_0 = \frac{1}{t'_{-1}} - a'_0 = t'_0.$$

Sei nun $0 < i \leq m$. Aus der Induktionsvoraussetzung ergibt sich $t_{i-1} = t'_{i-1} \neq 0$ und deshalb

$$a_i = \lfloor \frac{1}{t_{i-1}} \rfloor = \lfloor \frac{1}{t'_{i-1}} \rfloor = a'_i \qquad \text{und} \quad t_i = \frac{1}{t_{i-1}} - a_i = \frac{1}{t'_{i-1}} - a'_i = t'_i.$$

□

Beispiel 6.10. *Der Beweis hat gezeigt, dass man den Kettenbruchalgorithmus 6.4 für rationale Zahlen als Variante des Euklidischen Algorithmus 1.7 ansehen kann. In Beispiel 6.3 (a) erhalten wir:*

$$\begin{aligned}
65 &= 2 \cdot 27 + 11 && \Longrightarrow && \frac{65}{27} &= 2 + \frac{11}{27} \\
27 &= 2 \cdot 11 + 5 && \Longrightarrow && \frac{27}{11} &= 2 + \frac{5}{11} \\
11 &= 2 \cdot 5 + 1 && \Longrightarrow && \frac{11}{5} &= 2 + \frac{1}{5} \\
5 &= 5 \cdot 1 + 0 && \Longrightarrow && \frac{5}{1} &= 5 + 0.
\end{aligned}$$

Als Kettenbruchentwicklung von $\frac{65}{27}$ ergibt sich wie gehabt $((2,2,2,5), \frac{65}{27})$.

Die nächste Bemerkung zeigt insbesondere, dass es für jede rationale Zahl x genau eine endliche Kettenbruchentwicklung gibt:

Proposition 6.11. *Seien $a_0, b_0 \in \mathbb{Z}$, $a_1, \dots, a_n, b_1, \dots, b_m \in \mathbb{N}$ mit $a_n, b_m \neq 1$ und $[a_0, \dots, a_n] = [b_0, \dots, b_m]$. Dann gilt: $n = m$ und $a_i = b_i$ für $i = 0, \dots, n$.*

Beweis. Ohne Einschränkung sei $n \leq m$. Wir beweisen die Behauptung per Induktion nach n.

Sei zunächst $n = 0$. Wäre $m \geq 1$, so auch

$$a_0 = b_0 + \frac{1}{[b_1, \dots, b_m]},$$

wobei aufgrund von $b_m \neq 1$ die Ungleichung

$$0 < \frac{1}{[b_1, \ldots, b_m]} < 1$$

gälte. Es folgte, dass die linke Seite der vorigen Gleichung eine ganze Zahl wäre, die rechte Seite dagegen nicht. Somit ist $m = 0 = n$ und demzufolge $a_0 = [a_0] = [b_0] = b_0$.

Im Folgenden sei $n \geq 1$. Es sei

$$x = [a_0, \ldots, a_n] = a_0 + \frac{1}{[a_1, \ldots, a_n]} = b_0 + \frac{1}{[b_1, \ldots, b_m]} = [b_0, \ldots, b_m]$$

Hierbei ist zu beachten, dass mit demselben Argument wie oben aus $n \geq 1$ auch $m \geq 1$ folgt. Aufgrund von $a_n \neq 1 \neq b_m$ erhalten wir

$$0 < \frac{1}{[a_1, \ldots, a_n]} < 1 \text{ sowie } 0 < \frac{1}{[b_1, \ldots, b_m]} < 1$$

und deshalb $a_0 = \lfloor x \rfloor = b_0$ und schließlich $[a_1, \ldots, a_n] = [b_1, \ldots, b_m]$. Aus der Induktionsannahme folgern wir $n = m$ und $a_i = b_i$ für $i = 1, \ldots, n$. □

Lässt man in Proposition 6.11 die Voraussetzung $a_n, b_m \neq 1$ weg, gilt die Eindeutigkeitsaussage nicht mehr:

$$[a_0, \ldots, a_{n-1}, a_n] = \begin{cases} [a_0, \ldots, a_n - 1, 1] & \text{für } a_n > 1 \text{ oder } n = 0, \\ [a_0, \ldots, a_{n-1} + 1] & \text{für } a_n = 1 \text{ und } n \geq 1. \end{cases}$$

Im Folgenden werden wir uns mit der Kettenbruchentwicklung irrationaler Zahlen beschäftigen. Dazu starten wir mit einer Folge ganzer Zahlen $(a_n)_{n \in \mathbb{N}_0}$ mit $a_n \geq 1$ für $n \geq 1$ und werden Folgendes beweisen:

- Die Folge $([a_0, \ldots, a_n])_{n \in \mathbb{N}_0}$ konvergiert.
- Stammt die Folge $(a_n)_{n \in \mathbb{N}_0}$ aus der Ausgabe des Kettenbruchalgorithmus 6.4 für eine irrationale Zahl x, dann konvergiert die Folge $([a_0, \ldots, a_n])_{n \in \mathbb{N}_0}$ gegen x, der Kettenbruchalgorithmus liefert also als Ausgabe eine unendliche Kettenbruchentwicklung von x.

Das nächste Lemma hat einen sehr technischen Charakter, wird sich aber im weiteren Verlauf des Kapitels als nützlich herausstellen und an vielerlei Stellen Anwendung finden:

Lemma 6.12. *Sei $(a_n)_{n \in \mathbb{N}_0}$ eine Folge ganzer Zahlen mit $a_n \geq 1$ für $n \geq 1$. Wir setzen*

$$\begin{array}{llll} p_{-2} := 0, & p_{-1} := 1, & p_n := a_n p_{n-1} + p_{n-2} & \text{für alle } n \geq 0 \quad (\text{insb. } p_0 = a_0), \\ q_{-2} := 1, & q_{-1} := 0, & q_n := a_n q_{n-1} + q_{n-2} & \text{für alle } n \geq 0 \quad (\text{insb. } q_0 = 1), \end{array}$$

oder alternativ in Matrixschreibweise:

$$\begin{pmatrix} p_{-1} & p_{-2} \\ q_{-1} & q_{-2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ und } \begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix} = \begin{pmatrix} p_{n-1} & p_{n-2} \\ q_{n-1} & q_{n-2} \end{pmatrix} \cdot \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} \text{ für alle } n \geq 0.$$

Dann gelten die folgenden Aussagen:

(a) $\begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdot \ldots \cdot \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix}$ *für alle* $n \in \mathbb{N}_0$.

(b) $[a_0, \ldots, a_n] = \dfrac{p_n}{q_n}$ *für alle* $n \in \mathbb{N}_0$.

(c) $[a_0, \ldots, a_n, \xi] = \dfrac{\xi p_n + p_{n-1}}{\xi q_n + q_{n-1}}$ *für alle* $n \in \mathbb{N}_0, \xi \in \mathbb{R}_{>0}$.

(d) $q_{n+1} > q_n$ *für alle* $n \in \mathbb{N}$, *insbes.* $q_n \geq n$.

(e) $q_1 \geq q_0$ *mit Gleichheit genau für* $a_1 = 1$.

(f) $p_n q_{n-1} - p_{n-1} q_n = (-1)^{n+1}$ *für alle* $n \in \mathbb{N}_0$.

(g) $p_n q_{n-2} - p_{n-2} q_n = (-1)^n a_n$ *für alle* $n \in \mathbb{N}_0$.

(h) $\mathrm{ggT}(p_n, q_n) = 1$ *für alle* $n \in \mathbb{N}_0$.

Beweis. Behauptung (a) folgt unmittelbar aus der Rekursionsformel in Matrixschreibweise.

Wir zeigen nun Behauptung (c) per Induktion nach n: Im Fall $n = 0$ ist

$$[a_0, \xi] = a_0 + \frac{1}{\xi} = \frac{\xi a_0 + 1}{\xi} = \frac{\xi p_0 + p_{-1}}{\xi q_0 + q_{-1}}.$$

Sei $n \geq 1$. Nach Induktionsvoraussetzung erhalten wir

$$\begin{aligned} [a_0, \ldots, a_n, \xi] &= [a_0, \ldots, a_{n-1}, a_n + \frac{1}{\xi}] = \frac{(a_n + \frac{1}{\xi}) p_{n-1} + p_{n-2}}{(a_n + \frac{1}{\xi}) q_{n-1} + q_{n-2}} \\ &= \frac{(a_n \xi + 1) p_{n-1} + \xi p_{n-2}}{(a_n \xi + 1) q_{n-1} + \xi q_{n-2}} = \frac{\xi(a_n p_{n-1} + p_{n-2}) + p_{n-1}}{\xi(a_n q_{n-1} + q_{n-2}) + q_{n-1}} \\ &= \frac{\xi p_n + p_{n-1}}{\xi q_n + q_{n-1}}. \end{aligned}$$

Nun folgt sofort Behauptung (b) via

$$[a_0, \ldots, a_n] \overset{\text{(c)}}{=} \frac{a_n p_{n-1} + p_{n-2}}{a_n q_{n-1} + q_{n-2}} = \frac{p_n}{q_n}.$$

Weiter ist $q_0 = 1$, $q_1 = a_1 q_0 = a_1 \geq 1$, $q_{n+1} = a_{n+1} q_n + q_{n-1} \geq q_n + q_{n-1}$. Induktiv ergibt sich $q_{n+1} > q_n \geq n$ für $n \in \mathbb{N}$ und somit die Behauptungen (d) und (e).

Der Beweis von Behauptung (f) ergibt sich aus

$$\begin{aligned} p_n q_{n-1} - p_{n-1} q_n &= \det \begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix} = \det\left(\begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdot \ldots \cdot \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix}\right) \\ &= \det \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \ldots \cdot \det \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} = (-1)^{n+1}. \end{aligned}$$

Behauptung (g) folgt mit

$$\begin{aligned} p_n q_{n-2} - p_{n-2} q_n &= \big(a_n p_{n-1} + p_{n-2}\big) q_{n-2} - p_{n-2}\big(a_n q_{n-1} + q_{n-2}\big) \\ &= a_n (p_{n-1} q_{n-2} - p_{n-2} q_{n-1}) \overset{\text{(f)}}{=} (-1)^n a_n. \end{aligned}$$

Zum Beweis von Behauptung (h) betrachten wir schließlich ein $d \in \mathbb{Z}$ mit $d \mid p_n$ und $d \mid q_n$. Dann gilt $d \mid \big(p_n q_{n-1} - p_{n-1} q_n\big) = (-1)^n$ und also $d = \pm 1$. Das impliziert $\operatorname{ggT}(p_n, q_n) = 1$. □

Da wir im weiteren Verlauf des Kapitels gelegentlich die Indexmenge $\{-2, -1, 0, 1, 2, \ldots\}$ benötigen werden, führen wir an dieser Stelle dafür die Bezeichnung $\mathbb{N}_{-2}$ ein.

Satz 6.13. *Sei $(a_n)_{n \in \mathbb{N}_0}$ eine Folge ganzer Zahlen mit $a_n \geq 1$ für $n \geq 1$. Dann gelten die folgenden Aussagen:*

(a) *Die Näherungsbrüche $[a_0, \ldots, a_n] = \frac{p_n}{q_n}$ aus Lemma 6.12 bilden eine konvergente Folge.*

(b) *Die Teilfolge $\left(\frac{p_{2n}}{q_{2n}}\right)_{n \in \mathbb{N}_0}$ ist streng monoton wachsend, die Teilfolge $\left(\frac{p_{2n+1}}{q_{2n+1}}\right)_{n \in \mathbb{N}_0}$ ist streng monoton fallend. Insbesondere gilt für $x = \lim_{n \to \infty} \frac{p_n}{q_n} = [a_0, a_1, \ldots]$ die Abschätzung*

$$a_0 = \frac{p_0}{q_0} < \frac{p_2}{q_2} < \frac{p_4}{q_4} < \ldots < x < \ldots < \frac{p_3}{q_3} < \frac{p_1}{q_1}.$$

(c) *Die Zahl $[a_0, a_1, \ldots]$ ist irrational.*

Ist $x = [a_0, \ldots, a_m] \in \mathbb{Q}$, und sind $\frac{p_0}{q_0}, \ldots, \frac{p_m}{q_m}$ die zugehörigen Näherungsbrüche, dann gilt Aussage (b) entsprechend mit $\ldots \leq x \leq \ldots$.

Beweis. Nach Lemma 6.12 gilt

$$\frac{p_i}{q_i} - \frac{p_{i-1}}{q_{i-1}} = \frac{p_i q_{i-1} - p_{i-1} q_i}{q_i q_{i-1}} = \frac{(-1)^{i+1}}{q_i q_{i-1}} \quad \text{für alle } i \in \mathbb{N}.$$

Es folgt

$$\frac{p_n}{q_n} = \frac{p_0}{q_0} + \sum_{i=1}^{n} \left(\frac{p_i}{q_i} - \frac{p_{i-1}}{q_{i-1}}\right) = a_0 + \sum_{i=1}^{n} \frac{(-1)^{i+1}}{q_i q_{i-1}}.$$

Nach Lemma 6.12 (d),(e) ist die Folge $\left(\frac{1}{q_i q_{i-1}}\right)_{i \in \mathbb{N}}$ eine streng monoton fallende Nullfolge, weswegen aus dem Leibniz-Kriterium die Konvergenz von $\sum_{i=1}^{n} \frac{(-1)^{i+1}}{q_i q_{i-1}}$ folgt. Somit ist die Folge $(\frac{p_n}{q_n})_{n \in \mathbb{N}}$ konvergent und wir haben Behauptung (a) gezeigt.

Weiter gilt nach Lemma 6.12 (g)

$$\frac{p_n}{q_n} - \frac{p_{n-2}}{q_{n-2}} = \frac{p_n q_{n-2} - p_{n-2} q_n}{q_n q_{n-2}} = (-1)^n \frac{a_n}{q_n q_{n-2}} \quad \text{für alle } n \in \mathbb{N}_0$$

Demzufolge gilt für alle $n \geq 2$ wegen $a_n, q_n, q_{n-2} \geq 1$

$$\begin{aligned} \frac{p_n}{q_n} &> \frac{p_{n-2}}{q_{n-2}} \quad \text{für } n \text{ gerade,} \\ \frac{p_n}{q_n} &< \frac{p_{n-2}}{q_{n-2}} \quad \text{für } n \text{ ungerade.} \end{aligned}$$

Hieraus folgt Behauptung (b).

Zum Beweis von Behauptung (c) nehmen wir schließlich an, $x = [a_0, a_1, \ldots]$ wäre rational. Der Kettenbruchalgorithmus lieferte in diesem Fall eine endliche Kettenbruchentwicklung $((b_0, \ldots, b_m), x)$ von x. Wir zeigen zunächst induktiv, dass hierbei $a_k = b_k$ für $k = 0, \ldots, m$ wäre. Zunächst gälte $a_0 = \lfloor x \rfloor = b_0$. Ausgehend von $[a_0, a_1, \ldots] = [a_0, a_1, \ldots, a_{k-1}, b_k, \ldots, b_m]$ setzten wir nun $\xi_{k-1} := [a_k, a_{k+1}, \ldots]$. Das wäre aufgrund von Aussage (a) wohldefiniert und es gälte

$$[a_0, a_1, \ldots, a_{k-1}, \xi_{k-1}] = [a_0, a_1, \ldots] = [a_0, a_1, \ldots, a_{k-1}, b_k, \ldots, b_m].$$

Durch Termumformung ergäbe sich $\xi_{k-1} = [b_k, \ldots, b_m]$, was $a_k = \lfloor \xi_{k-1} \rfloor = b_k$ zur Folge hätte und die Induktion beendete. Mit $\xi_m = [a_{m+1}, a_{m+2}, \ldots]$ ergäbe sich die Gleichung $[a_0, \ldots, a_m] = [a_0, \ldots, a_m, \xi_m]$, was zum Widerspruch führt. □

Beispiel 6.14. *Sei $a_n = 1$ für alle $n \in \mathbb{N}_0$. Für $n \geq 0$ ergibt sich so*

$$p_n = p_{n-1} + p_{n-2}, \quad q_n = q_{n-1} + q_{n-2}$$

und insbesondere $p_0 = 1$, $p_1 = 2$, $q_0 = 1$ sowie $q_1 = 1$. Bezeichnet $(F_n)_{n \in \mathbb{N}_0}$ die Folge der Fibonaccizahlen, dann ist $p_n = F_{n+1}$, $q_n = F_n$ für alle $n \in \mathbb{N}_0$. Die Folge $\frac{p_n}{q_n} = \frac{F_{n+1}}{F_n}$ ist aufgrund von Satz 6.13 konvergent und aus der Überlegung in Beispiel 6.3 erhalten wir

$$\lim_{n \to \infty} \frac{p_n}{q_n} = \lim_{n \to \infty} \frac{F_{n+1}}{F_n} = [1, 1, \ldots] = \frac{1 + \sqrt{5}}{2}.$$

Aus Satz 6.13 folgt insbesondere, dass die Folge der Näherungsbrüche, die man über den Kettenbruchalgorithmus 6.4 zu einer irrationalen Zahl x bestimmt, konvergiert. Im nächsten Satz werden wir zeigen, dass der Grenzwert durch x selbst gegeben ist:

Satz 6.15. *Seien $x \in \mathbb{R} \setminus \mathbb{Q}$, $((a_n)_{n \in \mathbb{N}_0}, x)$ die Ausgabe des Kettenbruchalgorithmus bei Eingabe von x sowie $(\frac{p_n}{q_n})_{n \in \mathbb{N}_0}$ die Folge der Näherungsbrüche wie in Lemma 6.12. Dann gelten die folgenden Aussagen:*

(a) *Die Folge der Näherungsbrüche $[a_0, \ldots, a_n] = \frac{p_n}{q_n}$ konvergiert gegen x, es ist also $x = [a_0, a_1, \ldots]$.*

(b) *Für alle $n \in \mathbb{N}_0$ ist*

$$\left| x - \frac{p_n}{q_n} \right| < \frac{1}{q_n q_{n+1}},$$

für $n \geq 1$ ist insbesondere

$$\left| x - \frac{p_n}{q_n} \right| < \frac{1}{n(n+1)}.$$

(c) *Für alle* $n \in \mathbb{N}_0$ *ist*

$$\left| x - \frac{p_n}{q_n} \right| > \frac{1}{q_n(q_n + q_{n+1})},$$

Somit liefert der Kettenbruchalgorithmus eine unendliche Kettenbruchentwicklung von x *als Ergebnis.*

Beweis. Wir beginnen mit dem Beweis von Aussage (b), da diese Aussage (a) impliziert. Die Folge $(\xi_n)_{n\in\mathbb{N}_0}$ sei definiert wie im Kettenbruchalgorithmus. Aufgrund von Lemma 6.8 und 6.12 (c) erhalten wir für jedes $n \in \mathbb{N}_0$:

$$x = [a_0, \ldots, a_n, \xi_n] = \frac{\xi_n p_n + p_{n-1}}{\xi_n q_n + q_{n-1}}$$

und deshalb

$$x - \frac{p_n}{q_n} = \frac{(\xi_n p_n + p_{n-1})q_n - p_n(\xi_n q_n + q_{n-1})}{q_n(\xi_n q_n + q_{n-1})} = \frac{p_{n-1}q_n - p_n q_{n-1}}{q_n(\xi_n q_n + q_{n-1})} \overset{6.12(f)}{=} \frac{(-1)^n}{q_n(\xi_n q_n + q_{n-1})}.$$

Wegen $a_{n+1} = \lfloor \xi_n \rfloor < \xi_n$ – andernfalls würde der Kettenbruchalgorithmus an dieser Stelle terminieren – erhalten wir

$$\left| x - \frac{p_n}{q_n} \right| = \frac{1}{q_n(\xi_n q_n + q_{n-1})} < \frac{1}{q_n(a_{n+1}q_n + q_{n-1})} = \frac{1}{q_n q_{n+1}}.$$

Für $n \geq 1$ ist nach Lemma 6.12 (d) $q_n \geq n$, was

$$\left| x - \frac{p_n}{q_n} \right| < \frac{1}{q_n q_{n+1}} \leq \frac{1}{n(n+1)}$$

zur Folge hat.

Behauptung (c) ergibt sich wegen $\xi_n < \lfloor \xi_n \rfloor + 1 = a_{n+1} + 1$ durch

$$\begin{aligned} \left| x - \frac{p_n}{q_n} \right| &= \frac{1}{q_n(\xi_n q_n + q_{n-1})} > \frac{1}{q_n((a_{n+1}+1)q_n + q_{n-1})} = \frac{1}{q_n(a_{n+1}q_n + q_{n-1} + q_n)} \\ &= \frac{1}{q_n(q_{n+1} + q_n)}. \end{aligned}$$

□

Proposition 6.16. *Sei* $x = [a_0, \ldots, a_m] \in \mathbb{Q}$ *mit* $a_m \neq 1$. *Dann gilt:*

$$\left| x - \frac{p_n}{q_n} \right| \leq \frac{1}{q_n q_{n+1}} \quad \textit{und} \quad \left| x - \frac{p_n}{q_n} \right| > \frac{1}{q_n(q_n + q_{n+1})}$$

für alle $n \in \{0, \ldots, m-1\}$, *wobei bei der ersten Ungleichung Gleichheit nur im Fall* $n = m-1$ *auftritt.*

Beweis. Der Beweis verläuft analog zum Beweis von Satz 6.15. □

Zum Beweis von Satz 6.5 verbleibt noch zu zeigen, dass jede reelle Zahl eine eindeutig bestimmte Kettenbruchentwicklung besitzt. In Verbindung mit Proposition 6.11 und Satz 6.13 (c) genügt dafür die folgende Proposition:

Proposition 6.17. *Seien $(a_n)_{n\in\mathbb{N}_0}$, $(b_n)_{n\in\mathbb{N}_0}$ Folgen ganzer Zahlen mit $a_n, b_n \geq 1$ für $n \geq 1$ und $[a_0, a_1, \ldots] = [b_0, b_1, \ldots]$. Dann gilt: Für alle $n \in \mathbb{N}_0$ ist $a_n = b_n$.*

Beweis. Wir zeigen die Aussage per Induktion nach n und setzen dafür $x = [a_0, a_1, \ldots] = [b_0, b_1, \ldots]$. Es ist dann $a_0 = \lfloor x \rfloor = b_0$. Es sei nun $a_0 = b_0, \ldots, a_n = b_n$. Setzen wir nun $\xi = [a_{n+1}, a_{n+2}, \ldots]$, $\xi' = [b_{n+1}, b_{n+2}, \ldots]$, so ergibt sich $[a_0, \ldots, a_n, \xi] = [b_0, \ldots, b_n, \xi'] = [a_0, \ldots, a_n, \xi']$ und daraus $\xi = \xi'$. Aufgrunddessen ist $a_{n+1} = \lfloor \xi \rfloor = \lfloor \xi' \rfloor = b_{n+1}$. □

Beispiel 6.18. (a) *Der Kettenbruchalgorithmus 6.4 liefert für $x = \sqrt{2}$*

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

Aus Satz 6.15 folgt, dass $\left((1,2,2,2,\ldots), \sqrt{2}\right)$ die Kettenbruchentwicklung von $\sqrt{2}$ ist.

(b) $e = [2,1,2,1,1,4,1,1,6,1,1,8,1,1,10,\ldots]$.

(c) $\pi = [3,7,15,1,292,1,1,1,2,1,3,1,\ldots]$. *Es ist hierbei kein Muster bekannt. Der dritte Näherungsbruch ist durch $[3,7,15,1] = \frac{355}{113} \approx 3,1415929$ gegeben und approximiert π bereits sehr gut.*

6.2 Periodische Kettenbrüche

Definition 6.19. *Sei $(a_n)_{n\in\mathbb{N}_0}$ eine Folge ganzer Zahlen mit $a_n \geq 1$ für $n \geq 1$. Der Kettenbruch $((a_n)_{n\in\mathbb{N}_0}, [a_0, a_1, \ldots])$ heißt **periodisch**, wenn es ein $h \in \mathbb{N}$ und ein $n \in \mathbb{Z}_{\geq -1}$ mit $a_{m+h} = a_m$ für alle $m \geq n+1$ gibt. In diesem Fall nennen wir das minimale h mit dieser Eigenschaft die **Periodenlänge** und für den Kettenbruch verwenden wir die Notation*

$$((a_0, a_1, \ldots, a_n, \overline{a_{n+1}, \ldots, a_{n+h}}), [a_0, a_1, \ldots, a_n, \overline{a_{n+1}, \ldots, a_{n+h}}]).$$

*Der Kettenbruch heißt **reinperiodisch**, wenn $n = -1$ gewählt werden kann, wenn es also keine Vorperiode gibt.*

Beispiel 6.20. (a) *Der Goldene Schnitt $\phi = \frac{1+\sqrt{5}}{2} \overset{6.14}{=} [\overline{1}]$ hat eine reinperiodische Kettenbruchentwicklung mit Periodenlänge 1.*

(b) $\sqrt{2} \overset{6.18}{=} [1, \overline{2}]$ *hat eine periodische Kettenbruchentwicklung mit Periodenlänge 1.*

Satz 6.21 (Euler-Lagrange). *Für ein beliebiges $x \in \mathbb{R}$ sind die folgenden beiden Aussagen äquivalent:*

(i) *Die Kettenbruchentwicklung von x ist periodisch.*

(ii) *Die Zahl x ist eine **quadratische Irrationalzahl**, es ist also x irrational und x erfüllt eine quadratische Gleichung der Form $ax^2 + bx + c = 0$ mit $a, b, c \in \mathbb{Z}$.*

Beweis. Gelte zunächst Aussage (i), die Kettenbruchentwicklung von x sei also periodisch. Damit ist sie insbesondere unendlich, weswegen x nach Satz 6.5 irrational ist. Sei die Kettenbruchentwicklung von x explizit durch $\big((a_0, a_1, \ldots, a_n, \overline{a_{n+1}, \ldots, a_{n+h}}), x\big)$ gegeben. Wir setzen $\xi := [\overline{a_{n+1}, \ldots, a_{n+h}}]$. Es ergibt sich $\xi = [a_{n+1}, \ldots, a_{n+h}, \xi]$. Die Folge der Näherungszähler bzw. -nenner zu ξ gemäß Lemma 6.12 bezeichnen wir im Folgenden mit $(p'_i)_{i\in\mathbb{N}_{-2}}$ bzw. $(q'_i)_{i\in\mathbb{N}_{-2}}$. Aus Lemma 6.12(c) erhalten wir

$$\xi = \frac{\xi p'_{h-1} + p'_{h-2}}{\xi q'_{h-1} + q'_{h-2}}$$

und daraus

$$\xi^2 q'_{h-1} + (q'_{h-2} - p'_{h-1})\xi - p'_{h-2} = 0.$$

Wir bezeichen die Folge der Näherungszähler bzw. -nenner zu x gemäß mit $(p_i)_{i\in\mathbb{N}_{-2}}$ bzw. $(q_i)_{i\in\mathbb{N}_{-2}}$. Dann gilt

$$x = [a_0, \ldots, a_n, \xi] = \frac{\xi p_n + p_{n-1}}{\xi q_n + q_{n-1}}$$

und aufgrunddessen

$$\xi = -\frac{q_{n-1}x - p_{n-1}}{q_n x - p_n}.$$

Das Einsetzen von ξ in die obige quadratische Gleichung für ξ und anschließendes Multiplizieren mit $(q_n x - p_n)^2$ liefert eine quadratische Gleichung für x mit Koeffizienten in $\mathbb{Z}$.

Gelte umgekehrt Aussage (ii) und sei x also eine quadratische Irrationalzahl mit $ax^2 + bx + c = 0$ für $a, b, c \in \mathbb{Z}$. Nach Satz 6.5 ist dann die Kettenbruchentwicklung von x unendlich, etwa $((a_0, a_1, \ldots), x)$. Seien $(\xi_n)_{n\in\mathbb{N}_0}$ wie im Kettenbruchalgorithmus definiert und $(p_n)_{n\in\mathbb{N}_{-2}}$ bzw. $(q_n)_{n\in\mathbb{N}_{-2}}$ die Folge der Näherungszähler bzw. -nenner. Dann ist insbesondere

$$x = [a_0, \ldots, a_n, \xi_n] = \frac{\xi_n p_n + p_{n-1}}{\xi_n q_n + q_{n-1}}$$

für alle $n \in \mathbb{N}_0$. Durch Einsetzen dieses Ausdrucks in die quadratische Gleichung für x erhalten wir

$$a\left(\frac{\xi_n p_n + p_{n-1}}{\xi_n q_n + q_{n-1}}\right)^2 + b\frac{\xi_n p_n + p_{n-1}}{\xi_n q_n + q_{n-1}} + c = 0$$

und deshalb

$$\begin{aligned}0 &= a(\xi_n p_n + p_{n-1})^2 + b(\xi_n p_n + p_{n-1})(\xi_n q_n + q_{n-1}) + c(\xi_n q_n + q_{n-1})^2 \\ &= \xi_n^2(ap_n^2 + bp_n q_n + cq_n^2) + \xi_n(2ap_n p_{n-1} + b(p_n q_{n-1} + p_{n-1}q_n) + 2cq_n q_{n-1}) \\ &+ ap_{n-1}^2 + bp_{n-1}q_{n-1} + cq_{n-1}^2\end{aligned}$$

Wir setzen für $n \in \mathbb{N}_0$

$$\begin{aligned}A_n &:= ap_n^2 + bp_n q_n + cq_n^2, \\ B_n &:= 2ap_n p_{n-1} + b(p_n q_{n-1} + p_{n-1}q_n) + 2cq_n q_{n-1}, \\ C_n &:= ap_{n-1}^2 + bp_{n-1}q_{n-1} + cq_{n-1}^2,\end{aligned}$$

so dass also $A_n\xi_n^2 + b_n\xi_n + C_n = 0$ gilt. Wir bemerken zudem, dass offenbar $C_{n+1} = A_n$ ist. Eine längere Rechnung ergibt

$$B_n^2 - 4A_nC_n = (b^2 - 4ac)(p_n q_{n-1} - q_n p_{n-1})^2 \overset{6.12}{=} b^2 - 4ac.$$

Nach Satz 6.15 (b) und Lemma 6.12 gilt

$$\left|x - \frac{p_n}{q_n}\right| < \frac{1}{q_n q_{n+1}} \leq \frac{1}{q_n^2},$$

es existiert also ein $\delta_n \in \mathbb{R}$ mit $|\delta_n| < 1$ und

$$x - \frac{p_n}{q_n} = -\delta_n \frac{1}{q_n^2}.$$

Das impliziert

$$p_n = xq_n + \frac{\delta_n}{q_n}$$

und deswegen

$$\begin{aligned}|A_n| &= |ap_n^2 + bp_n q_n + cq_n^2| \\ &= \left|a\left(xq_n + \frac{\delta_n}{q_n}\right)^2 + bq_n\left(xq_n + \frac{\delta_n}{q_n}\right) + cq_n^2\right| \\ &= \left|q_n^2(ax^2 + bx + c) + 2ax\delta_n + b\delta_n + a\frac{\delta_n^2}{q_n^2}\right| \\ &= \left|2ax\delta_n + b\delta_n + a\frac{\delta_n^2}{q_n^2}\right| \\ &< 2|ax| + |b| + |a|.\end{aligned}$$

Die rechte Seite ist unabhängig von n, also treten in der Folge $(A_n)_{n\in\mathbb{N}_0}$ nur endlich viele verschiedene Werte auf. Wegen $C_{n+1} = A_n$ gilt dies auch für die Folge $(C_n)_{n\in\mathbb{N}_0}$ und aufgrund von $B_n^2 - 4A_nC_n = b^2 - 4ac$ ebenso für die Folge $(B_n)_{n\in\mathbb{N}_0}$. Da $A_n\xi_n^2 + B_n\xi_n + C_n = 0$ gilt, können auch in der Folge $(\xi_n)_{n\in\mathbb{N}_0}$ nur endlich viele verschiedene Werte auftreten. Demzufolge gibt es ein $h \in \mathbb{N}$ und ein $m \in \mathbb{N}_0$ mit $\xi_{m+h} = \xi_m$. Das hat zur Folge, dass die Kettenbruchentwicklung von x periodisch ist. □

Proposition 6.22. *Sei $d \in \mathbb{Z}$ keine Quadratzahl. Dann erfüllt die Menge*

$$\mathbb{Q}(\sqrt{d}) := \{u + v\sqrt{d} : u, v \in \mathbb{Q}\} \subseteq \mathbb{C}.$$

die folgenden Eigenschaften:

(a) *$(1, \sqrt{d})$ ist eine Basis von $\mathbb{Q}(\sqrt{d})$ als $\mathbb{Q}$-Vektorraum.*

(b) *$\mathbb{Q}(\sqrt{d})$ ist mit der eingeschränkten Addition und Multiplikation von $\mathbb{C}$ ein Körper.*

(c) *Die Abbildung*

$$\bar{\cdot}: \begin{cases} \mathbb{Q}(\sqrt{d}) & \to \mathbb{Q}(\sqrt{d}), \\ u + v\sqrt{d} & \mapsto u - v\sqrt{d} \end{cases}$$

ist ein Körperautomorphismus von $\mathbb{Q}(\sqrt{d})$, es ist also $\bar{\cdot}$ bijektiv und für alle $x_1, x_2 \in \mathbb{Q}(\sqrt{d})$ gilt: $\overline{x_1 + x_2} = \overline{x_1} + \overline{x_2}$ sowie $\overline{x_1 \cdot x_2} = \overline{x_1} \cdot \overline{x_2}$.

(d) *Ein Element $x \in \mathbb{Q}(\sqrt{d})$ liegt genau dann in $\mathbb{Q}$, wenn $\overline{x} = x$ ist.*

(e) *Erfüllt $x \in \mathbb{Q}(\sqrt{d})$ die quadratische Gleichung $ax^2 + bx + c = 0$ mit $a, b, c \in \mathbb{Q}$, so ist $a\overline{x}^2 + b\overline{x} + c = 0$. Ist insbesondere $x \notin \mathbb{Q}$, so ist $\overline{x}$ die zweite Lösung dieser Gleichung.*

Beweis. Nach Definition erzeugt $(1, \sqrt{d})$ den $\mathbb{Q}$-Vektorraum $\mathbb{Q}(\sqrt{d})$. Weiter ist $(1, \sqrt{d})$ linear unabhängig über $\mathbb{Q}$, denn wäre $u \cdot 1 + v\sqrt{d} = 0$ mit $(u, v) \in \mathbb{Q}^2 \setminus \{(0, 0)\}$, so auch $v \neq 0$ und $\sqrt{d} = -\frac{u}{v} \in \mathbb{Q}$, was ein Widerspruch ist, denn d ist kein Quadrat. Das zeigt Behauptung (a).

Behauptung (b) überprüft man leicht.

Zum Beweis von Behauptung (c) betrachten wir $u_1, u_2, v_1, v_2 \in \mathbb{Q}$ und berechnen

$$\begin{aligned} \overline{(u_1 + v_1\sqrt{d}) + (u_2 + v_2\sqrt{d})} &= \overline{(u_1 + u_2) + (v_1 + v_2\sqrt{d})} = u_1 + u_2 - (v_1 + v_2)\sqrt{d} \\ &= (u_1 - v_1\sqrt{d}) + (u_2 - v_2)\sqrt{d} = \overline{u_1 + v_1\sqrt{d}} + \overline{u_2 + v_2\sqrt{d}} \end{aligned}$$

sowie

$$\begin{aligned} \overline{(u_1 + v_1\sqrt{d})(u_2 + v_2\sqrt{d})} &= \overline{u_1u_2 + v_1v_2d + (u_1v_2 + u_2v_1)\sqrt{d}} \\ &= u_1u_2 + v_1v_2d - (u_1v_2 + u_2v_1)\sqrt{d} \\ &= (u_1 - v_1\sqrt{d})(u_2 - v_2\sqrt{d}) \\ &= \overline{u_1 + v_1\sqrt{d}} \cdot \overline{u_2 + v_2\sqrt{d}}. \end{aligned}$$

Die Bijektivität der Abbildung ergibt sich daraus, dass es sich sich offenbar um eine Involution handelt, denn zweimaliges Anwenden liefert die Identität auf $\mathbb{Q}(\sqrt{d})$.

Behauptung (d) ist klar.

Behauptung (e) folgt vermöge Aussage (c) aus $ax^2 + bx + c = 0$ durch Anwenden von $\bar{\cdot}$, denn dann erhalten wir

$$0 = \overline{0} = \overline{ax^2 + bx + c} = a\overline{x}^2 + b\overline{x} + c.$$

□

Proposition 6.23. *Sei x eine quadratische Irrationalzahl. Dann gilt:*

(a) *Es gibt ein eindeutig bestimmtes quadratfreies $1 < d \in \mathbb{N}$ mit $x \in \mathbb{Q}(\sqrt{d})$. Damit existieren nach Proposition 6.22 eindeutig bestimmte $u, v \in \mathbb{Q}$ mit $x = u + v\sqrt{d}$. Anwendung von $\bar{\cdot}$ in $\mathbb{Q}(\sqrt{d})$ liefert $\overline{x} = u - v\sqrt{d}$. $\overline{x}$ heißt die zu x **konjugierte Zahl**.*

(b) *$\overline{x}$ ist eine quadratische Irrationalzahl.*

Beweis. Wir zeigen zunächst die Existenzaussage in Behauptung (a). Seien dafür $a, b, c \in \mathbb{Z}$ mit $ax^2 + bx + c = 0$. Da x irrational ist, gilt $a \neq 0$. In $\mathbb{R}$ erhalten wir

$$x = -\frac{b}{2a} \pm \frac{1}{2a}\sqrt{b^2 - 4ac}.$$

Wir schreiben $b^2 - 4ac = r^2 d$ mit $1 < d \in \mathbb{N}$ quadratfrei und $r \in \mathbb{N}$. Das impliziert

$$x = -\frac{b}{2a} \pm \frac{r}{2a}\sqrt{d}.$$

Mit $u := -\frac{b}{2a}$ und $v := \pm\frac{r}{2a}$ folgt $x = u + v\sqrt{d}$.

Zum Nachweis der Eindeutigkeit sei $x \in \mathbb{Q}(\sqrt{d_1}) \cap \mathbb{Q}(\sqrt{d_2})$ und $x \notin \mathbb{Q}$, wobei $1 < d_1, d_2 \in \mathbb{N}$ quadratfrei seien. Dann existieren $u_1, u_2, v_1, v_2 \in \mathbb{Q}$ mit $x = u_1 + v_1\sqrt{d_1} = u_2 + v_2\sqrt{d_2}$. Nach Multiplikation mit den auftretenden Nennern können wir ohne Einschränkung $u_1, u_2, v_1, v_2 \in \mathbb{Z}$ annehmen. Es ist dann

$$(u_1 - u_2)^2 = (v_2\sqrt{d_2} - v_1\sqrt{d_1})^2 = v_1^2 d_1 + v_2^2 d_2 - 2v_1 v_2\sqrt{d_1 d_2},$$

also

$$(u_1 - u_2)^2 - v_1^2 d_1 - v_2^2 d_2 + 2v_1 v_2\sqrt{d_1 d_2} = 0$$

Aufgrund von $x \notin \mathbb{Q}$ gilt hierbei $v_1, v_2 \neq 0$. Nach Proposition 6.22 (a) ist $d_1 d_2$ ein Quadrat und deshalb $d_1 = d_2$.

Behauptung (b) folgt direkt aus Proposition 6.22 (e). □

Schwächt man die Forderung der Quadratfreiheit von d ab, indem man nur noch fordert, dass d kein Quadrat ist, so gilt die Existenzaussage in (a) natürlich immer noch, die Eindeutigkeit geht allerdings verloren. Die nächste Bemerkung zeigt jedoch, dass das Berechnen des Konjugierten davon unbeschadet bleibt:

Proposition 6.24. *Sei x eine quadratische Irrationalzahl der Form $x = u + v\sqrt{d}$ mit $u, v \in \mathbb{Q}$ und nicht-quadratischem $d \in \mathbb{N}$. Dann gilt: $\overline{x} = u - v\sqrt{d}$.*

Beweis. Wir schreiben d in der Form $d = r^2 d'$ mit einem quadratfreien $1 < d' \in \mathbb{N}$ und $r \in \mathbb{N}$. Es ergibt sich

$$\overline{x} = \overline{u + v\sqrt{d}} = \overline{u + v\sqrt{r^2 d'}} = \overline{u + vr\sqrt{d'}} = u - vr\sqrt{d'} = u - v\sqrt{d}.$$

□

Beispiel 6.25. *Sei $x \in \mathbb{R}$ die positive reelle Nullstelle von $2X^2 - 6X - 1$. Dann ist $x = \frac{3}{2} + \frac{1}{4}\sqrt{44} = \frac{3}{2} + \frac{1}{2}\sqrt{11}$, also $\overline{x} = \frac{3}{2} - \frac{1}{2}\sqrt{11}$.*

Proposition 6.26. *Sei $x \in \mathbb{R}$ eine quadratische Irrationalzahl mit reinperiodischer Kettenbruchentwicklung $\left((\overline{a_0, a_1, \ldots, a_{h-1}}), x\right)$. Dann gilt:*

$$-\frac{1}{\overline{x}} = [\overline{a_{h-1}, \ldots, a_1, a_0}].$$

Beweis. Wir setzen $y := [\overline{a_{h-1}, \ldots, a_1, a_0}]$. Weiter seien $(p_n)_{n\in\mathbb{N}_{-2}}$, $(q_n)_{n\in\mathbb{N}_{-2}}$ bzw. $(p'_n)_{n\in\mathbb{N}_{-2}}$, $(q'_n)_{n\in\mathbb{N}_{-2}}$ die Folgen der Näherungsbruchzähler und -nenner zu x bzw. y. Es gilt dann

$$x = [a_0, a_1, \ldots, a_{h-1}, x], \quad y = [a_{h-1}, \ldots, a_1, a_0, y],$$

woraus sich mittels Lemma 6.12

$$x = \frac{xp_{h-1} + p_{h-2}}{xq_{h-1} + q_{h-2}}, \quad y = \frac{yp'_{h-1} + p'_{h-2}}{qq'_{h-1} + q'_{h-2}}$$

ergibt. Das liefert

$$\begin{aligned} q_{h-1}x^2 + (q_{h-2} - p_{h-1})x - p_{h-2} &= 0, \\ q'_{h-1}y^2 + (q'_{h-2} - p'_{h-1})y - p'_{h-2} &= 0. \end{aligned}$$

Durch Multiplikation der letzten Gleichung mit $-\frac{1}{y^2}$ finden wir

$$p'_{h-2}\left(-\frac{1}{y}\right)^2 + (q'_{h-2} - p'_{h-1})\left(-\frac{1}{y}\right) - q'_{h-1} = 0.$$

Nach Lemma 6.12 ist

$$\begin{pmatrix} p_{h-1} & p_{h-2} \\ q_{h-1} & q_{h-2} \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdot \ldots \cdot \begin{pmatrix} a_{h-1} & 1 \\ 1 & 0 \end{pmatrix},$$

was

$$\begin{pmatrix} p_{h-1} & p_{h-2} \\ q_{h-1} & q_{h-2} \end{pmatrix}^t = \begin{pmatrix} a_{h-1} & 1 \\ 1 & 0 \end{pmatrix} \cdot \ldots \cdot \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \overset{6.12}{=} \begin{pmatrix} p'_{h-1} & p'_{h-2} \\ q'_{h-1} & q'_{h-2} \end{pmatrix}$$

zur Folge hat. Das impliziert

$$p_{h-1} = p'_{h-1},\ p_{h-2} = q'_{h-1},\ q_{h-1} = p'_{h-2},\ q_{h-2} = q'_{h-2}$$

und somit erfüllt $-\frac{1}{y}$ dieselbe quadratische Gleichung wie x. Nach Proposition 6.22 (e) gilt dann $x = -\frac{1}{y}$ oder $\overline{x} = -\frac{1}{y}$. Aus $a_0 = a_h \geq 1$ folgt $x, y > 0$ und deshalb $-\frac{1}{y} < 0$, so dass der Fall $x = -\frac{1}{y}$ nicht auftritt. Demzufolge ist $\overline{x} = -\frac{1}{y}$ und also $y = -\frac{1}{\overline{x}}$. □

Beispiel 6.27. *Für $x = \frac{3+\sqrt{11}}{2}$ berechnen wir $x = [\overline{3,6}]$. Aus Proposition 6.26 ergibt sich $-\frac{1}{\overline{x}} = [\overline{6,3}]$, also*

$$[\overline{6,3}] = -\frac{1}{\frac{3-\sqrt{11}}{2}} = \frac{2}{\sqrt{11}-3} = \frac{2(\sqrt{11}+3)}{2} = 3+\sqrt{11}.$$

Definition 6.28. *Sei x eine quadratische Irrationalzahl. Die Zahl x heißt **reduziert**, wenn $x > 1$ ist und $-1 < \overline{x} < 0$ gilt.*

Beispiel 6.29. *$\frac{3+\sqrt{11}}{2}$ ist reduziert, denn es gilt $\frac{3+\sqrt{11}}{2} > 1$ und $-1 < \frac{3-\sqrt{11}}{2} < 0$.*

Satz 6.30. *Es sei x eine quadratische Irrationalzahl. Dann sind äquivalent:*

(i) *x ist reduziert.*

(ii) *Die Kettenbruchentwicklung von x ist reinperiodisch.*

Beweis. Gelte zunächst Aussage (ii) und sei die Kettenbruchentwicklung von x durch $\left((\overline{a_0, a_1, \ldots, a_{h-1}}), x\right)$ gegeben. Dann ist $x > a_0 = a_h \geq 1$ und aufgrund von Proposition 6.26 gilt

$$-\frac{1}{\overline{x}} = [\overline{a_{h-1}, \ldots, a_0}] > 1.$$

Damit ist $\frac{1}{\overline{x}} < -1$ und also $-1 < \overline{x} < 0$, so dass x reduziert ist.

Gelte umgekehrt Aussage (i) und sei also x reduziert. Ist $(\xi_i)_{i\in\mathbb{N}_0}$ die zugehörige Hilfsfolge aus dem Kettenbruchalgorithmus 6.4, so bemerken wir zunächst, dass ξ_0 eine quadratische Irrationalzahl ist. Dies ergibt sich daraus, dass mit der Kettenbruchentwicklung der quadratischen Irrationalzahl x auch die Kettenbruchentwicklung von ξ_0 periodisch ist. Dann ist ξ_0 reduziert,

denn: Nach Definition ist

$$\xi_0 = \frac{1}{x - \lfloor x \rfloor} > 1,$$

denn $x - \lfloor x \rfloor \in (0,1)$. Sei $d \in \mathbb{N}$ mit $x \in \mathbb{Q}(\sqrt{d})$. Nach Proposition 6.22 (b) ist auch $\xi_0 = \frac{1}{x-\lfloor x \rfloor} \in \mathbb{Q}(\sqrt{d})$ und es ist

$$\overline{\xi_0} = \frac{1}{\overline{x - \lfloor x \rfloor}} \overset{6.22}{=} \frac{1}{\overline{x} - \lfloor x \rfloor}.$$

Aufgrund von $-1 < \overline{x} < 0$ und $\lfloor x \rfloor \geq 1$ folgt $\overline{x} - \lfloor x \rfloor < -1$ und somit $-1 < \overline{\xi_0} < 0$. #

Induktiv folgt mit der gleichen Argumentation, dass ξ_i für jedes $i \in \mathbb{N}_0$ eine reduzierte quadratische Irrationalzahl ist – im Beweis hiervon spielt ξ_{i-1} die Rolle von x. Da x quadratische Irrationalzahl ist, besitzt x nach Satz 6.21 eine periodische Kettenbruchentwicklung

$\big((a_0, \ldots, a_n, \overline{a_{n+1}, \ldots, a_{n+h}}), x\big)$. Wir zeigen im Folgenden $a_n = a_{n+h}$. Die wiederholte Anwendung dieses Resultats liefert schließlich, dass die Kettenbruchentwicklung von x reinperiodisch ist, und der Beweis ist beendet. Nach den obigen Überlegungen ist ξ_{n-1} reduziert, also $0 < -\overline{\xi_{n-1}} < 1$ – im Fall $n = 0$ setzen wir hierbei $\xi_{-1} := x$. Aufgrund von

$$\xi_{n-1} = a_n + \frac{1}{\xi_n}$$

ist

$$-\frac{1}{\xi_n} = a_n - \xi_{n-1},$$

woraus

$$-\frac{1}{\overline{\xi_n}} = a_n + (-\overline{\xi_{n-1}}) \quad \text{mit } -\overline{\xi_{n-1}} \in (0,1)$$

folgt. Insbesondere ist

$$\lfloor -\frac{1}{\overline{\xi_n}} \rfloor = a_n.$$

Mit Proposition 6.26 folgt außerdem

$$-\frac{1}{\overline{\xi_n}} = [\overline{a_{n+h}, \ldots, a_{n+1}}]$$

und deshalb

$$a_{n+h} = \lfloor -\frac{1}{\overline{\xi_n}} \rfloor = a_n.$$

□

Abschließend untersuchen wir die Kettenbruchentwicklungen von Quadratwurzeln:

Beispiel 6.31.

$$\begin{aligned}
\sqrt{2} &= [1, \overline{2}] \\
\sqrt{3} &= [1, \overline{1, 2}] \\
\sqrt{5} &= [2, \overline{4}] \\
\sqrt{7} &= [2, \overline{1, 1, 1, 4}] \\
\sqrt{19} &= [4, \overline{2, 1, 3, 1, 2, 8}]
\end{aligned}$$

Proposition 6.32. *Sei $d \in \mathbb{N}$ kein Quadrat. Dann ist die Kettenbruchentwicklung von $\sqrt{d}$ vom Typ $\big((a_0, \overline{a_1, \ldots, a_{h-1}, 2a_0}), \sqrt{d}\big)$ mit $a_{h-i} = a_i$ für $i = 1, \ldots, h-1$.*

Beweis. Die Kettenbruchentwicklung von $\sqrt{d}$ sei durch $\big((a_n)_{n\in\mathbb{N}_0}, \sqrt{d}\big)$ gegeben. Zunächst ist $a_0 = \lfloor\sqrt{d}\rfloor$. Wir setzen $x := a_0 + \sqrt{d}$. Die Kettenbruchentwicklungen von $\sqrt{d}$ und x unterscheiden sich nur an der nullten Stelle: Dort steht a_0 bei $\sqrt{d}$ sowie $2a_0$ bei x. Die quadratische Irrationalzahl x ist reduziert, denn es gilt $x > 1$ und

$$\overline{x} = a_0 - \sqrt{d} = \lfloor\sqrt{d}\rfloor - \sqrt{d} \in (-1, 0).$$

Nach Satz 6.30 hat x eine reinperiodische Kettenbruchentwicklung $\big((\overline{2a_0, a_1, \ldots, a_{h-1}}), x\big)$, weshalb wir $\big((a_0, \overline{a_1, \ldots, a_{h-1}, 2a_0}), \sqrt{d}\big)$ als Kettenbruchentwicklung von $\sqrt{d}$ erhalten. Es verbleibt der Nachweis der Symmetrieeigenschaft. Mit

$$\xi_0 = \frac{1}{x - 2a_0} = [\overline{a_1, \ldots, a_{h-1}, 2a_0}]$$

ergibt sich

$$-\frac{1}{\overline{\xi_0}} = [\overline{2a_0, a_{h-1}, \ldots, a_1}].$$

Andererseits ist

$$-\frac{1}{\overline{\xi_0}} = -\frac{1}{\frac{1}{\overline{x} - 2a_0}} = -(\overline{x} - 2a_0) = -(a_0 - \sqrt{d} - 2a_0) = a_0 + \sqrt{d} = x.$$

Das impliziert

$$[\overline{2a_0, a_1, \ldots, a_{h-1}}] = [\overline{2a_0, a_{h-1}, \ldots, a_1}].$$

In Verbindung mit Proposition 6.26 folgt daraus $a_{h-i} = a_i$ für $i = 1, \ldots, h-1$. □

6.3 Die Pell'sche Gleichung und diophantische Approximation

In diesem Abschnitt studieren wir mit der ***Pell'schen Gleichung***

$$X_1^2 - dX_2^2 = 1 \quad \text{für ein Nicht-Quadrat } d \in \mathbb{N}$$

und ihren Verallgemeinerungen

$$X_1^2 - dX_2^2 = c \quad \text{für ein Nicht-Quadrat } d \in \mathbb{N} \text{ und ein } c \in \mathbb{Z}$$

eine weitere Klasse diophantischer Gleichungen, deren Lösungstheorie eng mit der Theorie quadratischer Zahlkörper zusammenhängt. Wir schreiben

$$L_d := \{(x, y) \in \mathbb{Z}^2 : x^2 - dy^2 = 1\}$$

für die Lösungsmenge der Pell'schen Gleichung zum Parameter d. Diese enthält stets die beiden trivialen Lösungen $(\pm 1, 0)$. Die Frage ist, ob L_d darüber hinaus weitere Elemente enthält. Wir zeigen zunächst, dass L_d unter der Annahme der Existenz einer nichttrivialen Lösung aus unendlich vielen Elementen besteht, und geben eine Beschreibung von L_d an. Wichtig hierfür ist die Faktorisierung

$$(X_1 + X_2\sqrt{d})(X_1 - X_2\sqrt{d}) = 1$$

der Pell'schen Gleichung zum Parameter d, aufgrund derer jedes Element aus L_d zu einem Element

$$x + y\sqrt{d} \in \mathbb{Q}(\sqrt{d}) \quad \text{mit } x, y \in \mathbb{Z} \text{ und } (x + y\sqrt{d})\overline{(x + y\sqrt{d})} = 1$$

korrespondiert.

Satz 6.33. *Sei $d \in \mathbb{N}$ kein Quadrat. Dann gilt: Falls die Pell'sche Gleichung $X_1^2 - dX_2^2 = 1$ eine nichttriviale ganzzahlige Lösung besitzt, so gibt es unter den Lösungen (x, y) in $L_d \cap \mathbb{N}^2$ eine eindeutig bestimmte Lösung mit minimalem x. Diese heißt die **Fundamentallösung** in L_d. Ist (a, b) die Fundamentallösung, so gilt*

$$L_d = \{\pm(x_n, y_n) \in \mathbb{Z}^2 : x_n + y_n\sqrt{d} = (a + b\sqrt{d})^n, n \in \mathbb{Z}\}.$$

Beweis. Aufgrund der vorausgesetzten Existenz einer nichttrivialen Lösung in L_d ist auch $L_d \cap \mathbb{N}^2 \neq \emptyset$. Da für eine Lösung $(x, y) \in L_d \cap \mathbb{N}^2$ der Wert von y durch den Wert von x eindeutig festgelegt ist, gibt es unter den Lösungen (x, y) in $L_d \cap \mathbb{N}^2$ eine eindeutig bestimmte Lösung mit minimalem x. Damit ist die Existenz und Eindeutigkeit der Fundamentallösung bereits gezeigt.

Sei im Folgenden (a, b) die Fundamentallösung. Wir bemerken, dass für $(x_1, y_1), (x_2, y_2) \in L_d \cap \mathbb{N}^2$ mit $x_1 < x_2$ auch $y_1 < y_2$ gilt, denn es ist

$$y_2^2 = \frac{x_2^2 - 1}{d} > \frac{x_1^2 - 1}{d} = y_1^2.$$

Damit gilt offenbar für von (a, b) verschiedenes $(x, y) \in L_d \cap \mathbb{N}^2$ die Ungleichung

$$1 < a + b\sqrt{d} < x + y\sqrt{d}.$$

Sei nun $(x, y) \in L_d$. Wir bemerken, dass $x = 0$ zu $dy^2 = 1$ und damit zu einem Widerspruch führt, während $y = 0$ zu $x = \pm 1$ führt. Es ergeben sich daher die folgenden fünf Fälle:

Fall 1: $x = \pm 1$ **und** $y = 0$**.** Dann ist $x + y\sqrt{d} = \pm 1 = \pm(a + b\sqrt{d})^0$.

Fall 2: $x > 0$ **und** $y > 0$**.** Dann gibt es ein $n \in \mathbb{N}$ mit $x + y\sqrt{d} = (a + b\sqrt{d})^n$,

denn: Nehmen wir an, dies wäre nicht der Fall. Dann existierte ein $n \in \mathbb{N}$ mit

$$(a + b\sqrt{d})^n < x + y\sqrt{d} < (a + b\sqrt{d})^{n+1}.$$

Mit $(a+b\sqrt{d})(a-b\sqrt{d}) = a^2 - db^2 = 1$ folgte

$$\begin{aligned} 1 &= (a+b\sqrt{d})^n(a-b\sqrt{d})^n < (x+y\sqrt{d})(a-b\sqrt{d})^n \\ &< (a+b\sqrt{d})^{n+1}(a-b\sqrt{d})^n = a+b\sqrt{d}. \end{aligned}$$

Schrieben wir $(x+y\sqrt{d})(a-b\sqrt{d})^n = \tilde{a}+\tilde{b}\sqrt{d}$ mit $\tilde{a},\tilde{b} \in \mathbb{Z}$, so erhielten wir

$$\begin{aligned} (x-y\sqrt{d})(a+b\sqrt{d})^n &= \overline{x+y\sqrt{d}} \cdot \overline{(a-b\sqrt{d})^n} = \overline{(x+y\sqrt{d})(a-b\sqrt{d})^n} \\ &= \overline{\tilde{a}+\tilde{b}\sqrt{d}} = \tilde{a}-\tilde{b}\sqrt{d}. \end{aligned}$$

Das lieferte

$$\begin{aligned} \tilde{a}^2 - d\tilde{b}^2 &= (\tilde{a}+\tilde{b}\sqrt{d})(\tilde{a}-\tilde{b}\sqrt{d}) = (x+y\sqrt{d})(a-b\sqrt{d})^n(x-y\sqrt{d})(a+b\sqrt{d})^n \\ &= (x^2-dy^2)(a^2-db^2)^n = 1 \end{aligned}$$

und somit $(\tilde{a},\tilde{b}) \in L_d$. Wegen $\tilde{a}+\tilde{b}\sqrt{d} < a+b\sqrt{d}$ könnte $(\tilde{a},\tilde{b})$ dabei nicht in $L_d \cap \mathbb{N}^2$ liegen. Im Fall $\tilde{a} \leq 0$ und $\tilde{b} > 0$ wäre aber

$$0 > -\frac{1}{\tilde{a}+\tilde{b}\sqrt{d}} = -(\tilde{a}-\tilde{b}\sqrt{d}) = -\tilde{a}+\tilde{b}\sqrt{d} > 0$$

und im Fall $\tilde{a} > 0$ und $\tilde{b} \leq 0$ gälte

$$1 > \frac{1}{\tilde{a}+\tilde{b}\sqrt{d}} = \tilde{a}-\tilde{b}\sqrt{d} \geq \tilde{a}+\tilde{b}\sqrt{d} > 1.$$

Folglich erhielten wir $\tilde{a} \leq 0$ und $\tilde{b} \leq 0$, im Widerspruch zu $\tilde{a}+\tilde{b}\sqrt{d} > 1$. #

Fall 3: $x < 0$ **und** $y < 0$**.** Dann ist

$$x+y\sqrt{d} = -(-x-y\sqrt{d}) = -(a+b\sqrt{d})^n$$

für ein $n \in \mathbb{N}$ nach Fall 2.

Fall 4: $x > 0, y < 0$**.** Dann ist

$$\frac{1}{x+y\sqrt{d}} = x-y\sqrt{d} = (a+b\sqrt{d})^n$$

für ein $n \in \mathbb{N}$ nach Fall 2 und deshalb $x+y\sqrt{d} = (a+b\sqrt{d})^{-n}$.

Fall 5: $x < 0, y > 0$**.** Dann ist

$$-\frac{1}{x+y\sqrt{d}} = -x+y\sqrt{d} = (a+b\sqrt{d})^n$$

für ein $n \in \mathbb{N}$ nach Fall 2 und deshalb $x+y\sqrt{d} = -(a+b\sqrt{d})^{-n}$.

Seien nun umgekehrt $n \in \mathbb{Z}$ und $x_n, y_n \in \mathbb{Z}$ mit $x_n + y_n\sqrt{d} = (a + b\sqrt{d})^n$. Dann ist

$$x_n - y_n\sqrt{d} = \overline{x_n + y_n\sqrt{d}} = \overline{(a + b\sqrt{d})^n} = (a - b\sqrt{d})^n.$$

und somit

$$x_n^2 - dy_n^2 = (x_n + y_n\sqrt{d})(x_n - y_n\sqrt{d}) = (a + b\sqrt{d})^n(a - b\sqrt{d})^n = (a^2 - db^2)^n = 1,$$

und also $(x_n, y_n) \in L_d$. Damit ist auch $(-x_n, -y_n) \in L_d$. □

Satz 6.33 sagt leider nichts über die Existenz einer nichttrivialen Lösung der Pell'schen Gleichung aus. Unser Ziel im weiteren Verlauf des Abschnitts ist die Konstruktion solch nichttrivialer Lösungen. Die Theorie der Kettenbrüche kommt dabei wie folgt ins Spiel: Ist $(x, y) \in \mathbb{N}^2$ eine Lösung von $X_1^2 - dX_2^2 = 1$, so ist

$$\frac{x}{y} = \sqrt{d + \frac{1}{y^2}}$$

eine sehr gute rationale Näherung von $\sqrt{d}$. Wir werden zeigen, dass es sich um eine sogenannte diophantische Approximation von $\sqrt{d}$ handelt und dass solche diophantischen Approximationen durch Näherungsbrüche von $\sqrt{d}$ gegeben sind. Zunächst definieren wir:

Definition 6.34. *Seien $\alpha \in \mathbb{R}$ und $z = \frac{p}{q} \in \mathbb{Q}$ mit $p \in \mathbb{Z}, q \in \mathbb{N}$ und $\mathrm{ggT}(p, q) = 1$. Die rationale Zahl z heißt eine **diophantische Approximation** von α, wenn für alle $\tilde{p} \in \mathbb{Z}, \tilde{q} \in \mathbb{N}$ mit $\tilde{q} \leq q$ und $\frac{\tilde{p}}{\tilde{q}} \neq \frac{p}{q}$ die Ungleichung*

$$|\alpha q - p| < |\alpha\tilde{q} - \tilde{p}|$$

gilt.

Ist $z = \frac{p}{q}$ mit $p \in \mathbb{Z}, q \in \mathbb{N}$ und $\mathrm{ggT}(p, q) = 1$ eine diophantische Approximation von $\alpha \in \mathbb{R}$, dann gibt es keine rationale Zahl $\frac{\tilde{p}}{\tilde{q}}$ mit $\tilde{p} \in \mathbb{Z}, \tilde{q} \in \mathbb{N}$ und $\tilde{q} \leq q$, für die

$$\left|\alpha - \frac{\tilde{p}}{\tilde{q}}\right| \leq \left|\alpha - \frac{p}{q}\right|,$$

gilt, denn andernfalls wäre

$$|\alpha\tilde{q} - \tilde{p}| = \tilde{q}\left|\alpha - \frac{\tilde{p}}{\tilde{q}}\right| \leq q\left|\alpha - \frac{p}{q}\right| = |\alpha q - p|.$$

Die Umkehrung hiervon ist falsch: Es gibt etwa keine rationale Zahl $\frac{\tilde{p}}{\tilde{q}} \neq \frac{1}{3}$ mit $\tilde{p} \in \mathbb{Z}, \tilde{q} \in \mathbb{N}$ und $\tilde{q} \leq 3$, für die

$$\left|\frac{1}{5} - \frac{\tilde{p}}{\tilde{q}}\right| \leq \left|\frac{1}{5} - \frac{1}{3}\right| = \frac{2}{15}$$

gilt, aber $\frac{1}{3}$ ist keine diophantische Approximation von $\frac{1}{5}$, denn es ist $\frac{0}{1} \neq \frac{1}{3}$, $1 < 3$ und

$$\left|\frac{1}{5} \cdot 1 - 0\right| = \frac{1}{5} < \left|\frac{1}{5} \cdot 3 - 1\right| = \frac{2}{5}.$$

Satz 6.35. *Seien $\alpha \in \mathbb{R}$ und $\left(\frac{p_n}{q_n}\right)_{n\in I}$ die Folge der Näherungsbrüche von α mit $I = \mathbb{N}_0$ für $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ ist und $I = \{0, \ldots, k\}$ für $\alpha \in \mathbb{Q}$. Sei weiter $z \in \mathbb{Q}$ eine diophantische Approximation von α. Dann gibt es ein $n \in I$ mit $z = \frac{p_n}{q_n}$, es ist also z ein Näherungsbruch von α.*

Beweis. Wir schreiben $z = \frac{p}{q}$ mit $p \in \mathbb{Z}$, $q \in \mathbb{N}$ und $\mathrm{ggT}(p, q) = 1$. Ist $\alpha = a_0 \in \mathbb{Z}$, so folgt $|\alpha \cdot 1 - a_0| = 0$, so dass $\frac{a_0}{1} = \alpha$ die einzige diophantische Approximation von α ist und also $z = \frac{a_0}{1} = \frac{p_0}{q_0}$ gilt. Im Folgenden sei $\alpha \notin \mathbb{Z}$. Insbesondere ist $k \geq 1$, falls $\alpha \in \mathbb{Q}$ ist. Nach Satz 6.13 gilt

$$a_0 = \frac{p_0}{q_0} < \frac{p_2}{q_2} < \frac{p_4}{q_4} < \ldots \leq \alpha \leq \ldots < \frac{p_3}{q_3} < \frac{p_1}{q_1}.$$

Ist z nicht von der Form $\frac{p_n}{q_n}$ für ein $n \in \mathbb{N}_0$, dann liegt z in einem der Intervalle $(-\infty, \frac{p_0}{q_0})$, $(\frac{p_1}{q_1}, \infty)$ oder in einem Intervall zwischen zwei Näherungsbrüchen. Wir unterscheiden sechs Fälle:

Fall 1: $z < \frac{p_0}{q_0}$**.** Wegen $\frac{p_0}{q_0} = a_0 \leq \alpha$ gilt $|\alpha - a_0| < |\alpha - z|$. Die rationale Zahl $\frac{a_0}{1}$ liegt somit näher an α als z, weswegen z keine diophantische Approximation von α sein kann.

Fall 2: $z > \frac{p_1}{q_1}$**.** Wegen $\frac{p_1}{q_1} \geq \alpha$ gilt

$$|\alpha - z| = \left|\alpha - \frac{p}{q}\right| \geq \left|\frac{p_1}{q_1} - \frac{p}{q}\right| = \frac{|p_1 q - p q_1|}{q_1 q} \geq \frac{1}{q_1 q}$$

und deshalb

$$|\alpha q - p| \geq \frac{1}{q_1} = \frac{1}{q_1 q_0} \overset{6.15,6.16}{\geq} \left|\alpha - \frac{p_0}{q_0}\right| = |\alpha \cdot 1 - a_0|.$$

Weil $z = \frac{p}{q}$ eine diophantische Approximation von α ist, folgt $\frac{a_0}{1} = \frac{p}{q}$ und deshalb

$$\frac{p_0}{q_0} = \frac{a_0}{1} = \frac{p}{q} = z > \frac{p_1}{q_1},$$

im Widerspruch zu Satz 6.13.

Fall 3: $\frac{p_{n-1}}{q_{n-1}} < \frac{p}{q} < \frac{p_{n+1}}{q_{n+1}}$ **für ein ungerades** $n \in \mathbb{N}$ **mit** $n + 1 \leq k$**, falls** $\alpha \in \mathbb{Q}$**.** Wir erhalten

$$\frac{1}{q q_{n-1}} \leq \frac{|p q_{n-1} - p_{n-1} q|}{q q_{n-1}} = \left|\frac{p}{q} - \frac{p_{n-1}}{q_{n-1}}\right| < \left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_{n-1}}{q_{n-1}}\right| \leq \left|\alpha - \frac{p_{n-1}}{q_{n-1}}\right| \overset{6.15,6.16}{\leq} \frac{1}{q_{n-1} q_n}$$

und somit $q_n < q$. Außerdem ist

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

woraus sich

$$|\alpha q - p| \geq \frac{1}{q_{n+1}} = q_n \frac{1}{q_n q_{n+1}} \overset{6.15,6.16}{\geq} q_n \left|\alpha - \frac{p_n}{q_n}\right| = |\alpha q_n - p_n|$$

ergibt. Da $z = \frac{p}{q}$ eine diophantische Approximation von α ist, folgt wegen $q_n < q$, dass $\frac{p}{q} = \frac{p_n}{q_n}$ ist, was ein Widerspruch zu $\mathrm{ggT}(p,q) = 1$ ist.

Fall 4: $\frac{p_{n+1}}{q_{n+1}} < \frac{p}{q} < \frac{p_{n-1}}{q_{n-1}}$ **für ein gerades** $n \in \mathbb{N}$ **mit** $n+1 \leq k$**, falls** $\alpha \in \mathbb{Q}$**.** Dieser Fall wird analog zu Fall 3 behandelt.

Fall 5: $\alpha = \frac{p_k}{q_k} < \frac{p}{q} < \frac{p_{k-1}}{q_{k-1}}$ **für** $\alpha \in \mathbb{Q}$ **und** k **gerade.** Dieser Fall wird analog zu Fall 3 behandelt.

Fall 6: $\frac{p_{k-1}}{q_{k-1}} < \frac{p}{q} < \frac{p_k}{q_k} = \alpha$ **für** $\alpha \in \mathbb{Q}$ **und** k **ungerade.** Dieser Fall wird analog zu Fall 3 behandelt.

Da alle Fälle zum Widerspruch führen, ist z von der Form $\frac{p_n}{q_n}$ für ein $n \in \mathbb{N}_0$. □

Satz 6.36. *Seien $\alpha \in \mathbb{R}$ und $\left(\frac{p_n}{q_n}\right)_{n\in I}$ die Folge der Näherungsbrüche von α mit $I = \mathbb{N}_0$ für $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ ist und $I = \{0,\dots,k\}$ für $\alpha \in \mathbb{Q}$. Dann ist $\frac{p_n}{q_n}$ eine diophantische Approximation von α für alle $n \in I$ mit $n \geq 1$.*

Beweis. Im Folgenden sei $n \in I$ mit $n \geq 1$. Dann ist

$$B_n := \big\{(p,q) \in \mathbb{Z} \times \mathbb{N} : q \leq q_n \text{ und } |\alpha q - p| \text{ minimal}\big\}.$$

wohldefiniert und nichtleer, denn die zweite Komponente kann nur endlich viele Werte annehmen, und für festes q gilt $|\alpha q - p| \to \infty$ für $p \to \infty$ und $p \to -\infty$. Darüber hinaus setzen wir

$$q^* := \min\big\{q \in \mathbb{N} : \text{Es existiert ein } p \in \mathbb{Z} \text{ mit } (p,q) \in B_n\big\}.$$

Es gibt genau ein $p^* \in \mathbb{Z}$ mit $(p^*,q^*) \in B_n$,

denn: Angenommen, es gäbe $p^*, \tilde{p}$ mit $(p^*,q^*), (\tilde{p},q^*) \in B_n$ und $p^* \neq \tilde{p}$. Dann gälte $|\alpha q^* - p^*| = |\alpha q^* - \tilde{p}|$ und deshalb

$$\left|\alpha - \frac{p^*}{q^*}\right| = \left|\alpha - \frac{\tilde{p}}{q^*}\right|.$$

Wegen $p^* \neq \tilde{p}$ wäre $\frac{p^*}{q^*} \neq \frac{\tilde{p}}{q^*}$ und deshalb $\alpha = \frac{p^*+\tilde{p}}{2q^*}$. Das lieferte

$$|\alpha q^* - p^*| = \left|\frac{p^*+\tilde{p}}{2} - p^*\right| = \left|\frac{\tilde{p}-p^*}{2}\right| \geq \frac{1}{2}.$$

Wir unterscheiden nun drei Fälle:

Fall 1: $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ **oder** $\alpha \in \mathbb{Q}$ **mit** $k \geq 2$**, jeweils mit** $a_1 > 1$**.** Dann wäre $q_2 > q_1 > q_0 = 1$, also $q_2 \geq 3$ und somit

$$|\alpha q_1 - p_1| = q_1\left|\alpha - \frac{p_1}{q_1}\right| \leq q_1 \frac{1}{q_1 q_2} = \frac{1}{q_2} \leq \frac{1}{3},$$

was ein Widerspruch zur Minimalität von $|\alpha q^* - p^*| \geq \frac{1}{2}$ ist.

Fall 2: $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ **oder** $\alpha \in \mathbb{Q}$ **mit** $k \geq 2$**, jeweils mit** $a_1 = 1$**.** Es ergäbe sich $q_1 = q_0 = 1$, $\frac{p_0}{q_0} = a_0$ und $\frac{p_1}{q_1} = a_0 + 1$. Wegen $\alpha \neq [a_0, 2]$ wäre $|\alpha - a_0| < \frac{1}{2}$ oder $|\alpha - (a_0 + 1)| < \frac{1}{2}$. Andererseits gälte $|\alpha - a_0| = |\alpha q_0 - p_0|$ und $|\alpha - (a_0 + 1)| = |\alpha q_1 - p_1|$. Das lieferte $|\alpha q_0 - p_0| < \frac{1}{2}$ oder $|\alpha q_1 - p_1| < \frac{1}{2}$, im Widerspruch zur Minimalität von $|\alpha q^* - p^*| \geq \frac{1}{2}$.

Fall 3: $\alpha \in \mathbb{Q}$ **mit** $k = 1$**.** Dann wäre $\alpha = \frac{p_1}{q_1}$, also $|\alpha q_1 - p_1| = 0$, was wiederum zum Widerspruch führt. #

Es ist $\mathrm{ggT}(p^*, q^*) = 1$, andernfalls wären p^*, q^* von der Form $p^* = d\tilde{p}$ und $q^* = d\tilde{q}$ mit einem $d > 1$. Das hätte

$$|\alpha\tilde{q} - \tilde{p}| < d\,|\alpha\tilde{q} - \tilde{p}| = |\alpha q^* - p^*|$$

zur Folge, was ein Widerspruch ist. Nach Konstruktion ist $\frac{p^*}{q^*}$ eine diophantische Approximation von α. Nach Satz 6.35 gibt es ein $m \in \mathbb{N}_0$ mit $\frac{p^*}{q^*} = \frac{p_m}{q_m}$. Wegen $q^* \leq q_n$ folgt $m \leq n$ – hier geht $n \geq 1$ ein; für $n = 0$ wäre auch $m = 1$ möglich. Weil $\mathrm{ggT}(p^*, q^*) = 1$ ist, erhalten wir $p^* = p_m$ und $q^* = q_m$. Es gilt $m = n$,

denn: Wir nehmen an, es gälte $m < n$. Nach Satz 6.15 hätten wir dann

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

Nach Konstruktion von $p^* = p_m$, $q^* = q_m$ gälte

$$|\alpha q_m - p_m| \leq |\alpha q_n - p_n| = q_n \left|\alpha - \frac{p_n}{q_n}\right| \overset{6.15}{\leq} q_n \frac{1}{q_n q_{n+1}} = \frac{1}{q_{n+1}}.$$

Damit erhielten wir

$$\frac{1}{q_{n-1} + q_n} < \frac{1}{q_{n+1}},$$

also $q_{n+1} < q_n + q_{n-1}$, was ein Widerspruch ist, denn es gilt $q_{n+1} = a_{n+1}q_n + q_{n-1} \geq q_n + q_{n-1}$. #

Somit ist $\frac{p_n}{q_n} = \frac{p^*}{q^*}$ eine diophantische Approximation von α. □

Eine genaue Analyse des Beweises zeigt, dass die Aussage von Satz 6.36 auch im Fall $n = 0$ gültig ist, allerdings mit folgenden Ausnahmen:

- $\alpha = [a_0, 2]$,
- $\alpha = [a_0, 1, \ldots, a_k]$ mit $k \geq 2$,
- $\alpha = [a_0, 1, a_2, \ldots]$,

bei denen $\frac{p_0}{q_0}$ keine diophantische Approximation von α ist.

Satz 6.37. *Seien $\alpha \in \mathbb{R}$ und $p \in \mathbb{Z}$ sowie $q \in \mathbb{N}$ mit $\mathrm{ggT}(p,q) = 1$ und*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2}.$$

Dann ist $\frac{p}{q}$ eine diophantische Approximation von α, insbesondere ist $\frac{p}{q}$ ein Näherungsbruch von α.

Beweis. Angenommen, es gäbe $\tilde{p} \in \mathbb{Z}$, $\tilde{q} \in \mathbb{N}$ mit $\tilde{q} \leq q$, $\frac{\tilde{p}}{\tilde{q}} \neq \frac{p}{q}$ und $|\alpha\tilde{q} - \tilde{p}| \leq |\alpha q - p|$. Dann gälte

$$\left|\alpha - \frac{\tilde{p}}{\tilde{q}}\right| = \frac{1}{\tilde{q}}\,|\alpha\tilde{q} - \tilde{p}| \leq \frac{1}{\tilde{q}}\,|\alpha q - p| = \frac{q}{\tilde{q}}\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q\tilde{q}}.$$

Das lieferte

$$\left|\frac{\tilde{p}}{\tilde{q}} - \frac{p}{q}\right| \leq \left|\alpha - \frac{\tilde{p}}{\tilde{q}}\right| + \left|\alpha - \frac{p}{q}\right| < \frac{1}{2q\tilde{q}} + \frac{1}{2q^2} = \frac{q+\tilde{q}}{2q^2\tilde{q}}.$$

Andererseits wäre

$$\left|\frac{p}{q} - \frac{\tilde{p}}{\tilde{q}}\right| = \frac{|\tilde{p}q - p\tilde{q}|}{q\tilde{q}} \geq \frac{1}{q\tilde{q}}.$$

Wir erhielten

$$\frac{1}{q\tilde{q}} < \frac{q+\tilde{q}}{2q^2\tilde{q}},$$

deshalb auch

$$2q < q + \tilde{q}$$

und schließlich

$$q < \tilde{q},$$

was ein Widerspruch ist. Somit ist $\frac{p}{q}$ eine diophantische Approximation von α und aufgrund von Satz 6.35 auch ein Näherungsbruch von α. □

Satz 6.38. *Sei $d \in \mathbb{N}$ kein Quadrat und sei $c \in \mathbb{Z}$ mit $|c| < \frac{1}{2}(\sqrt{f} + \sqrt{d})$ mit*

$$f := \begin{cases} d & \text{für } c \geq 0, \\ \max\{c+d, 0\} & \text{für } c < 0. \end{cases}$$

Weiter bezeichne $\left(\frac{p_n}{q_n}\right)_{n\in\mathbb{N}_0}$ die Folge der Näherungsbrüche von $\sqrt{d}$. Dann gibt es für jede Lösung $(p,q) \in \mathbb{N}^2$ der Gleichung $X_1^2 - dX_2^2 = c$ ein $n \in \mathbb{N}_0$ mit $\frac{p}{q} = \frac{p_n}{q_n}$. Ist insbesondere $\mathrm{ggT}(p,q) = 1$, so ist $p = p_n$ und $q = q_n$.

Beweis. Seien $p, q \in \mathbb{N}$ mit $p^2 - dq^2 = c$ und $\tilde{p}, \tilde{q} \in \mathbb{N}$ mit $\mathrm{ggT}(\tilde{p}, \tilde{q}) = 1$ und $\frac{p}{q} = \frac{\tilde{p}}{\tilde{q}}$. Dann ist

$$p - q\sqrt{d} = \frac{c}{p + q\sqrt{d}} \quad \text{und} \quad p = \sqrt{c + dq^2}.$$

Das liefert

$$\left|\sqrt{d} - \frac{\tilde{p}}{\tilde{q}}\right| = \left|\sqrt{d} - \frac{p}{q}\right| = \frac{|c|}{q(p + q\sqrt{d})} = \frac{|c|}{q(\sqrt{c + dq^2} + q\sqrt{d})} = \frac{|c|}{q^2(\sqrt{\frac{c}{q^2} + d} + \sqrt{d})}$$
$$\leq \frac{|c|}{q^2(\sqrt{f} + \sqrt{d})} < \frac{1}{2q^2} \leq \frac{1}{2\tilde{q}^2},$$

weshalb $\frac{p}{q} = \frac{\tilde{p}}{\tilde{q}}$ nach Satz 6.37 eine diophantische Approximation von $\sqrt{d}$ und somit ein Näherungsbruch von $\sqrt{d}$ ist. □

Korollar 6.39. *Sei $d \in \mathbb{N}$ kein Quadrat und bezeichne $\left(\frac{p_n}{q_n}\right)_{n \in \mathbb{N}_0}$ die Folge der Näherungsbrüche von $\sqrt{d}$. Dann gilt:*

$$L_d \cap \mathbb{N}^2 \subseteq \{(p_n, q_n) : n \in \mathbb{N}_0\},$$

es ist also für jede Lösung $(p, q) \in \mathbb{N}^2$ der Pell'schen Gleichung $X_1^2 - dX_2^2 = 1$ der Bruch $\frac{p}{q}$ ein Näherungsbruch von $\sqrt{d}$.

Beweis. Wir bemerken zum Beweis, dass für $c = 1$ die Abschätzung aus Satz 6.38 trivialerweise erfüllt ist und dass für jede Lösung $(p, q) \in \mathbb{N}^2$ der Pell'schen Gleichung $X_1^2 - dX_2^2 = 1$ stets $\mathrm{ggT}(p, q) = 1$ gilt, denn jeder gemeinsame Teiler von p, q teilt auch $p^2 - dq^2 = 1$. □

Die Aussage des Korollars impliziert noch nicht, dass unter den Näherungsbrüchen wie oben auch tatsächlich Lösungen der Pell'schen Gleichung auftreten. Davon müssen wir uns im weiteren Verlauf noch überzeugen.

Beispiel 6.40. *Sei $d = 3$. Es gilt $\sqrt{3} = [1, \overline{1, 2}]$ und daher*

$$\frac{p_0}{q_0} = \frac{1}{1}, \ \frac{p_1}{q_1} = \frac{2}{1}, \ \frac{p_2}{q_2} = \frac{5}{3}, \ \frac{p_3}{q_3} = \frac{7}{4}, \ \frac{p_4}{q_4} = \frac{19}{11}.$$

Das liefert

$$p_0^2 - 3q_0^2 = -2, \ p_1^2 - 3q_1^2 = 1, \ p_2^2 - 3q_2^2 = -2, \ p_3^2 - 3q_3^2 = 1, \ p_4^2 - 3q_4^2 = -2.$$

Unter den ersten fünf Näherungsbrüchen liefern also $\frac{p_1}{q_1}$ und $\frac{p_3}{q_3}$ Lösungen der Pell'schen Gleichung $X_1^2 - 3X_2^2 = 1$. Die Fundamentallösung ist offenbar durch $(p_1, q_1) = (2, 1)$ gegeben.

Satz 6.41. *Sei $d \in \mathbb{N}$ kein Quadrat und sei die Kettenbruchentwicklung von $\sqrt{d}$ durch*

$$\left((a_0, \overline{a_1, \ldots, a_h}), \sqrt{d}\right)$$

mit Periodenlänge h gegeben. Sei weiter $\left(\frac{p_n}{q_n}\right)_{n \in \mathbb{N}_0}$ die Folge der Näherungsbrüche von $\sqrt{d}$ und die Folge $(\xi_n)_{n \in \mathbb{N}_0}$ wie im Kettenbruchalgorithmus 6.4 definiert. Schließlich setzen wir $b_0 := \lfloor \sqrt{d} \rfloor$, $c_{-1} := 1$ und $c_0 := d - b_0^2$ sowie $b_{n+1} := a_n c_n - b_n$ und $c_{n+1} := c_{n-1} + 2a_n b_n - a_n^2 c_n$ für $n \geq 0$. Dann gelten für alle $n \in \mathbb{N}_0$ die folgenden Aussagen:

(a) $\xi_n = \frac{b_n+\sqrt{d}}{c_n}$,

(b) $p_n^2 - dq_n^2 = (-1)^{n+1}c_n$,

(c) $0 < c_n < 2\sqrt{d}$,

(d) $c_n = 1 \iff n \equiv -1 \bmod (h)$.

Beweis. Wir zeigen zunächst die Gleichung

$$d - b_{n+1}^2 = c_n c_{n+1}$$

für $n \geq -1$ per Induktion: Für $n = -1$ ist $d - b_0^2 = c_0 = c_0 c_{-1}$. Für $n > -1$ ist

$$\begin{aligned} d - b_{n+1}^2 &= d - (a_n c_n - b_n)^2 = (d - b_n^2) + (2a_n c_n b_n - a_n^2 c_n^2) = d - b_n^2 + c_n(c_{n+1} - c_{n-1}) \\ &= c_{n-1}c_n + c_n c_{n+1} - c_n c_{n-1} = c_n c_{n+1}. \end{aligned}$$

Da d kein Quadrat ist, impliziert dies insbesondere $c_n \neq 0$ für alle $n \in \mathbb{N}_0$.

Auch Behauptung (a) zeigen wir per Induktion: Für $n = 0$ ist $a_0 = \lfloor \sqrt{d} \rfloor$ und

$$\xi_0 = \frac{1}{\sqrt{d} - \lfloor \sqrt{d} \rfloor} = \frac{1}{\sqrt{d} - b_0} = \frac{b_0 + \sqrt{d}}{d - b_0^2} = \frac{b_0 + \sqrt{d}}{c_0}.$$

Für $n > 1$ erhalten wir

$$\begin{aligned} \xi_{n+1} &= \frac{1}{\xi_n - a_n} = \frac{c_n}{b_n + \sqrt{d} - a_n c_n} = \frac{c_n}{\sqrt{d} - b_{n+1}} = \frac{c_n(b_{n+1} + \sqrt{d})}{d - b_{n+1}^2} = \frac{c_n(b_{n+1} + \sqrt{d})}{c_n c_{n+1}} \\ &= \frac{b_{n+1} + \sqrt{d}}{c_{n+1}}. \end{aligned}$$

Zum Beweis von Behauptung (b) betrachten wir ein $n \in \mathbb{N}_0$. Nach Lemma 6.12 gilt

$$\sqrt{d} = \frac{\xi_n p_n + p_{n-1}}{\xi_n q_n + q_{n-1}} = \frac{(b_n + \sqrt{d})p_n + c_n p_{n-1}}{(b_n + \sqrt{d})q_n + c_n q_{n-1}}.$$

und somit

$$\big((b_n + \sqrt{d})q_n + c_n q_{n-1}\big)\sqrt{d} = (b_n + \sqrt{d})p_n + c_n p_{n-1}.$$

Das liefert

$$(b_n p_n + c_n p_{n-1} - dq_n) + (p_n - b_n q_n - c_n q_{n-1})\sqrt{d} = 0,$$

was nach Proposition 6.23

$$b_n p_n + c_n p_{n-1} - dq_n = 0 \text{ und } p_n - b_n q_n - c_n q_{n-1} = 0$$

zur Folge hat. Wir erhalten

$$q_n(b_n p_n + c_n p_{n-1} - dq_n) + p_n(p_n - b_n q_n - c_n q_{n-1}) = 0$$

und damit

$$p_n^2 + c_n(p_{n-1}q_n - p_n q_{n-1}) - dq_n^2 = 0.$$

Unter Verwendung von Lemma 6.12 ergibt sich

$$p_n^2 - dq_n^2 = (-1)^{n+1} c_n.$$

Behauptung (c) zeigen wir wieder per Induktion nach n: Für $n = 0$ ist

$$c_0 = d - \left\lfloor \sqrt{d} \right\rfloor^2 = (\sqrt{d} - \left\lfloor \sqrt{d} \right\rfloor)(\sqrt{d} + \left\lfloor \sqrt{d} \right\rfloor),$$

woraus sich $0 < c_0 < 2\sqrt{d}$ ergibt. Sei nun $n \geq 1$. Nach Proposition 6.32 besitzt ξ_n eine reinperiodische Kettenbruchentwicklung und nach Satz 6.30 ist ξ_n reduziert, es ist also $\xi_n > 1$ und $-1 < \overline{\xi_n} < 0$. Wir erhalten

$$0 < \xi_n - \overline{\xi_n} = \frac{b_n + \sqrt{d}}{c_n} - \frac{b_n - \sqrt{d}}{c_n} = \frac{2\sqrt{d}}{c_n},$$

was $c_n > 0$ zur Folge hat. Das liefert

$$|b_n| = \sqrt{d - c_{n-1}c_n} < \sqrt{d}.$$

Aufgrund von $\xi_n > 1$ ergibt sich $c_n < c_n \xi_n = b_n + \sqrt{d} \leq |b_n| + \sqrt{d} < 2\sqrt{d}$.

Zum Beweis von Behauptung (d) betrachten wir zunächst ein $n \in \mathbb{N}_0$ mit $n \equiv -1 \bmod (h)$ und ein $k \in \mathbb{N}$ mit $n = kh - 1$. Es ist dann

$$\begin{aligned}\xi_n &= [a_{n+1}, a_{n+2}, \ldots] = [a_{kh}, a_{kh+1}, \ldots] = [\overline{a_h, a_1, \ldots, a_{h-1}}] = [a_h, \overline{a_1, \ldots, a_h}] \overset{6.32}{=} [2a_0, \overline{a_1, \ldots, a_h}] \\ &= a_0 + [a_0, \overline{a_1, \ldots, a_h}] = a_0 + \sqrt{d}\end{aligned}$$

und damit $c_n = 1$. Sei nun umgekehrt $n \in \mathbb{N}_0$ mit $c_n = 1$. Dann ist $\xi_n = b_n + \sqrt{d}$, deshalb ist ξ_n von der Form

$$\xi_n = [\tilde{a}_0, a_1, a_2, \ldots]$$

mit einem $\tilde{a}_0 \in \mathbb{Z}$. Da ξ_n reduziert ist – siehe Beweis von (c); das gilt auch für $n = 0$ – ist $\xi_n > 1$ und deshalb $\tilde{a}_0 \in \mathbb{N}$. Wegen $\sqrt{d} = [a_0, a_1, \ldots, a_n, \xi_n]$ erhalten wir

$$[a_0, a_1, \ldots] = \sqrt{d} = [a_0, a_1, \ldots, a_n, \tilde{a}_0, a_1, a_2, \ldots].$$

Aus der Eindeutigkeit der Kettenbruchentwicklung ergibt sich $a_{i+(n+1)} = a_i$ für alle $i \geq 1$. Andererseits gilt ebenfalls $a_{i+h} = a_i$ für alle $i \geq 1$. Wir schreiben $n + 1 = qh + r$ mit einem $r \in \mathbb{N}_0$ mit $0 \leq r < h$. Dann erhalten wir für alle $i \geq 1$ die Identität

$$a_i = a_{i+(n+1)} = a_{i+qh+r} = a_{i+r},$$

was wegen der Minimalität von h zu $r = 0$ führt. Deshalb folgt $h \mid (n+1)$ und somit $n \equiv -1 \bmod (h)$. □

Korollar 6.42 (Legendre). *Seien $d \in \mathbb{N}$ kein Quadrat und $\left(\frac{p_n}{q_n}\right)_{n\in\mathbb{N}_0}$ die Folge der Näherungsbrüche von $\sqrt{d}$ sowie h die Periodenlänge von $\sqrt{d}$. Ferner sei*

$$\tilde{h} := \begin{cases} h & \text{für } h \text{ gerade,} \\ 2h & \text{für } h \text{ ungerade.} \end{cases}$$

Dann gilt

$$L_d \cap \mathbb{N}^2 = \{(p_{k\tilde{h}-1}, q_{k\tilde{h}-1}) : k \in \mathbb{N}\}.$$

Die Fundamentallösung in L_d ist durch $(p_{\tilde{h}-1}, q_{\tilde{h}-1})$ gegeben.

Beweis. Sei zunächst $(p,q) \in L_d \cap \mathbb{N}^2$. Nach Korollar 6.39 gibt es dann ein $n \in \mathbb{N}_0$ mit $p = p_n$ und $q = q_n$. Nach Satz 6.41 gilt dabei

$$1 = p^2 - dq^2 = p_n^2 - dq_n^2 = (-1)^{n+1} c_n$$

mit einem c_n wie dort, insbesondere gilt $c_n > 0$. Somit ist n ungerade und $c_n = 1$. Mit Satz 6.41 folgt $n \equiv -1 \bmod (h)$, so dass es ein $\tilde{k} \in \mathbb{N}$ mit $n = \tilde{k}h - 1$ gibt, wobei $\tilde{k}$ genau dann gerade ist, wenn h ungerade ist. Somit existiert ein $k \in \mathbb{N}$ mit $n = k\tilde{h} - 1$ und es ist also $(p,q) = (p_{k\tilde{h}-1}, q_{k\tilde{h}-1})$.

Ist umgekehrt $n = k\tilde{h} - 1$ mit einem $k \in \mathbb{N}$, so ist

$$p_n^2 - dq_n^2 = p_{k\tilde{h}-1}^2 - dq_{k\tilde{h}-1}^2 \overset{6.41}{=} (-1)^{k\tilde{h}} c_{k\tilde{h}-1} \overset{6.41}{=} 1$$

und also $(p_n, q_n) \in L_d \cap \mathbb{N}^2$.

Es verbleibt, die Fundamentallösung zu identifizieren. Nach Lemma 6.12 ist $q_{\tilde{h}-1} < q_{2\tilde{h}-1} < \ldots$, und wegen $p_{\tilde{k}h-1} = \sqrt{1 + dq_{\tilde{k}h-1}^2}$ folgt $p_{\tilde{h}-1} < p_{2\tilde{h}-1} < \ldots$. Somit ist $(p_{\tilde{h}-1}, q_{\tilde{h}-1})$ die Fundamentallösung in L_d. □

Beispiel 6.43. *Sei $d = 23$. Dann ist $\sqrt{23} = [4, \overline{1,3,1,8}]$ und somit $h = \tilde{h} = 4$. Nach Korollar 6.42 ist daher (p_3, q_3) die Fundamentallösung der Pell'schen Gleichung $X_1^2 - 23X_2^2 = 1$. Wir berechnen*

$$\begin{aligned} \begin{pmatrix} p_3 & p_2 \\ q_3 & q_2 \end{pmatrix} &= \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} a_2 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} a_3 & 1 \\ 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 4 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 24 & 19 \\ 5 & 4 \end{pmatrix}, \end{aligned}$$

so dass $(24, 5)$ die Fundamentallösung der Pell'schen Gleichung $X_1^2 - 23X_2^2 = 1$ ist.

Korollar 6.44. *Seien $d \in \mathbb{N}$ kein Quadrat und $\left(\frac{p_n}{q_n}\right)_{n\in\mathbb{N}_0}$ die Folge der Näherungsbrüche von $\sqrt{d}$ sowie h die Periodenlänge von $\sqrt{d}$. Dann gilt:*

(a) *Ist h gerade, dann hat die Gleichung $X_1^2 - dX_2^2 = -1$ keine Lösung $(p,q) \in \mathbb{Z}^2$.*

(b) *Ist h ungerade, dann sind die Lösungen $(p,q) \in \mathbb{N}^2$ der Gleichung $X_1^2 - dX_2^2 = -1$ durch (p_{kh-1}, q_{kh-1}) mit ungeraden $k \in \mathbb{N}$ gegeben.*

Beweis. Offenbar hat die Gleichung $X_1^2 - dX_2^2 = -1$ keine ganzzahligen Lösungen (x,y) mit $x = 0$ oder $y = 0$. Nach Satz 6.38 mit $c = -1$ und unter Verwendung von

$$|-1| = 1 < \frac{1}{2}(1+\sqrt{2}) \leq \frac{1}{2}(\sqrt{d-1}+\sqrt{d})$$

folgt, dass es für jede Lösung $(p,q) \in \mathbb{N}^2$ ein $n \in \mathbb{N}_0$ mit $p = p_n$ und $q = q_n$ gibt. Hierbei verwenden wir $\mathrm{ggT}(p,q) = 1$, denn jeder gemeinsame Teiler von p und q teilt auch $p^2 - dq^2 = -1$. Nach Satz 6.41 ist

$$p_n^2 - dq_n^2 = (-1)^{n+1} c_n$$

mit $c_n > 0$. Im Folgenden nehmen wir an, dass (p_n, q_n) eine Lösung ist. Dann folgt $c_n = 1$, nach Satz 6.41 also $n \equiv -1 \bmod (h)$, so dass es ein $k \in \mathbb{N}$ mit $n = kh - 1$ gibt.

Ist nun h gerade, so ist $n = kh - 1$ ungerade und demzufolge

$$p_n^2 - dq_n^2 = (-1)^{n+1} = 1,$$

was ein Widerspruch ist. Unter dieser Voraussetzung kann es also keine Lösungen in $\mathbb{N}^2$ und demzufolge auch keine in $\mathbb{Z}^2$ geben. Das ist Behauptung (a).

Ist h ungerade, so folgt analog

$$p_n^2 - dq_n^2 = (-1)^{kh}.$$

Die Lösungen $(p,q) \in \mathbb{N}^2$ sind in diesem Fall genau durch die (p_{kh-1}, q_{kh-1}) mit $k \in \mathbb{N}$ ungerade gegeben. Das ist Behauptung (b). □

Beispiel 6.45. (a) *Sei $d = 23$. Nach Beispiel 6.43 ist dann $h = 4$ und nach Korollar 6.44 hat die Gleichung $X_1^2 - 23X_2^2 = -1$ keine ganzzahligen Lösungen. Das kann man natürlich auch dadurch sehen, dass man die Gleichung modulo 23 betrachtet und feststellt, dass $\left(\frac{-1}{23}\right) = -1$ ist.*

(b) *Sei $d = 5$. Dann ist $\sqrt{5} = [2,\overline{4}]$ und also $h = 1$. Nach Korollar 6.44 sind somit die Lösungen $(p,q) \in \mathbb{N}^2$ von $X_1^2 - 5X_2^2 = -1$ durch (p_{k-1}, q_{k-1}) mit $k \in \mathbb{N}$ ungerade gegeben, also durch (p_{2k}, q_{2k}) mit $k \in \mathbb{N}_0$ gegeben. Es gilt: $(p_0, q_0) = (2,1)$, $(p_2, q_2) = (38,17), \ldots$ Die Lösungen von $X_1^2 - 5X_2^2 = 1$ in $\mathbb{N}^2$ sind durch (p_{2k-1}, q_{2k-1}) mit $k \in \mathbb{N}$ gegeben.*

6.4 Die Einheitengruppe des Ganzheitsringes quadratischer Zahlkörper

Definition 6.46. *Sei K ein Körper mit $\mathbb{Q} \subseteq K \subseteq \mathbb{C}$ und den von $\mathbb{C}$ eingeschränkten Verknüpfungen. Insbesondere kann man K mit der skalaren Multiplikation $\mathbb{Q} \times K \to K$, $(\alpha, x) \mapsto \alpha x$ als $\mathbb{Q}$-Vektorraum auffassen. K heißt ein **quadratischer Zahlkörper**, wenn $\dim_{\mathbb{Q}} K = 2$ ist.*

Proposition 6.47. *Sei K ein Körper mit $\mathbb{Q} \subseteq K \subseteq \mathbb{C}$ und den von $\mathbb{C}$ eingeschränkten Verknüpfungen. Dann sind die folgenden beiden Aussagen äquivalent:*

(i) *K ist ein quadratischer Zahlkörper.*

(ii) *Es gibt ein eindeutig bestimmtes quadratfreies $d \in \mathbb{Z} \setminus \{0,1\}$ mit $K = \mathbb{Q}(\sqrt{d})$.*

*Ist $\tilde{d} \in \mathbb{Z}$ mit $\tilde{d} = r^2 d$ und $r \in \mathbb{N}$, $d \in \mathbb{Z} \setminus \{0,1\}$ quadratfrei, so ist $\mathbb{Q}(\sqrt{\tilde{d}}) = \mathbb{Q}(\sqrt{d})$. Im Fall $d > 0$ heißt K ein **reellquadratischer Zahlkörper**, im Fall $d < 0$ ein **imaginärquadratischer Zahlkörper**.*

Beweis. Gelte zunächst Aussage (i) und sei also K ein quadratischer Zahlkörper. Wir zeigen nun zuerst die Existenz. Sei $x \in K \setminus \mathbb{Q}$. Dann ist das System $(1, x)$ offenbar $\mathbb{Q}$-linear unabhängig und wegen $\dim_{\mathbb{Q}} K = 2$ also eine $\mathbb{Q}$-Basis von K. Das System $(1, x, x^2)$ ist wegen $\dim_{\mathbb{Q}} K = 2$ linear abhängig über $\mathbb{Q}$, so dass es $a, b, c \in \mathbb{Q}$ mit $ax^2 + bx + c = 0$ und $a \neq 0$ gibt, wobei wir ohne Einschränkung $a, b, c \in \mathbb{Z}$ annehmen können. In $\mathbb{C}$ erhalten wir die Gleichung

$$x = -\frac{b}{2a} \pm \frac{1}{2a}\sqrt{b^2 - 4ac}.$$

Wir schreiben $b^2 - 4ac = r^2 d$ mit $r \in \mathbb{N}$ und $d \in \mathbb{Z}$ quadratfrei. Wegen $x \notin \mathbb{Q}$ ist $d \neq 0, 1$. Das liefert $x = -\frac{b}{2a} \pm \frac{r}{2a}\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ und somit $K = \mathbb{Q} + \mathbb{Q}x \subseteq \mathbb{Q}(\sqrt{d})$. Nach Proposition 6.22 ist $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{d}) = 2 = \dim_{\mathbb{Q}} K$ und deshalb $K = \mathbb{Q}(\sqrt{d})$. Es verbleibt der Nachweis der Eindeutigkeit. Sei $K = \mathbb{Q}(\sqrt{d_1}) = \mathbb{Q}(\sqrt{d_2})$ mit $d_1, d_2 \in \mathbb{Z} \setminus \{0,1\}$ quadratfrei. Insbesondere ist dann $\sqrt{d_1} \in \mathbb{Q}(\sqrt{d_2})$ und es gibt $u, v \in \mathbb{Q}$ mit $\sqrt{d_1} = u + v\sqrt{d_2}$. Das liefert $d_1 = u^2 + v^2 d_2 + 2uv\sqrt{d_2}$. Aus Proposition 6.22 erhalten wir $uv = 0$. Wäre $v = 0$, dann wäre $\sqrt{d_1} = u \in \mathbb{Z}$, was ein Widerspruch ist. Also ist $u = 0$ und damit $d_1 = v^2 d_2$. Da d_1 quadratfrei ist, ist $v = 1$ und deshalb $d_1 = d_2$.

Gelte umgekehrt Aussage (ii). Nach Proposition 6.22 ist $\mathbb{Q}(\sqrt{d})$ ein Körper, und $(1, \sqrt{d})$ eine Basis von $\mathbb{Q}(\sqrt{d})$ als $\mathbb{Q}$-Vektorraum. Insbesondere ist $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{d}) = 2$.

Sei nun $\tilde{d} = r^2 d$ mit $r \in \mathbb{N}$ und $d \in \mathbb{Z}$ quadratfrei, $d \neq 0, 1$. Offenbar ist $(1, \sqrt{\tilde{d}}) = (1, r\sqrt{d})$ und damit aber auch $(1, \sqrt{d})$ eine $\mathbb{Q}$-Basis von $\mathbb{Q}(\sqrt{\tilde{d}})$. Es folgt $\mathbb{Q}(\sqrt{\tilde{d}}) = \mathbb{Q}(\sqrt{d})$. □

Wir erinnern an dieser Stelle daran, dass wir nach Proposition 6.22 auf dem Körper $\mathbb{Q}(\sqrt{d})$ den Körperautomorphismus

$$\bar{\cdot}\colon \begin{cases} \mathbb{Q}(\sqrt{d}) & \to \mathbb{Q}(\sqrt{d}), \\ u + v\sqrt{d} & \mapsto u - v\sqrt{d} \end{cases}$$

haben.

Definition 6.48. *Sei K ein quadratischer Zahlkörper und $d \in \mathbb{Z}$ quadratfrei mit $K = \mathbb{Q}(\sqrt{d})$. Wir definieren die Abbildungen **Norm** und **Spur** als*

$$\mathrm{N}\colon \begin{cases} K & \to \mathbb{Q}, \\ x = u + v\sqrt{d} & \mapsto x\overline{x} = u^2 - v^2 d \end{cases} \quad \textit{bzw.} \quad \mathrm{Sp}\colon \begin{cases} K & \to \mathbb{Q}, \\ x = u - v\sqrt{d} & \mapsto x + \overline{x} = 2u. \end{cases}$$

Wie man leicht nachrechnet, erfüllen Norm und Spur die folgenden Eigenschaften:

Proposition 6.49. *Seien K ein quadratischer Zahlkörper und $x, y \in K$. Dann gilt:*

(a) $\mathrm{N}(xy) = \mathrm{N}(x)\,\mathrm{N}(y)$,
(b) $\mathrm{Sp}(x+y) = \mathrm{Sp}(x) + \mathrm{Sp}(y)$,
(c) $\mathrm{N}(x) = \mathrm{N}(\overline{x})$,
(d) $\mathrm{Sp}(x) = \mathrm{Sp}(\overline{x})$,
(e) $x^2 - \mathrm{Sp}(x)x + \mathrm{N}(x) = 0$.

Definition 6.50. *Seien K ein quadratischer Zahlkörper und $x \in K$. Das Element x heißt **ganz**, wenn $\mathrm{Sp}(x) \in \mathbb{Z}$ und $\mathrm{N}(x) \in \mathbb{Z}$ ist. Wir setzen*

$$\mathcal{O}_K := \{x \in K : x \text{ ist ganz}\}.$$

Proposition 6.51. *Seien K ein quadratischer Zahlkörper und $x \in K$. Dann gilt:*

(a) $\mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$.
(b) $x \in \mathcal{O}_K \iff \overline{x} \in \mathcal{O}_K$.

Beweis. Behauptung (a) ergibt sich aus

$$\mathcal{O}_K \cap \mathbb{Q} = \{x \in \mathbb{Q} : x \text{ ist ganz}\} = \{x \in \mathbb{Q} : \mathrm{Sp}(x) = 2x \in \mathbb{Z} \text{ und } \mathrm{N}(x) = x^2 \in \mathbb{Z}\} = \mathbb{Z}.$$

Behauptung (b) folgt aus Proposition 6.49 (c),(d). □

Beispiel 6.52. *Sei $K = \mathbb{Q}(\sqrt{5})$.*

- $x = 2 - \sqrt{5}$: $\mathrm{Sp}(x) = 4$, $\mathrm{N}(x) = (2-\sqrt{5})(2+\sqrt{5}) = 4 - 5 = -1$ *und also* $x \in \mathcal{O}_K$.
- $x = 1 + \frac{1}{2}\sqrt{5}$: $\mathrm{Sp}(x) = 2$, $\mathrm{N}(x) = (1+\frac{1}{2}\sqrt{5})(1-\frac{1}{2}\sqrt{5}) = 1 - \frac{5}{4} = -\frac{1}{4}$ *und also* $x \notin \mathcal{O}_K$.
- $x = \frac{3}{2} + \frac{1}{2}\sqrt{5}$: $\mathrm{Sp}(x) = 3$, $\mathrm{N}(x) = (\frac{3}{2}+\frac{1}{2}\sqrt{5})(\frac{3}{2}-\frac{1}{2}\sqrt{5}) = \frac{9}{4} - \frac{5}{4} = 1$ *und also* $x \in \mathcal{O}_K$.

Wie man im obigen Beispiel sieht, können bei ganzen Elementen in quadratischen Zahlkörpern sehr wohl Nenner auftreten.

Proposition 6.53. *Seien K ein quadratischer Zahlkörper und $x \in K \setminus \mathbb{Q}$. Dann sind äquivalent:*

(i) $x \in \mathcal{O}_K$.
(ii) *Es gibt ein normiertes quadratisches Polynom $f = X^2 + aX + b \in \mathbb{Z}[X]$ mit $f(x) = 0$.*

Beweis. Gelte zunächst Aussage (i) und sei also $x \in \mathcal{O}_K$. Dann ist $\mathrm{N}(x) \in \mathbb{Z}$ und $\mathrm{Sp}(x) \in \mathbb{Z}$, weshalb das Polynom $f := X^2 - \mathrm{Sp}(x)X + \mathrm{N}(x)$ in $\mathbb{Z}[X]$ liegt. Nach Proposition 6.49 gilt weiter $f(x) = 0$.

Gelte nun umgekehrt Aussage (ii) und sei $f(x) = x^2 + ax + b = 0$ mit $a, b \in \mathbb{Z}$. Wegen $x \in K \setminus \mathbb{Q}$ ist dann $x \neq \overline{x}$ und nach Proposition 6.22 ist $\overline{x}^2 + a\overline{x} + b = 0$; es sind also $x, \overline{x}$ die zwei Nullstellen von f. Es folgt

$$f = (X - x)(X - \overline{x}) = X^2 - \mathrm{Sp}(x)X + \mathrm{N}(x).$$

Wegen $f \in \mathbb{Z}[X]$ ist $\mathrm{Sp}(x) = -a \in \mathbb{Z}$ und $\mathrm{N}(x) = b \in \mathbb{Z}$ und also x ganz. □

Der nächste Satz liefert eine explizite Beschreibung der ganzen Elemente eines quadratischen Zahlkörpers. Als Nebenprodukt erhalten wir, dass diese einen Ring bilden:

Satz 6.54. *Seien K ein quadratischer Zahlkörper und $d \in \mathbb{Z}$ quadratfrei mit $K = \mathbb{Q}(\sqrt{d})$. Dann gilt:*

(a) $\mathcal{O}_K = \mathbb{Z}[\omega] = \{a + b\omega : a, b \in \mathbb{Z}\}$ *mit* $\omega = \begin{cases} \frac{1}{2}(1 + \sqrt{d}) & \text{für } d \equiv 1 \bmod (4), \\ \sqrt{d} & \text{für } d \equiv 2, 3 \bmod (4). \end{cases}$

(b) $\mathcal{O}_K$ *ist ein Ring, der sogenannte* ***Ganzheitsring*** *von K.*

(c) $\mathcal{O}_K^\times = \{x \in \mathcal{O}_K : \mathrm{N}(x) = \pm 1\}$.

Beweis. Für den Beweis von Behauptung (a) sei zunächst $x \in \mathcal{O}_K$. Wir schreiben x in der Form $x = u + v\sqrt{d}$ mit $u, v \in \mathbb{Q}$. Es ist $\mathrm{Sp}(x) = 2u \in \mathbb{Z}$, so dass es ein $p \in \mathbb{Z}$ mit $u = \frac{p}{2}$ gibt. Somit ist $x = \frac{p}{2} + v\sqrt{d}$ und

$$\mathrm{N}(x) = \frac{p^2}{4} - v^2 d \in \mathbb{Z}.$$

Es gibt demzufolge ein $a \in \mathbb{Z}$ mit $v^2 d = \frac{a}{4}$. Weil d quadratfrei ist, existiert ein $q \in \mathbb{Z}$ mit $v = \frac{q}{2}$. Wir erhalten $x = \frac{p}{2} + \frac{q}{2}\sqrt{d}$ und deshalb

$$\mathrm{N}(x) = \frac{p^2 - q^2 d}{4} \in \mathbb{Z},$$

also $p^2 \equiv q^2 d \bmod (4)$. Wir unterscheiden nun zwei Fälle:

Fall 1: $d \equiv 2, 3 \bmod (4)$**.** Wäre $q^2 \equiv 1 \bmod (4)$, so folgte $p^2 \equiv q^2 d \equiv d \equiv 2, 3 \bmod (4)$, was ein Widerspruch ist. Es ist also $q^2 \equiv 0 \bmod (4)$ und folglich $p^2 \equiv 0 \bmod (4)$. Das liefert $2 \mid p$ und $2 \mid q$ und somit $u, v \in \mathbb{Z}$, also $x = u + v\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$.

Fall 2: $d \equiv 1 \bmod (4)$**.** Dann ist $p^2 \equiv q^2 \pmod 4$ und deshalb $p \equiv q \pmod 2$. Wir erhalten

$$x = \frac{p}{2} + \frac{q}{2}\sqrt{d} = \frac{p - q}{2} + q\frac{1}{2}(1 + \sqrt{d}) = \frac{p - q}{2} + q\omega \in \mathbb{Z}[\omega].$$

Damit ist die Inklusion $\mathcal{O}_K \subseteq \mathbb{Z}[\omega]$ gezeigt. Sei nun umgekehrt $x \in \mathbb{Z}[\omega]$. Wir unterscheiden wieder dieselben zwei Fälle:

Fall 1: $d \equiv 2,3 \bmod (4)$**.** Dann existieren $a, b \in \mathbb{Z}$ mit $x = a + b\sqrt{d}$. Demzufolge ist

$$\mathrm{Sp}(x) = \mathrm{Sp}(a + b\sqrt{d}) = 2a \in \mathbb{Z}, \quad \mathrm{N}(x) = \mathrm{N}(a + b\sqrt{d}) = a^2 - b^2 d \in \mathbb{Z}$$

und also $x \in \mathcal{O}_K$.

Fall 2: $d \equiv 1 \bmod (4)$**.** In diesem Fall existieren $a, b \in \mathbb{Z}$ mit

$$x = a + b\omega = a + b\frac{1+\sqrt{d}}{2} = a + \frac{b}{2} + \frac{b}{2}\sqrt{d}.$$

Es ergeben sich

$$\begin{aligned}
\mathrm{Sp}(x) &= \mathrm{Sp}(a + \frac{b}{2} + \frac{b}{2}\sqrt{d}) = 2a + b \in \mathbb{Z}, \\
\mathrm{N}(x) &= \mathrm{N}(a + \frac{b}{2} + \frac{b}{2}\sqrt{d}) = (a + \frac{b}{2})^2 - \frac{b^2}{4}d = a^2 + ab + \frac{b^2}{4}(1-d),
\end{aligned}$$

was wegen $d \equiv 1 \bmod (4)$ ebenfalls in $\mathbb{Z}$ liegt. Somit ist $x \in \mathcal{O}_K$.

Wir zeigen nun Behauptung (b). Wegen $\mathcal{O}_K \subseteq \mathbb{C}$ und $0, 1 \in \mathcal{O}_K$ müssen wir nur nachrechnen, dass $\mathcal{O}_K$ abgeschlossen unter Addition und Multiplikation ist. Nach Aussage (a) ist $\mathcal{O}_K = \mathbb{Z}[\omega]$ für ω wie in (a) angegeben. Für beliebige $x = a_1 + b_1\omega$ und $y = a_2 + b_2\omega$ in $\mathcal{O}_K$ mit $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ gilt dann

$$\begin{aligned}
x + y &= (a_1 + a_2) + (b_1 + b_2)\omega \in \mathbb{Z}[\omega] = \mathcal{O}_K, \\
xy &= (a_1 + b_1\omega)(x_2 + y_2\omega) = a_1a_2 + (a_1b_2 + b_1a_2)\omega + b_1b_2\omega^2.
\end{aligned}$$

Um $xy \in \mathcal{O}_K$ zu folgern, genügt es $\omega^2 \in \mathbb{Z}[\omega]$ zu zeigen. Im Fall $d \equiv 2,3 \bmod (4)$ ist $\omega^2 = (\sqrt{d})^2 = d \in \mathbb{Z}[\omega]$. Im Fall $d \equiv 1 \bmod (4)$ gilt

$$\omega^2 = \left(\frac{1+\sqrt{d}}{2}\right)^2 = \frac{1 + 2\sqrt{d} + d}{4} = \frac{2 + 2\sqrt{d} + d - 1}{4} = \frac{d-1}{4} + \omega \in \mathbb{Z}[\omega].$$

Zum Beweis von Behauptung (c) sei schließlich zunächst $x \in \mathcal{O}_K^\times$. Dann ist $x^{-1} \in \mathcal{O}_K^\times$ und wir erhalten

$$1 = \mathrm{N}(1) = \mathrm{N}(xx^{-1}) = \mathrm{N}(x)\,\mathrm{N}(x^{-1})$$

mit $\mathrm{N}(x), \mathrm{N}(x^{-1}) \in \mathbb{Z}$. Das liefert $\mathrm{N}(x) \in \{\pm 1\}$. Sei nun umgekehrt $x \in \mathcal{O}_K$ mit $\mathrm{N}(x) \in \{\pm 1\}$. Dann ist $x \neq 0$ und in $\mathbb{Q}(\sqrt{d})$ gilt die Identität

$$\frac{1}{x} = \frac{\overline{x}}{x\overline{x}} = \frac{\overline{x}}{\mathrm{N}(x)} = \pm\overline{x} \in \mathcal{O}_K,$$

was $x \in \mathcal{O}_K^\times$ impliziert. □

Für einen quadratischen Zahlkörper $K = Q(\sqrt{d})$ mit $d \in \mathbb{Z}$ quadratfrei ist also $\mathbb{Z}[\sqrt{d}]$ im Fall $d \equiv 1 \bmod (4)$ eine echte Teilmenge von $\mathcal{O}_K$.

Satz 6.55. *Seien K ein imaginärquadratischer Zahlkörper und $0 > d \in \mathbb{Z}$ quadratfrei mit $K = \mathbb{Q}(\sqrt{d})$. Dann gilt:*

(a) *Im Fall $d \neq -1, -3$ gilt $\mathcal{O}_K^\times = \{\pm 1\} = \langle -1 \rangle \cong \mathbb{Z}/2\mathbb{Z}$.*

(b) *Im Fall $d = -1$ gilt $\mathcal{O}_K^\times = \{\pm 1, \pm i\} = \langle i \rangle \cong \mathbb{Z}/4\mathbb{Z}$.*

(c) *Im Fall $d = -3$ gilt $\mathcal{O}_K^\times = \left\{\pm 1, \frac{\pm 1 \pm \sqrt{-3}}{2}\right\} = \langle \frac{1+\sqrt{-3}}{2} \rangle \cong \mathbb{Z}/6\mathbb{Z}$.*

Beweis. Für $d \neq -1, -3$ unterscheiden wir zwei Fälle:

Fall 1: $d \equiv 2, 3 \bmod (4)$**.** Dann ist $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$ und wegen $d < 0$ sowie $d \neq -1$ gilt $d \leq -2$. Wir schreiben $x = u + v\sqrt{d} \in \mathcal{O}_K$ mit $u, v \in \mathbb{Z}$. Nach Satz 6.54 gilt:

$$x \in \mathcal{O}_K^\times \iff \mathrm{N}(x) = \pm 1 \iff u^2 - v^2 d = \pm 1.$$

Die Gleichung $u^2 - v^2 d = -1$ hat wegen $d < 0$ keine Lösung, die Gleichung $u^2 - v^2 d = 1$ hat wegen $d \leq -2$ nur die Lösungen $(u, v) = (\pm 1, 0)$. Das liefert

$$\mathcal{O}_K^\times = \{\pm 1\} \cong \mathbb{Z}/2\mathbb{Z}.$$

Fall 2: $d \equiv 1 \bmod (4)$**.** In diesem Fall ist $\mathcal{O}_K = \mathbb{Z}[\frac{1}{2}(1 + \sqrt{d})]$. Wir schreiben $x = u + v\frac{1}{2}(1 + \sqrt{d}) \in \mathcal{O}_K$ mit $u, v \in \mathbb{Z}$ bzw. $x = \frac{1}{2}(\tilde{u} + \tilde{v}\sqrt{d})$ für $\tilde{u} := 2u + v$ und $\tilde{v} := v$. Nach Satz 6.54 gilt:

$$x \in \mathcal{O}_K^\times \iff \mathrm{N}(x) = \pm 1 \iff \mathrm{N}(\frac{1}{2})\,\mathrm{N}(\tilde{u} + \tilde{v}\sqrt{d}) = \pm 1 \iff \tilde{u}^2 - \tilde{v}^2 d = \pm 4.$$

Wegen $d < 0$ und $d \equiv 1 \bmod (4)$ ist $d \leq -7$. Daher hat die Gleichung $\tilde{u}^2 - \tilde{v}^2 d = \pm 4$ nur die Lösungen $(\tilde{u}, \tilde{v}) = (\pm 2, 0)$. Es ergibt sich

$$\mathcal{O}_K^\times = \{\pm 1\} \cong \mathbb{Z}/2\mathbb{Z}.$$

Sei nun $d = -1$. Dann gilt $\mathcal{O}_K = \mathbb{Z}[i]$. Wir schreiben $x = u + vi \in \mathcal{O}_K$ mit $u, v \in \mathbb{Z}$ und erhalten

$$x \in \mathcal{O}_K^\times \iff \mathrm{N}(x) = \pm 1 \iff u^2 + v^2 = \pm 1.$$

Diese Gleichung hat die Lösungen $(u, v) = (\pm 1, 0), (0, \pm 1)$. Das liefert

$$\mathcal{O}_K^\times = \{\pm 1, \pm i\} = \langle i \rangle \cong \mathbb{Z}/4\mathbb{Z}.$$

Sei schließlich $d = -3$. Dann ist $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$. Wie im Beweis von Aussage (a) ergibt sich für $x = u + v\frac{1}{2}(1 + \sqrt{-3})$ mit $\tilde{u} := 2u + v$ und $\tilde{v} := v$ die Äquivalenz

$$x \in \mathcal{O}_K^\times \iff \tilde{u}^2 + 3\tilde{v}^2 = \pm 4.$$

Diese Gleichung besitzt die Lösungen $(\tilde{u},\tilde{v}) = (\pm 2,0),(\pm 1,\pm 1)$, also $\mathcal{O}_K^\times = \{\pm 1, \frac{\pm 1 \pm \sqrt{-3}}{2}\}$. Wegen $\frac{1+\sqrt{-3}}{2} = e^{\frac{2\pi i}{6}}$ ist $\operatorname{ord}(\frac{1+\sqrt{-3}}{2}) = 6$, also

$$\mathcal{O}_K^\times = \langle \frac{1+\sqrt{-3}}{2} \rangle \cong \mathbb{Z}/6\mathbb{Z}.$$

□

Nach Satz 6.55 ist die Einheitengruppe des Ganzheitsringes eines imaginärquadratischen Zahlkörpers endlich. Für reellquadratische Zahlkörper gilt das nicht: Für $K = \mathbb{Q}(\sqrt{d})$ mit $d > 1$ quadratfrei ist stets $\mathbb{Z}[\sqrt{d}] \subseteq \mathcal{O}_K$ und für $x = u + v\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ ist

$$x \in \mathcal{O}_K^\times \iff \mathrm{N}(x) = \pm 1 \iff u^2 - dv^2 = \pm 1.$$

Diese Gleichung hat nach den Ergebnissen des vorangegangenen Abschnitts unendlich viele Lösungen, so dass die Einheitengruppe eines reellquadratischen Zahlkörpers stets unendlich ist.

Satz 6.56. *Sei K ein reellquadratischer Zahlkörper. Dann gibt es eine eindeutig bestimmte minimale Einheit > 1 in $\mathcal{O}_K$, die sogenannte **Fundamentaleinheit** η. Jedes Element $x \in \mathcal{O}_K^\times$ lässt sich in der Form $x = \pm\eta^n$ mit einem eindeutig bestimmten $n \in \mathbb{Z}$ schreiben. Insbesondere ist $\mathcal{O}_K^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$.*

Beweis. Im Folgenden sei $K = \mathbb{Q}(\sqrt{d})$ mit $d > 1$ quadratfrei. Die Gleichung $x^2 - dy^2 = 1$ hat nach den Ergebnissen des letzten Abschnitts eine Lösung $(p,q) \in \mathbb{N}^2$. Es ist dann $\mathrm{N}(p + q\sqrt{d}) = p^2 - dq^2 = 1$ und also $p + q\sqrt{d} \in \mathcal{O}_K^\times$. Wir setzen $N := \lfloor p + q\sqrt{d} \rfloor + 1$. Dann ist $(1,N] \cap \mathcal{O}_K^\times \neq \emptyset$. Die Menge $(1,N] \cap \mathcal{O}_K^\times$ ist endlich,

denn: Angenommen, die Menge $(1,N] \cap \mathcal{O}_K^\times$ wäre unendlich. Dann wäre auch $[1,N] \cap \mathcal{O}_K^\times$ unendlich; insbesondere existierte eine Folge $(x_n)_{n\in\mathbb{N}}$ mit paarweise verschiedenen Folgegliedern aus $[1,N] \cap \mathcal{O}_K^\times$. Wegen der Kompaktheit von $[1,N]$ besäße diese Folge eine Teilfolge, die gegen ein $x \in [1,N]$ konvergiert, so dass wir ohne Einschränkung annehmen könnten, die Folge $(x_n)_{n\in\mathbb{N}}$ konvergierte gegen x. Nach Satz 6.54 gäbe es weiter für alle $n \in \mathbb{N}$ Elemente $a_n, b_n \in \mathbb{Z}$ mit $x_n = \frac{a_n + b_n\sqrt{d}}{2}$. Die Folge $(a_n)_{n\in\mathbb{N}}$ könnte nicht beschränkt sein, sonst wäre wegen

$$\pm 1 = \mathrm{N}(x_n) = x_n\overline{x_n} = \frac{a_n^2 - b_n^2 d}{4} \quad \text{und also} \quad b_n^2 = \frac{a_n^2 \pm 4}{d}$$

auch die Folge $(b_n)_{n\in\mathbb{N}}$ beschränkt. Damit träten nur endlich viele Werte in der Folge $(x_n)_{n\in\mathbb{N}}$ auf, im Widerspruch dazu, dass die Werte x_n für $n \in \mathbb{N}$ paarweise verschieden sein müssten. Es existierte deshalb eine Teilfolge (a_{n_i}) von (a_n) mit $a_{n_i} \to \infty$ für $n_i \to \infty$ oder mit $a_{n_i} \to -\infty$ für $n_i \to \infty$. Wir betrachten hier nur den Fall $a_{n_i} \to \infty$, im anderen Fall kann man analog argumentieren. Die entsprechende Teilfolge (b_{n_i}) von (b_n) erfüllte $b_{n_i} \to -\infty$, denn

$$x_{n_i} = \frac{a_{n_i} + b_{n_i}\sqrt{d}}{2} \to x \text{ für } n_i \to \infty.$$

Die Folge $(\overline{x_{n_i}})$ mit

$$\overline{x_{n_i}} = \frac{a_{n_i} - b_{n_i}\sqrt{d}}{2}$$

erfüllte deshalb $\overline{x_{n_i}} \to \infty$ für $n_i \to \infty$. Andererseits gälte

$$|\overline{x_{n_i}}| = \left|\frac{x_{n_i}\overline{x_{n_i}}}{x_{n_i}}\right| = \left|\frac{\mathrm{N}(x_{n_i})}{x_{n_i}}\right| = \frac{1}{|x_{n_i}|} \to \frac{1}{x}$$

für $n_i \to \infty$, was zum Widerspruch führte. #

Somit existiert ein minimales $\eta \in \mathcal{O}_K^\times$ mit $\eta > 1$. Jedes Element aus $\mathcal{O}_K^\times$ lässt sich in der Form $\pm\eta^n$ mit einem eindeutig bestimmten Element $n \in \mathbb{Z}$ schreiben,

denn: Wir zeigen zunächst die Existenzaussage. Sei $x \in \mathcal{O}_K^\times$, ohne Einschränkung $x > 0$. Für $n \to -\infty$ gilt $\eta^n \to 0$, für $n \to \infty$ gilt $\eta^n \to \infty$. Es existiert folglich ein $n \in \mathbb{Z}$ mit $\eta^n \leq x < \eta^{n+1}$. Das liefert $1 \leq x\eta^{-n} < \eta$. Aus $x\eta^{-n} \in \mathcal{O}_K^\times$ ergibt sich $x\eta^{-n} = 1$ wegen der Minimalität von η. Somit folgt $x = \eta^n$. Zum Nachweis der Eindeutigkeitsaussage bemerken wir, dass die Elemente $\pm\eta^n$ für $n \in \mathbb{Z}$ wegen $\eta > 1$ paarweise verschieden sind. #

Wir betrachten die Abbildung

$$\psi\colon \begin{cases} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z} & \to \mathcal{O}_K^\times, \\ (\bar{i}, n) & \mapsto (-1)^i\eta^n. \end{cases}$$

Diese ist wohldefiniert wegen $(-1)^2 = 1$ und bijektiv aufgrund dessen, was wir bereits gezeigt haben. Schließlich ist ψ ein Gruppenhomomorphismus, denn für $\overline{i_1}, \overline{i_2} \in \mathbb{Z}/2\mathbb{Z}$ und $n_1, n_2 \in \mathbb{Z}$ gilt

$$\begin{aligned}\psi\big((\overline{i_1}, n_1) + (\overline{i_2}, n_2)\big) &= \psi(\overline{i_1 + i_2}, n_1 + n_2) = (-1)^{i_1+i_2}\eta^{n_1+n_2} = (-1)^{i_1}\eta^{n_1}(-1)^{i_2}\eta^{n_2} \\ &= \psi(\overline{i_1}, n_1)\psi(\overline{i_2}, n_2).\end{aligned}$$

□

Im Rest des Abschnittes werden wir daran arbeiten, einen Algorithmus zur Berechnung der Fundamentaleinheit des Ganzheitsringes reellquadratischer Zahlkörper zu finden.

Proposition 6.57. *Seien K ein reellquadratischer Zahlkörper und $d \in \mathbb{N}$ quadratfrei mit $K = \mathbb{Q}(\sqrt{d})$. Seien weiter $a, b \in \mathbb{Z}$ mit $\varepsilon := \frac{a+b\sqrt{d}}{2} \in \mathcal{O}_K^\times$. Dann sind die folgenden beiden Aussagen äquivalent:*

(i) $\varepsilon > 1$,

(ii) $a, b \geq 1$.

Beweis. Gelte zunächst Aussage (i) und sei also $\varepsilon > 1$. Dann sind die Elemente $\varepsilon, -\varepsilon, \varepsilon^{-1}, -\varepsilon^{-1}$ paarweise verschieden und von diesen vier Elementen ist ε das größte. Es ist

$$\varepsilon^{-1} = \frac{\overline{\varepsilon}}{\varepsilon\overline{\varepsilon}} = \frac{\overline{\varepsilon}}{\mathrm{N}(\varepsilon)} = \pm\overline{\varepsilon} = \pm\frac{a - b\sqrt{d}}{2}$$

Es folgt $a \geq 1$, denn eines der beiden Elemente $\varepsilon^{-1}, -\varepsilon^{-1}$ ist von der Form $\frac{-a+b\sqrt{d}}{2}$ und wäre im Falle $a \leq 0$ größer als oder gleich ε. Analog gilt $b \geq 1$.

Gelte nun umgekehrt Aussage (ii) und sei also $a, b \geq 1$. Dann ist

$$\varepsilon = \frac{a+b\sqrt{d}}{2} \geq \frac{1+\sqrt{d}}{2} > 1.$$

□

Proposition 6.58. *Seien K ein reellquadratischer Zahlkörper und $d \in \mathbb{N}$ quadratfrei mit $K = \mathbb{Q}(\sqrt{d})$. Dann gilt: Ist $d \not\equiv 5 \bmod (8)$, so liegt die Fundamentaleinheit η von $\mathcal{O}_K$ in $\mathbb{Z}[\sqrt{d}]$.*

Beweis. Im Fall $d \not\equiv 1 \bmod (4)$ ist $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$ und deshalb $\eta \in \mathbb{Z}[\sqrt{d}]$. Seien im Folgenden $d \equiv 1 \bmod (4)$ und $\eta \notin \mathbb{Z}[\sqrt{d}]$. Nach Satz 6.54 gibt es $u, v \in \mathbb{Z}$ mit

$$\eta = u + v\frac{1}{2}(1+\sqrt{d}) = \frac{a+b\sqrt{d}}{2} \quad \text{mit } a := 2u+v \text{ und } b := v.$$

Wegen $\eta \notin \mathbb{Z}[\sqrt{d}]$ ist $b = v$ ungerade, also ist auch a ungerade. Aufgrund von $\eta \in \mathcal{O}_K^\times$ gilt $\mathrm{N}(\eta^2) = \mathrm{N}(\eta)^2 = (\pm 1)^2 = 1$. Es ist

$$\eta^2 = \frac{a^2+db^2+2ab\sqrt{d}}{4} \overset{ab \text{ ungerade}}{\notin} \mathbb{Z}[\sqrt{d}].$$

Wir schreiben analog zu oben $\eta^2 = \frac{x+y\sqrt{d}}{2}$ mit $x, y \in \mathbb{Z}$ ungerade. Aufgrund von $\mathrm{N}(\eta^2) = 1$ ergibt sich $x^2 - y^2 d = 4$. Da x, y ungerade sind, folgt $x^2, y^2 \equiv 1 \bmod (8)$ und damit $1 - d \equiv 4 \bmod (8)$, also $d \equiv 5 \bmod (8)$. □

Proposition 6.59. *Seien K ein reellquadratischer Zahlkörper und $d \in \mathbb{N}$ quadratfrei mit $K = \mathbb{Q}(\sqrt{d})$. Es bezeichne η die Fundamentaleinheit von $\mathcal{O}_K$, diese liege in $\mathbb{Z}[\sqrt{d}]$. Für $n \in \mathbb{N}$ sei $\eta^n = a_n + b_n\sqrt{d}$ mit $a_n, b_n \in \mathbb{N}$ wie in Proposition 6.57. Für $m, n \in \mathbb{N}$ sind dann die folgenden Aussagen äquivalent:*

(i) $n < m$,
(ii) $\eta^n < \eta^m$,
(iii) $a_n < a_m$,
(iv) $b_n < b_m$.

Beweis. Wegen $\eta > 1$ ist die Folge $(\eta^n)_{n\in\mathbb{N}}$ streng monoton wachsend, so dass die Aussagen (i) und (ii) äquivalent sind. Zum Nachweis der restlichen Äquivalenzen genügt es in analoger Überlegung, $a_n < a_{n+1}$ und $b_n < b_{n+1}$ für alle $n \in \mathbb{N}$ zu zeigen. Es ist

$$\eta^{n+1} = \eta^n \cdot \eta = (a_n + b_n\sqrt{d})(a_1 + b_1\sqrt{d}) = a_n a_1 + b_n b_1 d + (a_n b_1 + b_n a_1)\sqrt{d}$$

und deshalb $a_{n+1} = a_n a_1 + b_n b_1 d$ sowie $b_{n+1} = a_n b_1 + b_n a_1$. Wegen $a_n, b_n, a_1, b_1 \in \mathbb{N}$ ergibt sich

$$a_{n+1} \geq a_n + d > a_n \quad \text{und} \quad b_{n+1} \geq b_n + 1 > b_n.$$

□

Proposition 6.60. *Seien K ein reellquadratischer Zahlkörper und $d \in \mathbb{N} \setminus \{5, 13\}$ quadratfrei mit $K = \mathbb{Q}(\sqrt{d})$. Es bezeichne η die Fundamentaleinheit von $\mathcal{O}_K$, diese liege nicht in $\mathbb{Z}[\sqrt{d}]$. Für $n \in \mathbb{N}$ sei $\eta^n = \frac{a_n + b_n\sqrt{d}}{c_n}$ mit $a_n, b_n \in \mathbb{N}$, $c_n \in \{1, 2\}$, $\mathrm{ggT}(a_n, b_n, c_n) = 1$, vgl. 6.57. Für $m, n \in \mathbb{N}$ sind dann die folgenden Aussagen äquivalent:*

(i) $n < m$,

(ii) $\eta^n < \eta^m$,

(iii) $a_n < a_m$,

(iv) $b_n < b_m$.

Beweis. Wegen $\eta > 1$ ist die Folge $(\eta^n)_{n\in\mathbb{N}}$ streng monoton wachsend, woraus sich die Äquivalenz der Aussagen (i) und (ii) ergibt. Zum Nachweis der restlichen Äquivalenzen genügt es $a_n < a_{n+1}$ und $b_n < b_{n+1}$ für alle $n \in \mathbb{N}$ zu zeigen. Aufgrund von $\eta \notin \mathbb{Z}[\sqrt{d}]$ ist $c_1 = 2$ und demzufolge

$$\frac{a_{n+1}}{c_{n+1}} + \frac{b_{n+1}}{c_{n+1}}\sqrt{d} = \eta^{n+1} = \eta^n \cdot \eta = \frac{a_n + b_n\sqrt{d}}{c_n}\frac{a_1 + b_1\sqrt{d}}{2} = \frac{a_n a_1 + b_n b_1 d}{2c_n} + \frac{a_n b_1 + b_n a_1}{2c_n}\sqrt{d}.$$

Dies impliziert

$$a_{n+1} = \frac{c_{n+1}}{c_n}\frac{a_n a_1 + b_n b_1 d}{2} \quad \text{und} \quad b_{n+1} = \frac{c_{n+1}}{c_n}\frac{a_n b_1 + b_n a_1}{2}.$$

Wie wir im Beweis von Proposition 6.58 gesehen haben, ist darüber hinaus a_1 ungerade. Es ergeben sich die folgenden Fälle:

Fall 1: $a_1 = 1$**.** Dann ist $db_1^2 = -3$ oder $db_1^2 = 5$. Wegen $d > 0$ und $d \neq 5$ haben diese Gleichungen jedoch keine Lösung und es kommt zum Widerspruch.

Fall 2: $a_1 = 3$**.** Es ergibt sich $db_1^2 = 5$ oder $db_1^2 = 13$. Aufgrund von $d \neq 5, 13$ haben diese Gleichungen keine Lösungen, somit führt auch dieser Fall zum Widerspruch.

Fall 3: $a_1 \geq 5$**.** Wir erhalten

$$a_{n+1} = \frac{c_{n+1}}{c_n}\frac{a_n a_1 + b_n b_1 d}{2} \geq \frac{1}{2}\frac{5a_n + b_n b_1 d}{2} > a_n$$

sowie

$$b_{n+1} = \frac{c_{n+1}}{c_n}\frac{a_n b_1 + b_n a_1}{2} \geq \frac{1}{2}\frac{a_n b_1 + 5b_n}{2} > b_n.$$

□

Algorithmus 6.61 (Bestimmung der Fundamentaleinheit)**.** *Seien K ein reellquadratischer Zahlkörper und $d \in \mathbb{N}$ quadratfrei mit $K = \mathbb{Q}(\sqrt{d})$. Es soll die Fundamentaleinheit η von $\mathcal{O}_K$ bestimmt werden.*

(1) *Im Fall* $d = 5$ *ist* $\eta = \frac{1+\sqrt{5}}{2}$.

(2) *Im Fall* $d \neq 5$ *berechne solange Näherungsbrüche* $\frac{p_n}{q_n}$, $n \in \mathbb{N}_0$, *von* $\sqrt{d}$, *bis erstmalig*

$$p_n^2 - dq_n^2 \in \{\pm 1, \pm 4\}$$

gilt. Es ist dann

$$\eta = \begin{cases} p_n + q_n\sqrt{d} & \text{für } p_n^2 - dq_n^2 \in \{\pm 1\}, \\ \frac{p_n+q_n\sqrt{d}}{2} & \text{für } p_n^2 - dq_n^2 \in \{\pm 4\}. \end{cases}$$

Ist $d \not\equiv 5 \bmod (8)$, *so ist* $\eta = p_{h-1} + q_{h-1}\sqrt{d}$, *wobei* h *die Periodenlänge von* $\sqrt{d}$ *ist.*

Beweis. Sei $(\frac{p_n}{q_n})_{n\in\mathbb{N}_0}$ die Folge der Näherungsbrüche von $\sqrt{d}$. Wir unterscheiden vier Fälle:

Fall 1: $\eta \in \mathbb{Z}[\sqrt{d}]$**.** Nach Proposition 6.57 ist η von der Form $\eta = a + b\sqrt{d}$ mit $a, b \in \mathbb{N}$ und es ist $\mathrm{N}(\eta) = a^2 - b^2 d = \pm 1$. Nach Satz 6.38 gibt es ein $n \in \mathbb{N}_0$ mit $\frac{a}{b} = \frac{p_n}{q_n}$. Mit $t := \mathrm{ggT}(a, b)$ gilt $t \mid (a^2 - b^2 d) = \pm 1$ und deshalb $t = 1$. Es folgt $(a, b) = (p_n, q_n)$. Es gibt kein $k \in \{0, 1, \ldots, n-1\}$ mit $p_k^2 - dq_k^2 \in \{\pm 1, \pm 4\}$,

denn: Wäre zunächst $k \in \{0, 1, \ldots, n-1\}$ mit $p_k^2 - dq_k^2 \in \{\pm 1\}$. Dann wäre $\alpha := p_k + q_k\sqrt{d} \in \mathcal{O}_K^\times$ und es gälte $\alpha > 1$. Daher gäbe es ein $m \in \mathbb{N}$ mit $\alpha = \eta^m$. Wäre dabei $m = 1$, so auch $\alpha = \eta$ und also $p_k = p_n$ sowie $q_k = q_n$, im Widerspruch zu $k < n$. Wäre andernfalls $m > 1$, so gälte nach Proposition 6.59 jedoch $q_k > q_n$ und damit $k > n$, was ebenfalls ein Widerspruch ist.

Wäre nun $k \in \{0, 1, \ldots, n-1\}$ mit $p_k^2 - dq_k^2 \in \{\pm 4\}$. Dann gälte $\alpha := \frac{p_k+q_k\sqrt{d}}{2} \in \mathcal{O}_K^\times$, denn $\mathrm{N}(\alpha) = \frac{1}{4}(p_k^2 - dq_k^2) = \pm 1$ und $\mathrm{Sp}(\alpha) = p_k \in \mathbb{Z}$. Wegen $\eta \in \mathbb{Z}[\sqrt{d}]$ wäre $\mathcal{O}_K^\times \subseteq \mathbb{Z}[\sqrt{d}]$ und also $\alpha \in \mathbb{Z}[\sqrt{d}]$. Somit wären sowohl p_k als auch q_k gerade, im Widerspruch zu $\mathrm{ggT}(p_k, q_k) = 1$. #

Folglich ist $\eta = p_n + q_n\sqrt{d}$, wobei n minimal mit der Eigenschaft $p_n^2 - dq_n^2 \in \{\pm 1, \pm 4\}$ ist – wobei der Fall $p_n^2 - dq_n^2 = \pm 4$ nach den obigen Überlegungen niemals eintreten kann.

Fall 2: $\eta \notin \mathbb{Z}[\sqrt{d}]$**,** $d \neq 5, 13$**.** Wie im Beweis zu Proposition 6.60 erhalten wir, dass η von der Form $\eta = \frac{a+b\sqrt{d}}{2}$ mit $a, b \in \mathbb{N}$ ungerade ist. Wegen $\mathrm{N}(\eta) = \pm 1$ erhalten wir $a^2 - db^2 = \pm 4$. Da $\eta \notin \mathbb{Z}[\sqrt{d}]$ ist, ergibt sich aus Proposition 6.58 die Kongruenz $d \equiv 5 \bmod (8)$. Insbesondere ist $d \geq 21$ und deshalb $4 < \frac{1}{2}(\sqrt{d-4} + \sqrt{d})$. Nach Satz 6.38 gibt es ein $n \in \mathbb{N}_0$ mit $\frac{a}{b} = \frac{p_n}{q_n}$. Mit $t := \mathrm{ggT}(a, b)$ gilt $t^2 \mid (a^2 - b^2 d) = \pm 4$ und deshalb $t \in \{1, 2\}$. Weil a, b beide ungerade sind, ist $t = 1$ und deshalb $(a, b) = (p_n, q_n)$. Es gibt kein $k \in \{0, 1, \ldots, n-1\}$ mit $p_k^2 - dq_k^2 \in \{\pm 1, \pm 4\}$,

denn: Wäre zunächst $k \in \{0, 1, \ldots, n-1\}$ mit $p_k^2 - dq_k^2 \in \{\pm 1\}$. Wie in Fall 1 gälte $\alpha := p_k + q_k\sqrt{d} \in \mathcal{O}_K^\times$ und $\alpha > 1$. Aus diesem Grund gäbe es ein $m \in \mathbb{N}$ mit $\alpha = \eta^m$. Wegen $\eta \notin \mathbb{Z}[\sqrt{d}]$ wäre $\alpha \neq \eta$ und also $m > 1$. Nach Proposition 6.60 gälte $q_k > q_n$ und deshalb $k > n$, was ein Widerspruch ist.

Wäre nun $k \in \{0, 1, \ldots, n-1\}$ mit $p_k^2 - dq_k^2 \in \{\pm 4\}$. Wie in Fall 1 wäre $\alpha := \frac{p_k+q_k\sqrt{d}}{2} \in \mathcal{O}_K^\times$ und es gäbe ein $m \in \mathbb{N}$ mit $\alpha = \eta^m$. Wäre $m = 1$, so folgte $\alpha = \eta$, also $p_k = p_n$ und $q_k = q_n$,

im Widerspruch zu $k < n$. Wäre andernfalls $m > 1$, so gälte nach Proposition 6.59 wegen $\mathrm{ggT}(p_k, q_k, 2) = 1$ und $d \geq 21$ jedoch $q_k > q_n$ und damit $k > n$, was ein Widerspruch ist. #

Folglich ist $\eta = \frac{p_n + q_n\sqrt{d}}{2}$, wobei n minimal mit der Eigenschaft $p_n^2 - dq_n^2 \in \{\pm 1, \pm 4\}$ ist.

Fall 3: $d = 5$. Offensichtlich ist $\frac{1+\sqrt{5}}{2} \in \mathbb{Z}[\frac{1+\sqrt{5}}{2}] = \mathcal{O}_K$ und wegen $\mathrm{N}(\frac{1+\sqrt{5}}{2}) = -1$ handelt es sich um eine Einheit in $\mathcal{O}_K$. Darüber hinaus ist $\frac{1+\sqrt{5}}{2}$ minimal unter allen Elementen $\frac{a+b\sqrt{5}}{2} \in \mathcal{O}_K^\times$ mit $a, b \in \mathbb{N}$. Wir schließen, dass $\eta = \frac{1+\sqrt{5}}{2}$ die Fundamentaleinheit von $\mathcal{O}_K$ ist.[3]

Fall 4: $d = 13$. Offenbar ist $\frac{3+\sqrt{13}}{2} = 1 + \frac{1+\sqrt{13}}{2} \in \mathbb{Z}[\frac{1+\sqrt{13}}{2}] = \mathcal{O}_K$ und wegen $\mathrm{N}(\frac{3+\sqrt{13}}{2}) = -1$ handelt es sich um eine Einheit in $\mathcal{O}_K$. Man rechnet leicht nach, dass $\frac{3+\sqrt{13}}{2}$ minimal unter den Elementen $\frac{a+b\sqrt{13}}{2} \in \mathcal{O}_K^\times$ mit $a, b \in \mathbb{N}$ ist. Das impliziert, dass $\eta = \frac{3+\sqrt{13}}{2}$ die Fundamentaleinheit von $\mathcal{O}_K$ ist. Wegen $\sqrt{13} = [3, \overline{1, 1, 1, 6}]$ ist $p_0 = 3$, $q_0 = 1$ und $p_0^2 - 13q_0^2 = -4$. Der Algorithmus liefert daher das korrekte Resultat $\eta = \frac{3+\sqrt{13}}{2}$.

Im Fall $d \not\equiv 5 \bmod (8)$ liegt die Fundamentaleinheit η nach Proposition 6.58 in $\mathbb{Z}[\sqrt{d}]$. Nach den obigen Überlegungen ist $\eta = p_n + q_n\sqrt{d}$, wobei n minimal mit $p_n^2 - dq_n^2 \in \{\pm 1\}$ ist. Falls h gerade ist, hat die Gleichung $x^2 - dy^2 = -1$ nach Korollar 6.44 keine Lösung, die Fundamentallösung von $x^2 - dy^2 = 1$ ist durch (p_{h-1}, q_{h-1}) gegeben. Falls h ungerade ist, so ist (p_{h-1}, q_{h-1}) nach Korollar 6.44 diejenige Lösung von $x^2 - dy^2 = -1$ in $\mathbb{N}^2$ mit minimalem y, die Fundamentallösung von $x^2 - dy^2 = 1$ ist durch (p_{2h-1}, q_{2h-1}) gegeben. Wir erhalten $\eta = p_{h-1} + q_{h-1}\sqrt{d}$. □

Beispiel 6.62. (a) *Für $d = 53$ ist $\sqrt{53} = [7, \overline{3, 1, 1, 3, 14}]$ und demzufolge $p_0 = 7$ sowie $q_0 = 1$. Wir erhalten $p_0^2 - 53q_0^2 = -4$ und deshalb $\eta = \frac{7+\sqrt{53}}{2}$. Hierbei ist $\mathrm{N}(\eta) = -1$.*

(b) *Für $d = 31$ ist $\sqrt{31} = [5, \overline{1, 1, 3, 5, 3, 1, 1, 10}]$. Wegen $31 \not\equiv 5 \bmod (8)$ ist $\eta = p_{h-1} + q_{h-1}\sqrt{31}$. Es ist $h = 8$ und $\frac{p_7}{q_7} = \frac{1520}{273}$, also $\eta = 1520 + 273\sqrt{31}$. Da h gerade ist, ist (p_7, q_7) die Fundamentallösung von $x^2 - 31y^2 = 1$ und es gilt also $\mathrm{N}(\eta) = 1$.*

Satz 6.63. *Seien K ein reellquadratischer Zahlkörper und $d \in \mathbb{N}$ quadratfrei mit $K = \mathbb{Q}(\sqrt{d})$. Es bezeichne η die Fundamentaleinheit von $\mathcal{O}_K$ und es sei (a, b) die Fundamentallösung der Pell'schen Gleichung $X_1^2 - dX_2^2 = 1$. Dann gilt:*

$$a + b\sqrt{d} = \begin{cases} \eta & \text{für } \eta \in \mathbb{Z}[\sqrt{d}] \text{ und } \mathrm{N}(\eta) = 1, \\ \eta^2 & \text{für } \eta \in \mathbb{Z}[\sqrt{d}] \text{ und } \mathrm{N}(\eta) = -1, \\ \eta^3 & \text{für } \eta \notin \mathbb{Z}[\sqrt{d}] \text{ und } \mathrm{N}(\eta) = 1, \\ \eta^6 & \text{für } \eta \notin \mathbb{Z}[\sqrt{d}] \text{ und } \mathrm{N}(\eta) = -1. \end{cases}$$

Beweis. Die Fundamentallösung (a, b) von $x^2 - dy^2 = 1$ korrespondiert nach Definition zu einer Einheit $\varepsilon = a + b\sqrt{d} \in \mathcal{O}_K^\times$ mit $\mathrm{N}(\varepsilon) = a^2 - db^2 = 1$, so dass a minimal ist. Wie wir im

[3] Die Kettenbruchentwicklung von $\sqrt{5}$ ist $\sqrt{5} = [2, \overline{4}]$, was $p_0 = 2$ und $q_0 = 1$ zur Folge hat. Es ist $p_0^2 - 5q_0^2 = -1$, dies liefert die Einheit $\varepsilon = 2 + \sqrt{5} = \eta^3$, jedoch nicht die Fundamentaleinheit. Aus diesem Grund ist bei unserem Algorithmus die Fallunterscheidung notwendig.

Beweis von Satz 6.33 gesehen haben, ist die Minimalität von a äquivalent zur Minimalität von $\varepsilon = a + b\sqrt{d}$. Gesucht ist somit das minimale $n \in \mathbb{N}$ mit $\eta^n \in \mathbb{Z}[\sqrt{d}]$ und $\mathrm{N}(\eta^n) = 1$. Wir unterscheiden vier Fälle:

Fall 1: $\eta \in \mathbb{Z}[\sqrt{d}]$ **und** $\mathrm{N}(\eta) = 1$**.** Dann ist $n = 1$.

Fall 2: $\eta \in \mathbb{Z}[\sqrt{d}]$ **und** $\mathrm{N}(\eta) = -1$**.** Dann ist $\mathrm{N}(\eta^2) = 1$ und $\eta^2 \in \mathbb{Z}[\sqrt{d}]$, also $n = 2$.

Fall 3: $\eta \notin \mathbb{Z}[\sqrt{d}]$ **und** $\mathrm{N}(\eta) = 1$**.** Wir schreiben $\eta = \frac{a+b\sqrt{d}}{2}$ mit $a, b \in \mathbb{N}$ ungerade. Wir erhalten

$$\eta^2 = \frac{a^2 + db^2 + 2ab\sqrt{d}}{4} \quad \text{und} \quad \eta^3 = \frac{a^3 + 3dab^2 + (3ba^2 + db^3)\sqrt{d}}{8}.$$

Wegen $4 \nmid 2ab$ ist $\eta^2 \notin \mathbb{Z}[\sqrt{d}]$. Aufgrund von $\eta \notin \mathbb{Z}[\sqrt{d}]$ ist $d \equiv 5 \bmod (8)$. Unter Verwendung von $a^2 \equiv b^2 \equiv 1 \bmod (8)$ liefert dies

$$\begin{aligned} a^3 + 3dab^2 &\equiv a + 3da = a(1 + 3d) \equiv 0 \bmod (8), \\ 3ba^2 + db^3 &\equiv 3b + db \equiv b(3 + d) \equiv 0 \bmod (8). \end{aligned}$$

Somit ist $\eta^3 \in \mathbb{Z}[\sqrt{d}]$. Da außerdem $\mathrm{N}(\eta^3) = \mathrm{N}(\eta)^3 = 1$ gilt, ist $n = 3$.

Fall 4: $\eta \notin \mathbb{Z}[\sqrt{d}]$ **und** $\mathrm{N}(\eta) = -1$**.** Wie in Fall 3 ist $\eta^2 \notin \mathbb{Z}[\sqrt{d}]$, $\mathrm{N}(\eta^3) = -1$ und $\mathrm{N}(\eta^5) = -1$. Darüber hinaus ist $\eta^3 \in \mathbb{Z}[\sqrt{d}]$ und damit auch $\eta^{-3} = \frac{\overline{\eta^3}}{\mathrm{N}(\eta)^3} = -\overline{\eta^3}$. Folglich ist $\eta^4 \notin \mathbb{Z}[\sqrt{d}]$, andernfalls wäre $\eta = \eta^4\eta^{-3} \in \mathbb{Z}[\sqrt{d}]$, was ein Widerspruch ist. Es ist $\eta^6 = (\eta^3)^2 \in \mathbb{Z}[\sqrt{d}]$ und $\mathrm{N}(\eta^6) = (-1)^6 = 1$. Dies impliziert $n = 6$. □