Verschränkungsmodul zur didaktischen Reduktion in der Zahlentheorie

Wintersemester 2022 / 23

Vorlesungsskript

Dr. Hendrik Kasten

27. Juli 2022

Inhaltsverzeichnis

KAPITEL 1

Einleitung

1.1 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 5.1) 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.
- $\mathbb{Z} := \mathbb{N}_0 \cup \{-a \mid a \in \mathbb{N}\}$ 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.
- $\mathbb{Q} := \{\frac{a}{b} \mid a \in \mathbb{Z}, b \in \mathbb{N}\}$ 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.
- $\mathbb{C} := \mathbb{R}[X]/(X^2+1) = \{a + bi \mid a, b \in \mathbb{R}\}$ 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.

1.2 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 2

Teilbarkeit

2.1 Division mit Rest

Definition 2.1. *Seien $a, b \in \mathbb{Z}$. Die Zahl a heißt ein **Teiler** von b – in Zeichen: $a \mid b$ – wenn es ein $q \in \mathbb{Z}$ mit $b = qa$ gibt. In diesem Fall nennt man die Zahl b auch ein **Vielfaches** von a.*

Das folgende Lemma ergibt sich unmittelbar aus Definition 2.1:

Lemma 2.2. *Für beliebige $a, b, c, d \in \mathbb{Z}$ gelten die folgenden Aussagen:*

(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 $ab \mid cd$.*

Der nächste Satz beschreibt ein elementares aber dennoch enorm nützliches Verfahren – die Division mit Rest auf den ganzen Zahlen:

Satz 2.3 (Satz von der Division mit Rest)**.** *Für beliebige $a, b \in \mathbb{Z}$ mit $b \neq 0$ gilt:*

Es gibt eindeutig bestimmte Zahlen $q, r \in \mathbb{Z}$ mit

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

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

Beweis. Wir zeigen zunächst die Existenz von $q, r \in \mathbb{Z}$ wie im Satz. Dazu setzen wir

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

Offenbar ist $R \subseteq \mathbb{N}_0$ nichtleer und besitzt somit ein eindeutig bestimmtes kleinstes Element r. Sei weiter q die ganze Zahl mit $a - qb = r$, also mit $a = qb + r$. Dann gilt $0 \leq r < |b|$,

denn: Angenommen, es gälte $r \geq |b|$. Dann folgte

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

und also ein Widerspruch zur Minimalität von r. #

Zum Beweis der Eindeutigkeit betrachten wir $r, \tilde{r}, q, \tilde{q} \in \mathbb{Z}$ mit

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

Wir erhalten $(q - \tilde{q})b = \tilde{r} - r$, also $b \mid (\tilde{r} - r)$. Nach Voraussetzung ist $|\tilde{r} - r| < |b|$. Es folgt $\tilde{r} - r = 0$ und hieraus $r = \tilde{r}$ sowie $q = \tilde{q}$. □

Bemerkung 2.4. *In der Sprache der Algebra besagt Satz 2.3, dass der Ring $\mathbb{Z}$ euklidisch ist.*

Definition 2.5. *Für beliebiges $n \in \mathbb{N}$ und beliebige $a_1, \ldots, a_n \in \mathbb{Z}$ sei*

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

*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 sie die folgenden Eigenschaften erfüllt:*

(ggT_1) $d \geq 0$,

(ggT_2) $d \in T(a_1, \ldots, a_n)$,

(ggT_3) *für alle $t \in T(a_1, \ldots, a_n)$ gilt $t \mid d$.*

Bemerkung 2.6. *Natürlich könnten wir für gegebene $a_1, \ldots, a_n \in \mathbb{Z}$ – vorausgesetzt diese sind nicht alle Null – den größten gemeinsamer 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 allerdings in Existenz und Eindeutigkeit etwas Arbeit investieren.*

Lemma 2.7. *Beliebige $a_1, \ldots, a_n \in \mathbb{Z}$ mit $n \in \mathbb{N}$ besitzen höchstens einen größten gemeinsamen Teiler.*

Beweis. Für größte gemeinsame Teiler d_1, d_2 von $a_1, \ldots, a_n$ gilt nach (ggT_3) sowohl $d_1 \mid d_2$ als auch $d_2 \mid d_1$. Somit existieren $q_1, q_2 \in \mathbb{Z}$ mit $d_2 = q_1 d_1$ sowie $d_1 = q_2 d_2$ und folglich also $d_1 = q_2 q_1 d_1$. Wir unterscheiden zwei Fälle:

Fall 1: $d_1 = 0$**.** Dann folgt sofort $d_2 = q_1 \cdot 0 = 0 = d_1$.

Fall 2: $d_1 \neq 0$**.** Dann erhalten wir $q_2 q_1 = 1$, also $q_1 \in \{\pm 1\}$ und also $d_2 = \pm d_1$. Mit (ggT_1) folgt auch in diesem Fall $d_2 = d_1$. □

Bemerkung 2.8. *Der Beweis zeigt insbesondere: Lässt man in Definition 2.5 Bedingung (ggT_1) weg, so ist der größte gemeinsame Teiler immer noch bis auf eine Einheit in $\mathbb{Z}^\times = \{\pm 1\}$ eindeutig, es gibt also höchstens zwei größte gemeinsame Teiler von $a_1, \ldots, a_n$ und mit d wäre stets auch $-d$ ein größter gemeinsamer Teiler von $a_1, \ldots, a_n$.*

In allgemeinen Ringen R definiert man den größten gemeinsamen Teiler nur anhand von (ggT_2) und (ggT_3) und erhält Eindeutigkeit nur bis auf eine Einheit in $R^\times$.

Die folgende elementare Feststellung wird im Weiteren große Konsequenzen haben:

Lemma 2.9. *Für beliebige $a, b, q, r \in \mathbb{Z}$ gilt:*

$$a = qb + r \quad \Longrightarrow \quad T(a,b) = T(b,r).$$

Beweis. Für $t \in T(a,b)$ gilt $t \mid (a - qb) = r$ und also $t \in T(b,r)$. Umgekehrt gilt für $t \in T(b,r)$ sofort $t \mid (qb + r) = a$ und somit $t \in T(a,b)$. □

Im Fall $a \geq b \in \mathbb{N}$ folgt aus Lemma 2.9, dass man die Berechnung der Menge der gemeinsamen Teiler $T(a,b)$ durch Division mit Rest – etwa in der Form $a = qb + r$ mit $0 \leq r < |b|$ – 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. Das ist die Grundidee des Euklid'schen Algorithmus:

Satz 2.10 (Euklid'scher Algorithmus)**.** *Für beliebige $a \geq b \in \mathbb{Z}$ gelten die folgenden Aussagen:*

(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) $\mathrm{ggT}(a,b)$ *kann mit dem **Euklid'schen Algorithmus** bestimmt werden:*

Ist $b = 0$, so gilt $\mathrm{ggT}(a,b) = \mathrm{ggT}(a,0) = |a|$. 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

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

Dieser Prozess bricht nach einer endlichen Anzahl r von 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: $\mathrm{ggT}(a,b) = z_{r+1}$.

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

$$\mathrm{ggT}(a,b) = ua + vb. \qquad \textbf{(Erweiterter Euklid'scher Algorithmus)}$$

Beweis. Wir betrachten zunächst den Fall $b = 0$. Hier gelten offenbar $|a| \geq 0$, $|a| \mid a$ und $|a| \mid 0$. Für ein $t \in T(a,0) = T(a)$ gilt zudem $t \mid |a|$. Nach Definition 2.5 ist $|a|$ also ein größter gemeinsamer Teiler von a und 0. Die Eindeutigkeit gilt nach Lemma 2.7. Schließlich gilt

$$|a| = \mathrm{ggT}(a,0) = \mathrm{sgn}(a) \cdot a + 0 \cdot 0$$

und insgesamt der ganze Satz in diesem Spezialfall.

Für den Rest des Beweises sei nun $b \neq 0$. Für die Folge der Reste gilt konstruktionsgemäß $z_2 > z_3 > z_4 > \ldots$, so dass das Verfahren nach einer endlichen Anzahl r von Schritten stoppt. Die letzten beiden Gleichungen sind dann von der Form

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

und nach Lemma 2.9 gilt

$$T(a,b) = T(a,|b|) = T(z_1,z_2) \overset{2.9}{=} \ldots \overset{2.9}{=} T(z_r,z_{r+1}) \overset{2.9}{=} T(z_{r+1},0) = T(z_{r+1}).$$

Es folgen $z_{r+1} \in T(z_{r+1}) = T(a,b)$ und $t \mid z_{r+1}$ für alle $t \in T(a,b) = T(z_{r+1})$. Da nach Konstruktion $z_{r+1} > 0$ gilt, haben wir somit nachgewiesen, dass z_{r+1} ein größter gemeinsamer Teiler von a, b ist. Die Eindeutigkeit gilt wieder nach Lemma 2.7. Hiermit sind die Behauptungen (a) und (b) gezeigt und es verbleibt Behauptung (c) zu zeigen. Wegen

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

ergibt sich

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

Wir benutzen nun (G_{r-3}), um z_{r-1} über z_{r-3}, z_{r-2} auszudrücken usw. 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 $u := u_2$, $v := v_2 \,\mathrm{sgn}(b)$, dann ist $\mathrm{ggT}(a,b) = ua + vb$. □

Der Erweiterte Euklid'sche Algorithmus ist ein sehr wichtiges Resultat über den größten gemeinsamen Teiler, das man sehr häufig in Beweisen benötigt. Als Beispiel dafür dient der Beweis der folgenden Proposition:

Proposition 2.11. *Für beliebige $a, b, c, d \in \mathbb{Z}$ mit $\mathrm{ggT}(a,b) = 1$[1] gelten die folgenden Aussagen:*

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

[1] Zahlen $a, b \in \mathbb{Z}$ mit $\mathrm{ggT}(a,b) = 1$ nennen wir ab sofort auch ***teilerfremd***.

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

Beweis. Wegen $\mathrm{ggT}(a,b) = 1$ und nach dem Erweiterten Euklid'schen Algorithmus gibt es $u, v \in \mathbb{Z}$ mit $ua + vb = 1$. Gilt $a \mid bc$, so existiert ein $q \in \mathbb{Z}$ mit $bc = qa$ und es ist

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

was $a \mid c$ und somit Behauptung (a) impliziert.

Gelten $a \mid d$ 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 $ab \mid d$, also Behauptung (b). □

Für das Studium des größten gemeinsamen Teilers mehrerer natürlicher Zahlen ist es sehr nützlich, sich mit Idealen in $\mathbb{Z}$ zu beschäftigen:

Satz 2.12. *Für jedes Ideal $\mathfrak{a} \trianglelefteq \mathbb{Z}$ gibt es ein eindeutig bestimmtes $m \in \mathbb{N}_0$ mit*

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

Beweis. Es gibt stets ein $m \in \mathbb{N}_0$ mit $\mathfrak{a} = m\mathbb{Z}$,

denn: Wegen $\mathfrak{a} = \{0\} = 0 \cdot \mathbb{Z}$ können wir ohne Einschränkung $\mathfrak{a} \neq \{0\}$ annehmen. Wegen $-1 \in \mathbb{Z}$ folgt zudem aus $n \in \mathfrak{a}$ stets $-n \in \mathfrak{a}$, so dass $\mathfrak{a} \cap \mathbb{N} \subseteq \mathbb{N}$ nichtleer ist und somit ein eindeutig bestimmtes kleinstes Element m besitzt. Jedes Element von $m\mathbb{Z}$ ist nun von der Form rm mit einem $r \in \mathbb{Z}$ und liegt somit in $\mathfrak{a}$. Es gilt also $m\mathbb{Z} \subseteq \mathfrak{a}$. Umgekehrt erhalten wir für ein $a \in \mathfrak{a}$ durch Division mit Rest $q, r \in \mathbb{Z}$ mit $a = qm + r$ und $0 \leq r < m$. Wegen

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

und der Minimalität von m in $\mathfrak{a} \cap \mathbb{N}$ folgt $r = 0$, also $a = qm \in m\mathbb{Z}$ und schließlich $\mathfrak{a} \subseteq m\mathbb{Z}$. #

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

Bemerkung 2.13. *In der Sprache der Algebra besagt Satz 2.12, dass $\mathbb{Z}$ ein Hauptidealring ist.*

Bekanntlich ist für je zwei Ideale $\mathfrak{a}, \mathfrak{b}$ in einem Integritätsring R die ***Summe***

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

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

Beispiel 2.14. *Es ist* $2\mathbb{Z} + 3\mathbb{Z} = \mathbb{Z}$,

denn:

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

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

Die Summe zweier Ideale verallgemeinert sich in naheliegender Weise auf Summen endlich vieler Ideale, wobei diese Summenbildung offensichtlich assoziativ ist. Mit dem folgenden Satz erhalten wir eine explizite Beschreibung von Summen von Idealen aus $\mathbb{Z}$ und damit gleichzeitig die Existenz des größten gemeinsamen Teilers einer endlichen Menge ganzer Zahlen:

Satz 2.15. *Sei* $n \in \mathbb{N}$ *beliebig. Dann besitzen beliebige* $a_1, \ldots, a_n \in \mathbb{Z}$ *je 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 unserer Vorüberlegung zu Summen von Idealen und nach Satz 2.12 gibt es ein $d \in \mathbb{N}_0$ mit $a_1\mathbb{Z} + \ldots + a_n\mathbb{Z} = d\mathbb{Z}$. Diese Zahl d ist ein größter gemeinsamer Teiler von $a_1, \ldots, a_n$,

denn: Für ein beliebiges $i \in \{1, \ldots, n\}$ gilt

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

so dass es ein $r_i \in \mathbb{Z}$ mit $a_i = dr_i$ gibt. Die Zahl d ist also ein Teiler von a_i. Da i beliebig gewählt war, folgt $d \in T(a_1, \ldots, a_n)$. Sei nun $t \in T(a_1, \ldots, a_n)$ beliebig. Wegen $d \in d\mathbb{Z} = a_1\mathbb{Z} + \ldots + a_n\mathbb{Z}$ gibt es $u_1, \ldots, u_n \in \mathbb{Z}$ mit $d = u_1a_1 + \ldots + u_na_n$ und wegen $t \mid a_1, \ldots, t \mid a_n$ folgt $t \mid d$. #

Die Eindeutigkeit ergibt sich wieder aus Lemma 2.7. □

Korollar 2.16. *Für beliebige* $a_1, \ldots, a_n \in \mathbb{Z}$ *mit* $n \in \mathbb{N}$ *gilt*

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

so dass $\mathrm{ggT}(a_1, \ldots, a_n)$ *durch iteratives Anwenden des Euklid'schen Algorithmus 2.10 berechnet werden kann.*

Beweis. Nach Satz 2.15 gilt

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

Die Behauptung ergibt sich dann aus der Eindeutigkeitsaussage in Satz 2.12. □

2.2 Der Fundamentalsatz der Arithmetik

Im vergangenen Abschnitt haben wir Teiler gegebenener ganzer Zahlen studiert. Das Ziel dieses Abschnitts ist es, ganze Zahlen eindeutig als Produkte geeigneter Teiler darzustellen. Als mögliche Bausteine einer solchen Darstellung definieren wir:

Definition 2.17. *Ein natürliche Zahl $p > 1$ heißt **Primzahl**, wenn $T(p) = \{\pm 1, \pm p\}$, also $T(p) \cap \mathbb{N} = \{1, p\}$ ist. Die Menge der Primzahlen bezeichnen wir mit $\mathbb{P}$.*

Proposition 2.18. *Der kleinste positive und von 1 verschiedene Teiler von $1 < a \in \mathbb{N}$ ist eine Primzahl.*

Beweis. Wegen

$$a \in T_+ := (T(a) \cap \mathbb{N}) \setminus \{1\} = \{t \in \mathbb{N} \mid t \mid a, t \neq 1\}$$

ist $\emptyset \neq T_+ \subseteq \mathbb{N}$, so dass T_+ ein kleinstes Element p besitzt. Dieses Element p ist eine Primzahl,

denn: Sei $1 < t \in \mathbb{N}$ mit $t \mid p$ beliebig. Mit $p \mid a$ und Teil (c) von Lemma 2.2 folgt dann $t \mid a$ 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 nach Definition 2.17 damit die Primalität von p. #

□

Satz 2.19 (Satz von Euklid)**.** *Es gibt unendlich viele Primzahlen.*

Beweis. Gäbe es nur endlich viele Primzahlen $p_1, \ldots, p_n$ mit einem geeigneten $n \in \mathbb{N}$, so könnten wir eine natürliche Zahl $N := p_1 \cdot \ldots \cdot p_n + 1 > 1$ definieren. Nach Proposition 2.18 gäbe es eine Primzahl p mit $p \mid N$. Nach Annahme gälte $p \in \{p_1, \ldots, p_n\}$ und nach Teil (b) von Lemma 2.2 somit auch $p \mid p_1 \cdot \ldots \cdot p_n$. Nach Teil (a) von Lemma 2.2 folgte $p \mid (N - p_1 \cdot \ldots \cdot p_n) = 1$, was im Widerspruch zur Primalität von p steht. □

Wir führen nun eine Reihe klassischer Primzahlprobleme auf, auf die wir im Rahmen dieser Vorlesung nicht tiefer eingehen können und die teilweise auch noch ungelöst sind:

Bemerkung 2.20. (a) *Wie verhält sich die **Primzahlanzahlfunktion***

$$\pi(x) := \#\{p \in \mathbb{P} \mid p \leq x\}$$

asymptotisch für $x \to \infty$?

Carl Friedrich Gauß vermutete 1793 *den nach ihm benannten **Gauß'schen Primzahlsatz***

$$\lim_{x \to \infty} \frac{\pi(x)}{\frac{x}{\ln x}} \to 1.$$

Erst 1896 *wurde dieser unabhängig von Jacques Hadamard und Charles-Jean de la Vallée-Poussin mit Methoden der Analytischen Zahlentheorie bewiesen.*

(b) *Wie verteilen sich die Primzahlen in die Restklassen bei Division mit einem festen $n \in \mathbb{N}$?*

Johann Dirichlet bewies 1837, *dass es zu jedem Paar natürlicher Zahlen $k, n \in \mathbb{N}$ mit $\mathrm{ggT}(k,n) = 1$ unendlich viele Primzahlen p der Form $p = k + an$ mit einem $a \in \mathbb{N}$ gibt. Dieses Ergebnis wird heute der* ***Dirichlet'sche Primzahlsatz*** *genannt. Mit den damals revolutionären Methoden, die Dirichlet zum Beweis dieses Resultats einsetzte, begründete er die Analytische Zahlentheorie. Für $\mathrm{ggT}(k,n) > 1$ gibt es übrigens trivialerweise höchstens eine Primzahl p der oben gegebenen Form.*

(c) *Wie viele* ***Primzahlzwillinge*** *$(p, p+2)$ gibt es?*

Diese Frage ist bis heute unbekannt. Im Jahr 2014 *zeigten Zhang und Polymath, dass es unendlich viele Paare aufeinanderfolgender Primzahlen mit Abstand ≤ 246 gibt.*

(d) *Ist jede gerade Zahl > 2 die Summe zweier Primzahlen?*

Das ist die ***Goldbach-Vermutung*** *aus dem Jahr* 1742 *und ist bis heute ungelöst. Im Jahr* 2015 *löste Harald Helfgott die sogenannte* ***schwache Goldbach-Vermutung****, indem er zeigte, dass jede ungerade Zahl > 5 die Summer dreier Primzahlen ist.*

Die nachfolgende Charakterisierung von Primzahlen ist sehr wichtig und in vielen Beweisen tauglicher als die direkte Verwendung von Definition 2.17:

Proposition 2.21. *Für ein beliebiges $1 < p \in \mathbb{N}$ sind die folgenden Aussagen äquivalent:*

(i) *p ist eine Primzahl.*

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

Beweis. Gelte zunächst Aussage (i), sei also p eine Primzahl. Betrachten wir

$$a, b \in \mathbb{Z} \quad \text{mit } p \mid ab \text{ und } p \nmid a.$$

Dann ist $\mathrm{ggT}(p,a) = 1$ und mit Teil (a) von Proposition 2.11 folgt $p \mid b$. Das zeigt Aussage (ii).

Gelte nun umgekehrt Aussage (ii) und betrachten wir ein $a \in \mathbb{N}$ mit $a \mid p$. Zu diesem existiert ein $b \in \mathbb{Z}$ mit $p = ab$. Nach (ii) folgt $p \mid a$ oder $p \mid b$. Trivialerweise gilt zudem $a \mid p$ und $b \mid p$ und zusammengenommen also eine der beiden Aussagen

$$\big(p \mid a \text{ und } a \mid p\big) \quad \text{bzw.} \quad \big(p \mid b \text{ und } b \mid p\big).$$

Dies impliziert $a = p$ oder $b = p$ und demzufolge $a = 1$ oder $a = p$. Nach Definition 2.17 ist p also eine Primzahl und es gilt Aussage (i). □

Als erste Anwendung von Proposition 2.21 werden wir zeigen, dass die Primzahlen tatsächlich die gesuchten Bausteine der natürlichen (und somit auch der ganzen) Zahlen darstellen:

Satz 2.22 (Fundamentalsatz der Arithmetik)**.** *Jede natürliche Zahl $a \in \mathbb{N}$ lässt sich bis auf die Reihenfolge der Faktoren eindeutig als Produkt von Primzahlen schreiben.*

Beweis. Jede natürliche Zahl a besitzt eine ***Primfaktorzerlegung***, lässt sich also als Produkt von Primzahlen schreiben,

denn: Wir zeigen die Behauptung per Induktion nach a. Die Zahl $a = 1$ ist konventionsgemäß das leere Produkt, so dass wir ohne Einschränkung $a \geq 2$ annehmen können. Ist a eine Primzahl, so ist nichts zu zeigen. Ist andererseits a keine Primzahl, so ist $a = bc$ für geeignete $b, c \in \mathbb{N}$ mit $1 < b, c < a$. Nach Induktionsvoraussetzung besitzen dann b und c jeweils eine Primfaktorzerlegung und nach Multiplizieren erhalten wir eine Primfaktorzerlegung des Produkts $a = bc$. #

Seien nun für geeignete $r, s \in \mathbb{N}$

$$a = p_1 \cdot \ldots \cdot p_r = q_1 \cdot \ldots \cdot q_s \quad \text{mit } p_1, \ldots p_r, q_1, \ldots, q_s \in \mathbb{P}$$

zwei Primfaktorzerlegungen derselben natürlichen Zahl a. Dann gilt $p_1 \mid a = q_1 \cdot \ldots \cdot q_s$. Mit $p_1 \in \mathbb{P}$ und Proposition 2.21 erhalten wir die Existenz eines $i \in \{1, \ldots, s\}$ mit $p_1 \mid q_i$. Nach Umnummerieren können wir ohne Einschränkung $p_1 \mid q_1$ annehmen. Da q_1 und p_1 Primzahlen sind, folgt hieraus $p_1 = q_1$ und durch Kürzen von p_1 erhalten wir aus der Ausgangsgleichung

$$p_2 \cdot \ldots \cdot p_r = q_2 \cdot \ldots \cdot q_s.$$

Iterativ lässt sich so zeigen, dass $r = s$ ist, und dass für die Primfaktoren nach möglichem Vertauschen die Identitäten $p_i = q_i$ für alle $i \in \{1, \ldots, r = s\}$ gelten. □

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

Bemerkung 2.23. *Sei $a \in \mathbb{N}$. Fasst man in der im Fundamentalsatz 2.22 gegebenen Primfaktorzerlegung von a mehrfach vorkommende Primfaktoren in der Form $p \cdot \ldots \cdot p = p^\nu$ zusammen, so erhält man die Existenz einer* ***kanonischen Primfaktorzerlegung***

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

von a. Die Exponenten $\nu_p(a) \in \mathbb{N}_0$ sind hierbei durch a eindeutig bestimmt und heißen die ***Vielfachheiten*** *der Primzahlen p in a. Nach Konstruktion gilt dabei $\nu_p(a) \neq 0$ 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 2.24. *Für beliebige $a, b \in \mathbb{N}$ gilt:*

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

Beweis. Die Aussage $a \mid b$ ist gleichwertig mit der Existenz eines $c \in \mathbb{N}$ mit $a = bc$. Mit der Existenz der eindeutigen kanonischen Primfaktorzerlegung aus Bemerkung 2.23 folgt hieraus

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

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

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

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

Satz 2.25. *Für eine natürliche Zahl a mit kanonischer Primfaktorzerlegung $a = \prod_{p\in\mathbb{P}} p^{\nu_p(a)}$ gibt*

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

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

*an. Die so definierten Funktionen $\tau : \mathbb{N} \to \mathbb{N}$ und $\sigma : \mathbb{N} \to \mathbb{N}$ nennen wir daher auch die **Teileranzahlfunktion** bzw. die **Teilersummenfunktion**.*

Beweis. Nach Lemma 2.24 sind die Teiler von a genau diejenigen natürlichen Zahlen mit einer kanonischen Primfaktorzerlegung der Form

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

Da diese Zahlen nach dem Fundamentalsatz 2.22 paarweise verschieden sind, erhalten wir hieraus einerseits unmittelbar die behauptete Formel für τ und andererseits

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

□

Definition 2.26. *Eine Funktion $\psi : \mathbb{N} \to \mathbb{C}$ heißt **schwach multiplikativ**, wenn gilt:*

$$\psi(a \cdot b) = \psi(a) \cdot \psi(b) \quad \textit{für je zwei teilerfremde Zahlen } a, b \in \mathbb{N}.$$

Unmittelbar aus den in Satz 2.25 angegebenen Formeln folgt nun:

Korollar 2.27. *Für eine gegebene natürliche Zahl a mit kanonischer Primfaktorzerlegung $a = \prod_{p\in\mathbb{P}} p^{\nu_p(a)}$ gelten*

$$\tau(a) = \prod_{p\in\mathbb{P}} \tau(p^{\nu_p(a)}),$$

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

und also die schwache Multiplikativität der Teileranzahlfunktion τ sowie der Teilersummenfunktion σ.

2.3 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 2.28. *Für eine natürliche Zahl $a \in \mathbb{N}$ gilt:*

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

Satz 2.29. *Für ein beliebiges $k \in \mathbb{N}$ heißt $M_k := 2^k - 1$ die k-te **Mersenne-Zahl**. Für eine beliebige gerade natürliche Zahl $2 \mid a \in \mathbb{N}$ sind die folgenden beiden Aussagen äquivalent:*

(i) *a ist vollkommen.*

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

Beweis. Gelte zunächst Aussage (ii). Wegen der schwachen Multiplikativität 2.27 der Teilersummenfunktion und wegen $M_k \in \mathbb{P} \setminus \{2\}$ ist

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

also ist a vollkommen, es gilt also Aussage (i).

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

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

Wegen der Vollkommenheit von a und der schwachen Multiplikativität 2.27 von σ folgt

$$2^k b = 2a = \sigma(a) = \sigma(2^{k-1})\sigma(b) = (2^k - 1)\sigma(b).$$

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

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

und nach Einsetzen in die obige Gleichung erhalten wir

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

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

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

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

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

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

Bemerkung 2.30. *Dass die in Aussage (ii) von Satz 2.29 beschriebenen Zahlen vollkommen sind, geht auf Euklid (ca. 350 v. Chr.) zurück. Die umgekehrte Implikation zeigte Leonhard Euler im Jahr 1747.*

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

Beispiel 2.31. *Die kleinsten geraden vollkommenen Zahlen sind* 6, 28, 496, 8128.

Nach Satz 2.29 ist die Frage nach geraden vollkommenen Zahlen äquivalent mit derjenigen danach, welche Mersenne-Zahlen Primzahlen sind. Eine hierfür notwendige Bedingung liefert:

Proposition 2.32. *Für eine beliebiges $k \in \mathbb{N}$ gilt: Ist M_k prim, so notwendig auch k.*

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

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

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

$$M_k = 2^k - 1 = (2^b)^a - 1^a = (2^b - 1) \cdot \sum_{\nu=0}^{a-1} 2^{b\nu} = M_b \cdot \sum_{\nu=0}^{a-1} 2^{b\nu}$$

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

Bemerkung 2.33. *Umgekehrt zur Aussage von Proposition 2.32 gibt es sehr viele Primzahlen k, für die M_k keine Primzahl ist. Derzeit (Stand: Dezember 2018) sind genau* 51 *Mersenne-Primzahlen – und somit auch genau* 51 *gerade vollkommene Zahlen – bekannt, deren größte über* 24 *Millionen Stellen aufweist. Da es einen besonders effizienten Primzahltest für sie gibt, sind tatsächlich die größten derzeit bekannten Primzahlen Mersenne-Primzahlen.*

KAPITEL 3

Zahlentheoretische Funktionen

3.1 Schwach multiplikative Funktionen

Definition 3.1. *Eine **zahlentheoretische Funktion** ist eine Abbildung* $f : \mathbb{N} \to \mathbb{C}$.

Von besonderem Interesse sind schwach multiplikative zahlentheoretische Funktionen im Sinne von Definition 2.26. Die einfachste zahlentheoretische Funktion ist die ***Nullfunktion*** $f(a) \equiv 0$. Diese ist schwach multiplikativ, aber ohne Bedeutung. Nach Korollar 2.27 sind die Teileranzahlfunktion τ und die Teilersummenfunktion σ weitere (und interessantere) Beispiele schwach multiplikativer zahlentheoretischer Funktionen.

Lemma 3.2. *Für zwei schwach multiplikative zahlentheoretische Funktionen f, g gelten:*

(a) *Ist f nicht die Nullfunktion, so gilt $f(1) = 1$.*

(b) *Die durch $(fg)(a) := f(a)g(a)$ für alle $a \in \mathbb{N}$ gegebene Funktion ist schwach multiplikativ.*

Beweis. Für alle $a \in \mathbb{N}$ gilt $\mathrm{ggT}(a, 1) = 1$ und mit der schwachen Multiplikativität daher

$$f(a) = f(a \cdot 1) = f(a) \cdot f(1).$$

Nach Voraussetzung gibt es ein $a_0 \in \mathbb{N}$ mit $f(a_0) \neq 0$. Es folgt $f(1) = 1$, also Behauptung (a).

Für alle $a, b \in \mathbb{N}$ mit $\mathrm{ggT}(a, b) = 1$ gilt

$$(fg)(ab) = f(ab)g(ab) = f(a)f(b)g(a)g(b) = f(a)g(a)f(b)g(b) = (fg)(a)(fg)(b),$$

also Behauptung (b). □

Wir beschreiben nun schwach multiplikative Funktionen mithilfe des Fundamentalsatzes 2.22:

Satz 3.3. *Für eine von der Nullfunktion verschiedene zahlentheoretische Funktion f sind äquivalent:*

(i) *f ist schwach multiplikativ.*

(ii) *Ist $a \in \mathbb{N}$ mit kanonischer Primfaktorzerlegung $a = \prod_{i=1}^{r} p_i^{\nu_{p_i}(a)}$, so gilt $f(a) = \prod_{i=1}^{r} f(p_i^{\nu_{p_i}(a)})$.*

Beweis. Gelte zunächst Aussage (i), sei also f schwach multiplikativ. Zum Beweis von Aussage (ii) führen wir eine Induktion nach r durch, wobei der Fall $r = 0$ mit Teil (a) von Lemma 3.2 folgt und der Fall $r = 1$ trivial ist. Sei also $r > 1$ und nehmen wir an, Aussage (ii) sei für $r - 1$ bereits bewiesen. Nach dem Fundamentalsatz der Arithmetik 2.22 gilt $\mathrm{ggT}(p_1^{\nu_{p_1}(a)}, \prod_{i=2}^{r} p_i^{\nu_{p_i}(a)}) = 1$ und wegen der schwachen Multiplikativität somit

$$f(a) = f(p_1^{\nu_{p_1}(a)}) \cdot f(\prod_{i=2}^{r} p_i^{\nu_{p_i}(a)}) \overset{\text{IV}}{=} \prod_{i=1}^{r} f(p_i^{\nu_{p_i}(a)}).$$

Es folgt Aussage (ii).

Gelte nun umgekehrt (ii). Für beliebige $a, b \in \mathbb{N}$ mit $\mathrm{ggT}(a, b) = 1$ und kanonischen Primfaktorzerlegungen

$$a = \prod_{i=1}^{r} p_i^{\nu_{p_i}(a)} \quad \text{und} \quad b = \prod_{j=1}^{s} q_j^{\nu_{q_j}(b)}$$

gilt

$$f(ab) = f(\prod_{i=1}^{r} p_i^{\nu_{p_i}(a)} \cdot \prod_{j=1}^{s} q_j^{\nu_{q_j}(b)}) \overset{\text{(ii)}}{=} \prod_{i=1}^{r} f(p_i^{\nu_{p_i}(a)}) \cdot \prod_{j=1}^{s} f(q_j^{\nu_{q_j}(b)}) = f(a)f(b)$$

und somit die schwache Multiplikativität (i). □

Hieraus folgt unmittelbar:

Korollar 3.4. *Stimmen zwei schwach multiplikative zahlentheoretische Funktionen auf allen Primpotenzen überein, so sind sie bereits als Funktionen identisch.*

3.2 Die Euler'sche φ-Funktion

Definition 3.5. *Die Abbildung*

$$\varphi : \begin{cases} \mathbb{N} & \to \mathbb{N}, \\ n & \mapsto \#\{a \in \mathbb{N} \mid 1 \leq a \leq n \text{ und } \mathrm{ggT}(a, n) = 1\} \end{cases}$$

*heißt die **Euler'sche φ-Funktion**.*

Die Werte der φ-Funktion auf den Primpotenzen lassen sich leicht bestimmen:

Proposition 3.6. *Für eine Primzahl p und $n \in \mathbb{N}$ beliebig gilt:*

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

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

Um eine geschlossene Formel für die Werte der φ-Funktion zu erhalten, ist unser nächstes Ziel der Nachweis der schwachen Multiplikativität von φ. Zum Ausgangspunkt unserer Überlegungen hierzu machen wir die von Carl Friedrich Gauß 1801 gegebene

Satz 3.7 (Teilersummenformel)**.**

$$\sum_{\substack{d \mid a \\ d>0}} \varphi(d) = a \quad \textit{für alle } a \in \mathbb{N}.$$

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

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

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

$$a = \#\{1, \ldots, a\} = \#\Big(\bigcup_{\substack{d \mid a \\ d>0}} G_d(a)\Big) = \sum_{\substack{d \mid a \\ d>0}} \#G_d(a). \tag{3.1}$$

Wir bestimmen nun die einzelnen Summanden rechts genauer. Es gilt

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

denn: Gelte $\operatorname{ggT}(a,cd) = d$. Nach dem Erweiterten Euklid'schen Algorithmus 2.10 gibt es dann $u, v \in \mathbb{Z}$ mit $ua + vcd = d$ und also mit $u\frac{a}{d} + vc = 1$. #

Es folgt

$$\#G_d(a) = \#\{n \in \mathbb{N} \mid \text{es gibt ein } c \in \mathbb{N} \text{ mit } n = cd,\ 1 \leq c \leq \frac{a}{d} \text{ und } \operatorname{ggT}(\frac{a}{d}, c) = 1\} \overset{3.5}{=} \varphi(\frac{a}{d}).$$

Insgesamt erhalten wir

$$a \overset{(3.1)}{=} \sum_{\substack{d \mid a \\ d>0}} \#G_d(a) = \sum_{\substack{d \mid a \\ d>0}} \varphi(\frac{a}{d}) = \sum_{\substack{d \mid a \\ d>0}} \varphi(d).$$

□

Beispiel 3.8. *Für $a = 12$ besagt die Teilersummenformel 3.7*

$$\sum_{d \mid 12} \varphi(d) = \varphi(1) + \varphi(2) + \varphi(3) + \varphi(4) + \varphi(6) + \varphi(12) = 1 + 1 + 2 + 2 + 2 + 4 = 12.$$

Mit der Teilersummenformel 3.7 erhalten wir nun die schwache Multiplikativität von φ:

Satz 3.9. *Die Euler'sche φ-Funktion ist schwach multiplikativ und es gilt*

$$\varphi(a) = a \cdot \prod_{\substack{p \in \mathbb{P} \\ p|a}} (1 - \frac{1}{p}) \quad \textit{für alle } a \in \mathbb{N}.$$

Beweis. Wir zeigen zunächst die schwache Multiplikativität von φ per Indukion nach $c \in \mathbb{N}$. In jedem Schritt zeigen wir dabei, dass sich jede Zerlegung $c = ab$ mit teilerfremden $a, b \in \mathbb{N}$ als

$$\varphi(ab) = \varphi(c) = \varphi(a)\varphi(b)$$

in die Werte der φ-Funktion übersetzt. Der Induktionsanfang für $c = 1$ ist hierbei klar. Sei nun also $c > 1$ und sei die Behauptung für alle $1 \leq \tilde{c} < c$ bereits gezeigt. Für eine Zerlegung $c = ab$ mit teilerfremden $a, b \in \mathbb{N}$ gilt mit der Teilersummenformel 3.7 und dem Fundamentalsatz 2.22

$$\sum_{\substack{d_a|a \\ d_b|b}} \varphi(d_a)\varphi(d_b) = \Big(\sum_{d_a|a} \varphi(d_a)\Big) \cdot \Big(\sum_{d_b|b} \varphi(d_b)\Big) \overset{3.7}{=} ab \overset{3.7}{=} \sum_{d|ab} \varphi(d) \overset{2.22}{=} \sum_{\substack{d_a|a \\ d_b|b}} \varphi(d_a d_b). \tag{3.2}$$

Wir fixieren nun positive Teiler $d_a \mid a$ und $d_b \mid b$. Außer im Fall $(d_a = a) \wedge (d_b = b)$ gilt dann

$$\tilde{c} := d_a d_b < ab = c$$

und nach Induktionsvoraussetzung somit

$$\varphi(d_a)\varphi(d_b) = \varphi(d_a d_b).$$

Setzen wir dies in (3.2) ein, so folgt die Multiplikativität auch für den Summanden zu $d_a = a$ und $d_b = b$ und also

$$\varphi(c) = \varphi(a)\varphi(b).$$

Insgesamt haben wir die schwache Multiplikativität der Euler'schen φ-Funktion gezeigt.

Für ein beliebiges $a \in \mathbb{N}$ mit kanonischer Primfaktorzerlegung

$$a = \prod_{\substack{p \in \mathbb{P} \\ p|a}} p^{\nu_p(a)}$$

folgt hieraus

$$\varphi(a) = \prod_{\substack{p \in \mathbb{P} \\ p|a}} \varphi(p^{\nu_p(a)}) \overset{3.6}{=} \prod_{\substack{p \in \mathbb{P} \\ p|a}} p^{\nu_p(a)-1}(p-1) = \prod_{\substack{p \in \mathbb{P} \\ p|a}} p^{\nu_p(a)}(1 - \frac{1}{p}) = a \cdot \prod_{\substack{p \in \mathbb{P} \\ p|a}} (1 - \frac{1}{p})$$

und somit die geschlossene Formel für φ. □

Beispiel 3.10. *In der Praxis berechnet man Werte der Euler'schen φ-Funktion meist nicht mit der Formel aus Satz 3.9 sondern einfacher direkt mit schwacher Multiplikativität und Proposition 3.6:*

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

KAPITEL 4

Kongruenzen

4.1 Restklassenringe

Es sei R ein Ring,[2] „$\sim$“ eine Äquivalenzrelation auf R und $\mathfrak{a}$ das durch

$$a \sim b \quad :\Longleftrightarrow \quad a - b \in \mathfrak{a}$$

definierte Ideal in R. Dann ist bekanntlich die Menge $R/\sim := R/\mathfrak{a}$ aller Restklassen bezüglich „$\sim$“ ein Ring mit den Verknüpfungen

$$\overline{a} + \overline{b} = \overline{a+b} \text{ und } \overline{a} \cdot \overline{b} = \overline{a \cdot b}$$

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

Da die Ideale in $\mathbb{Z}$ nach Satz 2.12 von der Form $n\mathbb{Z}$ mit einem $n \in \mathbb{N}_0$ sind, erhalten wir hieraus leicht die folgende Charakterisierung der Äquivalenzrelationen auf $\mathbb{Z}$:

Proposition 4.1. *Für jede Äquivalenzrelation „$\sim$“ auf $\mathbb{Z}$ gibt es ein eindeutig bestimmtes $n \in \mathbb{N}_0$ mit*

$$a \sim b \quad \Longleftrightarrow \quad a - b \in n\mathbb{Z} \quad \Longleftrightarrow \quad n \mid (a-b).$$

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

$$a \sim b \quad :\Longleftrightarrow \quad a - b \in n\mathbb{Z} \quad \Longleftrightarrow \quad n \mid (a-b)$$

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

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

[2] In diesem Kapitel betrachten wir bis auf offensichtliche Ausnahmen nur kommutative Ringe mit Eins, schreiben aber kurz nur „Ring“ für diese.

Korollar 4.2. *Die Restklassenringe von $\mathbb{Z}$ sind nach Proposition 4.1 gerade die Ringe $\mathbb{Z}/n\mathbb{Z}$ mit $n \in \mathbb{N}_0$. Explizit 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 $\{\{a\} \mid a \in \mathbb{Z}\}$ identifizieren. #

- $\mathbb{Z}/1\mathbb{Z} = 0$ *ist der Nullring (hier sind Eins- und Nullelement gleich),*

  denn: Für ein beliebiges $a \in \mathbb{Z}$ ist $a + \mathbb{Z} = \mathbb{Z} = 0 + \mathbb{Z}$. #

- $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ *für alle $n > 1$,*

  denn: Für jedes $a \in \mathbb{Z}$ gibt es $q, r \in \mathbb{Z}$ mit $0 \leq r \leq n-1$ und $a = qn + r$. Es gilt daher $\overline{a} = \overline{qn + r} = \overline{qn} + \overline{r} = \overline{r}$. Hieraus folgt für $a \neq b \in \mathbb{Z}$ mit $0 \leq a, b \leq n-1$ die Inäquivalenz $a \not\equiv b \bmod n$ und also $\overline{a} \neq \overline{b}$. #

Definition 4.3. *Ein Element x eines Ringes R heißt ein **Nullteiler**, wenn es ein $0 \neq y \in R$ mit $xy = 0$ gibt. Der Ring R heißt **nullteilerfrei**, wenn $R \neq 0$ ist und 0 der einzige Nullteiler in R ist.*

Definition 4.4. *Ein Element x eines Ringes R heißt eine **Einheit**, wenn es ein $y \in R$ mit $xy = 1$ gibt.*

In dieser Sprache gilt im Beispiel $\mathbb{Z}/3\mathbb{Z}$:

- Nullteiler: $\overline{0}$ (es ist also $\mathbb{Z}/3\mathbb{Z}$ nullteilerfrei),
- Einheiten: $\overline{1}, \overline{2}$.

Im Beispiel $\mathbb{Z}/4\mathbb{Z}$ gilt:

- Nullteiler: $\overline{0}, \overline{2}$ (es ist also $\mathbb{Z}/4\mathbb{Z}$ nicht nullteilerfrei),
- Einheiten: $\overline{1}, \overline{3}$.

Bekanntlich bildet für einen gegebenen Ring R die Menge

$$R^\times := \{x \in R \mid x \text{ ist Einheit } \}$$

zusammen mit der Multiplikation eine abelsche Gruppe, die ***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.

Proposition 4.5. *Sei R ein Ring. Dann gelten die folgenden beiden Aussagen:*

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

(b) *Ist R speziell endlich, so gilt umgekehrt auch: Ist $x \in R$ kein Nullteiler, so ist $x \in R^\times$.*

*Insbesondere gilt im Fall $R = \mathbb{Z}/n\mathbb{Z}$ mit einem $n \in \mathbb{N}$: Ein $\overline{x} \in R$ ist genau dann eine Einheit, wenn es kein Nullteiler ist. Die Einheiten im Ring $\mathbb{Z}/n\mathbb{Z}$ nennt man die **primen Restklassen** modulo n, die Gruppe $\left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ die **Gruppe der primen Restklassen** modulo n.*

Beweis. Wir zeigen zunächst Behauptung (a). Im Fall des Nullrings $R = 0$ ist das Element 0 eine Einheit, aber kein Nullteiler. Im Fall $R \neq 0$ betrachten wir $x \in R^\times$ und $y \in R$ mit $xy = 0$. Wir erhalten $y = x^{-1}xy = 0$, so dass x kein Nullteiler sein kann.

Zum Beweis von Behauptung (b) setzen wir R nun als endlich voraus. Wir betrachten ein $x \in R$, das kein Nullteiler ist, und die Abbildung

$$\lambda_x : \begin{cases} R & \to R, \\ a & \mapsto xa. \end{cases}$$

Letztere ist injektiv, denn aus $\lambda_x(a) = \lambda_x(b)$ folgt $xa = xb$ und also $x(a-b) = 0$. Weil x kein Nullteiler ist, folgt $a - b = 0$ und somit $a = b$. Als injektive Selbstabbildung der endlichen Menge R ist λ_x auch surjektiv, insbesondere existiert ein $y \in R$ mit $\lambda_x(y) = 1$, was $xy = 1$ und deshalb $x \in R^\times$ impliziert. □

Satz 4.6. *Für $n \in \mathbb{N}$ sind die folgenden Aussagen 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 kurz $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.

Beweis. Gelte zunächst Aussage (i) und seien n eine Primzahl sowie $\overline{a} \in \mathbb{Z}/n\mathbb{Z} \setminus \{\overline{0}\}$. Aus $\overline{a} \neq \overline{0}$ folgt $n \nmid a$ und wegen der Primalität von n weiter $\mathrm{ggT}(n, a) = 1$. Nach dem Erweiterten Euklid'schen Algorithmus 2.10 (c) gibt es $u, v \in \mathbb{Z}$ mit $un + va = 1$. Es folgt $\overline{un} + \overline{va} = \overline{1}$ und also $\overline{v} \cdot \overline{a} = \overline{1}$. Mit $\overline{v}$ haben wir somit ein Inverses von $\overline{a}$ gefunden, so dass $\mathbb{Z}/n\mathbb{Z}$ ein Körper ist. Das ist 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 $\left(\mathbb{Z}/n\mathbb{Z}\right)^\times = \mathbb{Z}/n\mathbb{Z} \setminus \{\overline{0}\}$. Nach Proposition 4.5 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).

Um zu zeigen, dass Aussage (i) aus Aussage (iii) folgt, nehmen wir an, Aussage (i) gelte nicht, n sei also keine Primzahl. Im Fall $n = 1$ ist $\mathbb{Z}/n\mathbb{Z} = 0$ nicht nullteilerfrei. Im Fall $n > 1$ gibt es $a, b \in \mathbb{N}$ mit $1 < a, b < n$ mit $n = ab$. Es ergibt sich $\overline{0} = \overline{n} = \overline{ab} = \overline{a}\overline{b}$ mit $\overline{a}, \overline{b} \neq \overline{0}$, also sind $\overline{a}, \overline{b}$ Nullteiler und $\mathbb{Z}/n\mathbb{Z}$ ist nicht nullteilerfrei. Das ist die Negation von Aussage (iii), so dass wir unsere Behauptung nachgewiesen haben. □

4.2 Der Satz von Euler-Fermat

Proposition 4.7. *Seien $n \in \mathbb{N}$ und $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$. Dann sind die folgenden Aussagen äquivalent:*

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

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

Beweis. Sei zunächst $\overline{a} \in \left(\mathbb{Z}/n\mathbb{Z}\right)^\times$. Dann gibt es ein $\overline{b} \in \left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ mit $\overline{a}\overline{b} = \overline{1}$ und also ein $k \in \mathbb{Z}$ mit $ab = 1 + kn$. Für einen beliebigen gemeinsamen Teiler $d \in \mathbb{Z}$ von a und n folgt dann $d \mid (ab - kn) = 1$. Wir erhalten $\mathrm{ggT}(a, n) = 1$.

Sei nun umgekehrt $\mathrm{ggT}(a, n) = 1$. Nach dem Erweiterten Euklid'schen Algorithmus 2.10 (c) gibt es dann $u, v \in \mathbb{Z}$ mit $au + vn = 1$. Wir erhalten $\overline{a}\overline{u} = \overline{1}$ und insbesondere $\overline{a} \in \left(\mathbb{Z}/n\mathbb{Z}\right)^\times$. □

Aus der Algebra ist das folgende gruppentheoretische Resultat bekannt:

Proposition 4.8. *Für ein beliebiges Element g einer endlichen abelschen Gruppe G gilt*

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

Beweis. Die Abbildung

$$\lambda_g : \begin{cases} G & \to G, \\ x & \mapsto gx \end{cases}$$

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

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

woraus $g^{|G|} = 1$ folgt. □

Korollar 4.9 (Satz von Euler-Fermat)**.** *Für $n \in \mathbb{N}$ und $\overline{a} \in \left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ gilt*

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

Beweis. Nach Definition 3.5 und Proposition 4.7 ist $\varphi(n) = |\left(\mathbb{Z}/n\mathbb{Z}\right)^\times|$. Die Behauptung folgt nun direkt aus Proposition 4.8, angewendet auf $G = \left(\mathbb{Z}/n\mathbb{Z}\right)^\times$. □

Beispiel 4.10. *Es ist* $3^{19} \equiv 10 \bmod 17$,

denn: Nach dem Satz von Euler-Fermat 4.9 gilt

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

Hieraus folgt sofort

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

#

Korollar 4.11 (Kleiner Satz von Fermat)**.** *Für eine beliebige Primzahl p gelten:*

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

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

Beweis. Nach Proposition 3.6 gilt $\varphi(p) = p - 1$. Behauptung (a) ergibt sich daher direkt aus dem Satz von Euler-Fermat 4.9.

Ist nun $\overline{a} \in \mathbb{F}_p^\times$, so gilt $\overline{a}^{p-1} = \overline{1}$ nach Aussage (a) und deshalb auch

$$\overline{a}^p = \overline{a} \cdot \overline{a}^{p-1} = \overline{a} \cdot \overline{1} = \overline{a}.$$

Für $\overline{a} = \overline{0}$ gilt trivialerweise

$$\overline{a}^p = \overline{0}^p = \overline{0} = \overline{a}.$$

Insgesamt haben wir Behauptung (b) gezeigt. □

Korollar 4.12. *Für eine beliebige Primzahl p ist die Einheitengruppe $\mathbb{F}_p^\times$* ***zyklisch****, es gibt also einen* ***Erzeuger*** $\overline{w} \in \mathbb{F}_p^\times$ *mit* $\mathbb{F}_p^\times = \{\overline{1}, \overline{w}, \ldots, \overline{w}^{p-2}\}$.

Beweis. Sei e die kleinste natürliche Zahl mit

$$\overline{a}^e = \overline{1} \quad \text{für alle } \overline{a} \in \mathbb{F}_p^\times.$$

Dann ist also jedes Element von $\mathbb{F}_p^\times$ Nullstelle des Polynoms

$$X^e - \overline{1} \in \mathbb{F}_p[X].$$

Da $\mathbb{F}_p$ ein Körper ist, lassen sich Nullstellen von Polynomen über $\mathbb{F}_p$ als Linearfaktoren abspalten, so dass insbesondere dieses Polynom höchstens e Nullstellen hat. Es folgt

$$|\mathbb{F}_p^\times| \leq e \overset{4.11}{\leq} |\mathbb{F}_p^\times|$$

und also $|\mathbb{F}_p^\times| = e$. Durch genaue Buchführung kann man hieraus die Existenz eines Elements $\overline{w} \in \mathbb{F}_p^\times$ mit $\overline{w}^n \neq \overline{1}$ für alle $n \in \{1, \ldots, p-2\}$ zeigen und damit die Zyklizität von $\mathbb{F}_p^\times$. □

4.3 Quadratische Reste und der Satz von Euler

Definition 4.13. *Für $p \in \mathbb{P}$ ungerade heißt ein $a \in \mathbb{Z}$ (bzw. die Restklasse $\overline{a} \in \mathbb{F}_p$) ein* ***quadratischer Rest*** *bzw.* ***quadratischer Nichtrest*** *modulo p, falls $p \nmid a$ gilt und es ein bzw. kein $x \in \mathbb{Z}$ mit $x^2 \equiv a \bmod (p)$ gibt. Wir definieren das* ***Legendre-Symbol*** *modulo p durch*

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{für } a \text{ quadratischer Rest modulo } p, \\ 0 & \text{für } p \mid a, \\ -1 & \text{für } a \text{ quadratischer Nichtrest modulo } p \end{cases} \qquad \text{für alle } a \in \mathbb{Z}.$$

Offenbar hängt das Legendre-Symbol $\left(\frac{a}{p}\right)$ nur von der Restklasse von a modulo p ab.

Beispiel 4.14. *In* $(\mathbb{Z}/5\mathbb{Z})^\times$ *ist* $\overline{1}^2 = \overline{1}, \overline{2}^2 = \overline{4}, \overline{3}^2 = \overline{4}$ *und* $\overline{4}^2 = \overline{1}$. *Dementsprechend erhalten wir*

$$\left(\frac{a}{5}\right) = \begin{cases} 1 & \text{für } a \equiv 1,4 \bmod (5), \\ 0 & \text{für } a \equiv 0 \bmod (5), \\ -1 & \text{für } a \equiv 2,3 \bmod (5). \end{cases}$$

Lemma 4.15. *Für eine ungerade Primzahl* p, *einen Vertreter* $w \in \mathbb{Z}$ *eines Erzeugers von* $\mathbb{F}_p^\times$ *und ein beliebiges* $r \in \mathbb{N}_0$ *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 im Folgenden.

Sei zunächst w^r quadratischer Rest modulo p. Dann gibt es ein $x \in \mathbb{Z}$ mit $\overline{w}^r = \overline{x}^2$ in $\mathbb{F}_p$. Da $\overline{w}$ die Gruppe $\mathbb{F}_p^\times$ erzeugt, gibt es ein $n \in \mathbb{N}_0$ mit $\overline{x} = \overline{w}^n$. Es folgt $\overline{w}^r = \overline{w}^{2n}$ und somit $\overline{w}^{r-2n} = \overline{1}$. Die Zahl $r - 2n$ ist also ein Vielfaches der Ordnung von $\overline{w}$. Da $\overline{w}$ die Gruppe $\mathbb{F}_p^\times$ erzeugt, ist diese Ordnung $p - 1$ und insbesondere gerade. Es folgt die Geradheit zunächst von $r - 2n$ und dann auch von r.

Sei nun umgekehrt r gerade. Dann gibt es ein $q \in \mathbb{N}_0$ mit $r = 2q$. Das liefert $\overline{w}^r = (\overline{w}^q)^2$, so dass $\overline{w}^r$ ein quadratischer Rest modulo p ist. □

Es ist $\mathbb{F}_p^\times = \{\overline{1}, \overline{w}, \ldots, \overline{w}^{p-2}\}$. In dieser Darstellung sind die quadratischen (Nicht-)Reste modulo p also genau diejenigen Restklassen mit (un-)geradem Exponenten.

Proposition 4.16. *Für eine ungerade Primzahl* p *und* $a, b \in \mathbb{Z}$ *gilt:*

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

Wir sagen, das Legendre-Symbol ist ***stark multiplikativ****.*

Beweis. Da p eine Primzahl ist, gilt die Äquivalenz

$$p \mid ab \quad \Longleftrightarrow \quad p \mid a \text{ oder } p \mid b.$$

Die linke Seite der Behauptung ist also genau dann Null, wenn die rechte Seite verschwindet. Für den Rest des Beweises können wir daher ohne Einschränkung $p \nmid a$ und $p \nmid b$ annehmen. Für einen beliebigen Vertreter $w \in \mathbb{Z}$ eines Erzeugers von $\mathbb{F}_p^\times$ gibt es $r, s \in \mathbb{N}_0$ mit $\overline{a} = \overline{w}^r$ und $\overline{b} = \overline{w}^s$ und es gilt

$$\left(\frac{ab}{p}\right) = \left(\frac{w^{r+s}}{p}\right) = (-1)^{r+s} = (-1)^r(-1)^s = \left(\frac{w^r}{p}\right)\left(\frac{w^s}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

□

Satz 4.17 (Satz von Euler)**.** *Für eine ungerade Primzahl $p \in \mathbb{P}$ und $a \in \mathbb{Z}$ gilt:*

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

Beweis. Im Fall $p \mid a$ gilt

$$\left(\frac{a}{p}\right) = 0 \equiv a^{\frac{p-1}{2}} \bmod (p),$$

so dass wir für den Rest des Beweises $p \nmid a$ annehmen können. Nach dem Kleinen Satz von Fermat 4.11 erhalten wir in $\mathbb{F}_p$ die Gleichung

$$(\overline{a}^{\frac{p-1}{2}})^2 = \overline{a}^{p-1} = \overline{1}.$$

Da $\mathbb{F}_p$ ein Körper ist, lassen sich Nullstellen von Polynomen in $\mathbb{F}_p[X]$ als Linearfaktoren abspalten und das quadratische Polynom $X^2 - \overline{1} \in \mathbb{F}_p[X]$ hat höchstens zwei Nullstellen. Diese sind offensichtlich $\overline{1}, \overline{-1} \in \mathbb{F}_p$. Es folgt

$$\overline{a}^{\frac{p-1}{2}} \in \{\overline{1}, \overline{-1}\}.$$

Der Beweis des Satzes reduziert sich somit auf die Behauptung

$$\left(\frac{a}{p}\right) = 1 \quad \Longleftrightarrow \quad \overline{a}^{\frac{p-1}{2}} = \overline{1}.$$

Für deren Beweis nehmen wir zunächst $(\frac{a}{p}) = 1$ an, also die Existenz eines $\overline{x} \in (\mathbb{Z}/p\mathbb{Z})^\times$ mit $\overline{a} = \overline{x}^2$. Wieder mit dem Kleinen Satz von Fermat 4.11 folgt dann

$$\overline{a}^{\frac{p-1}{2}} = \overline{x}^{p-1} = \overline{1}.$$

Gelte nun umgekehrt $\overline{a}^{\frac{p-1}{2}} = \overline{1}$. Schreiben wir $\overline{a} = \overline{w}^r$ mit einem Vertreter $w \in \mathbb{Z}$ eines Erzeugers von $\mathbb{F}_p^\times$ und einem Exponenten $r \in \mathbb{N}_0$, so erhalten wir

$$(\overline{w}^r)^{\frac{p-1}{2}} = \overline{a}^{\frac{p-1}{2}} = \overline{1}.$$

Die Zahl $r\,\frac{p-1}{2}$ ist also ein Vielfaches der Ordnung von $\overline{w}$, also von $p-1$, und es folgt, dass r gerade ist. Mit Lemma 4.15 erhalten wir

$$\left(\frac{a}{p}\right) = \left(\frac{w^r}{p}\right) = (-1)^r = 1.$$

□

Wegen $p > 2$ sind die Restklassen von $-1, 0, 1$ modulo p paarweise verschieden und das Legendre-Symbol ist durch seine Restklasse modulo p eindeutig bestimmt.

Mit nur ein klein wenig mehr Arbeit erhält man das berühmte Quadratische Reziprozitätsgesetz, dessen Entdeckung durch Euler und dessen Beweis durch Gauß 1796 die Ausgangspunkte der Entwicklung der modernen Zahlentheorie waren:

Satz 4.18 (Quadratisches Reziprozitätsgesetz)**.** *Für je zwei ungerade Primzahlen p, q gelten die folgenden Aussagen:*

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{q}{p}\right), \qquad \textbf{(Quadratisches Reziprozitätsgesetz)}$$

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \qquad \textbf{(Erster Ergänzungssatz)}$$

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}. \qquad \textbf{(Zweiter Ergänzungssatz)}$$

Beispiel 4.19. *Das Reziprozitätsgesetz kann benutzt werden, um Legendre-Symbole auszurechnen:*

$$\left(\frac{273}{307}\right) = \left(\frac{3\cdot 7\cdot 13}{307}\right) \overset{4.16}{=} \left(\frac{3}{307}\right)\left(\frac{7}{307}\right)\left(\frac{13}{307}\right).$$

Wegen $7 \equiv 307 \equiv 3 \bmod (4)$ *und* $13 \equiv 1 \bmod (4)$ *ergibt sich:*

$$\left(\frac{273}{307}\right) \overset{4.18}{=} (-1)\left(\frac{307}{3}\right)(-1)\left(\frac{307}{7}\right)\left(\frac{307}{13}\right) = \left(\frac{307}{3}\right)\left(\frac{307}{7}\right)\left(\frac{307}{13}\right).$$

Aufgrund von $307 \equiv 1 \bmod (3)$, $307 \equiv -1 \bmod (7)$ *und* $307 \equiv 8 \bmod (13)$ *erhalten wir*

$$\left(\frac{273}{307}\right) = \left(\frac{1}{3}\right)\left(\frac{-1}{7}\right)\left(\frac{8}{13}\right) \overset{4.18}{=} 1(-1)\left(\frac{8}{13}\right) \overset{4.16}{=} (-1)\left(\frac{2}{13}\right).$$
$$\overset{4.18}{=} (-1)(-1) = 1.$$

4.4 Primzahltests

In diesem Abschnitt werden wir uns mit effizienten Algorithmen beschäftigen, die testen, ob eine vorgegebene Zahl eine Primzahl ist. Die naive Methode der Probedivisionen geht von der Definition einer Primzahl aus und testet bei Vorgabe einer Zahl n für alle Primzahlen $x \leq \sqrt{n}$, ob x ein Teiler von n ist. Für große Zahlen n ist dies jedoch zu aufwändig. Um effizientere Verfahren zu erhalten, benötigen wir geeignete Primzahlkriterien. Um solche zu erhalten, kann man sich die bisher bewiesenen Sätze für Primzahlen anschauen und fragen, ob sich diese in geeigneter Weise umkehren und zur Charakterisierung von Primzahlen verwenden lassen.

Es stellt sich heraus, dass sich der Kleine Satz von Fermat 4.11 nicht zur Charakterisierung von Primzahlen eignet, denn es gibt Nicht-Primzahlen $1 < n \in \mathbb{N}$, die

$$\overline{a}^{n-1} = \overline{1} \quad \text{für alle } \overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$$

erfüllen, so etwa $n = 561$. Solche Zahlen werden ***Carmichael-Zahlen*** genannt und sind – wie man leicht zeigen kann – stets von der Form $n = p_1 \cdot \ldots \cdot p_r$ mit paarweise verschiedenen, ungeraden Primzahlen und einem $r \geq 3$. Nach einem Ergebnis von Alford, Granville und Pomerance aus dem Jahr 1994 gibt es unendlich viele Carmichael-Zahlen.

Der Satz von Euler 4.17 lässt sich jedoch verwenden. Dafür definieren wir für eine beliebige ungerade Zahl $n = \prod_{p\in\mathbb{P}} p^{\nu_p(n)}$ das ***Jacobi-Symbol*** modulo n durch

$$\left(\frac{a}{n}\right) := \prod_{p\in\mathbb{P}} \left(\frac{a}{p}\right)^{\nu_p(n)} \quad \text{für alle } a \in \mathbb{Z}.$$

Nach Konstruktion und Proposition 4.16 ist dieses stark multiplikativ und man kann zeigen, dass das Quadratische Reziprozitätsgesetz 4.18 auch für das Jacobi-Symbol Gültigkeit hat. Aber Achtung: Das Jacobi-Symbol modulo n gibt nicht darüber Auskunft, ob eine Zahl $a \in \mathbb{Z}$ modulo n ein quadratischer Rest ist oder nicht, denn es gilt etwa

$$\left(\frac{5}{9}\right) = \left(\frac{5}{3}\right)^2 = 1,$$

aber 5 ist modulo 9 kein quadratischer Rest. Mit dem Jacobi-Symbol lässt sich nun die folgende Umkehrung des Satzes von Euler formulieren:

Satz 4.20. *Für ungerades $1 < n \in \mathbb{N}$ sind die folgenden Aussagen äquivalent:*

(i) *n ist eine Primzahl.*

(ii) *Für alle $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$ ist $\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \bmod (n)$.*

Beweis. Dass Aussage (ii) aus Aussage (i) folgt, ist gerade der Satz von Euler 4.17.

Gelte also Aussage (ii). Durch Quadrieren ergibt sich hieraus

$$\overline{a}^{n-1} = \overline{1} \quad \text{für alle } \overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times.$$

Somit ist n eine Primzahl oder eine Carmichael-Zahl. Letzeres kann jedoch nicht sein,

denn: Wäre n eine Carmichael-Zahl, so gälte

$$n = p_1 \cdot \ldots \cdot p_r \quad \text{mit paarweise verschiedenen ungeraden } p_1, \ldots, p_r \in \mathbb{P} \text{ und } r \geq 3.$$

Wäre nun $a_1 \in \mathbb{Z}$ ein Nichtquadrat modulo p_1, so gäbe es nach dem Chinesischen Restsatz ein $b \in \mathbb{Z}$ mit

$$b \equiv a_1 \bmod (p_1),\ b \equiv 1 \bmod (p_2),\ \ldots,\ b \equiv 1 \bmod (p_r)$$

und somit

$$\left(\frac{b}{n}\right) = \left(\frac{b}{p_1}\right)\left(\frac{b}{p_2}\right)\ldots\left(\frac{b}{p_n}\right) = (-1)\cdot 1 \cdot \ldots \cdot 1 = -1.$$

Nach Voraussetzung und wegen $\overline{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$ folgte

$$-1 = \left(\frac{b}{n}\right) \equiv b^{\frac{n-1}{2}} \bmod (n).$$

und somit insbesondere

$$-1 \equiv b^{\frac{n-1}{2}} \equiv 1^{\frac{n-1}{2}} \equiv 1 \bmod (p_2),$$

was nicht sein kann. #

Damit haben wir gezeigt, dass n eine Primzahl ist. □

Definition 4.21. *Sei $1 < n \in \mathbb{N}$ ungerade und sei $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$. Die Zahl a heißt ein **Euler'scher Zeuge für die Zerlegbarkeit** von n, wenn*

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

gilt. Wir setzen

$$E_n := \{\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times \mid a \text{ ist Euler'scher Zeuge für die Zerlegbarkeit von } n\}.$$

Proposition 4.22. *Für eine ungerade Nicht-Primzahl $1 < n \in \mathbb{N}$ gilt:*

$$\#E_n \geq \frac{1}{2}|(\mathbb{Z}/n\mathbb{Z})^\times| = \frac{\varphi(n)}{2}.$$

Beweis. Da n keine Primzahl ist, gibt es nach Satz 4.20 ein $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$ mit $\overline{a} \in E_n$. Wir setzen

$$E_n^C := (\mathbb{Z}/n\mathbb{Z})^\times \setminus E_n \quad \text{und} \quad \overline{a}E_n^C := \{\overline{a}\overline{b} \mid \overline{b} \in E_n^C\}.$$

Es ist $\#(\overline{a}E_n^C) = \#E_n^C$, denn für $\overline{b_1}, \overline{b_2} \in E_n^C$ gilt $\overline{a}\overline{b_1} = \overline{a}\overline{b_2}$ genau dann, wenn $\overline{b_1} = \overline{b_2}$ ist. Darüber hinaus gilt $\overline{a}E_n^C \cap E_n^C = \emptyset$,

denn: Für jedes $\overline{c} \in \overline{a}E_n^C \cap E_n^C$ gäbe es ein $\overline{b} \in E_n^C$ mit $\overline{c} = \overline{a}\overline{b}$. Das lieferte

$$\overline{a} = \overline{c}\overline{b}^{-1} = \overline{c}\overline{b}^{\varphi(n)-1} = \overline{cb^{\varphi(n)-1}}$$

und also

$$\left(\frac{a}{n}\right) = \left(\frac{cb^{\varphi(n)-1}}{n}\right) = \left(\frac{c}{n}\right)\left(\frac{b}{n}\right)^{\varphi(n)-1}$$
$$\overset{\overline{c},\overline{b}\in E_n^C}{\equiv} c^{\frac{n-1}{2}}(b^{\frac{n-1}{2}})^{\varphi(n)-1} \equiv (cb^{\varphi(n)-1})^{\frac{n-1}{2}} \equiv a^{\frac{n-1}{2}} \bmod (n).$$

Es folgte $\overline{a} \in E_n^C$, was ein Widerspruch ist. #

Wir erhalten

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

und somit

$$\#E_n = \#\left((\mathbb{Z}/n\mathbb{Z})^\times \setminus E_n^C\right) = \varphi(n) - \#E_n^C \geq \frac{\varphi(n)}{2}.$$

□

Algorithmus 4.23 (Primzahltest von Solovay-Strassen, 1977)**.** *Prüfe, ob die ungerade Zahl* $1 < n \in \mathbb{N}$ *eine Primzahl ist:*

(1) Wähle zufällig Zahlen $a_1, \ldots, a_r$ *mit* $\mathrm{ggT}(a_i, n) = 1$ *für* $i \in \{1, \ldots, r\}$.

(2) Bestimme für $i \in \{1, \ldots, r\}$*, ob* a_i *ein Euler'scher Zeuge für die Zerlegbarkeit von* n *ist.*

(3) Ist eines der a_i *ein Euler'scher Zeuge für die Zerlegbarkeit von* n*, 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 4.20; die Abschätzung für die Wahrscheinlickeit W unmittelbar aus Proposition 4.22.

Dass es sich bei dem Primzahltest von Solovay-Strassen 4.23 um einen *probabilistischen* Primzahltest handelt, ist für die Praxis 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 4.24. *Wir untersuchen* $n = 73$ *mit dem Primzahltest von Solovay-Strassen 4.23 auf Primalität und wählen dafür* $r = 2$ *sowie* $a_1 = 3$ *und* $a_2 = 5$*. Es ist dann*

$$a_1^{\frac{n-1}{2}} = 3^{36} \equiv 1 \bmod (73) \quad \textit{und} \quad \left(\frac{a_1}{n}\right) = \left(\frac{3}{73}\right) = \left(\frac{73}{3}\right) = \left(\frac{1}{3}\right) = 1,$$

$$a_2^{\frac{n-1}{2}} = 5^{36} \equiv -1 \bmod (73) \quad \textit{und} \quad \left(\frac{a_2}{n}\right) = \left(\frac{5}{73}\right) = \left(\frac{73}{5}\right) = \left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{-1}{3}\right) = -1.$$

Somit sind $a_1 = 3$ *und* $a_2 = 5$ *keine Euler'schen Zeugen für die Zerlegbarkeit von* n*. Die Ausgabe des Solovay-Strassen-Tests lautet:* $n = 73$ *ist vermutlich eine Primzahl.*

4.5 Das RSA-Verfahren

Problemstellung: Ein ***Absender*** A möchte einem ***Empfänger*** E verschlüsselt eine Nachricht übertragen, ohne vorher gemeinsam auf sichere Weise einen Schlüssel austauschen zu müssen.

Idee: E erzeugt einen ***öffentlichen Schlüssel*** und einen ***privaten Schlüssel***. A verschlüsselt die Nachricht mit dem öffentlichen Schlüssel und sendet sie an E. E entschlüsselt die Nachricht mit dem privaten Schlüssel.

Schwierigkeit: Das Erzeugen beider Schlüssel muss schnell gehen, ebenso das Verschlüsseln mit dem öffentlichen Schlüssel und das Entschlüsseln mit dem privaten Schlüssel. Das Bestimmen des privaten Schlüssels aus dem öffentlichen Schlüssel darf dagegen 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 4.25 (Schlüsselerzeugung beim RSA-Verfahren)**.** *E möchte ein Paar von Schlüsseln erzeugen, um künftig als Empfänger von verschlüsselten Nachrichten in Frage zu kommen:*

(1) E bestimmt zufällig zwei große voneinander verschiedene Primzahlen p, q. „Groß" heißt hier: mehrere hundert Stellen.

*(2) E berechnet den **RSA-Modul** $n = pq$.*

(3) E berechnet $\varphi(n) \overset{3.9}{=} (p-1)(q-1)$.

(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 Euklid'schen Algorithmus 2.10 geschehen.

(6) E setzt

$$\textbf{\textit{öffentlicher Schlüssel}} := (n, e), \quad \textbf{\textit{privater Schlüssel}} := (n, d)$$

und gibt den öffentlichen Schlüssel bekannt. Der private Schlüssel verbleibt bei E.

Beispiel 4.26. *Zur Veranschaulichung der Schlüsselerzeugung betrachten wir ein Beispiel mit unpraktikabel kleinen $p = 17$ und $q = 19$. Es gilt*

$$n = 17 \cdot 19 = 323 \quad \textit{und} \quad \varphi(n) = (17-1) \cdot (19-1) = 16 \cdot 18 = 288.$$

Es ist

$$\mathrm{ggT}(95, 288) = 32 \cdot 288 - 97 \cdot 95 = 1,$$

so dass wir $e = 95$ wählen können. Insbesondere ist $191 \cdot 95 \equiv (-97) \cdot 95 \equiv 1 \bmod (288)$ und deshalb $d = 191$. Der öffentliche Schlüssel ist also durch $(323, 95)$, der private Schlüssel durch $(323, 191)$ gegeben.

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 Umwandlung von üblichen Nachrichten (etwa Text) in eine Folge von Elementen von $\mathbb{Z}/n\mathbb{Z}$ und zurück vornimmt, werden wir an dieser Stelle nicht behandeln. Es sollte jedoch klar sein, dass man auch hier geschickt vorgehen muss, damit das ganze Verfahren nicht angreifbar wird.

Algorithmus 4.27 (Verschlüsselung mit dem RSA-Verfahren)**.** *A möchte eine Nachricht verschlüsselt an E senden:*

(1) A besorgt sich den öffentlichen Schlüssel (n, e) von E.

(2) A formatiert die Nachricht als Folge von Elementen $\overline{x_1}, \ldots, \overline{x_r} \in \mathbb{Z}/n\mathbb{Z}$.

*(3) Mithilfe der **Verschlüsselungsfunktion***

$$V : \begin{cases} \mathbb{Z}/n\mathbb{Z} & \to \mathbb{Z}/n\mathbb{Z}, \\ \overline{x} & \mapsto \overline{x}^e \end{cases}$$

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 4.28 (Entschlüsselung mit dem RSA-Verfahren)**.** *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***

$$E : \begin{cases} \mathbb{Z}/n\mathbb{Z} & \to \mathbb{Z}/n\mathbb{Z}, \\ \overline{y} & \mapsto \overline{y}^d \end{cases}$$

entschlüsselt E die Nachricht als $E(\overline{y_1}), \ldots, E(\overline{y_r})$.

Wir müssen an dieser Stelle nachweisen, dass die Entschlüsselung tatsächlich funktioniert, dass also

$$E(V(\overline{x})) = \overline{x} \quad \text{für alle } \overline{x} \in \mathbb{Z}/n\mathbb{Z}$$

gilt. Dies folgt jedoch recht schnell aus der folgenen Überlegung:

Proposition 4.29. *Für ein quadratfreies $n \in \mathbb{N}$, $k \in \mathbb{N}$ und $a \in \mathbb{Z}$ gilt:*

$$a^{k\varphi(n)+1} \equiv a \bmod (n).$$

Beweis. Sei $n = p_1 \cdot \ldots \cdot p_r$ mit paarweise verschiedenen Primzahlen $p_1, \ldots, p_r$. Nach Satz 3.9 ist dann

$$\varphi(n) = (p_1 - 1) \cdot \ldots \cdot (p_r - 1).$$

Sei nun $i \in \{1, \ldots, r\}$ beliebig. Wir unterscheiden zwei Fälle:

Fall 1: $p_i \nmid a$**.** Nach dem Kleinen Satz von Fermat 4.11 gilt dann $a^{p_i - 1} \equiv 1 \bmod (p_i)$, also $a^{k\varphi(n)} \equiv 1 \bmod (p_i)$ und somit $a^{k\varphi(n)+1} \equiv a \bmod (p_i)$.

Fall 2: $p_i \mid a$**.** Hier ist offenbar $a^{k\varphi(n)+1} \equiv 0 \equiv a \bmod (p_i)$.

Insgesamt 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 gilt weiter $ed \equiv 1 \bmod (\varphi(n))$, so dass wegen $ed > 1$ ein $k \in \mathbb{N}$ mit $ed = k\varphi(n) + 1$ existiert. Es ergibt sich

$$E(V(\overline{x})) = \overline{x}^{ed} = \overline{x}^{k\varphi(n)+1} \overset{4.29}{=} \overline{x}$$

und es ist gezeigt, dass das RSA-Verfahren korrekt arbeitet.

Wieso sieht man das RSA-Verfahren als sicher an? „Naiv“ argumentiert man wie folgt: Zum 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 benötigt man 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 dieses naive Argument nicht wirklich tragfähig, denn es könnte ja andere Möglichkeiten geben, den privaten Schlüssel aus dem öffentlichen Schlüssel zu bestimmen, oder vielleicht kommt man auch ohne Kenntnis des privaten Schlüssels zum Ziel der Entschlüsselung.

Tatsächlich kann man zeigen, dass es „vergleichbar schwer“ ist, aus dem öffentlichen Schlüssel den privaten Schlüssel zu gewinnen wie ein Produkt zweier unbekannter Primzahlen in letztere zu zerlegen. Ob aber auch das Gewinnen der Ausgangsnachricht aus verschlüsselter Nachricht und öffentlichem Schlüssel ein „vergleichbar schweres“ Problem ist, ist derzeit nicht öffentlich bekannt. Da das Verfahren in der realen Welt auf real existierenden Computern durchgeführt wird, gibt es auch eine nicht unbeträchtliche Zahl von Angriffsmöglichkeiten auf das RSA-Verfahren.

KAPITEL 5

Darstellungen von Zahlen

5.1 Die g-adische Zahldarstellung

In diesem Abschnitt sei $g \geq 2$ stets eine feste natürliche Zahl und S_g das kleinste nichtnegative Restesystem $\{0, 1, \ldots, g-1\}$ modulo g.

Proposition 5.1. *Jedes $n \in \mathbb{N}$ hat eine eindeutige Darstellung der Form*

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

*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

$$\nu_i = \nu_{i+1} g + a_i \quad \text{und} \quad 0 \leq a_i < g \leq \nu_i \qquad \text{für alle } i \in \{0, \ldots, j-1\} \tag{5.1}$$

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 2.3 durch und erhalten (5.1) 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 (5.1) 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

$$\sum_{i=0}^{r} (a_i - \tilde{a}_i) g^i = 0 \tag{5.2}$$

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 (5.2), 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 5.2 (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

$$n = \sum_{i=0}^{r} a_i \big((g-1)+1\big)^i \equiv \sum_{i=0}^{r} a_i \qquad \mod (g-1),$$

$$n = \sum_{i=0}^{r} a_i g^i \equiv a_0 \qquad \mod (g),$$

$$n = \sum_{i=0}^{r} a_i \big((g+1)-1\big)^i \equiv \sum_{i=0}^{r} (-1)^i a_i \qquad \mod (g+1).$$

□

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.

Satz 5.3. *Jede reelle Zahl $0 < x \in \mathbb{R}$ hat eine eindeutige Darstellung der Form*

$$x = \sum_{i=-\infty}^{r} a_i g^i \quad \text{mit einem } r \in \mathbb{N}_0 \text{ und } a_i \in S_g \text{ für alle } i \in \{r, r-1, \ldots\},$$
$$a_i \neq g-1 \text{ für unendlich viele } i,$$
$$a_r = 0 \Longleftrightarrow 0 \leq x < 1.$$

*Diese heißt die g-**adische Entwicklung** von x und die a_i ihre **Ziffern**.*

Beweis. Ist $x \geq 1$, so besitzt $\lfloor x \rfloor \in \mathbb{N}$ nach Proposition 5.1 eine eindeutige g-adische Darstellung

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

Ohne Einschränkung können wir daher für den Rest des Beweises $0 \leq x < 1$ annehmen.

Zum Beweis der Existenz einer g-adischen Entwicklung setzen wir nun

$$x_1 := x, \quad a_i := \lfloor x_i g \rfloor \quad \text{und} \quad x_{i+1} := x_i g - \lfloor x_i g \rfloor \qquad \text{für alle } i \in \mathbb{N}.$$

Konstruktionsgemäß ist dann $0 \leq x_i < 1$ für alle $i \in \mathbb{N}$. Zudem gilt

$$x_j g = \lfloor x_j g \rfloor + x_{j+1} = a_j + x_{j+1}, \text{ also} \quad x_j = a_j g^{-1} + x_{j+1} g^{-1} \qquad \text{für alle } j \in \mathbb{N}$$

und somit rekursiv

$$x_j = \sum_{i=j}^{j+r-1} a_i^{j-1-i} g^{-r} + x_{j+r} g^{-1} \qquad \text{für alle } j \in \mathbb{N}, r \in \mathbb{N}_0.$$

Es gibt hierbei unendlich viele a_i ungleich $g-1$,

denn: Gäbe es nun ein $j \in \mathbb{N}$ mit $a_i = g-1$ für alle $i \geq j$, so erhielten wir für $r \to \infty$

$$x_j = (g-1) \sum_{r=1}^{\infty} g^{-r} = 1,$$

was wir bereits ausgeschlossen hatten. #

Eine g-adische Darstellung erhalten wir schließlich, indem wir in der obigen Formel $j = 1$ setzen und r gegen unendlich gehen lassen.

Zum Beweis der Eindeutigkeit seien nun

$$\sum_{i=-\infty}^{r} a_i g^i = x = \sum_{i=-\infty}^{r} \tilde{a}_i g^i \tag{5.3}$$

zwei g-adische Entwicklungen von x. Wir nehmen an, es gäbe Zahlen $i \in \mathbb{N}$ mit $a_i \neq \tilde{a}_i$ und wählen j als die kleinste dieser Zahlen. Mit dieser Wahl folgte

$$1 \leq |a_j - \tilde{a}_j| \overset{(5.3)}{=} |\sum_{i>j} (a_i - \tilde{a}_i) g^{j-i}| \leq \sum_{i>j} |a_i - \tilde{a}_i| g^{j-i} \leq (g-1) \sum_{r=1}^{\infty} g^{-r} = 1,$$

so dass an allen Stellen Gleichheit gälte. Insbesondere hätten alle Terme der Form $a_i - \tilde{a}_i$ mit $i > j$ dasselbe Vorzeichen und erfüllten $|a_i - \tilde{a}_i| = g - 1$. Wegen $a_i, \tilde{a}_i \in S_g$ wäre dies nur in einem von zwei Szenarien möglich: Entweder gälten

$$a_i = 0, \tilde{a}_i = g - 1 \qquad \text{für alle } i > j,$$

oder

$$a_i = g - 1, \tilde{a}_i = 0 \qquad \text{für alle } i > j.$$

In beiden Fällen gäbe es eine g-adische Entwicklung von x mit nur endlich vielen von $g - 1$ verschiedenen Ziffern, was nicht sein kann. Je zwei g-adischen Entwicklungen von x stimmen also überein. Es folgt die Eindeutigkeit. □

Definition 5.4. *Eine Folge $(a_i)_{i \in \mathbb{N}}$ in $\mathbb{Z}$ heißt **periodisch**, wenn es ein $p \in \mathbb{N}$ und ein $\ell \in \mathbb{N}_0$ mit*

$$a_{p+i} = a_i \quad \textit{für alle } \ell < i$$

*gibt. Das minimal mögliche p hierbei heißt die **Periodenlänge** der Folge. Hat die Folge Periodenlänge p, so heißt das minimale ℓ, das die obige Gleichung mit p erfüllt, die **Vorperiodenlänge** der Folge.*

Proposition 5.5. *Für eine reelle Zahl $x \in \mathbb{R}$ sind die folgenden beiden Aussagen äquivalent:*

(i) $x \in \mathbb{Q}$.

(ii) *Die Ziffernfolge der g-adischen Entwicklung von x ist periodisch.*

Beweis. Gelte zunächst Aussage (i) und seien $p \in \mathbb{Z}$ und $q \in \mathbb{N}$ mit $\mathrm{ggT}(p, q) = 1$ und $x = \frac{p}{q}$. Die Ziffern der g-adischen Entwicklung von x sind dann nach unseren Überlegungen im Beweis von Satz 5.3 durch

$$x_1 := \frac{p}{q} - \lfloor \frac{p}{q} \rfloor, \quad a_i := \lfloor x_i g \rfloor \quad \text{und} \quad x_{i+1} := x_i g - \lfloor x_i g \rfloor \qquad \text{für alle } i \in \mathbb{N}$$

rekursiv zu ermitteln. Setzen wir nun noch $b_i := x_i b$, so folgt aus dem Obigen leicht $b_i \in S_g$. Es gibt daher natürliche $1 \leq s < t$ mit $b_s = b_t$ und also auch $x_s = x_t$. Die Proposition folgt, da sich

hieraus mit der Rekursionsformel $x_{s+j} = x_{t+j}$ und somit auch $a_{s+j} = a_{t+j}$ für alle $j \in \mathbb{N}$ ergibt. Das ist Aussage (ii).

Gelte nun umgekehrt Aussage (ii) und sei die g-adische Entwicklung von x durch $x = \sum_{i=-\infty}^{r} a_i g^i$ mit $r \in \mathbb{N}_0$ gegeben. Dann gibt es $\ell, p \in \mathbb{N}$ mit

$$\begin{aligned} x - \lfloor x \rfloor &= \sum_{i=-\infty}^{-1} a_i g^i = \sum_{i=1}^{\ell} a_i g^{-i} + g^{-\ell} \cdot \Big(\sum_{j=0}^{\infty} g^{-jp}\Big) \cdot \Big(\sum_{k=1}^{p} a_{k+\ell} g^{-k}\Big) \\ &= \frac{1}{g^\ell (g^p - 1)} \cdot \Bigg((g^p - 1) \cdot \sum_{i=-\ell}^{-1} a_i g^{\ell - i} + \sum_{k=1}^{p} a_{k+\ell} g^{-k} \Bigg). \end{aligned}$$

Es folgt die Rationalität von $x - \lfloor x \rfloor$ und somit auch die von x selbst. □

Proposition 5.6. *Seien $p \in \mathbb{Z}$ und $q \in \mathbb{N}$ mit $\mathrm{ggT}(p,q) = 1$. Wir schreiben $q = de$, wobei d der größte positive, zu g teilerfremde Teiler von q sei. Nach Proposition 5.5 ist dann die Ziffernfolge der g-adischen Entwicklung der rationalen Zahl $\frac{p}{q}$ periodisch. Es gilt nun:*

(a) *Die Periodenlänge p ist* $\min\{i \in \mathbb{N} \mid g^i \equiv 1 \bmod (d)\}$.

(b) *Die Vorperiodenlänge ℓ ist* $\min\{\nu \in \mathbb{N}_0 \mid e \mid g^\nu\}$.

Insbeondere bricht die g-adische Entwicklung genau dann nach endlich vielen Ziffern ab, wenn $d = 1$ gilt, d. h. wenn jeder Primfaktor von q in g aufgeht.

Beweis. Nach den Überlegungen im Beweis von Proposition 5.5 gibt es $A, B \in \mathbb{Z}$ mit

$$\frac{p}{q} = \lfloor \frac{p}{q} \rfloor + \frac{A}{g^\ell (g^p - 1)} = \frac{B}{g^\ell (g^p - 1)}.$$

Wegen $\mathrm{ggT}(p,q) = 1$ folgt $q \mid g^\ell (g^p - 1)$ und daraus nach Konstruktion $d \mid (g^p - 1)$ sowie $e \mid g^\ell$. Mit

$$\tilde{p} := \min\{i \in \mathbb{N} \mid g^i \equiv 1 \bmod (d)\} \quad \text{und} \quad \tilde{\ell} := \min\{\nu \in \mathbb{N}_0 \mid e \mid g^\nu\}$$

folgen hieraus sofort

$$\tilde{\ell} \le \ell \quad \text{und} \quad \tilde{p} \le p.$$

Nach Konstruktion gilt andererseits $d \mid (g^{\tilde{p}} - 1)$ sowie $e \mid g^{\tilde{\ell}}$ und also $q \mid g^{\tilde{\ell}} (g^{\tilde{p}} - 1)$. Es folgt

$$(\frac{p}{q} - \lfloor \frac{p}{q} \rfloor) \cdot g^{\tilde{\ell}} (g^{\tilde{p}} - 1) \in \mathbb{N}_0$$

und nach dem Satz von der Division mit Rest 2.3 gibt es $u, v \in \mathbb{Z}$ mit

$$(\frac{p}{q} - \lfloor \frac{p}{q} \rfloor) \cdot g^{\tilde{\ell}} (g^{\tilde{p}} - 1) = u(g^{\tilde{p}} - 1) + v \quad \text{mit } 0 \le v < g^{\tilde{p}} - 1 \text{ sowie } 0 \le u < g^{\tilde{\ell}}.$$

Nach Proposition 5.1 besitzen u, v eindeutige g-adische Darstellungen

$$u = u_{\tilde{\ell}} + u_{\tilde{\ell}-1}g + \ldots + u_1 g^{\tilde{\ell}-1} \quad \text{und} \quad v = v_{\tilde{p}} + v_{\tilde{p}-1}g + \ldots + v_1 g^{\tilde{p}-1},$$

wobei wegen $v < g^{\tilde{p}} - 1$ nicht alle v_i gleich $g-1$ sind. Insgesamt erhalten wir

$$(\frac{p}{q} - \lfloor \frac{p}{q} \rfloor) = ug^{-\tilde{\ell}} + v(1-g^{-\tilde{p}})^{-1} g^{-\tilde{\ell}-\tilde{p}} = \sum_{i=1}^{\tilde{\ell}} u_i g^{-i} + g^{-\tilde{\ell}} \cdot (\sum_{j=1}^{\tilde{p}} v_j g^{-j}) \cdot (\sum_{k=0}^{\infty} g^{-k\tilde{p}})$$

und also

$$(\frac{p}{q} - \lfloor \frac{p}{q} \rfloor) = \sum_{i=1}^{\infty} d_i g^i \quad \text{mit } d_i := u_i \text{ für } 1 \le i \le \tilde{\ell} \text{ und } d_{\tilde{\ell}+j\tilde{p}+k} = v_k \text{ für } j \in \mathbb{N}_0, 1 \le k \le \tilde{p}.$$

Folglich sind alle d_i aus S_g und es gilt $d_i \neq g-1$ für unendlich viele i, weil nicht alle v_k gleich $g-1$ sind. Durch

$$\lfloor \frac{p}{q} \rfloor + \sum_{i=1}^{\infty} d_i g^i$$

ist daher die g-adische Entwicklung von $\frac{p}{q}$ gegeben, deren Periodenlänge p bzw. Vorperiodenlänge ℓ nach Konstruktion höchstens $\tilde{p}$ bzw. $\tilde{\ell}$ ist. Es folgen

$$\ell \le \tilde{\ell} \quad \text{und} \quad p \le \tilde{p}.$$

□

Bemerkung 5.7. *Die Periodenlänge ist laut der Formel in Proposition 5.6 gerade die Ordnung der Restklasse von g modulo d in der Einheitengruppe $(\mathbb{Z}/d\mathbb{Z})^\times$ und nach dem Satz von Euler-Fermat 4.9 höchstens $\varphi(d)$.*

Betrachten wir ein Beispiel: $g = 10$, $q = 7$. Dann ist $\mathrm{ggT}(q, g) = 1$ und also $d = q$. Die Restklasse von 10 modulo 7 ist ein Erzeuger von $(\mathbb{Z}/7\mathbb{Z})^\times$, die Periodenlänge von (gekürzten) Brüchen mit Nenner 7 in der Dezimaldarstellung ist also $\varphi(7) = 6$.

5.2 Kettenbrüche

Definition 5.8. *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 5.9. *Für endliche Kettenbrüche formulieren auch induktiv: Es ist* $[a_0] := a_0$ *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 5.10. (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.*

Kettenbruchentwicklungen können in der Zahlentheorie beispielsweise dazu benutzt werden, um die Einheitengruppen der Ganzzahlringe quadratischer Zahlkörper zu beschreiben. Das ist von Vorteil, da sich mit Kettenbrüchen besonders effizient umgehen lässt.

Das Ziel an dieser Stelle ist nun zu zeigen, dass jede reelle Zahl eine eindeutig bestimmte Kettenbruchentwicklung hat. Hierzu betrachten wir den folgenden Algorithmus:

Algorithmus 5.11 (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 $((a_0,\dots,a_m),x)$ die Kettenbruchentwicklung von x. Falls die Schleife nicht terminiert, so ist $((a_n)_{n\in\mathbb{N}_0},x)$ die Kettenbruchentwicklung von x.

Es gilt nun zu zeigen, dass der Kettenbruchalgorithmus ein korrektes Ergebnis liefert, genauer:

Satz 5.12. *Sei $x \in \mathbb{R}$. Dann gilt:*

(a) *Die Zahl x besitzt eine eindeutig bestimmte Kettenbruchentwicklung. Diese wird durch den Kettenbruchalgorithmus 5.11 geliefert.*

(b) *Die Kettenbruchentwicklung von x ist genau dann endlich, wenn x rational ist.*

*Ist die Kettenbruchentwicklung von x durch $((a_0,\dots,a_m),x)$ bzw. $((a_n)_{n\in\mathbb{N}_0},x)$ gegeben, dann heißen rationalen Zahlen $[a_0,\dots,a_n]$ mit $n \in \mathbb{N}_0$ – und $n \le m$ für $x \in \mathbb{Q}$ – die **Näherungsbrüche** von x.*

Beispiel 5.13. (a) *Mit den Bezeichnungen aus dem Kettenbruchalgorithmus 5.11 stellt sich die Rechnung in Beispiel 5.10 (a) wie folgt dar:*

$$\begin{aligned} a_0 &= 2, & t_0 &= \tfrac{11}{27}, & \xi_0 &= \tfrac{27}{11}, \\ a_1 &= 2, & t_1 &= \tfrac{5}{11}, & \xi_1 &= \tfrac{11}{5}, \\ a_2 &= 2, & t_2 &= \tfrac{1}{5}, & \xi_2 &= 5, \\ a_3 &= 5, & t_3 &= 0. \end{aligned}$$

(b) *Kettenbruchentwicklungen liefern gute Approximationen reeller Zahlen durch rationale Zahlen mit kleinstmöglichen Nennern: Christiaan Huygens baute 1682 ein Zahnradmodell des Planetensystems. Das Verhältnis der Umlaufzeiten von Saturn und Erde ist in guter Näherung*

$$x = \frac{77.708.431}{2.640.858}.$$

Dieses Verhältnis soll durch Zahnräder mit möglichst wenig Zähnen möglichst exakt realisiert werden. Der naive Ansatz bestünde in der Rundung anhand der Dezimaldarstellung dieser Zahlen:

$$x \approx \frac{77.700.000}{2.600.000} = \frac{777}{26}.$$

Allerdings beträgt der Fehler hier bereits ca. 1,6% und man benötigt ein Zahnrad mit 777 Zähnen. Der Kettenbruchalgorithmus liefert

$$x = [29,2,2,1,5,1,4,1,1,2,1,6,1,10,2,2,3].$$

Der vierte Näherungsbruch ist $[29,2,2,1] = \frac{206}{7}$. Der Fehler liegt hier nur bei ca. 0,01% und man benötigt höchstens 206 Zähne in einem Zahnrad. Genau ein solches baute Huygens.

Ein kompletter Beweis von Satz 5.12 liegt absolut in Reichweite, sprengt aber den Rahmen dieser Vorlesung. Wir betrachten im Folgenden nur den Fall rationaler Zahlen:

Lemma 5.14. *Für ein beliebiges $x \in \mathbb{R}$ sind die folgenden beiden Aussagen äquivalent:*

(i) *Der Kettenbruchalgorithmus 5.11 terminiert bei Eingabe von x nach endlich vielen Schritten.*

(ii) $x \in \mathbb{Q}$.

Insbesondere gibt Algorithmus 5.11 für rationale Eingaben endliche Kettenbruchentwicklungen aus.

Beweis. Nehmen wir zunächst (i) an, der Kettenbruchalgorithmus 5.11 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 5.11 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 Euklid'schen Algorithmus 2.10 aus:

$$\begin{array}{lllll}
r_0 & = a_0' r_1 + r_2 & \text{mit } a_0' \in \mathbb{Z} & \text{und } 0 < r_2 < r_1, \\
r_1 & = a_1' r_2 + r_3 & \text{mit } a_1' \in \mathbb{N} & \text{und } 0 < r_3 < r_2, \\
 & \vdots & & \\
r_i & = a_i' r_{i+1} + r_{i+2} & \text{mit } a_i' \in \mathbb{N} & \text{und } 0 < r_{i+2} < r_{i+1}, \\
 & \vdots & & \\
r_{m-1} & = a_{m-1}' r_m + r_{m+1} & \text{mit } a_{m-1}' \in \mathbb{N} & \text{und } 0 < r_{m+1} < r_m, \\
r_m & = a_m' r_{m+1} & \text{mit } a_m' \in \mathbb{N}. &
\end{array}$$

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

$$\frac{1}{t_{i-1}'} = a_i' + t_i' \qquad \text{für } i \in \{0, \ldots, m\},$$

wobei $t_i' \in (0,1)$ für $i = 0, \ldots, m-1$ ist. Wir vergleichen dies mit den Formeln aus dem Kettenbruchalgorithmus 5.11: 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 5.15. *Der Beweis hat gezeigt, dass man den Kettenbruchalgorithmus 5.11 für rationale Zahlen als Variante des Euklid'schen Algorithmus 2.10 ansehen kann. In Beispiel 5.10 (a) erhalten wir:*

$$\begin{aligned}
65 &= 2 \cdot 27 + 11 && \Longrightarrow \quad \frac{65}{27} = 2 + \frac{11}{27} \\
27 &= 2 \cdot 11 + 5 && \Longrightarrow \quad \frac{27}{11} = 2 + \frac{5}{11} \\
11 &= 2 \cdot 5 + 1 && \Longrightarrow \quad \frac{11}{5} = 2 + \frac{1}{5} \\
5 &= 5 \cdot 1 + 0 && \Longrightarrow \quad \frac{5}{1} = 5 + 0.
\end{aligned}$$

Als Kettenbruchentwicklung von $\frac{65}{27}$ ergibt sich wie gehabt $((2, 2, 2, 5), \frac{65}{27})$.

KAPITEL 6

Diophantische Gleichungen

6.1 Pythagoräische Tripel und der Große Satz von Fermat

Definition 6.1. *Eine **diophantische Gleichung** ist eine Gleichung der Form*

$$F(X_1, \ldots, X_n) = 0 \quad \text{mit } F \in \mathbb{Z}[X_1, \ldots, X_n] \text{ für ein } n \in \mathbb{N}. \tag{6.1}$$

*Eine **Lösung** der diophantischen Gleichung (6.1) 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 (6.1) 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

$$X_1^2 + X_2^2 - X_3^2 = 0. \tag{6.2}$$

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 (6.2) 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 6.1 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 (6.2) 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 (6.2) also $a_3^2 \equiv 2 \bmod (4)$, was nicht sein kann. #

Der folgende Satz war bereits Euklid bekannt:

Satz 6.2. *Für ein beliebiges primitives pythagoräisches Tripel (a_1, a_2, a_3) mit geradem a_2 gibt es teilerfremde natürliche Zahlen $a, b \in \mathbb{N}$ mit*

$$a_1 = a^2 - b^2, \quad a_2 = 2ab, \quad a_3 = a^2 + b^2,$$

für die die Differenz $a - b$ positiv und ungerade ist.

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 vorausgesetzen 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 (6.2) 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 (6.2) den Zusammenhang

$$(a_2')^2 = \frac{a_2^2}{4} = \frac{a_3^2 - a_1^2}{4} = \frac{a_3 - a_1}{2} \cdot \frac{a_3 + a_1}{2} = a_1' \cdot a_3'. \tag{6.3}$$

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 (6.3) die kanonische Primfaktorzerlegung 2.23 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

$$a_2^2 = 4(a_2')^2 \overset{(6.3)}{=} 4a_1'a_3' = (2ab)^2 \quad \text{und also} \quad a_2 = 2ab.$$

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 6.3 (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.

In den folgenden Jahrhunderten konnte der Große Satz von Fermat 6.3 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 2.22 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 6.3 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.

Wir lösen in dieser Vorlesung keine weiteren diophantischen Gleichungen und befassen uns stattdessen mit elementaren Lösbarkeitskriterien. Mit ein wenig Algebra erhalten wir:

Proposition 6.4 (Lösbarkeitskriterium für diophantische Gleichungen)**.** *Ist $P = (a_1, \dots, a_n)$ eine Lösung einer diophantischen Gleichung*

$$F(X_1, \dots, X_n) = 0 \quad \textit{mit } n \in \mathbb{N} \textit{ und } F \in \mathbb{Z}[X_1, \dots, X_n],$$

so ist für jedes $m \in \mathbb{N}$ durch $(a_1 + m\mathbb{Z}, \dots, a_n + m\mathbb{Z})$ eine Lösung der Gleichung $F(X_1, \dots, X_n)$ 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

$$0 = F(a_1, \dots, a_n) + m\mathbb{Z} = F(a_1 + m\mathbb{Z}, \dots, a_n + m\mathbb{Z}).$$

□

Beispiel 6.5. *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 6.4 hat somit auch die ursprüngliche, diophantische Gleichung keine Lösung. #

6.2 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 6.6 (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 Euklid'schen Algorithmus 2.10 (c) gibt es ganze Zahlen u_1 und v mit

$$\operatorname{ggT}(c_1, \ldots, c_n) \overset{2.16}{=} \operatorname{ggT}(c_1, \operatorname{ggT}(c_2, \ldots, c_n)) = u_1c_1 + v \operatorname{ggT}(c_2, \ldots, c_n).$$

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 6.7. *Das Lösbarkeitskriterium 6.6 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 $\mathrm{ggT}(80, 95, 155, 270) = 5 \mid 700$. *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 6.8 (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 Euklid'schen Algorithmus 2.10 ganze Zahlen $u, v \in \mathbb{Z}$ mit $\mathrm{ggT}(a_{11}, a) = ua_{11} + va$. Im Fall $a = a_{1j}$ mit einem $j \in \{1, \ldots, n\}$ 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

$$1.\ \text{Spalte} \mapsto u \cdot (1.\ \text{Spalte}) + v \cdot (j.\ \text{Spalte}),$$

$$j.\,\text{Spalte} \;\mapsto\; -\frac{a_{1j}}{\operatorname{ggT}(a_{11},a_{1j})}\cdot(1.\,\text{Spalte}) + \frac{a_{11}}{\operatorname{ggT}(a_{11},a_{1j})}\cdot(j.\,\text{Spalte}).$$

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 6.9 (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 6.8:*

$$\begin{aligned} &\textit{Das System } A\begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix} = b \textit{ linearer diophantischer Gleichungen hat eine Lösung} \\ \iff\quad & e_i \mid (Mb)_i \textit{ für alle } i \in \{1,\dots,n\} \textit{ und } (Mb)_i = 0 \textit{ für alle } i > n. \end{aligned}$$

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 6.8 ist letzeres Gleichungssystem von der Form

$$\begin{aligned} e_1X_1 &= (Mb)_1, \\ &\vdots \\ e_nX_n &= (Mb)_n, \\ 0 &= (Mb)_{n+1}, \\ &\vdots \\ 0 &= (Mb)_m. \end{aligned}$$

□

Beispiel 6.10. *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 6.8 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 6.9 ist das gegebene System linearer diophantischer Gleichungen also lösbar. #

Tatsächlich ist

$$\begin{pmatrix} -2 \\ 2 \end{pmatrix} \in \mathbb{Z}^2$$

eine Lösung.