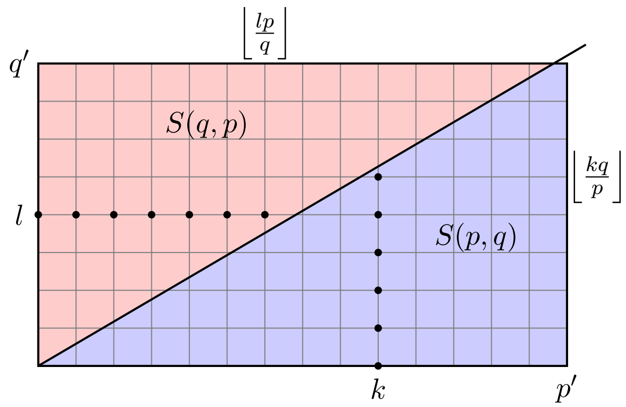
Elementare Zahlentheorie

Benjamin Sambale
Leibniz Universität Hannover

Version: 29. September 2024



Inhaltsverzeichnis

Vorwort

Die Zahlentheorie ist neben der Geometrie eines der ältesten Teilgebiete der reinen Mathematik. Im Zentrum der Untersuchung stehen die natürlichen Zahlen $1, 2, \ldots$ und deren arithmetische Eigenschaften. Im Gegensatz zur anderen mathematisch Gebieten, lassen sich in der Zahlentheorie scheinbar einfache Probleme angeben, die seit Jahrhunderten im Zentraum der Forschung stehen. Dies betrifft besonders die Verteilung der Primzahlen. Erwähnt seien die *Goldbach-Vermutung* (jede gerade Zahl größer als 2 ist die Summe von zwei Primzahlen), die *Primzahlzwillingsvermutung* (es gibt unendlich viele Paare von Primzahlen (p, q) mit $q = p + 2$) oder das Millennium-Problem, die *Riemannsche Vermutung* (die nicht-trivialen Nullstellen der ζ-Funktion haben Realteil $1/2$). In dieser Vorlesung werden wir die aus meiner Sicht schönsten Kapitel der Zahlentheorie behandeln. An vielen Stellen gebe ich Anwendungsbeispiele. Es werden Vorkenntnisse der linearen Algebra und Analysis 1 vorausgesetzt. Kenntnisse der Algebra 1 sind hilfreich, aber nicht zwingend erforderlich.

Literatur:

- Bundschuh, *Einführung in die Zahlentheorie*, 6. Auflage, Springer, 2008
- Scheid, *Zahlentheorie*, 3. Auflage, 2003
- Leutbecher, *Zahlentheorie*, Springer, 1996
- Schmidt, *Einführung in die algebraische Zahlentheorie*, Springer, 2007

1 Teilbarkeit

Bemerkung 1.1. Wir benutzen die üblichen Zahlbereiche:

- Natürliche Zahlen: $\mathbb{N} = \{1, 2, \ldots\}$, $\mathbb{N}_0 = \{0, 1, \ldots\}$.
- Ganze Zahlen: $\mathbb{Z} = \{\ldots, -1, 0, 1, \ldots\}$.
- Rationale Zahlen: $\mathbb{Q} = \{\frac{a}{b} : a, b \in \mathbb{Z},\ b \neq 0\}$.
- Reelle Zahlen: $\mathbb{R}$ (Analysis).
- Komplexe Zahlen: $\mathbb{C} = \{a + b\mathrm{i} : a, b \in \mathbb{R}\}$.

Satz 1.2 (Division mit Rest)**.** *Für $a \in \mathbb{Z}$ und $d \in \mathbb{N}$ existieren eindeutig bestimmte $q, r \in \mathbb{Z}$ mit $a = qd + r$ und $0 \leq r < d$.*

Beweis. Offenbar ist die Menge $M := \{a - cd : c \in \mathbb{Z} \text{ mit } a - cd \geq 0\} \subseteq \mathbb{N}_0$ nicht leer und besitzt daher ein minimales Element $r := a - qd \geq 0$ mit $q \in \mathbb{Z}$. Im Fall $r \geq d$ wäre auch $a - (q+1)d = r - d \in M$ im Widerspruch zur Minimalität von r. Also ist $0 \leq r < d$. Seien nun $q', r' \in \mathbb{Z}$ mit $a = q'd + r'$ und $0 \leq r' < d$. Aus $d|q - q'| = |dq - dq'| = |r' - r| < d$ folgt dann $q = q'$ und $r = r'$. □

Bemerkung 1.3. Man nennt r in Satz 1.2 den *Rest* bei der Division von a durch d.

Beispiel 1.4. Die Division 20 durch 7 lässt Rest 6, denn $20 = 2 \cdot 7 + 6$.

Satz 1.5 (b-adische Entwicklung)**.** *Sei $b \in \mathbb{N}$ mit $b \geq 2$. Für jedes $n \in \mathbb{N}$ existieren eindeutig bestimmte Zahlen $k \in \mathbb{N}$ und $0 \leq n_0, n_1, \ldots, n_k \leq b - 1$ mit*

$$n = n_k b^k + n_{k-1} b^{k-1} + \ldots + n_1 b + n_0 =: [n_k, \ldots, n_0]_b.$$

und $n_k > 0$.

Beweis. Induktion nach n: Für $n = 1$ muss offenbar $k = 0$ und $b_0 = 1$ gelten. Sei nun $n \geq 2$. Division mit Rest durch b liefert $n = qb + r$ mit $q, r \in \mathbb{Z}$ und $0 \leq r < b$. Im Fall $q < 0$ wäre $n \leq -b + r < 0$. Also ist $0 \leq q < n$. Nach Induktion existieren $0 \leq q_0, q_1, \ldots, q_l \leq b - 1$ mit $q = q_0 + \ldots + q_l b^l$ (im Fall $q = 0$ sei $l = 0 = q_0$). Wir können nun $k := l + 1$, $n_0 := r$ und $n_i := q_{i-1}$ für $i = 1, \ldots, k$ definieren. Dann gilt $n = qb + r = n_k b^k + \ldots + n_1 b + n_0$.

Angenommen es gilt auch $n = n'_{k'} b^{k'} + \ldots + n'_0$ mit $0 \leq n'_0, n'_1, \ldots, n'_{k'} \leq b - 1$ und $n_{k'} > 0$. Dann ist $n_0 = n'_0$ der eindeutig bestimmte Rest bei der Division von n durch b. Daraus erhält man

$$n_k b^{k-1} + \ldots + n_2 b + n_1 = \frac{n - n_0}{b} = n'_{k'} b^{k'} + \ldots + n'_2 b + n_1 < n.$$

Nach Induktion gilt $k = k'$ und $n_i = n'_i$ für $i = 1, \ldots, k$. □

Beispiel 1.6.

(i) Die 10-adische Entwicklung ist genau die gewohnte Dezimalzahlschreibweise. Die 3-adische Entwicklung von 100 lautet: $100 = 81 + 18 + 1 = 3^4 + 2 \cdot 3^2 + 3^0 = [1, 0, 2, 0, 1]_3$.

(ii) Wir werden später (positive) reelle Zahlen in eine unendliche p-adische Reihe entwickeln (siehe Satz 5.2).

(iii) Auf Computern rechnet man im *Binärsystem* also mit 2-adischen Entwicklungen.

(iv) (Nim-Spiel) Euler und Gauß spielen folgendes Spiel: Gegeben sind n Stapel mit jeweils m_i Münzen für $i = 1, \ldots, n$. Die Spieler nehmen abwechselnd in jedem Zug eine beliebige positive Anzahl von Münzen von einem der Stapel (es ist auch erlaubt den gesamten Stapel zu nehmen). Wer die letzte Münze nimmt, gewinnt. Kann Euler als beginnender Spieler einen Sieg erzwingen? Im Fall $m_1 = \ldots = m_n = 1$ gewinnt Euler offenbar genau dann, wenn n ungerade ist. Für $n = 2$ und $(m_1, m_2) = (3, 2)$ kann Euler wie folgt gewinnen:

$$\begin{tikzcd}
 & & (2,0) \arrow[r, "E"] & (0,0) & & \\
(3,2) \arrow[r, "E"] & (2,2) \arrow[ur, "G"] \arrow[dr, "G"'] & & & & \\
 & & (2,1) \arrow[r, "E"'] & (1,1) \arrow[r, "G"'] & (1,0) \arrow[r, "E"'] & (0,0)
\end{tikzcd}$$

Sei $m_i = \sum_{j \geq 0} m_{ij} 2^j$ die 2-adische Entwicklung und $\alpha_j := \sum_{i=1}^{n} m_{ij}$ für $j \geq 0$ (für genügend große j gilt $\alpha_j = 0$). Wir behaupten:

Euler kann genau dann den Sieg erzwingen, wenn ein α_j ungerade ist.

Beweis. Seien $j_1 < j_2 < \ldots < j_k$ die Indizes, für die α_j ungerade ist. Dann existiert ein i mit $m_{ij_k} = 1$. Euler nimmt genau

$$2^{j_k} + \sum_{l=2}^{k-1} (-1)^{m_{ij_l}} 2^{j_l} > 0$$

Münzen vom Stapel i. Dadurch ändert sich jedes der α_{j_l} um ± 1. Nach Eulers Zug sind also alle α_j gerade. Beispiel:

$$\begin{array}{lll}
m_1 = 12 & = [0,1,1,0,0]_2 & & [0,1,1,0,0]_2 \\
m_2 = 17 & = [1,0,0,0,1]_2 & \xrightarrow{-(2^4-2^2)} & [0,0,1,0,1]_2 = 5 \\
m_3 = 9 & = [0,1,0,0,1]_2 & & [0,1,0,0,1]_2 \\
\hline
[\alpha_5, \ldots, \alpha_0] & = [1,2,1,0,2] & & [0,2,2,0,2]
\end{array}$$

Da Gauß nur einen Stapel verändern kann und muss, wird nach seinem Zug wieder ein α_j ungerade sein. Nach endlich vielen Zügen erreichen wir die Situation mit nur noch einem Stapel, sagen wir $m_1 > 0$. Offenbar ist dann ein $\alpha_j = m_{ij} = 1$, d. h. Euler ist am Zug und siegt, indem er den gesamten Stapel nimmt.

Nehmen wir nun an, dass zu Beginn alle α_j gerade sind. Wie eben gesehen, wird durch Eulers Zug mindestens ein α_j ungerade. Nun kann aber Gauß den Sieg erzwingen.[1] □

Definition 1.7. Für $a, b \in \mathbb{Z}$ sagt man a *teilt* b (oder a ist ein *Teiler* von b oder b ist durch a *teilbar*), falls ein $c \in \mathbb{Z}$ mit $ac = b$ existiert. Man schreibt dann $a \mid b$.

Lemma 1.8. *Für $a, b, c, d, e \in \mathbb{Z}$ gilt*

(i) $\pm 1 \mid a \mid 0$,

[1] Da mit Wahrscheinlichkeit $\frac{2^n-1}{2^n}$ mindestens ein α_j ungerade ist, genügt es gegen unerfahrene Spieler zunächst zufällig zu spielen, bis eine bekannte Situation auftritt (vgl. Aufgabe 2).

(ii) $0 \mid a \iff a = 0$,

(iii) $a \mid b \mid c \implies a \mid c$,

(iv) $a \mid b \mid a \implies a = \pm b$,

(v) $a \mid b, c \implies a \mid (bd + ce)$,

(vi) $a \mid b \neq 0 \implies |a| \leq |b|$.

Beweis. Alle Aussagen sind leicht. Wir beweisen als Muster (iv). Wegen $a \mid b \mid a$ existieren $c, d \in \mathbb{Z}$ mit $ac = b$ und $bd = a$. Also ist $a = bd = cda$. Im Fall $a = 0$ ist auch $b = ac = 0$. Anderenfalls ist $cd = 1$ und $c = \pm 1$. Dann ist $a = \pm b$. □

Definition 1.9. Für $a_1, \ldots, a_n \in \mathbb{Z}$ sei

$$\mathrm{gT}(a_1, \ldots, a_n) := \{d \in \mathbb{Z} : d \mid a_1, \ldots, a_n\}$$

die Menge der *gemeinsamen Teiler* von $a_1, \ldots, a_n$. Ein $g \in \mathrm{gT}(a_1, \ldots, a_n)$ heißt *größter gemeinsamer Teiler* von $a_1, \ldots, a_n$, falls $g \geq 0$ und $d \mid g$ für alle $d \in \mathrm{gT}(a_1, \ldots, a_n)$ gilt. Man schreibt dann $\mathrm{ggT}(a_1, \ldots, a_n) := g$. Im Fall $\mathrm{ggT}(a_1, \ldots, a_n) = 1$ nennt man $a_1, \ldots, a_n$ *teilerfremd*.

Bemerkung 1.10.

(i) Sind g und g' größte gemeinsame Teiler von $a_1, \ldots, a_n$, so gilt $g \mid g' \mid g$ und $g = \pm g'$ nach Lemma 1.8(iv). Wegen $g, g' \geq 0$ ist also $g = g'$, d. h. es existiert höchstens ein gemeinsamer Teiler von $a_1, \ldots, a_n$ (dies rechtfertigt die Schreibweise ggT).

(ii) Die Bezeichnung „größter gemeinsamer Teiler“ ist irreführend, denn $\mathrm{gT}(0, 0) = \mathbb{Z}$, aber $\mathrm{ggT}(0, 0) = 0$.

(iii) Für die Berechnung von $\mathrm{ggT}(a_1, \ldots, a_n)$ kann man offenbar $a_1 > \ldots > a_n > 0$ annehmen. Für $d \in \mathrm{gT}(a_1, \ldots, a_n)$ gilt $d \mid a_1$ und $d \mid \mathrm{ggT}(a_2, \ldots, a_n)$. Also ist $\mathrm{gT}(a_1, \ldots, a_n) \subseteq \mathrm{gT}(a_1, \mathrm{ggT}(a_2, \ldots, a_n))$. Für $d \in \mathrm{gT}(a_1, \mathrm{ggT}(a_2, \ldots, a_n))$ gilt umgekehrt $d \mid \mathrm{ggT}(a_2, \ldots, a_n) \mid a_i$ für $i = 2, \ldots, n$, also $d \in \mathrm{gT}(a_1, \ldots, a_n)$. Dies zeigt

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

Es genügt also den ggT von zwei natürlichen Zahlen berechnen zu können.

(iv) Sei $a > b > 0$. Division mit Rest liefert $a = bq + r$ mit $q, r \in \mathbb{Z}$ und $0 \leq r < b$. Nach Lemma 1.8(v) ist $\mathrm{gT}(a, b) = \mathrm{gT}(bq + r, b) = \mathrm{gT}(r, b)$ und daher $\mathrm{ggT}(a, b) = \mathrm{ggT}(r, b)$. Im Fall $r > 0$ kann man b mit Rest durch r teilen und erhält dadurch immer kleinere Zahlen. Man Ende ist $\mathrm{ggT}(a, b) = \mathrm{ggT}(r, b) = \ldots = \mathrm{ggT}(d, 0) = d$. Insbesondere existiert der ggT immer. Der folgende Satz gibt genauere Auskunft.

Satz 1.11 (Erweiterter euklidischer Algorithmus)**.**
Eingabe: $a, b \in \mathbb{N}$.
Initialisierung: $(x_0, y_0, z_0) := (1, 0, a)$, $(x_1, y_1, z_1) := (0, 1, b)$ *und* $k := 0$.
Solange $z_{k+1} > 0$ *wiederhole:*

Division mit Rest: $z_k = q_{k+1} z_{k+1} + r_{k+1}$ *mit* $0 \leq r_{k+1} < z_{k+1}$.

Setze $(x_{k+2}, y_{k+2}, z_{k+2}) := (x_k - x_{k+1} q_{k+1}, y_k - y_{k+1} q_{k+1}, r_{k+1})$ *und* $k := k + 1$.

Ausgabe: $z_k = x_k a + y_k b = \mathrm{ggT}(a, b)$.

Beweis. Wegen $z_1 > r_1 = z_2 > r_2 = z_3 > \ldots$ terminiert der Algorithmus. Am Ende gilt

$$\begin{aligned} z_k &= \operatorname{ggT}(z_k, 0) = \operatorname{ggT}(z_k, z_{k+1}) = \operatorname{ggT}(z_k, r_k) = \operatorname{ggT}(z_k, z_{k-1} - q_k z_k) \\ &= \operatorname{ggT}(z_k, z_{k-1}) = \ldots = \operatorname{ggT}(z_0, z_1) = \operatorname{ggT}(a, b). \end{aligned}$$

Für $i = 0, 1$ gilt $x_i a + y_i b = z_i$. Induktiv folgt

$$\begin{aligned} x_{i+1}a + y_{i+1}b &= (x_{i-1} - x_i q_i)a + (y_{i-1} - y_i q_i)b = x_{i-1}a + y_{i-1}b - (x_i a + y_i b)q_i \\ &= z_{i-1} - z_i q_i = r_i = z_{i+1}. \end{aligned}$$

Daher ist $\operatorname{ggT}(a, b) = z_k = x_k a + y_k b$. □

Beispiel 1.12. Für $a := 45$ und $b := 24$ erhält man:

x_i	y_i	z_i	q_i
1	0	45	
0	1	24	1
1	-1	21	1
-1	2	$\boxed{3}$	7
		0	

Also ist $\operatorname{ggT}(45, 24) = 3 = -45 + 2 \cdot 24$.

Folgerung 1.13. *Für $a_1, \ldots, a_n, b \in \mathbb{Z}$ gilt*

$$\operatorname{ggT}(a_1, \ldots, a_n) \mid b \iff \exists b_1, \ldots, b_n \in \mathbb{Z} : a_1 b_1 + \ldots + a_n b_n = b.$$

Beweis. Sei $g := \operatorname{ggT}(a_1, \ldots, a_n)$.

$\Rightarrow$: Sei $gd = b$. Nach Bemerkung 1.10(iii) und Satz 1.11 existieren $c_1, \ldots, c_n \in \mathbb{Z}$ mit $g = a_1 c_1 + \ldots + a_n c_n$. Die Behauptung folgt mit $b_i := dc_i$ für $i = 1, \ldots, n$.

$\Leftarrow$: Wegen $g \mid a_i$ für $i = 1, \ldots, n$ gilt $g \mid a_1 b_1 + \ldots + a_n b_n = b$. □

Definition 1.14. Man nennt $v \in \mathbb{Z}$ ein *gemeinsames Vielfaches* von $a_1, \ldots, a_n \in \mathbb{Z}$, falls $a_i \mid v$ für $i = 1, \ldots, n$ gilt. Ein gemeinsames Vielfaches $v \in \mathbb{N}_0$ heißt *kleinstes gemeinsames Vielfache*, falls v jedes gemeinsame Vielfache von $a_1, \ldots, a_n$ teilt. Man schreibt dann $\operatorname{kgV}(a_1, \ldots, a_n) := v$.

Bemerkung 1.15. Wie beim ggT zeigt man, dass höchstens ein kgV existiert. Außerdem ist

$$\operatorname{kgV}(a_1, \ldots, a_n) = \operatorname{kgV}(a_1, \operatorname{kgV}(a_2, \ldots, a_n)).$$

Wir berechnen das kgV über einen Umweg.

2 Primzahlen

Definition 2.1. Man nennt $p \in \mathbb{N}$ *Primzahl*, falls p genau zwei positive Teiler hat, nämlich 1 und p. Die Menge der Primzahlen bezeichnen wir mit $\mathbb{P}$. Man nennt $p \in \mathbb{P}$ *Primteiler* von $a \in \mathbb{Z}$, falls $p \mid a$.

Bemerkung 2.2.

(i) Beachte: 1 ist *keine* Primzahl!

(ii) Zwei verschiedene Primzahlen sind stets teilerfremd.

Lemma 2.3.

(i) Für $a, b \in \mathbb{Z}$ und $p \in \mathbb{P}$ gilt $p \mid ab \Longrightarrow p \mid a \vee p \mid b$.

(ii) Jedes $a \in \mathbb{N} \setminus \{1\}$ besitzt einen Primteiler.

Beweis.

(i) Sei $p \mid ab$ und $p \nmid a$. Nach dem euklidischen Algorithmus existieren $c, d \in \mathbb{Z}$ mit $1 = \mathrm{ggT}(a, p) = ac + pd$. Es folgt $p \mid abc + pbd = b1 = b$.

(ii) Sei $p > 1$ ein möglichst kleiner Teiler von a (notfalls $p = a$). Im Fall $p \notin \mathbb{P}$ existiert $1 < q < p$ mit $q \mid p \mid a$ im Widerspruch zur Wahl von p. Also ist $p \in \mathbb{P}$. □

Satz 2.4 (Euklid)**.** *Es gibt unendlich viele Primzahlen.*

Beweis (Hermite). Annahme: p ist die größte Primzahl. Für einen Primteiler q von $n = p! + 1$ gilt $q \leq p$ und man erhält den Widerspruch $q \mid (n - p!) = 1$. □

Bemerkung 2.5 (Sieb des Eratosthenes)**.** Ist $n \geq 2$ keine Primzahl, so existiert stets ein Primteiler $p \leq \sqrt{n}$ (falls $p > \sqrt{n}$ wähle man stattdessen einen Primteiler von $n/p < \sqrt{n}$). Mit dieser Überlegung kann man leicht eine Tabelle aller „kleinen“ Primzahlen aufstellen:

(1) Erstelle eine Liste der Zahlen von 2 bis n.

(2) Sei $p \leq \sqrt{n}$ die kleinste Zahl in der Liste, die noch nicht gestrichen ist (zu Beginn $p = 2$).

(3) Man streiche alle Vielfachen pq mit $q \geq p$ aus der Liste (zu Beginn $4, 6, 8, \ldots$).

(4) Man wiederhole Schritt 2 und 3 bis kein geeignetes p mehr existiert.

Die nicht gestrichenen Zahlen der Liste sind genau die Primzahlen zwischen 1 und n. Für $n = 100$ erhält man folgende Liste:

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

Satz 2.6 (Eindeutige Primfaktorzerlegung). *Für jedes $n \in \mathbb{N}$ existieren eindeutig bestimmte $a_p \in \mathbb{N}_0$ für $p \in \mathbb{P}$ mit*

$$n = \prod_{p \in \mathbb{P}} p^{a_p}.$$

Beweis. Induktion nach n: Im Fall $n = 1$ ist $a_p = 0$ für alle $p \in \mathbb{P}$. Sei nun $n \geq 2$ und p ein Primteiler von n. Nach Induktion besitzt n/p eine Primfaktorzerlegung und daher auch $n = p \cdot n/p$. Sei $n = \prod p^{a_p} = \prod p^{b_p}$ und $a_q < b_q$ für ein $q \in \mathbb{P}$. Dann ist

$$q \mid \frac{n}{q^{a_q}} = \prod_{p \neq q} p^{a_p}$$

und Lemma 2.3(i) zeigt $q = p$ für ein $p \in \mathbb{P} \setminus \{q\}$. Widerspruch. $\square$

Beispiel 2.7. Sei $k \geq 2$ und $n \in \mathbb{N}$ nicht die k-te Potenz einer natürlichen Zahl. Dann ist $\sqrt[k]{n}$ irrational, denn anderenfalls existieren teilerfremde $a, b \in \mathbb{N}$ mit $\sqrt[k]{n} = a/b$. Dann ist $nb^k = a^k$. Die eindeutige Primfaktorzerlegung zeigt $b^k = 1$ und man erhält den Widerspruch $n = a^k$. Insbesondere ist $\sqrt{2}$ irrational.

Bemerkung 2.8.

(i) Die Teiler von $n = \prod_{p \in \mathbb{P}} p^{a_p}$ haben die Form $n = \prod_{p \in \mathbb{P}} p^{a'_p}$ mit $0 \leq a'_p \leq a_p$ für alle $p \in \mathbb{P}$. Für $m = \prod_{p \in \mathbb{P}} p^{b_p}$ gilt daher

$$\boxed{\operatorname{ggT}(n, m) = \prod_{p \in \mathbb{P}} p^{\min\{a_p, b_p\}}, \quad \operatorname{kgV}(n, m) = \prod_{p \in \mathbb{P}} p^{\max\{a_p, b_p\}}.}$$

Dies zeigt

$$\boxed{nm = \operatorname{ggT}(n,m)\operatorname{kgV}(n,m),}$$

denn $a_p + b_p = \min\{a_p, b_p\} + \max\{a_p, b_p\}$. Da man keinen schnellen Algorithmus zur Primfaktorzerlegung kennt, ist der euklidische Algorithmus zur Berechnung von ggT und kgV in der Regel zu bevorzugen.

(ii) Für $x \in \mathbb{Q} \setminus \{0\}$ existieren eindeutig bestimmte $x_p \in \mathbb{Z}$ mit $x = \pm \prod_{p\in\mathbb{P}} p^{x_p}$.

(iii) Satz 2.6 erlaubt folgende Verallgemeinerung von Lemma 2.3(i): Sind $a, b \in \mathbb{Z}$ teilerfremd und $a \mid bc$, so folgt $a \mid c$.

(iv) Euklids Satz lässt sich in vielerlei Hinsicht verallgemeinern. Der folgende Satz ist ein Spezialfall von Dirichlets Primzahlsatz (siehe Satz 9.26).

Satz 2.9. *Es gibt unendlich viele Primzahlen der Form $p = 4k - 1$ mit $k \in \mathbb{N}$.*

Beweis. Angenommen es gibt nur endlich viele solchen Primzahlen, sagen wir $p_1, \ldots, p_n$. Dann haben alle Primteiler von $q := 4p_1 \ldots p_n - 1$ die Form $4k + 1$. Ein Produkt aus solchen Zahlen muss aber ebenfalls die Form $4k + 1$ haben. Widerspruch. □

Satz 2.10 (Euler)**.** *Es gilt $\sum_{p\in\mathbb{P}} \frac{1}{p} = \infty$.*

Beweis (Erdős)*.* Angenommen die Reihe konvergiert. Dann existiert ein $N \geq 2$ mit

$$\sum_{\substack{p\in\mathbb{P}\\ p>N}} \frac{1}{p} < \frac{1}{2}.$$

Sei n_1 die Anzahl aller Zahlen $n \leq 2^{4N}$, die einen Primteiler $p > N$ besitzen. Es gibt höchstens $2^{4N}/p$ solcher Zahlen, die durch ein festes p teilbar sind. Dies zeigt

$$n_1 \leq 2^{4N} \sum_{\substack{p\in\mathbb{P}\\ p>N}} \frac{1}{p} < 2^{4N-1}.$$

Also gibt es mindestens $2^{4N} - n_1 \geq 2^{4N-1}$ Zahlen $n \leq 2^{4N}$, die nur durch Primzahlen $p \leq N$ teilbar sind. Jede solche Zahl hat die Form $n = ab^2$ mit $\operatorname{ggT}(a,b) = 1$, wobei a ein Produkt von paarweise verschiedenen Primzahlen ist. Da es höchstens N Primzahlen $p \leq N$ gibt, hat man höchstens 2^N Möglichkeiten für a. Andererseits ist $b \leq \sqrt{n} \leq 2^{2N}$. Folglich gibt es für n höchstens $2^N 2^{2N} = 2^{3N} < 2^{4N-1}$ Möglichkeiten. Widerspruch. □

Lemma 2.11. *Sei $n \in \mathbb{N}$. Dann gilt*

(i) Ist $2^n - 1$ eine Primzahl, so ist n eine Primzahl.

(ii) Ist $2^n + 1$ eine Primzahl, so ist n eine 2-Potenz.

Beweis.

(i) Offenbar gilt $n \geq 2$. Sei p ein Primteiler von n und $m := 2^{n/p}$. Nach der geometrischen Reihe gilt

$$2^n - 1 = m^p - 1 = (m-1)(m^{p-1} + m^{p-2} + \ldots + 1).$$

Da $2^n - 1$ eine Primzahl ist, folgt $m = 2$ und $n = p \in \mathbb{P}$.

(ii) Besitzt n einen ungeraden Teiler $q > 1$, so ist

$$2^n + 1 = (2^{n/q} + 1) \sum_{i=0}^{q-1} (-2^{n/q})^i$$

keine Primzahl. $\square$

Definition 2.12. Man nennt $M_n := 2^n - 1$ die n-te MERSENNE-*Zahl* und $F_n := 2^{2^n} + 1$ die n-te FERMAT-*Zahl*.

Bemerkung 2.13.

(i) Die ersten Mersenne-*Prim*zahlen sind

$$M_2 = 3, \quad M_3 = 7, \quad M_5 = 31, \quad M_7 = 127, \quad M_{13} = 8191, \quad M_{17} = 131071, \quad M_{19} = 524287.$$

Dagegen ist $M_{11} = 2047 = 23 \cdot 89$ keine Primzahl. Man kennt bislang 51 Mersenne-Primzahlen, wobei $M_{82.589.933}$ mit 24.862.048 Dezimalstellen derzeit die größte bekannte Primzahl überhaupt ist.[2] Die Mersenne-Primzahl M_{19937} wird für den Zufallsgenerator *Mersenne-Twister* benutzt.

(ii) Die einzig bekannten Fermat-*Prim*zahlen sind $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ und $F_4 = 65537$. Es gilt

$$\begin{aligned}
&641 = 5^4 + 2^4 \mid 2^{28}(5^4 + 2^4) = 5^4 \cdot 2^{28} + 2^{32}, \\
&641 = 5 \cdot 2^7 + 1 \mid (5 \cdot 2^7 + 1)(5 \cdot 2^7 - 1)(5^2 \cdot 2^{14} + 1) = 5^4 \cdot 2^{28} - 1, \\
&641 \;\big|\; (5^4 \cdot 2^{28} + 2^{32}) - (5^4 \cdot 2^{28} - 1) = 2^{32} + 1 = F_5 \notin \mathbb{P}.
\end{aligned}$$

Allgemeiner weiß man $F_n \notin \mathbb{P}$ für $n = 5, \ldots, 32$.[3] Wir lernen in Kapitel 8 effiziente Primzahltests für Mersenne- und Fermat-Zahlen kennen.

Definition 2.14. Eine Zahl $n \in \mathbb{N}$ heißt *vollkommen*, wenn sie die Summe ihrer echten positiven Teiler ist, d. h. $\sigma(n) := \sum_{d|n} d = 2n$ (im Folgenden wird stets nur über die positiven Teiler summiert).

Satz 2.15 (EULER). *Eine gerade Zahl n ist genau dann vollkommen, wenn $n = 2^{p-1} M_p$ für eine Mersenne-Primzahl M_p gilt.*

Beweis. Ist $M_p \in \mathbb{P}$, so hat jeder Teiler von $n = 2^{p-1} M_p$ die Form $2^i M_p^j$ mit $0 \le i \le p-1$ und $j \in \{0, 1\}$. Dies zeigt

$$\sum_{d|n} d = (M_p + 1) \sum_{i=0}^{p-1} 2^i = 2^p (2^p - 1) = 2n.$$

Sei nun umgekehrt $n = 2^a m$ vollkommen mit $a \ge 0$ und $2 \nmid m$. Wegen $\mathrm{ggT}(2^a, m) = 1$ gilt

$$2^{a+1} m = 2n = \sum_{d|n} d = \Big(\sum_{i=0}^{a} 2^i \Big) \Big(\sum_{d|m} d \Big) = (2^{a+1} - 1) \sigma(m).$$

[2] Siehe `https://en.wikipedia.org/wiki/Largest_known_prime_number`

[3] Siehe `http://www.fermatsearch.org`

Es folgt

$$\frac{2^{a+1}}{2^{a+1}-1} = \frac{\sigma(m)}{m}.$$

Da der Bruch auf der linken Seite vollständig gekürzt ist (Zähler und Nenner sind teilerfremd), muss der Bruch auf der rechten Seite eine Erweiterung sein. Also existiert $b \in \mathbb{N}$ mit $m = (2^{a+1}-1)b$ und $\sigma(m) = 2^{a+1}b$. Im Fall $b > 1$ wäre

$$\sigma(m) \geq 1 + b + m = 2^{a+1}b + 1 > \sigma(m).$$

Daher gilt $m = 2^{a+1} - 1$ und $\sigma(m) = 2^{a+1}$. Wäre m keine Primzahl, so wäre $\sigma(m) > 1 + m = 2^{a+1}$. Daher ist $m = M_{a+1}$ eine Mersenne-Primzahl und $n = 2^a M_{a+1}$ wie gewünscht. □

Beispiel 2.16. Die kleinsten vollkommenen Zahlen sind $6 = 1 + 2 + 3 = 2^{2-1}M_2$ und $28 = 1 + 2 + 4 + 7 + 14 = 2^{3-1}M_3$. Man kennt bislang keine ungerade vollkommene Zahl.

Satz 2.17. *Die Abstände zwischen zwei aufeinanderfolgenden Primzahlen können beliebig groß werden.*

Beweis. Für $2 \leq k \leq n$ ist $n! + k$ durch k teilbar und somit keine Primzahl. Dies liefert $n - 1$ aufeinanderfolgende zusammengesetzte Zahlen. [4] □

Definition 2.18. Für $x \in \mathbb{R}$ sei $\pi(x) := |\{p \in \mathbb{P} : p \leq x\}|$.

Lemma 2.19. *Für $2 \leq x \in \mathbb{R}$ gilt $\prod_{p \leq x} p \leq 4^{x-1}$, wobei das Produkt über die Primzahlen $p \leq x$ läuft.*

Beweis. O. B. d. A. sei $x \in \mathbb{P}$. Für $x = 2$ ist die Behauptung trivial. Sei also $x = 2m + 1$ und die Behauptung für kleinere Werte bereits bewiesen. Dann gilt $\prod_{p \leq m+1} p \leq 4^m$ und

$$\prod_{m+1<p\leq 2m+1} p \leq \frac{(2m+1)!}{m!(m+1)!} = \binom{x}{m} = \frac{1}{2}\left(\binom{x}{m} + \binom{x}{m+1}\right) \leq \frac{1}{2}(1+1)^x = 2^{2m} = 4^m.$$

Insgesamt folgt

$$\prod_{p \leq x} p = \prod_{p \leq m+1} p \prod_{m+1<p\leq 2m+1} p \leq 4^m 4^m = 4^{x-1}.$$ □

Lemma 2.20. *Für $n \in \mathbb{N}$ gilt $\binom{2n}{n} \geq \frac{4^n}{2n}$.*

Beweis. Für $0 \leq k \leq n - 1$ gilt

$$\binom{2n}{k} < \frac{n+1}{n}\binom{2n}{k} \leq \frac{2n-k}{k+1}\binom{2n}{k} = \binom{2n}{k+1} < \ldots < \binom{2n}{n}$$

und $\binom{2n}{k} = \binom{2n}{2n-k}$ (vgl. Pascalsches Dreieck). Es folgt

$$4^n = (1+1)^{2n} = \sum_{k=0}^{2n} \binom{2n}{k} = 2 + \sum_{k=1}^{2n-1} \binom{2n}{k} \leq 2n\binom{2n}{n}.$$ □

[4] Ist $n + 1$ keine Primzahl, so kann auch $n! + n + 1$ keine Primzahl sein. Ist andererseits $n + 1 \in \mathbb{P}$, so ist $n + 1 \mid n! + 1$ nach Aufgabe 22. Für $n \geq 3$ erhält man in beiden Fällen sogar n aufeinanderfolgende zusammengesetzte Zahlen.

Lemma 2.21 (Legendre)**.** *Für $n \in \mathbb{N}$ gilt*

$$n! = \prod_{p \in \mathbb{P}} p^{\lfloor \frac{n}{p} \rfloor + \lfloor \frac{n}{p^2} \rfloor + \ldots},$$

wobei $\lfloor \alpha \rfloor := \max\{z \in \mathbb{Z} : z \le \alpha\}$ für $\alpha \in \mathbb{R}$.

Beweis. Von den Zahlen $1, 2, \ldots, n$ sind genau $\lfloor \frac{n}{p} \rfloor$ durch p teilbar, $\lfloor \frac{n}{p^2} \rfloor$ durch p^2 teilbar usw. □

Lemma 2.22. *Sei $n \ge 3$ und $p \le n$ ein Primteiler von $\binom{2n}{n}$. Dann gilt $p \le \frac{2}{3}n$. Ist p^2 ein Teiler von $\binom{2n}{n}$, so gilt $p \le \sqrt{2n}$.*

Beweis. Nach Legendre tritt p mit Vielfachheit

$$m := \sum_{k=1}^{\infty} \Big(\Big\lfloor \frac{2n}{p^k} \Big\rfloor - 2 \Big\lfloor \frac{n}{p^k} \Big\rfloor \Big)$$

in der Primfaktorzerlegung von $\binom{2n}{n} = \frac{(2n)!}{(n!)^2}$ auf. Dabei gilt

$$\Big\lfloor \frac{2n}{p^k} \Big\rfloor - 2 \Big\lfloor \frac{n}{p^k} \Big\rfloor < \frac{2n}{p^k} - 2 \Big(\frac{n}{p^k} - 1 \Big) \le 2$$

und $m \le \max\{k \in \mathbb{N}_0 : p^k \le 2n\}$. Dies zeigt $p^m \le 2n$. Insbesondere ist $p \le \sqrt{2n}$, falls $m \ge 2$. Im Fall $3p > 2n \ge 6$ gilt $p \ge 3$ und $p^2 > 2n$. Daher tritt p je zweimal im Zähler und Nenner von $\binom{2n}{n} = \frac{(2n)!}{(n!)^2}$ auf. Folglich ist $m = 0$. □

Satz 2.23 (Bertrands Postulat)**.** *Für alle $n \in \mathbb{N}$ existiert eine Primzahl p mit $n < p \le 2n$.*

Beweis (Erdős). Man überprüft leicht, dass

$$p_1, \ldots, p_{11} = 2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 521$$

Primzahlen sind, wobei $p_{i+1} < 2p_i$ für $i = 1, \ldots, 10$ gilt. Für $p_i \le n < p_{i+1}$ ist $p_{i+1} < 2p_i \le 2n$. Daher dürfen wir $n \ge 521$ annehmen.

Sei $\rho(n) := \pi(2n) - \pi(n)$ für $n \in \mathbb{N}$. Dann gilt

$$\begin{aligned}
\frac{4^n}{2n} &\overset{2.20}{\le} \binom{2n}{n} \overset{2.22}{\le} \prod_{p \le \sqrt{2n}} 2n \prod_{\sqrt{2n} < p \le \frac{2}{3}n} p \prod_{n < p \le 2n} p \overset{2.19}{\le} (2n)^{\sqrt{2n}} \cdot 4^{2n/3} \cdot (2n)^{\rho(n)} \\
4^{n/3} &< (2n)^{\sqrt{2n} + 1 + \rho(n)} \\
\rho(n) &> \frac{2n}{3 \log_2(2n)} - (\sqrt{2n} + 1).
\end{aligned}$$

Zum Nachweis von $\rho(n) > 0$ genügt es

$$3 \log_2(2n) < \frac{2n - 1}{\sqrt{2n} + 1} = \sqrt{2n} - 1$$

zu zeigen. Für $n = 2^9 = 512$ erhält man $30 < 31$. Für $x > 38 > 18\log_2(e)^2$ gilt

$$(3\log_2(2x))' = (3\log_2(e)\ln(2x))' = \frac{3\log_2(e)}{x} < \frac{1}{\sqrt{2x}} = (\sqrt{2x}-1)',$$

d. h. die Funktion $3\log_2(2x)$ wächst schneller als $\sqrt{2x}-1$. Da wir bereits $n \geq 521$ angenommen haben, gilt die Behauptung. □

Bemerkung 2.24. Man weiß bisher nicht, ob für $n \geq 2$ stets eine Primzahl zwischen n^2 und $(n+1)^2$ liegt.

Satz 2.25 (TSCHEBYSCHOW[5])**.** *Es gibt Konstanten $\alpha, \beta > 0$, sodass*

$$\alpha\frac{x}{\log x} \leq \pi(x) \leq \beta\frac{x}{\log x}$$

für $x \geq 2$ gilt.

Beweis. Wegen $\pi(x) \geq \pi(2) = 1$ können wir annehmen, dass x „groß genug" ist. Die Basis des Logarithmus spielt außerdem keine Rolle. Wie bisher sei stets $p \in \mathbb{P}$. Aus Lemma 2.19 folgt

$$\sqrt{x}^{\pi(x)-\pi(\sqrt{x})} \leq \prod_{\sqrt{x}<p\leq x} p \leq 4^x.$$

Logarithmieren ergibt

$$\pi(x) \leq \frac{4x}{\log_2 x} + \pi(\sqrt{x}) \leq \frac{4x}{\log_2 x} + \sqrt{x} \leq \frac{5x}{\log_2 x}$$

für x genügend groß.

Sei nun $n \in \mathbb{N}$ minimal mit $x \leq 2n$. Sei $\binom{2n}{n} = p_1^{a_1} \ldots p_s^{a_s}$ die Primfaktorzerlegung. Im Beweis von Lemma 2.22 haben wir $p_i^{a_i} \leq 2n$ für $i = 1, \ldots, s$ gezeigt. Dies impliziert $\binom{2n}{n} \leq (2n)^s$ und

$$\pi(x) \geq \pi(2n) - 1 \geq s - 1 \geq \frac{\log_2\binom{2n}{n}}{\log_2(2n)} - 1 \overset{2.20}{\geq} \frac{2n - \log_2(2n)}{\log_2(2n)} - 1 = \frac{2n}{\log_2(2n)} - 2.$$

Da die Funktion $\frac{x}{\log_2(x)}$ für $x > e$ monoton wächst, gilt $\pi(x) \geq \frac{x}{2\log_2 x}$ für große x. □

Bemerkung 2.26. Asymptotisch gilt der *Gaußsche Primzahlsatz*:[6]

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

d. h. $\pi(x)$ wächst ungefähr so schnell wie $\frac{x}{\ln x}$ (ohne Beweis). Im Gegensatz zu Satz 2.25 kann man hier den natürlichen Logarithmus $\ln x$ nicht durch den Logarithmus bzgl. einer anderen Basis ersetzen. Es gibt also eine Verbindung zwischen den Primzahlen und der eulerschen Zahl e.

[5] Laut Wikipedia sind die gebräuchlichen Transkriptionen Tschebyschef, Tschebyscheff, Tschebyschew oder Tschebyschev inkorrekt.

[6] bewiesen von HADAMARD und VALLÉE POUSSIN

3 Modulo-Arithmetik

Definition 3.1. Für $a, b \in \mathbb{Z}$ und $d \in \mathbb{N}$ schreiben wir $a \equiv b \pmod{d}$, falls $d \mid (a-b)$. Man sagt dann: a und b sind *kongruent modulo* d.

Beispiel 3.2.

(i) Im Dezimalsystem rechnet man modulo 10 und im Binärsystem modulo 2.

(ii) Man betrachtet Sekunden und Minuten modulo 60 und Stunden modulo 12 oder 24.

(iii) Wochentage zählt man modulo 7.

(iv) Eurocent rechnet man modulo 100.

(v) In der Musik betrachtet man Töne modulo 8 (*c, d, e, f, g, a, h*) oder 12 (*c, cis, d, …, h*).

Satz 3.3. *Die Kongruenz modulo $d \in \mathbb{N}$ ist eine Äquivalenzrelation auf $\mathbb{Z}$, d. h. es gilt*

(i) $a \equiv a \pmod{d}$ (*reflexiv*),

(ii) $a \equiv b \pmod{d} \Longrightarrow b \equiv a \pmod{d}$ (*symmetrisch*),

(iii) $a \equiv b \equiv c \pmod{d} \Longrightarrow a \equiv c \pmod{d}$ (*transitiv*).

Außerdem gilt

(iv)

$$\left.\begin{aligned} a &\equiv a' \pmod{d} \\ b &\equiv b' \pmod{d} \end{aligned}\right\} \Longrightarrow a \mathbin{\substack{+\\ \cdot}} b \equiv a' \mathbin{\substack{+\\ \cdot}} b' \pmod{d}.$$

Beweis.

(i) $d \mid 0 = a - a$.

(ii) $d \mid a - b \Longrightarrow d \mid -(a-b) = b - a$.

(iii) $d \mid a - b \wedge d \mid b - c \Longrightarrow d \mid (a-b) + (b-c) = a - c$.

(iv) Sei $d \mid a - a'$ und $d \mid b - b'$. Dann folgt $d \mid (a-a') + (b-b') = (a+b) - (a'+b')$ sowie $d \mid (a-a')b + (b-b')a' = ab - a'b'$. □

Bemerkung 3.4. Die Äquivalenzklassen in der Situation von Satz 3.3 heißen *Restklassen* modulo d. Sie haben die Form $a + d\mathbb{Z} := \{a + db : b \in \mathbb{Z}\}$ für $a \in \mathbb{Z}$ (alle Elemente in $a + d\mathbb{Z}$ lassen den gleichen Rest bei der Division durch d). Die Menge aller Restklassen modulo d bezeichnen wir mit $\mathbb{Z}/d\mathbb{Z}$. Offenbar ist

$$\mathbb{Z}/d\mathbb{Z} = \{0 + d\mathbb{Z} = d\mathbb{Z},\ 1 + d\mathbb{Z}, \ldots, d - 1 + d\mathbb{Z}\}$$

und $|\mathbb{Z}/d\mathbb{Z}| = d$.

Beispiel 3.5.

(i) Gleichung (iv) vereinfacht viele Rechnungen. Wir prüfen, ob $7^{90} + 111^7$ durch 5 teilbar ist:

$$7^{90} + 111^7 \equiv 2^{90} + 1^7 \equiv 4^{45} + 1 \equiv (-1)^{45} + 1 \equiv 0 \pmod{5}.$$

In Folgerung 4.8 zeigen wir, dass man auch die Exponenten reduzieren darf, allerdings modulo 4.

(ii) (*Freshman's Dream*) Sei $p \in \mathbb{P}$ und $1 \leq k \leq p-1$. Dann ist p ein Teiler von $\binom{p}{k} = \frac{p(p-1)\ldots(p-k+1)}{k!}$. Der binomische Satz zeigt

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k} \equiv a^p + b^p \pmod{p}.$$

Lemma 3.6 (Kürzen von Kongruenzen)**.** *Für $a, b \in \mathbb{Z}$ und $d, e \in \mathbb{N}$ gilt*

$$\boxed{ae \equiv be \pmod{d} \iff a \equiv b \left(\operatorname{mod} \frac{d}{\operatorname{ggT}(d,e)}\right).}$$

Beweis. Sei $ae \equiv be \pmod{d}$ und $g := \operatorname{ggT}(d,e)$. Dann ist $d \mid (a-b)e$ und $\frac{d}{g} \mid (a-b)\frac{e}{g}$. Wegen $\operatorname{ggT}(\frac{d}{g}, \frac{e}{g}) = 1$ folgt $\frac{d}{g} \mid (a-b)$ (Bemerkung 2.8(iii)) und $a \equiv b \pmod{\frac{d}{g}}$. Ist umgekehrt $a \equiv b \pmod{\frac{d}{g}}$, so gilt $d \mid d\frac{e}{g} = \frac{d}{g}e \mid (a-b)e$, also $ae \equiv be \pmod{d}$. □

Beispiel 3.7. Eine ISBN zur Indizierung von Büchern besteht aus neun Ziffern $z_1, \ldots, z_9 \in \{0, \ldots, 9\}$ sowie einer Prüfziffer $s \in \{0, \ldots, 9, X\}$ mit

$$s \equiv \sum_{k=1}^{9} k z_k \pmod{11},$$

wobei 10 durch X ersetzt wird. Wegen

$$\begin{aligned} kz_k \equiv kz_k' \pmod{11} &\iff z_k \equiv z_k' \pmod{11}, \\ kz_k + lz_k \equiv kz_l + lz_k \pmod{11} &\iff (k-l)z_k \equiv (k-l)z_l \pmod{11} \iff z_k \equiv z_l \pmod{11} \end{aligned}$$

erkennt die Prüfziffer eine fehlerhafte Ziffer oder eine Vertauschung von zwei Ziffern (aber nicht beides gleichzeitig).

Satz 3.8 (Kongruenzgleichungen)**.** *Seien $a, b \in \mathbb{Z}$ und $d \in \mathbb{N}$. Genau dann existiert ein $x \in \mathbb{Z}$ mit $ax \equiv b \pmod{d}$, falls $\operatorname{ggT}(a,d) \mid b$. Gegebenenfalls bilden diese x eine Restklasse modulo $\frac{d}{\operatorname{ggT}(a,d)}$.*

Beweis. Erste Aussage:

$$\exists x \in \mathbb{Z} : ax \equiv b \pmod{d} \iff \exists x, c \in \mathbb{Z} : b = ax + cd \overset{1.13}{\iff} \operatorname{ggT}(a,d) \mid b.$$

Zweite Aussage:

$$ax \equiv ay \pmod{d} \overset{3.6}{\iff} x \equiv y \left(\operatorname{mod} \frac{d}{\operatorname{ggT}(a,d)}\right).$$ □

Bemerkung 3.9. Satz 3.8 besagt, dass die Gleichung $ax \equiv b \pmod{d}$ im Falle der Lösbarkeit zu einer Gleichung der Form $x \equiv c \pmod{d/\operatorname{ggT}(a,d)}$ äquivalent ist.

Beispiel 3.10. Wie wertvoll ist ein 124,76 g schwerer Haufen von 1- und 2-Centmünzen? Eine 1-Centmünze wiegt 2300 mg und eine 2-Centmünze 3060 mg. Ansatz: $2300x + 3060y = 124.760$. Wir teilen durch $\operatorname{ggT}(2300, 3060) = 20$ und erhalten $115x + 153y = 6238$. Modulo 115 ergibt sich

$$38y \equiv 28 \pmod{115}.$$

Nach dem euklidischen Algorithmus ist $1 = \mathrm{ggT}(38, 115) = -3\cdot 38+115 \equiv -3\cdot 38 \pmod{115}$. Einsetzen liefert $38y \equiv 28 \cdot (-3 \cdot 38) \pmod{115}$. Lemma 3.6 zeigt

$$y \equiv -3 \cdot 28 \equiv 31 \pmod{115}.$$

Für $y \geq 31 + 115$ wäre $3060y \geq 446.760 > 124.760$. Also ist $y = 31$ die einzige Lösung und $x = \frac{6238-153y}{115} = 13$ folgt.

Antwort: $13 + 2 \cdot 31 = 75$ Cent.

Satz 3.11 (Chinesischer Restsatz)**.** *Seien $a_1, \ldots, a_n \in \mathbb{Z}$ und $d_1, \ldots, d_n \in \mathbb{N}$ paarweise teilerfremd. Dann bilden die Lösungen $x \in \mathbb{Z}$ des Gleichungssystems $x \equiv a_i \pmod{d_i}$ für $i = 1, \ldots, n$ eine Restklasse modulo $d_1 \ldots d_n$. Insbesondere existiert genau eine Lösung $0 \leq x < d_1 \ldots d_n$.*

Beweis. Nach der Primfaktorzerlegung ist $D_i := \prod_{j \neq i} d_j$ teilerfremd zu d_i. Nach Satz 3.8 existiert ein $x_i \in \mathbb{Z}$ mit $x_i D_i \equiv a_i \pmod{d_i}$ für $i = 1, \ldots, n$. Für $x := x_1 D_1 + \ldots + x_n D_n$ gilt $x \equiv x_i D_i \equiv a_i \pmod{d_i}$ für $i = 1, \ldots, n$. Offenbar ist auch jedes Element der Restklasse $x + d_1 \ldots d_n \mathbb{Z}$ eine Lösung des Gleichungssystems. Sei umgekehrt auch $y \in \mathbb{Z}$ eine Lösung. Dann gilt $x - y \equiv a_i - a_i \equiv 0 \pmod{d_i}$ für $i = 1, \ldots, n$. Da $d_1, \ldots, d_n$ paarweise teilerfremd sind, folgt $d_1 \ldots d_n \mid x - y$, d. h. $y \in x + d_1 \ldots d_n \mathbb{Z}$. □

Bemerkung 3.12. Achtung: Teilerfremde Zahlen sind nicht unbedingt *paarweise* teilerfremd (betrachte $6, 10, 15$).

Beispiel 3.13.

(i) Betrachte das System

$$\begin{aligned} x &\equiv 3 \pmod{7}, \\ x &\equiv 4 \pmod{11}, \\ x &\equiv 5 \pmod{13}. \end{aligned}$$

Der Ansatz $x = 3 + 7a$ löst zunächst die erste Gleichung und liefert $7a \equiv 1 \pmod{11}$ in der zweiten Gleichung. Nach Satz 3.8 ist dies zu $a \equiv -3 \pmod{11}$ äquivalent (die Lösung -3 kann man leicht erraten). Wir setzen nun $a = -3 + 11b$ und erhalten $x = -18 + 77b$. Dies löst die ersten beiden Gleichungen. Die dritte Gleichung liefert $77b \equiv 23 \pmod{13}$, also $b \equiv 3 \pmod{13}$. Die allgemeine Lösung des Systems lautet daher $x = -18 + 77(3 + 13c) = 213 + 1001c$ mit $c \in \mathbb{Z}$.

(ii) Was sind die letzten beiden Dezimalziffern von 47^{88}? Wir suchen $0 \leq x \leq 99$ mit

$$x \equiv 47^{88} \pmod{100}.$$

Wegen $\mathrm{kgV}(4, 25) = 100$ ist diese Kongruenz nach Satz 3.11 äquivalent zum System

$$\begin{aligned} x &\equiv 47^{88} \pmod{4}, \\ x &\equiv 47^{88} \pmod{25}. \end{aligned}$$

Es gilt $47^{88} \equiv (-1)^{88} \equiv 1 \pmod{4}$ und

$$47^{88} \equiv (-3)^{3\cdot 29+1} \equiv (-2)^{29}(-3) \equiv (-2)^{7\cdot 4+1}(-3) \equiv (-3)^4 6 \equiv 11 \pmod{25}.$$

Der Ansatz $x = 1 + 4a$ löst die erste Gleichung und ergibt $4a \equiv 10 \pmod{25}$ in der zweiten Gleichung. Es folgt $2a \equiv 5 \pmod{25}$ und $a \equiv 13 \cdot 2a \equiv 13 \cdot 5 \equiv 15 \pmod{25}$. Also ist $x = 1 + 4 \cdot 15 = 61$.

Definition 3.14. Man nennt

$$\begin{aligned}\varphi\colon \mathbb{N} &\to \mathbb{N},\\ n &\mapsto |\{1 \le k \le n : \mathrm{ggT}(n,k) = 1\}|\end{aligned}$$

EULER*sche φ-Funktion.*

Bemerkung 3.15. Für $b \in a + n\mathbb{Z}$ gilt $\mathrm{ggT}(b,n) = \mathrm{ggT}(a,n)$. Da $a + n\mathbb{Z}$ genau einen Repräsentanten b mit $1 \le b \le n$ besitzt, gilt

$$\varphi(n) = |\{a + n\mathbb{Z} : \mathrm{ggT}(a,n) = 1\}|.$$

Satz 3.16. *Es gilt*

(i) $\varphi(nm) = \varphi(n)\varphi(m)$*, falls* $\mathrm{ggT}(n,m) = 1$.

(ii) $\varphi(p^n) = p^n - p^{n-1}$ *für jede Primzahlpotenz* $p^n \ne 1$.

Beweis.

(i) Seien $1 \le a \le n$ und $1 \le b \le m$ mit $\mathrm{ggT}(a,n) = 1 = \mathrm{ggT}(b,m)$. Nach dem chinesischen Restsatz existiert genau ein $1 \le c \le nm$ mit $c \equiv a \pmod{n}$ und $c \equiv b \pmod{m}$. Offenbar ist dann $\mathrm{ggT}(c,nm) = 1$. Ist umgekehrt $1 \le c \le nm$ mit $\mathrm{ggT}(c,nm) = 1$ gegeben, so gilt auch $\mathrm{ggT}(c,n) = 1 = \mathrm{ggT}(c,m)$. Daher sind die Mengen

$$\{1 \le a \le n : \mathrm{ggT}(a,n) = 1\} \times \{1 \le b \le m : \mathrm{ggT}(b,m) = 1\}$$

und $\{1 \le c \le nm : \mathrm{ggT}(c,nm) = 1\}$ gleichmächtig und die Behauptung folgt.

(ii) Es gilt $\mathrm{ggT}(p^n,k) = 1$ genau dann, wenn $p \nmid k$. Zwischen 1 und p^n liegen genau p^{n-1} Vielfache von p, nämlich $p, 2p, \ldots, p^{n-1}p$. Dies zeigt die Behauptung. □

Bemerkung 3.17. Sei $n = \prod_{p\in\mathbb{P}} p^{a_p} \in \mathbb{N}$. Nach Satz 3.16 ist dann

$$\boxed{\varphi(n) = \prod_{p\in\mathbb{P}} \varphi(p^{a_p}) = \prod_{\substack{p\in\mathbb{P}\\ a_p>0}} (p^{a_p} - p^{a_p-1}).}$$

Beispiel 3.18. Es gilt

$$\varphi(36) = \varphi(2^2 \cdot 3^2) = (2^2 - 2^1)(3^2 - 3^1) = 2 \cdot 6 = 12$$

und

$$\{1 \le a \le 36 : \mathrm{ggT}(a,36) = 1\} = \{1,5,7,11,13,17,19,23,25,29,31,35\}.$$

Definition 3.19. Man nennt

$$\begin{aligned}\mu\colon \mathbb{N} &\to \mathbb{N},\\ n &\mapsto \begin{cases}(-1)^s & \text{falls } n = p_1 \ldots p_s \text{ mit paarweise verschiedenen } p_1,\ldots,p_s \in \mathbb{P},\\ 0 & \text{sonst}\end{cases}\end{aligned}$$

MÖBIUS-*Funktion*. Dabei ist $\mu(1) = 1$ $(s = 0)$.

Bemerkung 3.20. Sind $p_1, \dots, p_s$ die verschiedenen Primteiler von $n > 1$, so gilt

$$\sum_{d|n} \mu(d) = \sum_{k=0}^{s} \sum_{q_1,\dots,q_k \in \{p_1,\dots,p_s\}} \mu(q_1 \dots q_k) = \sum_{k=0}^{s} \sum_{\substack{M \subseteq \{p_1,\dots,p_s\} \\ |M|=k}} (-1)^k = \sum_{k=0}^{s} (-1)^k \binom{s}{k} = (1-1)^s = 0.$$

Satz 3.21 (Möbius-Inversion)**.** *Für $f, F \colon \mathbb{N} \to \mathbb{C}$ sind äquivalent:*

(1) $F(n) = \sum_{d|n} f(d)$ *für alle* $n \in \mathbb{N}$.

(2) $f(n) = \sum_{d|n} \mu(d) F(\frac{n}{d}) = \sum_{d|n} \mu(\frac{n}{d}) F(d)$ *für alle* $n \in \mathbb{N}$.

Beweis.

(1) $\Rightarrow$ (2):

$$\sum_{d|n} \mu(d) F(n/d) \overset{(1)}{=} \sum_{d|n} \sum_{e|\frac{n}{d}} \mu(d) f(e) = \sum_{de|n} \mu(d) f(e) = \sum_{e|n} f(e) \sum_{d|\frac{n}{e}} \mu(d) \overset{3.20}{=} f(n).$$

(2) $\Rightarrow$ (1):

$$\sum_{d|n} f(d) \overset{(2)}{=} \sum_{d|n} \sum_{e|d} \mu(d/e) F(e) = \sum_{e|n} F(e) \sum_{d|\frac{n}{e}} \mu(d) \overset{3.20}{=} F(n).$$ □

Beispiel 3.22. Für $n = \prod_{p \in \mathbb{P}} p^{a_p} \in \mathbb{N}$ gilt

$$\sum_{d|n} \varphi(d) \overset{2.8}{=} \prod_{p \in \mathbb{P}} \sum_{k=0}^{a_p} \varphi(p^k) \overset{3.16}{=} \prod_{p \in \mathbb{P}} (1 + (p-1) + (p^2 - p) + \ldots + (p^{a_p} - p^{a_p - 1})) = \prod_{p \in \mathbb{P}} p^{a_p} = n.$$

Für $f = \varphi$ ist also $F = \mathrm{id}_{\mathbb{N}}$ in Satz 3.21 und man erhält

$$\varphi(n) = \sum_{d|n} \mu(d) \frac{n}{d}$$

für alle $n \in \mathbb{N}$.

4 Restklassenringe

Bemerkung 4.1. Wir wissen aus Satz 3.3 bereits, dass Kongruenzen addiert, subtrahiert und multipliziert werden können. In diesem Kapitel untersuchen wir das Zusammenspiel dieser Operationen auf der Menge der Restklassen $\mathbb{Z}/n\mathbb{Z}$.

Satz 4.2. *Sei $n \in \mathbb{N}$. Mit den Operationen*

$$(a + n\mathbb{Z}) \overset{+}{\cdot} (b + n\mathbb{Z}) := (a \overset{+}{\cdot} b) + n\mathbb{Z}$$

wird $\mathbb{Z}/n\mathbb{Z}$ ein kommutativer Ring*, d. h. es gelten folgende Axiome:*

(i) $(\mathbb{Z}/n\mathbb{Z}, +)$ *ist eine abelsche Gruppe mit neutralem Element* $0 + n\mathbb{Z} = n\mathbb{Z}$.

(ii) $(a + n\mathbb{Z}) \cdot ((b + n\mathbb{Z}) \cdot (c + n\mathbb{Z})) = ((a + n\mathbb{Z}) \cdot (b + n\mathbb{Z})) \cdot (c + n\mathbb{Z})$ *(Assoziativgesetz).*

(iii) $(a+n\mathbb{Z})\cdot(b+n\mathbb{Z}) = (b+n\mathbb{Z})\cdot(a+n\mathbb{Z})$ *(Kommutativgesetz).*

(iv) $(1+n\mathbb{Z})\cdot(a+n\mathbb{Z}) = a+n\mathbb{Z}$ *(neutrales Element bzgl. $\cdot$).*

(v) $(a+n\mathbb{Z})\cdot((b+n\mathbb{Z})+(c+n\mathbb{Z})) = ((a+n\mathbb{Z})\cdot(b+n\mathbb{Z}))+((a+n\mathbb{Z})\cdot(c+n\mathbb{Z}))$ *(Distributivgesetz).*

Beweis. Die Wohldefiniertheit der Addition und Multiplikation wurden in Satz 3.3 gezeigt. Die Axiome folgen sofort aus den entsprechenden Regeln in $\mathbb{Z}$ ($\mathbb{Z}$ ist kommutativer Ring). □

Bemerkung 4.3.

(i) Wie üblich lassen wir den Multiplikationspunkt beim Rechnen mit Restklassen oft weg und benutzen „Punktrechnung vor Strichrechnung". Falls Missverständnisse ausgeschlossen sind, schreiben wir 0 für $0+n\mathbb{Z}$ und 1 für $1+n\mathbb{Z}$. Im (uninteressanten) Spezialfall $n=1$ gilt $0=1$.

(ii) Im Gegensatz zu einem Körper ist in einem Ring nicht jedes von 0 verschiedene Element invertierbar bzgl. Multiplikation. Zum Beispiel existiert kein $a+4\mathbb{Z}$ mit $(2+4\mathbb{Z})(a+4\mathbb{Z}) = 1+4\mathbb{Z}$. Nach Satz 3.8 haben die invertierbaren Elemente in $\mathbb{Z}/n\mathbb{Z}$ die Form $a+n\mathbb{Z}$ mit $\operatorname{ggT}(a,n)=1$. Sie bilden bzgl. Multiplikation eine Gruppe der Ordnung $\varphi(n)$ (Bemerkung 3.15).

Definition 4.4. Für $n\in\mathbb{N}$ nennt man

$$(\mathbb{Z}/n\mathbb{Z})^\times := \{a+n\mathbb{Z} : \operatorname{ggT}(a,n)=1\}$$

die *prime Restklassengruppe modulo n.*

Beispiel 4.5.

Wir wollen das Inverse von $7+31\mathbb{Z}$ in $(\mathbb{Z}/31\mathbb{Z})^\times$ bestimmen. Der euklidische Algorithmus liefert $1=\operatorname{ggT}(7,31) = 9\cdot 7 - 2\cdot 31$. Also ist $(7+31\mathbb{Z})^{-1} = 9+31\mathbb{Z}$.

Satz 4.6. *Genau dann ist $\mathbb{Z}/n\mathbb{Z}$ ein Körper, falls $n\in\mathbb{P}$.*

Beweis. Für $n=p\in\mathbb{P}$ ist $|(\mathbb{Z}/p\mathbb{Z})^\times| = \varphi(p) = p-1 = |(\mathbb{Z}/n\mathbb{Z})\setminus(0+n\mathbb{Z})|$, d. h. jedes von 0 verschiedene Element ist invertierbar. Damit ist $\mathbb{Z}/p\mathbb{Z}$ ein Körper. Ist $n\notin\mathbb{P}$, so existiert ein Primteiler p von n. Wegen $\operatorname{ggT}(p,n)=p\ne 1$ ist $0\ne p+n\mathbb{Z}$ nicht invertierbar in $(\mathbb{Z}/n\mathbb{Z})^\times$. Daher ist $\mathbb{Z}/n\mathbb{Z}$ kein Körper. □

Definition 4.7. Für eine Primzahl p setzt man $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.

Folgerung 4.8 (Euler-Fermat). *Für $a\in\mathbb{Z}$ und $n\in\mathbb{N}$ mit $\operatorname{ggT}(a,n)=1$ gilt*

$$\boxed{a^{\varphi(n)} \equiv 1 \pmod{n}.}$$

Insbesondere ist $a^{p-1}\equiv 1 \pmod{p}$ für $p\in\mathbb{P}$ mit $p\nmid a$.

Beweis. Sei $G := (\mathbb{Z}/n\mathbb{Z})^\times$. Wie in jeder Gruppe gilt $gx = gy \iff x = g^{-1}gx = g^{-1}gy = y$ für $g, x, y \in G$. Mit g durchläuft also auch gx alle Elemente aus G (nur in anderer Reihenfolge). Da G kommutativ ist, folgt

$$\prod_{g\in G} g = \prod_{g\in G}(xg) = x^{|G|}\prod_{g\in G} g = x^{\varphi(n)}\prod_{g\in G} g.$$

Durch Multiplizieren mit dem Inversen von $\prod g$ erhält man die erste Behauptung. Die zweite Aussage folgt aus $\varphi(p) = p - 1$. □

Bemerkung 4.9. Die Gleichung $a^{p-1} \equiv 1 \pmod p$ nennt man den *kleinen Satz von Fermat*. Aus ihr folgt $a^p \equiv a \pmod p$ sogar für alle $a \in \mathbb{Z}$. Wir untersuchen in Satz 4.24 die Umkehrung dieser Aussage.

Definition 4.10. Eine Gruppe $(G, \cdot)$ heißt *zyklisch*, falls ein Element $g \in G$ mit $G = \{g^k : k \in \mathbb{Z}\}$ existiert. Ggf. nennt man g einen *Erzeuger* von G.

Beispiel 4.11. Die Gruppe $(\mathbb{Z}/n\mathbb{Z}, +)$ ist zyklisch mit Erzeuger $1 + n\mathbb{Z}$, denn $a + n\mathbb{Z} = a(1 + n\mathbb{Z})$ für $a = 1, \ldots, n$ (aus der Potenz g^k wird hier das Vielfache, da die Verknüpfung $+$ und nicht $\cdot$ ist). In der Gruppe $G := (\mathbb{Z}/8\mathbb{Z})^\times$ gilt hingegen $a^2 \equiv 1 \pmod 8$ für alle $a + 8\mathbb{Z} \in G$. Daher ist G nicht zyklisch.

Definition 4.12. Für $a + n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times$ existiert nach Euler-Fermat eine kleinste natürliche Zahl $k \in \mathbb{N}$ mit $a^k \equiv 1 \pmod n$. Man nennt $\operatorname{ord}_n(a) := k$ die *Ordnung* von a modulo n.

Lemma 4.13. *Sei $a + n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times$ mit $d := \operatorname{ord}_n(a)$. Dann gilt*

(i) $a^k \equiv 1 \pmod n \iff d \mid k$. *Insbesondere ist $d \mid \varphi(n)$.*

(ii) $a^k \equiv a^l \pmod n \iff k \equiv l \pmod d$ *für $k, l \in \mathbb{N}$.*

(iii) Für $k \in \mathbb{N}$ ist

$$\boxed{\operatorname{ord}_n(a^k) = \frac{d}{\operatorname{ggT}(d,k)}.}$$

Beweis.

(i) Division mit Rest liefert $k = dq + r$ mit $q, r \in \mathbb{Z}$ und $0 \le r < d$. Nun gilt

$$a^r \equiv (a^d)^q a^r \equiv a^{dq+r} \equiv a^k \equiv 1 \pmod n \iff r = 0 \iff d \mid k.$$

(ii) Sei o. B. d. A. $k \le l$. Aus (i) folgt

$$a^k \equiv a^l \pmod n \iff a^{l-k} \equiv 1 \pmod n \iff d \mid l - k \iff k \equiv l \pmod d.$$

(iii) Es gilt

$$\begin{aligned}\operatorname{ord}_n(a^k) &= \min\bigl\{s \in \mathbb{N} : a^{ks} = (a^k)^s \equiv 1 \pmod n\bigr\} \overset{\text{(i)}}{=} \min\bigl\{s \in \mathbb{N} : ks \equiv 0 \pmod d\bigr\} \\ &\overset{3.6}{=} \min\Bigl\{s \in \mathbb{N} : s \equiv 0 \Bigl(\operatorname{mod} \frac{d}{\operatorname{ggT}(d,k)}\Bigr)\Bigr\} = \frac{d}{\operatorname{ggT}(d,k)}.\end{aligned}$$

□

Beispiel 4.14. Wie lang ist die (minimale) *Periode* der Dezimalbruchentwicklung einer rationalen Zahl $r = \frac{n}{k}$ mit $\operatorname{ggT}(n,k) = 1$ (die Existenz dieser Periode wird in allgemeineren Kontext in Satz 5.2 bewiesen)? Beispiel:

$$\frac{1}{3} = 0{,}\overline{3}, \qquad \frac{1}{7} = 0{,}\overline{142857}, \qquad \frac{1}{22} = 0{,}0\overline{45}.$$

Sei $k = 2^a 5^b k'$ mit $\operatorname{ggT}(10, k') = 1$. Dann gilt

$$10^{a+b} r = \frac{2^b 5^a n}{k'}.$$

Durch das Multiplizieren mit 10^{a+b} ändert sich weder die Periode und ihre Länge (es ändert sich lediglich die Startposition der Periode). Wir können daher $k = k'$ annehmen.

Satz 4.15 (Periodenlänge)**.** *Seien $n, k \in \mathbb{N}$ mit $\operatorname{ggT}(n,k) = 1 = \operatorname{ggT}(10,k)$. Dann ist $\operatorname{ord}_k(10)$ die Periodenlänge von $\frac{n}{k}$.*

Beweis. Indem wir $r = \frac{n}{k}$ mit einer geeigneten Potenz von 10 multiplizieren, können wir annehmen, dass die Periode direkt nach dem Komma beginnt. Sei also $r = \ldots,\overline{d_1 \ldots d_\rho}$, d. h. die Periodenlänge ist $\rho \geq 0$. Dann gilt

$$10^\rho r - r = \ldots d_1 \ldots d_\rho,\overline{d_1 \ldots d_\rho} - \ldots,\overline{d_1 \ldots d_\rho} \in \mathbb{N}$$

und es folgt $10^\rho n - n \equiv 0 \pmod{k}$. Wegen $\operatorname{ggT}(n,k) = 1$ ist dies zu $10^\rho \equiv 1 \pmod{k}$ äquivalent. Dies zeigt $t := \operatorname{ord}_k(10) \mid \rho$. Umgekehrt gilt $10^t \equiv 1 \pmod{k}$ und es folgt $10^t r - r \in \mathbb{N}$. Für die Nachkommastellen $d_1, d_2, \ldots$ bedeutet das $d_{i+t} = d_i$ für alle $i \in \mathbb{N}$. Also ist $\rho \leq t$. □

Bemerkung 4.16. Die Periodenlänge von $\frac{n}{k}$ ist also höchstens $\varphi(k)$. Wir untersuchen im Folgenden, wann das Maximum angenommen wird.

Lemma 4.17. *Sei K ein Körper, $n \in \mathbb{N}$ und $a_0, a_1, \ldots, a_{n-1} \in K$. Dann besitzt die Polynomgleichung*

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0$$

höchstens n verschiedene Lösungen $x \in K$.

Beweis. Angenommen es existieren $n+1$ paarweise verschiedene Lösungen $x_0, x_1, \ldots, x_n \in K$. Bekanntlich ist dann die Vandermonde-Matrix

$$A := \begin{pmatrix} 1 & x_0 & x_0^2 & \cdots & x_0^n \\ 1 & x_1 & x_1^2 & \cdots & x_1^n \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^n \end{pmatrix} \in K^{(n+1)\times(n+1)}$$

invertierbar (es gilt $\det(A) = \prod_{0 \leq i < j \leq n}(x_j - x_i) \neq 0$). Andererseits ist $v := (a_0, a_1, \ldots, a_{n-1}, 1)$ eine nicht-triviale Lösung des linearen Gleichungssystems $Av = 0$. Widerspruch. □

Satz 4.18. *Für $p \in \mathbb{P}$ ist $\mathbb{F}_p^\times$ zyklisch, d. h. es existiert ein $a \in \mathbb{Z}$ mit*

$$\mathbb{F}_p^\times = \{a^k + p\mathbb{Z} : k = 1, \ldots, p-1\}.$$

Beweis. Sei $f(d)$ die Anzahl der Elemente $a + p\mathbb{Z} \in (\mathbb{Z}/p\mathbb{Z})^\times$ der Ordnung d. Im Fall $d \nmid \varphi(p) = p-1$ ist $f(d) = 0$ nach Lemma 4.13. Sei nun $\operatorname{ord}_p(a) = d \mid p-1$. Dann sind die Restklassen $a^k + p\mathbb{Z}$ für $k = 1, \ldots, d$ paarweise verschieden und es gilt

$$(a^k)^d - 1 = a^{kd} - 1 = (a^d)^k - 1 \equiv 1^k - 1 \equiv 0 \pmod{p}.$$

Nach Lemma 4.17 sind die Restklassen von $a, a^2, \ldots, a^d$ also die einzigen Lösungen der Gleichung $x^d - 1$ im Körper $\mathbb{F}_p$. Nach Lemma 4.13 gilt außerdem $\operatorname{ord}_p(a^k) = \frac{d}{\operatorname{ggT}(d,k)}$. Daher haben nur die Elemente a^k mit $\operatorname{ggT}(d,k) = 1$ Ordnung d. Dies zeigt $f(d) \le \varphi(d)$. Da jedes Element aus $\mathbb{F}_p^\times$ eine Ordnung $d \mid p-1$ besitzt, gilt

$$p - 1 = \sum_{d \mid p-1} f(d) \le \sum_{d \mid p-1} \varphi(d) \overset{3.22}{=} p - 1.$$

Es folgt $f(d) = \varphi(d)$ für alle $d \mid p-1$. Insbesondere ist $f(p-1) = \varphi(p-1) > 0$. Hat $a + p\mathbb{Z}$ Ordnung $p-1$, so gilt in der Tat $\mathbb{F}_p^\times = \{a^k + p\mathbb{Z} : k = 1, \ldots, p-1\}$ nach Lemma 4.13. □

Bemerkung 4.19. Einen Erzeuger $a \in \mathbb{Z}$ von $\mathbb{F}_p^\times$ nennt man *Primitivwurzel* modulo p. Der Beweis von Satz 4.18 zeigt, dass es genau $\varphi(p-1)$ Primitivwurzeln gibt, ohne jedoch eine solche Wurzel zu konstruieren. Tatsächlich kennt man keine Formel für die Berechnung von Primitivwurzeln, aber in der Regel findet man „kleine“ Primitivwurzeln[7].

Lemma 4.20. *Für jede Primzahl $p > 2$ und $n \in \mathbb{N}$ gilt* $\operatorname{ord}_{p^n}(1+p) = p^{n-1}$.

Beweis. Für $n = 1$ ist die Aussage trivial. Wir beweisen induktiv

$$(1+p)^{p^{n-2}} \equiv 1 + p^{n-1} \pmod{p^n} \tag{4.1}$$

für $n \ge 2$. Im Fall $n = 2$ erhält man $1 + p \equiv 1 + p \pmod{p^2}$. Sei nun $n \ge 3$. Nach Induktion existiert ein $k \in \mathbb{Z}$ mit $(1+p)^{p^{n-3}} = 1 + p^{n-2} + kp^{n-1}$. Es folgt

$$\begin{aligned}(1+p)^{p^{n-2}} &= (1 + p^{n-2} + kp^{n-1})^p = \sum_{k=0}^{p} \binom{p}{k} (p^{n-2} + kp^{n-1})^k \\ &\equiv 1 + p^{n-1} + \sum_{k=2}^{p} \binom{p}{k} p^{(n-2)k} (1 + kp)^k \pmod{p^n}.\end{aligned}$$

Für $2 \le k < p$ ist $\binom{p}{k} = \frac{p(p-1)\ldots(p-k+1)}{k!}$ durch p teilbar und $(n-2)k \ge 2n - 4 \ge n - 1$. Daher ist die Summe über $2 \le k \le p$ durch p^n teilbar und die Induktion beendet. Für $n + 1$ wird (4.1) zu

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

Dies zeigt $\operatorname{ord}_{p^n}(1+p) \mid p^{n-1}$. Wegen $1 + p^{n-1} \not\equiv 1 \pmod{p^n}$ ist andererseits $\operatorname{ord}_{p^n}(1+p) > p^{n-2}$ nach (4.1). Also gilt $\operatorname{ord}_{p^n}(1+p) = p^{n-1}$. □

Satz 4.21 (Gauss)**.** *Genau dann ist $(\mathbb{Z}/n\mathbb{Z})^\times$ zyklisch, wenn $n \in \{4, p^m, 2p^m\}$ für eine ungerade Primzahl p und $m \in \mathbb{N}_0$ gilt.*

[7] Siehe Anhang und `https://oeis.org/A001918`

Beweis. Sei $G := (\mathbb{Z}/n\mathbb{Z})^\times$ und o. B. d. A. sei $n \ge 3$.

⇒: Nach Bemerkung 3.17 ist $2 \mid \varphi(n)$. Sei $a+n\mathbb{Z}$ ein Erzeuger von G. Nach Lemma 4.13 ist $a^{\varphi(n)/2}+n\mathbb{Z}$ das einzige Element der Ordnung 2 in G. Dies zeigt $a^{\varphi(n)/2}+n\mathbb{Z} = -1+n\mathbb{Z}$. Sei $n = p_1^{m_1} \ldots a_k^{m_k}$ die Primfaktorzerlegung von n. Nach dem chinesischen Restsatz existiert für jedes $1 \le i \le k$ ein $x_i \in \mathbb{Z}$ mit $x_i \equiv -1 \pmod{p_i^{m_i}}$ und $x_i \equiv 1 \pmod{p_j^{m_j}}$ für alle $j \ne i$. Offenbar ist $x_i^2 \equiv 1 \pmod{n}$, d. h. $\mathrm{ord}_n(x_i) \le 2$. Im Fall $k \ge 2$ besitzt n einen ungeraden Primteiler, sagen wir p_1. Nun ist $-1 \not\equiv 1 \pmod{p_1^{m_1}}$ und $\mathrm{ord}_n(x_i) = 2$. Dies zeigt $x_i \equiv -1 \pmod{n}$. Dann muss aber $-1 \equiv x_i \equiv 1 \pmod{p_i^{m_i}}$ für $i \ge 2$ gelten. Dies liefert $k = 2$ und $p_2^{m_2} = 2$.

Sei nun $k = 1$ und $n = 2^m$. Im Fall $m \ge 3$ wäre $-1 + 2^{m-1} + n\mathbb{Z}$ neben $-1 + n\mathbb{Z}$ ein weiteres Element der Ordnung 2, denn $(-1 + 2^{m-1})^2 = 1 + 2^m + 2^{2m-2} \equiv 1 \pmod{n}$.

⇐: Sei $n = p^m \ge p$ für eine Primzahl $p > 2$. Sei b eine Primitivwurzel modulo p und $a = (1+p)b^{p^m}$. Wegen $\mathrm{ggT}(b,p) = 1$ ist auch $\mathrm{ggT}(a,n) = 1$. Sei $d := \mathrm{ord}_n(a)$. Aus $a^d \equiv 1 \pmod{n}$ folgt

$$b^{p^m d} \equiv (1+p)^d b^{p^m d} \equiv a^d \equiv 1 \pmod{p}.$$

Nach Lemma 4.13 gilt $p-1 \mid d$. Daher ist $\varphi(n) = p^{m-1}(p-1) \mid p^m d$ und $b^{p^m d} \equiv 1 \pmod{n}$. Es folgt $(1+p)^d \equiv a^d \equiv 1 \pmod{n}$. Nach Lemma 4.20 gilt nun $p^{m-1} \mid d$. Insgesamt erhält man $\varphi(n) = \mathrm{kgV}(p^{m-1}, (p-1)) \mid d \mid \varphi(n)$. Dies zeigt, dass $a + n\mathbb{Z}$ ein Erzeuger von G ist.

Schließlich existiert nach dem chinesischen Restsatz ein $c \in \mathbb{Z}$ mit $c \equiv a \pmod{n}$ und $c \equiv 1 \pmod{2}$. Es gilt dann $\mathrm{ord}_{2n}(c) \ge \mathrm{ord}_n(c) = \varphi(n) = \varphi(2)\varphi(n) = \varphi(2n)$. Also ist $c + 2n\mathbb{Z}$ ein Erzeuger von $(\mathbb{Z}/2n\mathbb{Z})^\times$. □

Bemerkung 4.22. Die Periodenlänge von $\frac{n}{k}$ kann nur dann $\varphi(k)$ betragen, wenn $10+k\mathbb{Z}$ ein Erzeuger von $(\mathbb{Z}/k\mathbb{Z})^\times$ ist. Wegen $\mathrm{ggT}(10,k) = 1$ kommt dafür nur $k = p^m$ für eine Primzahl $p > 2$ in Frage. Angenommen 10 ist keine Primitivwurzel von p. Dann existieren $d < p-1$ und $a \in \mathbb{Z}$ mit $10^d = 1+pa$. Mit der binomischen Formel folgt

$$10^{dp^{m-1}} = (1+ap)^{p^{m-1}} \equiv 1 \pmod{p^m}$$

wie in Lemma 4.20. Also ist $\mathrm{ord}_k(10) < \varphi(k)$. Andererseits besagt eine offene Vermutung von Gauß, dass es unendlich viele Primzahlen p mit $\mathrm{ord}_p(10) = \varphi(p)$ gibt. In den allermeisten Fällen gilt dann auch $\mathrm{ord}_{p^2}(10) = \varphi(p^2)$ (die kleinsten Ausnahmen sind $p = 487$ und 56.598.313).[8] Aufgabe 32 zeigt, dass ggf. auch die Periodenlänge von $\frac{n}{p^m}$ für alle $m \ge 1$ maximal ist.

Definition 4.23. Man nennt $n \in \mathbb{N} \setminus \mathbb{P}$ eine CARMICHAEL-*Zahl*, falls $n \ge 1$ und $a^{n-1} \equiv 1 \pmod{n}$ für alle $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a,n) = 1$ gilt.

Satz 4.24 (KORSELT). *Genau dann ist $n \in \mathbb{N}$ eine Carmichael-Zahl, wenn n ein Produkt von mindestens drei paarweise verschiedenen ungeraden Primzahlen $p_1, \ldots, p_k$ ist und $n \equiv 1 \pmod{p_i - 1}$ für $i = 1, \ldots, k$ gilt.*

Beweis. Sei $p > 2$ ein Primteiler von n und p^m die maximale p-Potenz, die n teilt. Nach Gauß existiert ein Erzeuger $a + p^m\mathbb{Z}$ von $(\mathbb{Z}/p^m\mathbb{Z})^\times$. Nach dem chinesischen Restsatz können wir $\mathrm{ggT}(a,n) = 1$ annehmen. Aus $a^{n-1} \equiv 1 \pmod{p^m}$ folgt $p-1 \mid \varphi(p^m) = \mathrm{ord}_{p^m}(a) \mid n-1$, d. h. $n \equiv 1 \pmod{p-1}$. Im Fall $m \ge 2$ hätte man den Widerspruch $p \mid n-1$. Aus $n \equiv 1 \pmod{p-1}$ folgt außerdem $\mathrm{ggT}(p-1,n) = 1$. Also kann n nur dann gerade sein, wenn $n = 2^m$ mit $m \ge 2$ gilt ($m = 1$ ist ausgeschlossen, da

[8] siehe `https://oeis.org/A045616`

Carmichael-Zahlen keine Primzahlen sind). In diesem Fall wäre aber $-1 \equiv (-1)^{n-1} \equiv 1 \pmod 4$. Also ist n ein Produkt von paarweise verschiedenen ungeraden Primzahlen. Angenommen $n = pq$ mit Primzahlen $p < q$. Dann gilt

$$p - 1 \equiv n - 1 \equiv 0 \pmod{q-1}$$

und man erhält den Widerspruch $q - 1 \le p - 1 < p - 1$.

Sei umgekehrt $n = p_1 \dots p_k$ mit Primzahlen $p_1 < \dots < p_k$ und $n \equiv 1 \pmod{p_i - 1}$ für $i = 1, \dots, k$. Sei $\mathrm{ggT}(a, n) = 1$. Wegen $\varphi(p_i) \mid n - 1$ gilt $a^{n-1} \equiv 1 \pmod{p_i}$. Daraus folgt $a^{n-1} \equiv 1 \pmod n$. Also ist n eine Carmichael-Zahl (die Bedingungen $p_1 > 2$ und $k \ge 3$ werden nicht benötigt). $\square$

Beispiel 4.25. Sei $n = pqr$ eine Carmichael-Zahl mit ungeraden Primzahlen $p < q < r$. Für $p = 3$ ist $n \equiv 1 \pmod{p-1}$ offensichtlich erfüllt. Für $q = 5$ erhält man $15 \equiv 15r \equiv n \equiv 1 \pmod{r-1}$. Dafür gibt es kein r. Der Fall $q = 7$ ist ebenso ausgeschlossen, denn hier wäre $\mathrm{ggT}(n, 6) = 1$. Sei schließlich $q = 11$. Dann ist $3r \equiv 1 \pmod{10}$, also $r \equiv 7 \pmod{10}$. Die Wahl $r = 17$ verlangt $33 \equiv n \equiv 1 \pmod{16}$, was richtig ist. Also ist $n = 3 \cdot 11 \cdot 17 = 561$ eine (die kleinste) Carmichael-Zahl.

Bemerkung 4.26. Da Carmichael-Zahlen relativ selten sind, eignet sich die Fermat-Gleichung $a^{p-1} \equiv 1 \pmod p$ als (notwendiger aber nicht hinreichender) Primzahltest (Aufgabe 29). Alford-Granville-Pomerance haben allerdings gezeigt, dass es unendlich viele Carmichael-Zahlen gibt. Die folgende Verfeinerung liefert einen besseren Primzahltest.

Satz 4.27 (Miller-Rabin-Test)**.** *Sei $n \in \mathbb{N}$ und $n - 1 = 2^k m$ mit $k \ge 1$ und $2 \nmid m$.*

(i) Existieren Zahlen $a \in \mathbb{N}$ und $0 \le l < k$ mit $a^{2^l m} \not\equiv \pm 1 \pmod n$ und $a^{2^{l+1} m} \equiv 1 \pmod n$, so ist n keine Primzahl.

(ii) Ist n keine Primzahl, so existieren höchstens $\frac{1}{4}n$ Zahlen $a \in \{2, \dots, n-1\}$, für die $a^m \equiv 1 \pmod n$ oder $a^{2^l m} \equiv -1 \pmod n$ mit einem $l < k$ gilt.

Beweis. Sei zunächst $n \in \mathbb{P}$. Dann ist $G := (\mathbb{Z}/n\mathbb{Z})^\times$ zyklisch der Ordnung $n - 1$. Insbesondere ist $-1 + n\mathbb{Z}$ das einzige Element der Ordnung 2 in G. Für a mit $a^{2^l m} \not\equiv 1 \pmod n$ und $a^{2^{l+1} m} \equiv 1 \pmod n$ muss also $a^{2^l m} \equiv -1 \pmod n$ gelten. Dies zeigt (i).

Sei nun $n \notin \mathbb{P}$ und a wie in (ii). Sei A die Anzahl dieser Elemente a. Wegen $a^{n-1} = a^{2^k m} \equiv 1 \pmod n$ ist $\overline{a} := a + n\mathbb{Z} \in G$ und $t := |\langle \overline{a} \rangle|$ teilt $\mathrm{ggT}(\varphi(n), n-1)$. Sei $n = p_1^{r_1} \dots p_s^{r_s}$ die Primfaktorzerlegung von n. Wegen $\mathrm{ggT}(n - 1, p_1 \dots p_s) = 1$ ist $t \mid (p_1 - 1) \dots (p_s - 1)$. Da n ungerade ist, sind die Gruppen $G_i := (\mathbb{Z}/p_i^{r_i}\mathbb{Z})^\times$ zyklisch für $i = 1, \dots, s$. Nach dem chinesischen Restsatz gilt $G = G_1 \times \dots \times G_s$. Wir schreiben $\overline{a} = (\overline{a}_1, \dots, \overline{a}_s)$ mit $\overline{a}_i \in G_i$. Dann gibt es höchstens $p_i - 1$ Möglichkeiten für $\overline{a}_i$. Im Fall $r_i > 1$ gilt

$$A \le (p_1 - 1) \dots (p_s - 1) \le \frac{p_i - 1}{p_i^2} n \le \frac{2}{9} n < \frac{1}{4} n.$$

Wir können daher $r_1 = \dots = r_s = 1$ annehmen. Insbesondere ist $s \ge 2$ wegen $n \notin \mathbb{P}$.

Sei $p_i - 1 = 2^{d_i} q_i$ mit $d_i \ge 1$ und $2 \nmid q_i$ für $i = 1, \dots, s$. Im Fall $a^m \equiv 1 \pmod n$ hat $\overline{a}$ ungerade Ordnung. Hier gibt es für a höchstens $q_1 \dots q_s$ Möglichkeiten. Sei nun $a^{2^l m} \equiv -1 \pmod n$ für ein $l < k$. Dann gilt auch $a^{2^l m} \equiv -1 \pmod{p_i}$ für $i = 1, \dots, s$. Für $\overline{a}_i$ gibt es daher höchstens $\varphi(2^{l+1}) q_i = 2^l q_i$

Möglichkeiten (mit Gleichheit falls $q_i \mid m$). Folglich gibt es für a höchstens $2^{ls}q_1 \dots q_s$ Möglichkeiten. Mit $d := \max\{d_1, \dots, d_s, k\}$ erhält man

$$A \le q_1 \dots q_s + q_1 \dots q_s \sum_{l=0}^{d-1} 2^{ls} = \Big(1 + \frac{2^{sd}-1}{2^s-1}\Big) q_1 \dots q_s.$$

Im Fall $s \ge 3$ ist

$$A \le \frac{2^{sd}+6}{7} q_1 \dots q_s \le \frac{2^{sd}}{4} q_1 \dots q_s \le \frac{1}{4}(p_1-1)\dots(p_s-1) < \frac{1}{4}n.$$

Es bleibt der Fall $s = 2$. Ist $d_1 \ne d_2$, so erhält man

$$A \le \frac{2^{2d}+2}{3} q_1 q_2 \le \frac{2^{2d-1}+1}{3}(p_1-1)(p_2-1) \le 2^{2d-2}(p_1-1)(p_2-1) < \frac{1}{4}n.$$

Sei daher $d_1 = d_2 = d$. O. B. d. A. sei $q_1 < q_2$ Dann gilt

$$2^k m = n - 1 = (2^d q_1 + 1)(2^d q_2 + 1) - 1 \equiv 2^d q_1 \not\equiv 0 \pmod{q_2}$$

und $q_2 \nmid m$. Für $\overline{a}_2$ kommen also nur höchstens $\frac{1}{3}2^d q_2$ Elemente in Frage. Dies ergibt

$$A \le \frac{2^{2d}+2}{9} q_1 q_2 < \frac{1}{4}n. \qquad \square$$

Bemerkung 4.28.

(i) In der Praxis wählt man Zufallszahlen $a_1, \dots, a_s \in \{2, \dots, n-1\}$. Ist $a_i^{n-1} \not\equiv 1 \pmod n$ für ein i, so ist n keine Primzahl nach Fermat. Gilt Satz 4.27(i) für ein a_i, so ist n ebenfalls keine Primzahl. Anderenfalls können wir nach Satz 4.27(ii) schließen, dass n mit Wahrscheinlichkeit $\le 4^{-s}$ keine Primzahl ist. Es handelt sich also um einen *probabilistischen* Primzahltest. Eine eindeutige Antwort erhält man, indem man mehr als $\frac{1}{4}n$ viele a_i testet, was aber unpraktikabel ist.[9] Für den Erfolg des Miller-Rabin-Tests ist die Zufälligkeit der a_i unentbehrlich, denn für jede vorgegebene Menge $\{a_1, \dots, a_s\}$ lassen sich zusammengesetzte Zahlen n konstruieren, die den Miller-Rabin-Test bzgl. der a_i bestehen (ohne Beweis).

(ii) Unter Annahme der Riemannschen Vermutung kann man zeigen, dass der Miller-Rabin-Test bereits für relativ „kleine“ a_i eine eindeutige Antwort liefert. Damit hat der Algorithmus eine Laufzeit von $O(\log(n)^4)$. Mit dem *AKS-Test* fand man 2002 erstmals einen deterministischen Algorithmus mit polynomialer Laufzeit (in $\log(n)$), der nicht von unbewiesenen Vermutungen abhängt. Man beachte, dass Primzahltests in der Regel keinen konkreten Teiler von n liefern, falls n keine Primzahl ist. Die Primfaktorzerlegung ist aus algorithmischer Sicht ein viel schwierigeres Problem (siehe Kapitel 10).

Beispiel 4.29.

(i) Für die Carmichael-Zahl $n = 561$ gilt $n - 1 = 2^4 \cdot 75$. Für $a = 2$ berechnen wir $a^{4 \cdot 75} \equiv 67 \not\equiv \pm 1 \pmod n$ und $a^{8 \cdot 75} \equiv 1 \pmod n$. Also ist n keine Primzahl.

(ii) Für die Mersenne-Zahl $n = M_{11} = 2047$ gilt $n-1 = 2 \cdot 1023$. Für $a = 2$ ist $a^{1023} \equiv 1 \pmod n$, d. h. der Miller-Rabin-Test erkennt für dieses a nicht, dass n keine Primzahl ist. Wegen $3^{1023} \equiv 1565 \pmod n$ genügt jedoch der Test mit $a = 3$.

[9] Aufgrund von möglichen Hardwaredefekten kann man bei Computerberechnungen ohnehin keine hundertprozentige Aussage erwarten.

5 Kettenbrüche

Bemerkung 5.1. Irrationale Zahlen sind dadurch charakterisiert, dass ihre (unendliche) Dezimalbruchentwicklung keine Periode aufweist. Für gewisse irrationale Zahlen werden wir dennoch eine regelmäßige Folge konstruieren. Zunächst verallgemeinern wir die b-adische Entwicklung (Satz 1.5) und die Dezimalbruchentwicklung rationaler Zahlen (Satz 4.15).

Satz 5.2. *Sei $b \in \mathbb{N} \setminus \{1\}$ und $x \in \mathbb{R}$ mit $x > 0$. Dann existiert genau ein $n \in \mathbb{Z}$ und genau eine unendliche Folge $x_n, x_{n+1}, \ldots \in \{0, \ldots, b-1\}$ mit folgenden Eigenschaften:*

(i) Die Reihe $\sum_{k=n}^{\infty} x_k b^{-k}$ konvergiert gegen x.

(ii) $x_n \neq 0$ und unendlich viele x_i sind ungleich $b-1$.

(iii) Genau dann ist $x \in \mathbb{Q}$, wenn $p, n_0 \in \mathbb{N}$ mit $x_{k+p} = x_k$ für alle $k \geq n_0$ existieren. Ggf. heißt die Folge (x_i) periodisch. *Ist p minimal gewählt, so nennt man $x_{n_0}, x_{n_0+1}, \ldots, x_{n_0+p-1}$ die* Periode *der* Länge *p von x.*

Beweis. Sei $n \in \mathbb{Z}$ minimal und $x_n \in \{1, \ldots, b-1\}$ maximal mit $x_n b^{-n} \leq x$ (existiert da $x > 0$). Sei $n_1 > n$ minimal und $x_{n_1} \in \{1, \ldots, b-1\}$ maximal mit $x_n b^{-n} + x_{n_1} b^{-n_1} \leq x$ usw. Für $k \neq n_i$ setzen wir $x_k := 0$. Wegen

$$|x - x_n b^{-n} - \ldots - x_{n_k} b^{-n_k}| < b^{-n_k}$$

für $k \in \mathbb{N}$ konvergiert die Folge der Partialsummen $\sum_{k=n}^{m} x_k b^{-k}$ gegen x. Angenommen nur endlich viele x_i sind ungleich $b-1$. Dann existiert ein $N \in \mathbb{N}$ mit $x_k = b-1$ für $k > N$. Im Fall $N \geq n$ sei $x_N < b-1$. Dann wäre

$$x = \sum_{k=n}^{\infty} x_k b^{-k} = \sum_{k=n}^{N} x_k b^{-k} + \sum_{k=N+1}^{\infty} (b-1) b^{-k} = \sum_{k=n}^{N-1} x_k b^{-k} + (x_N + 1) b^{-N}$$

im Widerspruch zur Konstruktion von x_N.

Sei auch $x = \sum_{k=n'}^{\infty} x'_k b^{-k}$ mit $n' \in \mathbb{Z}$ und $0 \leq x'_k \leq b-1$. Sei $m \in \mathbb{Z}$ minimal mit $x_m \neq x'_m$, o. B. d. A. $x_m > x'_m$ (wobei wir $x_k := 0$ und $x'_k := 0$ für $k < n$ bzw. $k < n'$ setzen). Dann erhält man

$$0 \leq b^{-m} - \sum_{k=m+1}^{\infty} (b-1) b^{-k} \leq \sum_{k=m}^{\infty} (x_k - x'_k) b^{-k} = x - x = 0.$$

Gleichheit kann nur gelten, wenn $x_k = 0$ und $x'_k = b-1$ für $k \geq m+1$. Dann wären aber nur endlich viele der x'_k ungleich $b-1$. Dieser Widerspruch zeigt die Eindeutigkeit der x_k.

Nehmen wir nun an, dass $x_{k+p} = x_k$ für alle $k \geq n_0$ gilt. Dann ist

$$x(b^{-p} - 1) = x b^{-p} - x = \sum_{k=n}^{\infty} x_k (b^{-k-p} - p^{-k}) = \sum_{k=n}^{n_0-1} x_k (b^{-k-p} - p^{-k}) - \sum_{k=n_0}^{n_0+p-1} x_k b^{-k} \in \mathbb{Q}.$$

Dies zeigt $x \in \mathbb{Q}$. Sei umgekehrt $x = \frac{r}{s} \in \mathbb{Q}$ mit $r, s \in \mathbb{N}$. Multiplikation mit einer Potenz von b bewirkt eine Indexverschiebung der Folge (x_k). Wir können also $\operatorname{ggT}(s, b) = 1$ und $n \leq 0$ annehmen. Für $t := \varphi(s)$ gilt dann $b^t \equiv 1 \pmod{s}$. Also ist

$$\sum_{k=n}^{\infty} (x_{k+t} - x_k) b^{-k} = b^t \sum_{k=n}^{\infty} x_{k+t} b^{-k-t} - x = x(b^t - 1) - \sum_{k=n}^{n+t-1} x_k b^{-k+t} \in \mathbb{N}.$$

Aus der b-adischen Entwicklung folgt $x_{k+t} = x_k$ für $k \geq 1$, d. h. (x_k) ist periodisch mit Länge $\leq t$ (vgl. Satz 4.15). $\square$

Beispiel 5.3.

$$\frac{1}{3} = \frac{4^{-1}}{1 - 4^{-1}} = \sum_{k=1}^{\infty} 2^{-2k} = 0{,}\overline{01}_2.$$

Definition 5.4. Für $n \in \mathbb{N}$ besteht die Farey-*Reihe* $\mathcal{F}_n$ aus den aufsteigend geordneten gekürzten Brüchen der Form $\frac{a}{b}$ mit $a, b \in \mathbb{Z}$ und $0 \leq a \leq b \leq n$.

Beispiel 5.5.

$$\mathcal{F}_5 = \left\{ \frac{0}{1}, \frac{1}{5}, \frac{1}{4}, \frac{1}{3}, \frac{2}{5}, \frac{1}{2}, \frac{3}{5}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \frac{1}{1} \right\}.$$

Lemma 5.6. *Seien* $\frac{a}{b} < \frac{a'}{b'} < \frac{a''}{b''}$ *aufeinanderfolgende Glieder von* $\mathcal{F}_n$. *Dann gilt*

(i) $\frac{a}{b} < \frac{a+a'}{b+b'} < \frac{a'}{b'}$, $b + b' > n$ *und* $b \neq b'$.

(ii) $a'b - ab' = 1$.

(iii) $\frac{a'}{b'} = \frac{a+a''}{b+b''}$.

Beweis.

(i) Aus $ab' < a'b$ folgt $a(b + b') < b(a + a')$ und $b'(a + a') < a'(b + b')$. Dies zeigt $\frac{a}{b} < \frac{a+a'}{b+b'} < \frac{a'}{b'}$. Nach Voraussetzung gilt $\frac{a+a'}{b+b'} \notin \mathcal{F}_n$ und damit $b + b' > n$. Im Fall $b = b'$ wäre

$$\frac{a}{b} < \frac{a}{b-1} < \frac{a+1}{b} \leq \frac{a'}{b} = \frac{a'}{b'}.$$

(ii) Wegen $\mathrm{ggT}(a, b) = 1$ existieren teilerfremde $c, d \in \mathbb{Z}$ mit $bc - ad = 1$. Indem man (c, d) durch $(c + \lambda a, d + \lambda b)$ mit geeignetem $\lambda \in \mathbb{Z}$ ersetzt, kann man $n - b < d \leq n$ annehmen. Es gilt

$$\frac{a}{b} < \frac{a}{b} + \frac{1}{bd} = \frac{ad + 1}{bd} = \frac{c}{d}.$$

Im Fall $\frac{c}{d} = \frac{a'}{b'}$ folgt $c = a'$ und $d = b'$ aus $\mathrm{ggT}(c, d) = 1$. Wegen $d \leq n$ können wir also $\frac{c}{d} > \frac{a'}{b'}$ annehmen. Es folgt

$$\frac{c}{d} - \frac{a'}{b'} = \frac{cb' - a'd}{db'} \geq \frac{1}{db'},$$
$$\frac{a'}{b'} - \frac{a}{b} = \frac{a'b - ab'}{bb'} \geq \frac{1}{bb'}.$$

Dies liefert den Widerspruch

$$\frac{1}{bd} = \frac{bc - ad}{bd} = \frac{c}{d} - \frac{a'}{b'} + \frac{a'}{b'} - \frac{a}{b} \geq \frac{1}{db'} + \frac{1}{bb'} = \frac{b + d}{bb'd} > \frac{n}{bb'd} \geq \frac{1}{bd}.$$

(iii) Aus (ii) folgt $a'b - ab' = 1 = a''b' - a'b''$ und

$$b'(a''b - ab'') = (a'b - ab')b'' + (a''b' - a'b'')b = b + b''$$
$$a'(a''b - ab'') = (a'b - ab')a'' + (a''b' - a'b'')a = a + a''.$$

Dies zeigt die Behauptung. □

Bemerkung 5.7. Der Beweis liefert ein Verfahren zur Berechnung des Nachfolgers von $\frac{a}{b} \in \mathcal{F}_n$: Man bestimme $c, d \in \mathbb{Z}$ mit $bc - ad = 1$ und $n - b < d \le n$. Dann ist $\frac{c}{d}$ der Nachfolger von $\frac{a}{b}$. Beispiel: $\frac{3}{7} \in \mathcal{F}_{10}$. Wegen $7 \cdot 1 - 3 \cdot 2 = 1 = 7 \cdot (1 + 3) - 3 \cdot (2 + 7)$ gilt $\frac{a'}{b'} = \frac{4}{9}$.

Satz 5.8 (Dirichlets Approximationssatz)**.** *Für $n \in \mathbb{N}$ und $x \in \mathbb{R}$ existieren $a, b \in \mathbb{Z}$ mit $1 \le b \le n$ und*

$$\left|x - \frac{a}{b}\right| \le \frac{1}{b(n+1)} \le \frac{1}{b(b+1)} < \frac{1}{b^2}.$$

Beweis. O. B. d. A. sei $0 < x < 1$. Dann liegt x zwischen zwei aufeinanderfolgenden Gliedern der Farey-Folge $\mathcal{F}_n$:

$$\frac{a}{b} < x \le \frac{a'}{b'}.$$

Nach Lemma 5.6 ist

$$\frac{a}{b} < x \le \frac{a+a'}{b+b'} \qquad \text{oder} \qquad \frac{a+a'}{b+b'} < x \le \frac{a'}{b'}$$

mit

$$\frac{a+a'}{b+b'} - \frac{a}{b} = \frac{a'b - ab'}{b(b+b')} = \frac{1}{b(b+b')} \le \frac{1}{b(n+1)},$$
$$\frac{a'}{b'} - \frac{a+a'}{b+b'} = \frac{a'b - ab'}{b'(b+b')} \le \frac{1}{b'(n+1)}.$$

□

Bemerkung 5.9. Achtung: Nicht zu jedem $b \in \mathbb{N}$ existiert ein $a \in \mathbb{N}$ mit $|x - \frac{a}{b}| < \frac{1}{b^2}$. Für $x = \frac{1}{2}$ und $b = 3$ ist beispielsweise $|\frac{1}{2} - \frac{a}{3}| \ge \frac{1}{6} > \frac{1}{9}$.

Beispiel 5.10. Wählt man für $\pi \approx 3{,}14$ die naheliegende Näherung $\frac{a}{b} = \frac{314}{100} = \frac{157}{50}$, so erhält man nur

$$\left|\pi - \frac{a}{b}\right| = 0{,}0015 > \frac{1}{1000} > \frac{1}{2550} = \frac{1}{50 \cdot 51}.$$

Besser ist die Näherung $\frac{a}{b} = \frac{355}{113}$ mit

$$\left|\pi - \frac{a}{b}\right| = 2{,}7 \cdot 10^{-7} < 10^{-5} < \frac{1}{113 \cdot 114}.$$

Im Folgenden konstruieren wir solche *Näherungsbrüche* systematisch.

Bemerkung 5.11. Für $a \in \mathbb{Z}$ und $b \in \mathbb{N}$ liefert der euklidische Algorithmus Folgen $q_1, q_2, \ldots, q_n = \operatorname{ggT}(a, b)$ und $r_1, \ldots, r_n$ mit $a = q_1 b + r_1$, $b = q_2 r_1 + r_2$, $r_1 = q_2 r_2 + r_3, \ldots, r_{n-1} = q_n r_n$. Dies lässt sich in der Form

$$\frac{a}{b} = q_1 + \frac{1}{\frac{b}{r_1}} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{}{\ddots \, \frac{1}{q_n}}}}$$

schreiben.

Definition 5.12. Für $a_0 \in \mathbb{R}$ und $a_1, \ldots \in \mathbb{R} \setminus \{0\}$ definieren wir $[a_0] := a_0$ und $[a_0, \ldots, a_n] := [a_0, \ldots, a_{n-2}, a_{n-1} + \frac{1}{a_n}]$ für $n \geq 1$. Es gilt also

$$[a_0, \ldots, a_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{}{\ddots \; \cfrac{1}{a_n}}}}.$$

Im Fall $a_0 \in \mathbb{Z}$ und $a_1, \ldots \in \mathbb{N}$ nennt man $[a_0, \ldots, a_n]$ einen *Kettenbruch*.

Satz 5.13. *Jedes $x \in \mathbb{Q}$ lässt sich auf genau eine Weise als Kettenbruch $x = [a_0, \ldots, a_n]$ darstellen, wobei $a_n \geq 2$ falls $n \geq 1$.*

Beweis. Sei $x = \frac{a}{b}$ mit $\operatorname{ggT}(a, b) = 1$. Aus Bemerkung 5.11 erhält man natürliche Zahlen $q_1, \ldots, q_n = 1$ mit $x = [q_1, \ldots, q_n]$. Im Fall $n \geq 1$ ist auch $x = [q_1, \ldots, q_{n-1}+1]$ mit $q_{n-1}+1 \geq 2$. Für die Eindeutigkeit sei $x = [a_0, \ldots, a_n] = [b_0, \ldots, b_m]$. Für $n = 0$ ist $x = a_0 \in \mathbb{Z}$. Dann ist auch $m = 0$ und $a_0 = b_0$, denn anderenfalls wäre $0 < x - b_0 < 1$ wegen $b_m > 1$. Sei nun $n, m \geq 1$. Wegen $0 \leq x - a_0 < 1$ und $0 \leq x - b_0 < 1$ folgt $a_0 = b_0$. Aus $[a_1, \ldots, a_n] = \frac{1}{x-a_0} = [b_1, \ldots, b_m]$ folgt induktiv $n = m$ und $a_i = b_i$ für $i = 0, \ldots, n$. □

Beispiel 5.14.

(i)

$$\frac{19}{7} = 2 + \frac{1}{\frac{7}{5}} = 2 + \cfrac{1}{1 + \cfrac{1}{\frac{5}{2}}} = \ldots = [2, 1, 2, 2].$$

(ii) Die Umlaufzeit der Erde um die Sonne beträgt ca. 365,24219 Tage. Dies entspricht dem Kettenbruch $[365, 4, 7, 1, 3, 24, 6, 2, 2]$. Der Näherungsbruch $[365, 4] = 265 + \frac{1}{4}$ führt auf die Schaltjahresregel des julianischen Kalenders (alle 4 Jahre ein zusätzlicher Tag). Die Näherung

$$[365, 4, 7, 1, 3] = 365 + \frac{31}{128}$$

liefert eine genauerer Regel: 31 Schalttage alle 128 Jahre. Die derzeit gültige Regel des gregorianischen Kalenders (97 Schalttage alle 400 Jahre) ist ungenauer, aber leichter zu merken.

Lemma 5.15. *Sei $a_0 \in \mathbb{R}$, $a_1, \ldots \in \mathbb{R} \setminus \{0\}$ und*

$$\begin{aligned}
(p_0, q_0) &:= (a_0, 1),\\
(p_1, q_1) &:= (a_0 a_1 + 1,\ a_1),\\
(p_k, q_k) &:= (a_k p_{k-1} + p_{k-2},\ a_k q_{k-1} + q_{k-2})
\end{aligned}$$

für $k \geq 2$. Dann gilt $[a_0, \ldots, a_k] = \frac{p_k}{q_k}$ für $k = 0, \ldots, n$.

Beweis. Induktion nach k: Für $k = 0, 1$ gilt die Behauptung, denn $\frac{p_1}{q_1} = \frac{a_0 a_1 + 1}{a_1} = a_0 + \frac{1}{a_1} = [a_0, a_1]$. Für $k \geq 2$ gilt

$$[a_0, \ldots, a_{k+1}] = \left[a_0, \ldots, a_k + \frac{1}{a_{k+1}}\right] = \frac{(a_k + \frac{1}{a_{k+1}})p_{k-1} + p_{k-2}}{(a_k + \frac{1}{a_{k+1}})q_{k-1} + q_{k-2}}$$
$$= \frac{p_k + \frac{1}{a_{k+1}} p_{k-1}}{q_k + \frac{1}{a_{k+1}} q_{k-1}} = \frac{a_{k+1} p_k + p_{k-1}}{a_{k+1} q_k + q_{k-1}} = \frac{p_{k+1}}{q_{k+1}}. \qquad \square$$

Beispiel 5.16. Wir berechnen den Kettenbruch $[1, 1, \ldots, 1]$ mit Lemma 5.15:

a_k	1	1	1	1	1	$\cdots$
p_k	1	2	3	5	8	$\cdots$
q_k	1	1	2	3	5	$\cdots$

Hier sind $p_k = q_{k+1}$ die Glieder der bekannten FIBONACCI-*Folge* (Aufgabe 3).

Folgerung 5.17. *Sei $[a_0, \ldots, a_n]$ ein Kettenbruch. Mit den Bezeichnungen aus Lemma 5.15 gilt*

(i) $1 \leq q_1 < q_2 < \ldots$ *und* $q_k \geq k$ *für* $k \in \mathbb{N}$.

(ii) $p_k q_{k-1} - p_{k-1} q_k = (-1)^{k+1}$ *und*
$$\frac{p_k}{q_k} - \frac{p_{k-1}}{q_{k-1}} = \frac{(-1)^{k+1}}{q_k q_{k-1}}$$
für $k = 1, \ldots, n$. Insbesondere ist $\operatorname{ggT}(p_k, q_k) = 1$ *für* $k \geq 0$.

(iii) $p_k q_{k-2} - p_{k-2} q_k = (-1)^k a_k$ *und*
$$\frac{p_k}{q_k} - \frac{p_{k-2}}{q_{k-2}} = \frac{(-1)^k a_k}{q_k q_{k-2}}$$
für $k = 2, \ldots, n$.

Beweis.

(i) Nach Definition ist $q_0 = 1$, $q_1 = a_1 \geq 1$ und induktiv $q_k = a_k q_{k-1} + q_{k-2} \geq q_{k-1} + q_{k-2} > q_{k-1} \geq k - 1$.

(ii) Man kann die Definition von p_k und q_k als Matrixgleichung auffassen:
$$\begin{pmatrix} p_1 & p_0 \\ q_1 & q_0 \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix},$$
$$\begin{pmatrix} p_k & p_{k-1} \\ q_k & q_{k-1} \end{pmatrix} = \begin{pmatrix} p_{k-1} & p_{k-2} \\ q_{k-1} & q_{k-2} \end{pmatrix} \begin{pmatrix} a_k & 1 \\ 1 & 0 \end{pmatrix}.$$

Dann gilt
$$P_k := \begin{pmatrix} p_k & p_{k-1} \\ q_k & q_{k-1} \end{pmatrix} = \prod_{i=0}^{k} \begin{pmatrix} a_i & 1 \\ 1 & 0 \end{pmatrix}$$
und $p_k q_{k-1} - p_{k-1} q_k = \det P_k = (-1)^{k+1}$. Die zweite Gleichung folgt nach Division durch $q_{k-1} q_k$. Außerdem folgt $\operatorname{ggT}(p_k, q_k) = 1$ für $k \geq 0$.

(iii) Es gilt

$$p_k q_{k-2} - p_{k-2} q_k = \det \begin{pmatrix} p_k & p_{k-2} \\ q_k & q_{k-2} \end{pmatrix} = \det \begin{pmatrix} p_{k-1} & p_{k-2} \\ q_{k-1} & q_{k-2} \end{pmatrix} \det \begin{pmatrix} a_k & 0 \\ 1 & 1 \end{pmatrix} = (-1)^k a_k. \qquad \square$$

Lemma 5.18. *Sei $a_0 \in \mathbb{Z}$ und $a_1, \ldots \in \mathbb{N}$. Für $k \in \mathbb{N}_0$ sei $\alpha_k := [a_0, \ldots, a_k]$. Dann gilt*

$$\alpha_0 < \alpha_2 < \ldots < \alpha_{2k} < \alpha_{2k-1} < \alpha_{2k-3} < \ldots < \alpha_1.$$

Insbesondere existiert der Grenzwert $[a_0, \ldots] := \lim_{k\to\infty} \alpha_k$.

Beweis. Nach Folgerung 5.17 ist $\alpha_{2k} - \alpha_{2k-2} = \frac{a_{2k}}{q_{2k}q_{2k-2}} > 0$ und analog $\alpha_{2k-1} - \alpha_{2k} < 0$ sowie $\alpha_{2k-1} - \alpha_{2k-3} < 0$. Für $k < l$ gilt $\alpha_{2k} < \alpha_{2l} < \alpha_{2l-1} \le \alpha_{2k+1} < \alpha_{2k-1}$. Dies zeigt

$$|\alpha_l - \alpha_k| \le |\alpha_{k+1} - \alpha_k| \le \frac{1}{q_{k+1}q_k} < \frac{1}{k^2} \xrightarrow{k\to\infty} 0.$$

Also ist $(\alpha_k)_k$ eine Cauchy-Folge, die im vollständigen Raum $\mathbb{R}$ konvergiert. $\square$

Bemerkung 5.19. In der Situation von Lemma 5.18 nennt man $\alpha = [a_0, \ldots]$ einen (unendlichen) *Kettenbruch* und α_k den *k-ten Näherungsbruch* von α.

Satz 5.20. *Für alle $x \in \mathbb{R} \setminus \mathbb{Q}$ existieren eindeutig bestimmte Zahlen $a_0 \in \mathbb{Z}$ und $a_1, \ldots \in \mathbb{N}$ mit $x = [a_0, \ldots]$.*

Beweis. Wegen $x \notin \mathbb{Q}$ existieren $a_k \in \mathbb{Z}$ und $0 < \epsilon_k < 1$ mit $x = a_0 + \epsilon_0$ und $\epsilon_{k-1}^{-1} = a_k + \epsilon_k$ für $k \ge 1$. Wegen $\epsilon_{k-1}^{-1} > 1$ ist $a_k \in \mathbb{N}$ für $k \ge 1$. Außerdem gilt

$$x = a_0 + \epsilon_0 = [a_0, \epsilon_0^{-1}] = [a_0, a_1 + \epsilon_1] = [a_0, a_1, \epsilon_1^{-1}] = \ldots = [a_0, \ldots, a_k, \epsilon_k^{-1}].$$

für $k \ge 1$. Aus Lemma 5.15 folgt

$$\begin{aligned} |x - [a_0, \ldots, a_k]| &= \Big| \frac{\epsilon_k^{-1} p_k + p_{k-1}}{\epsilon_k^{-1} q_k + q_{k-1}} - \frac{p_k}{q_k} \Big| = \Big| \frac{(\epsilon_k^{-1} p_k + p_{k-1}) q_k - p_k(\epsilon_k^{-1} q_k + q_{k-1})}{(\epsilon_k^{-1} q_k + q_{k-1}) q_k} \Big| \\ &= \Big| \frac{p_{k-1} q_k - p_k q_{k-1}}{(\epsilon_k^{-1} q_k + q_{k-1}) q_k} \Big| \overset{5.17}{<} \frac{1}{q_k^2} \le \frac{1}{k^2}. \end{aligned}$$

Dies zeigt $x = [a_0, \ldots]$. Sei auch $x = [b_0, \ldots]$ ein Kettenbruch. Dann gilt $x = b_0 + \tau_0$ mit $\tau_0 = [b_1, \ldots]^{-1}$. Aus $0 < \tau_0 < 1$ folgt $\tau_0 = \epsilon_0$ und $a_0 = b_0$. Nun gilt $[a_1, \ldots] = \epsilon_0^{-1} = \tau_0^{-1} = [b_1, \ldots]$ und man erhält $a_1 = b_1$ usw. $\square$

Beispiel 5.21.

(i) Für $\pi = 3{,}1415926\ldots$ liefert der Algorithmus aus dem Beweis von Satz 5.20:

$$\begin{aligned} a_0 &= 3, & \epsilon_0^{-1} &= 7{,}0625, \\ a_1 &= 7, & \epsilon_1^{-1} &= 15{,}9965\ldots, \\ a_2 &= 15, & \epsilon_2^{-1} &= 1{,}0034\ldots, \\ a_3 &= 1, & \epsilon_3^{-1} &= 292{,}6345\ldots. \end{aligned}$$

Also ist $\pi = [3, 7, 15, 1, 292, \ldots]$ (wegen Rundungsfehlern benötigt man mehr als die angegebenen Nachkommastellen). Durch den hohen Wert 292 erhält man einen besonders guten Näherungsbruch durch $[3, 7, 15, 1] = \frac{355}{113} \approx 3{,}1415929$.

(ii) Für die eulersche Zahl e weißt der Kettenbruch ein offensichtliches Muster auf:

$$e = [2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, 1, \ldots]$$

(ohne Beweis). Für π gibt es zumindest einen regelmäßigen „Kettenbruch“ anderer Art:

$$\pi = 3 + \cfrac{1^2}{6 + \cfrac{3^2}{6 + \cfrac{5^2}{6 + \ldots}}}$$

(gefunden von Lange, 1999).

(iii) Für den *goldenen Schnitt* $\varphi = \frac{1+\sqrt{5}}{2}$ gilt $\varphi = 1 + \frac{1}{\varphi} = [1, \varphi] = [1, 1, \ldots] = [\overline{1}]$. Die Näherungsbrüche werden aus den Fibonacci-Zahlen gebildet $\frac{f_{n+1}}{f_n}$ (Beispiel 5.16).

(iv) Der nächste Satz verbessert Dirichlets Approximationssatz.

Satz 5.22 (Hurwitz)**.** *Sei $x \in \mathbb{R}$ und $n \in \mathbb{N}$. Dann existiert $\frac{p}{q} \in \mathbb{Q}$ mit $q \ge n$ und*

$$\left|x - \frac{p}{q}\right| < \frac{1}{\sqrt{5}q^2}.$$

Beweis. O. B. d. A. sei $x > 0$ (anderenfalls betrachte man $x + m > 0$ für ein $m \in \mathbb{N}$). Im Fall $x \in \mathbb{Q}$ kann man $\frac{p}{q} = x$ wählen und $q \ge n$ durch Erweitern garantieren. Sei also $x = [a_0, \ldots]$ irrational mit Näherungsbrüchen $\alpha_k = \frac{p_k}{q_k}$. O. B. d. A. sei $n \ge 5$ ungerade. Nach Lemma 5.15 und Lemma 5.18 gilt $n \le q_{n-1} \le q_n \le q_{n+1}$ und $\alpha_{n-1} < \alpha_{n+1} < x < \alpha_n$. Nehmen wir indirekt $|x - \alpha_k| > \frac{1}{\sqrt{5}q_k^2}$ für $k = n-1, n, n+1$ an. Dann gilt

$$\frac{1}{q_k q_{k+1}} = |\alpha_{k+1} - \alpha_k| > \frac{1}{\sqrt{5}q_k^2} + \frac{1}{\sqrt{5}q_{k+1}^2}$$

für $k = n-1, n$ nach Folgerung 5.17. Multiplikation mit $\sqrt{5}q_{k+1}^2$ ergibt

$$\left(\frac{q_{k+1}}{q_k}\right)^2 - \sqrt{5}\frac{q_{k+1}}{q_k} + 1 < 0.$$

Die Nullstellen von $X^2 - \sqrt{5}X + 1$ sind $(\sqrt{5}-1)/2$ und der goldene Schnitt $\varphi = (\sqrt{5}+1)/2$. Insbesondere gilt $\frac{q_{k+1}}{q_k} < \varphi$ für $k = n-1, n$. Mit Lemma 5.15 erhält man den Widerspruch

$$\frac{q_{n+1}}{q_n} \ge \frac{q_n + q_{n-1}}{q_n} = 1 + \frac{q_{n-1}}{q_n} > 1 + \varphi^{-1} = \varphi. \qquad \square$$

Beispiel 5.23. Die Abschätzung von Hurwitz ist in zweierlei Hinsicht optimal:

(i) Sei $\varphi = (\sqrt{5}+1)/2$ und $c > \sqrt{5}$. Angenommen es gibt unendlich viele $\frac{p}{q} \in \mathbb{Q}$ mit $\operatorname{ggT}(p, q) = 1$ und

$$\left|\varphi - \frac{p}{q}\right| < \frac{1}{cq^2}.$$

Sei $\varphi = \frac{p}{q} + \frac{\epsilon}{q^2}$ mit $|\epsilon| < 1/c$. Dann folgt

$$\frac{\epsilon^2}{q^2} - \epsilon\sqrt{5} = \left(\frac{\epsilon}{q} - \frac{1}{2}q\sqrt{5}\right)^2 - \frac{5}{4}q^2 = \left(\frac{1}{2}q - p\right)^2 - \frac{5}{4}q^2 = p^2 - pq - q^2.$$

Die linke Seite liegt für große q echt zwischen -1 und 1. Da die rechte Seite ganzzahlig ist, ergibt sich $p^2 - pq - q^2 = 0$. Dann wäre aber $p \mid q$ im Widerspruch zu $\operatorname{ggT}(p, q) = 1$. Daher lässt sich die Konstante $\sqrt{5}$ im Allgemeinen nicht verbessern. Man erhält außerdem, dass sich φ besonders „schlecht" durch rationale Zahle approximieren lässt.

(ii) Sei $x \in \mathbb{R}$ eine Nullstelle eines nicht-konstanten ganzzahligen Polynoms (z. B. $x = \sqrt{2}$). Der Satz von Thue-Siegel-Roth besagt, dass für jedes $\epsilon > 0$ nur endlich viele $\frac{p}{q} \in \mathbb{Q}$ mit

$$\left|x - \frac{p}{q}\right| < \frac{1}{q^{2+\epsilon}}.$$

existieren.

Folgerung 5.24. *Für jede Zahl $a \in \mathbb{N}$ existiert einer 2-Potenz, die mit den Ziffern von a beginnt.*

Beweis. Gesucht sind $n, k \in \mathbb{N}$ mit $a \cdot 10^k \le 2^n < (a + 1)10^k$, d. h.

$$\log_{10}(a) \le n \log_{10}(2) - k < \log_{10}(a + 1). \tag{5.1}$$

Nach Aufgabe 9 ist $\log_{10}(2)$ irrational. Nach Satz 5.22 existieren $p, q \in \mathbb{N}$ mit $\frac{1}{q} < \log_{10}(a+1) - \log_{10}(a)$ und $0 < \log_{10}(2) - \frac{p}{q} < \frac{1}{q^2}$ (da der Abstand von p/q zum folgenden Näherungsbruch kleiner als $1/q^2$ ist, kann man $p/q < \log_{10}(2)$ annehmen). Es folgt

$$0 < q \log_{10}(2) - p < \frac{1}{q} < \log_{10}(a + 1) - \log_{10}(a).$$

Nun existiert ein $s \in \mathbb{N}$ mit $\log_{10}(a) < s(q \log_{10}(2) - p) < \log_{10}(a + 1)$. Also gilt (5.1) für $n := sq$ und $k := sp$. □

Beispiel 5.25. Welche 2-Potenz beginnt mit $a = 7$? Der ersten beiden Näherungsbrüche für $\log_{10}(2) \approx 0{,}30$ sind $\frac{1}{3}$ und $\frac{3}{10}$. Es gilt

$$0 < 10 \log_{10}(2) - 3 < \log_{10}(8) - \log_{10}(7) \approx 0{,}058.$$

Im obigen Beweis kann man $s = 83$ wählen und erhält 2^{830}. Allerdings beginnt bereits 2^{46} mit einer 7.

Bemerkung 5.26. Sei $q \in \mathbb{Q}$ mit $\sqrt{q} \notin \mathbb{Q}$. Dann ist $\mathbb{Q}(\sqrt{q}) := \mathbb{Q} + \mathbb{Q}\sqrt{q}$ ein 2-dimensionaler $\mathbb{Q}$-Vektorraum mit Basis $1, \sqrt{q}$. Wegen

$$(a_1 + b_1\sqrt{q})(a_2 + b_2\sqrt{q}) = (a_1a_2 + b_1b_2d) + (a_1b_2 + a_2b_1)\sqrt{q} \in \mathbb{Q}(\sqrt{q})$$

ist $\mathbb{Q}(\sqrt{q})$ unter Multiplikation abgeschlossen. Für $x := a + b\sqrt{d} \in \mathbb{Q}(\sqrt{q})$ sei $x^* := a - b\sqrt{q}$ (im Fall $q < 0$ ist $x^* = \bar{x}$ das komplex-konjugierte von x). Es gilt $xx^* = a^2 - b^2q \in \mathbb{Q}$. Aus der eindeutigen Primfaktorzerlegung folgt leicht $xx^* \neq 0$ für $x \neq 0$. Ggf. ist $x^{-1} = \frac{x^*}{xx^*} \in \mathbb{Q}(\sqrt{q})$. Dies zeigt, dass $\mathbb{Q}(\sqrt{q})$ ein Körper ist. Wie bei der komplexen Konjugation gilt

$$(x \overset{+}{\cdot} y)^* = x^* \overset{+}{\cdot} y^*$$

für $x, y \in \mathbb{Q}(\sqrt{q})$.

Satz 5.27 (Euler-Lagrange). *Sei $x = [a_0, \ldots] \in \mathbb{R} \setminus \mathbb{Q}$ wie in Satz 5.20. Genau dann ist x die Lösung einer quadratischen Gleichung mit Koeffizienten in $\mathbb{Q}$, wenn die Folge $a_0, \ldots$ periodisch wird.*

Beweis. Sei zunächst $x = [\overline{a_0, \ldots, a_n}]$ ein *rein*periodischer Kettenbruch. Dann gilt $x = [\overline{a_0, \ldots, a_n}, x]$ und mit Folgerung 5.17 ergibt sich $x = \frac{xp_k + p_{k-1}}{xq_k + q_{k-1}}$ mit $p_k, p_{k-1}, q_k, q_{k-1} \in \mathbb{N}$. Durch Umstellen erhält man eine quadratische Gleichung in x. Sei nun $x = [a_0, \ldots, a_n, \overline{b_1, \ldots, b_m}]$ und $y := [\overline{b_1, \ldots, b_m}]$. Dann gilt $x = [a_0, \ldots, a_n, y]$ und $x = \frac{yp_k + p_{k-1}}{yq_k + q_{k-1}}$ mit $p_k, p_{k-1}, q_k, q_{k-1} \in \mathbb{N}$. Nach dem ersten Teil ist y eine Lösung einer quadratischen Gleichung, sagen wir $y = a + b\sqrt{d}$ mit $a, b \in \mathbb{Q}$ und $d \in \mathbb{N}$ (p-q-Formel). Nach Bemerkung 5.26 folgt $x \in \mathbb{Q}(\sqrt{d})$ und es existieren $a', b' \in \mathbb{Q}$ mit $x = a' + b'\sqrt{d}$. Also ist x Lösung einer quadratischen Gleichung.

Sei umgekehrt x Lösung einer quadratischen Gleichung. Dann existieren $a, b \in \mathbb{Z}$ und $d \in \mathbb{N}$ mit $x = \frac{a+\sqrt{d}}{b} = \frac{ab+\sqrt{db^2}}{b^2}$. Indem wir (a, b, d) durch (ab, b^2, b^2d) ersetzen, können wir $b \mid d - a^2$ annehmen. Definiere

$$k_0 := a, \quad m_0 := b, \quad \alpha_i := \frac{k_i + \sqrt{d}}{m_i}, \quad a_i := \lfloor \alpha_i \rfloor, \quad k_{i+1} := a_i m_i - k_i, \quad m_{i+1} := \frac{d - k_{i+1}^2}{m_i} \quad (i \geq 0).$$

Wegen $m_0 = b \mid d - a^2 = d - k_0^2$ und

$$d - k_{i+1}^2 = d - a_i m_i^2 + 2a_i m_i k_i - k_i^2 = m_i(m_{i-1} - a_i m_i + 2a_i k_i)$$

ist $m_i \in \mathbb{Z}$ für $i \in \mathbb{N}_0$. Wegen $x \notin \mathbb{Q}$ ist d keine Quadratzahl und $m_i \neq 0$. Aus $0 < \alpha_0 - a_0 < 1$ und

$$\alpha_{i+1} = \frac{k_{i+1} + \sqrt{d}}{m_{i+1}} = \frac{m_i(k_{i+1} + \sqrt{d})}{d - k_{i+1}^2} = \frac{m_i}{\sqrt{d} - k_{i+1}} = \frac{m_i}{\sqrt{d} - a_i m_i + k_i} = \frac{1}{\alpha_i - a_i} > 1$$

folgt induktiv $a_i \geq 1$ für $i \geq 1$. Dies zeigt

$$x = \alpha_0 = a_0 + \frac{1}{\alpha_1} = \ldots = [a_0, \ldots].$$

Mit den üblichen Bezeichnungen gilt

$$x = \frac{\alpha_k p_{k-1} + p_{k-2}}{\alpha_k q_{k-1} + q_{k-2}}, \qquad x^* \overset{5.26}{=} \frac{\alpha_k^* p_{k-1} + p_{k-2}}{\alpha_k^* q_{k-1} + q_{k-2}}$$

für alle $k \geq 2$. Wie zuvor berechnet man mit Lemma 5.15

$$\begin{aligned}\alpha_k^* q_{k-1}\Big(x^* - \frac{p_{k-1}}{q_{k-1}}\Big) &= \alpha_k^* \frac{q_{k-1}(\alpha_k^* p_{k-1} + p_{k-2}) - p_{k-1}(\alpha_k^* q_{k-1} + q_{k-2})}{\alpha_k^* q_{k-1} + q_{k-2}} = \frac{-\alpha_k^*(-1)^k}{\alpha_k^* q_{k-1} + q_{k-2}} \\ &= \frac{-(\alpha_k^* p_{k-1} + p_{k-2})q_{k-2} + p_{k-2}(\alpha_k^* q_{k-1} + q_{k-2})}{\alpha_k^* q_{k-1} + q_{k-2}} = -q_{k-2}\Big(x^* - \frac{p_{k-2}}{q_{k-2}}\Big).\end{aligned}$$

Wegen $q_k > 0$ und $\lim_{k\to\infty} \frac{p_k}{q_k} = x \neq x'$ muss ein $N \in \mathbb{N}$ mit $\alpha_i^* < 0$ für alle $i \geq N$ existieren. Dann ist $\frac{2\sqrt{d}}{m_i} = \alpha_i - \alpha_i^* > 0$ und $m_i > 0$. Wegen $m_i m_{i-1} = d - k_{i+1}^2$ ist $0 < m_i < d$ und $k_{i+1}^2 < d$ für alle $i \geq N$. Insbesondere können die Zahlen $m_0, m_1, \ldots$ und $k_0, k_1 \ldots$ nur endlich viele Werte annehmen. Daher existieren $s < t$ mit $\alpha_s = \alpha_t$. Dann gilt

$$x = [a_0, \ldots, a_{s-1}, \alpha_t] = [a_0, \ldots, a_{t-1}, \alpha_t] = [a_0, \ldots, a_{s-1}, \overline{a_s, \ldots, a_{t-1}}]. \qquad \square$$

Satz 5.28. *Genau dann ist $x \in \mathbb{R} \setminus \mathbb{Q}$ die Wurzel einer rationalen Zahl > 1, wenn der Kettenbruch die Form*

$$x = [a_0, \overline{a_1, \ldots, a_d, 2a_0}] = [a_0, \overline{a_d, a_{d-1}, \ldots, a_1, 2a_0}]$$

hat.

Beweis.

- $\Rightarrow$: Sei $r \in \mathbb{Q}$, $r > 1$, $\sqrt{r} = a_0 + \epsilon_0$ und $\epsilon_{k-1}^{-1} = a_k + \epsilon_k$ mit $0 < \epsilon_k < 1$ wie im Beweis von Satz 5.20. Mit Bemerkung 6.12 gilt $-\sqrt{r} = a_0 + \epsilon_0^*$ und $(\epsilon_{k-1}^*)^{-1} = a_k + \epsilon_k^*$. Wegen $\epsilon_0^* = -a_0 - \sqrt{r} < -1$ ist $-1 < (\epsilon_0^*)^{-1} < 0$. Sei induktiv $-1 < (\epsilon_{k-1}^*)^{-1} < 0$ bereits gezeigt. Dann ist $\epsilon_k^* = (\epsilon_{k-1}^*)^{-1} - a_k < -1$ und $-1 < (\epsilon_k^*)^{-1} < 0$. Dies zeigt $a_k = (\epsilon_{k-1}^*)^{-1} - \epsilon_k^* = \lfloor -\epsilon_k^* \rfloor$ für $k \ge 1$.

  Nach Satz 5.27 ist $\sqrt{r} = [a_0, \ldots, a_k, \epsilon_k^{-1}]$ periodisch, sagen wir $\epsilon_k = \epsilon_l$ mit $k < l$. Im Fall $k > 1$ ist $a_k = \lfloor -\epsilon_k^* \rfloor = \lfloor -\epsilon_l^* \rfloor = a_l$ und $\epsilon_{k-1} = \epsilon_{l-1}$. Induktiv erhält man $\epsilon_1 = \epsilon_s$, d. h. $\sqrt{r} = [a_0, \overline{a_1, \ldots, a_s}]$ mit $s := l - k + 1$. Wegen $\epsilon_0^{-1} = [\overline{a_1, \ldots, a_s}] = [a_1, \ldots, a_s, \epsilon_0^{-1}]$ gilt

$$\epsilon_0^{-1} = \frac{\epsilon_0^{-1} p_s + p_{s-1}}{\epsilon_0^{-1} q_s + q_{s-1}} = \frac{p_s + p_{s-1}\epsilon_0}{q_s + q_{s-1}\epsilon_0} \tag{5.2}$$

  mit den üblichen Bezeichnungen. Sei $\sigma := [\overline{a_s, a_{s-1}, \ldots, a_1}]$. Wie im Beweis von Folgerung 5.17 sei

$$P_s := \begin{pmatrix} p_s & p_{s-1} \\ q_s & q_{s-1} \end{pmatrix} = \prod_{i=1}^{s} \begin{pmatrix} a_i & 1 \\ 1 & 0 \end{pmatrix}$$

  Dann ist

$$\begin{pmatrix} p_s & q_s \\ p_{s-1} & q_{s-1} \end{pmatrix} = P_s^{\mathrm{t}} = \prod_{i=0}^{s-1} \begin{pmatrix} a_{s-i} & 1 \\ 1 & 0 \end{pmatrix}$$

  und

$$\sigma = \frac{\sigma p_s + q_s}{\sigma p_{s-1} + q_{s-1}}.$$

  Man erhält daraus quadratische Gleichungen mit den gleichen Koeffizienten:

$$\begin{aligned} p_{s-1}\epsilon_0^2 + (p_s - q_{s-1})\epsilon_0 - q_s &= \epsilon_0(p_s + p_{s-1}\epsilon_0) - (q_s + q_{s-1}\epsilon_0) \overset{(5.2)}{=} 0, \\ p_{s-1}(-\sigma)^2 + (p_s - q_{s-1})(-\sigma) - q_s &= \sigma(\sigma p_{s-1} + q_{s-1}) - (\sigma p_s + q_s) = 0. \end{aligned}$$

  Mit ϵ_0 ist auch $\epsilon_0^* \ne \epsilon_0$ eine Lösung dieser Gleichung nach Bemerkung 5.26. Wegen $\sigma > 0 > -\epsilon_0$ gilt daher

$$[\overline{a_s, \ldots, a_1}] = \sigma = -\epsilon_0^* = a_0 + \sqrt{r} = 2a_0 + \epsilon_0 = [2a_0, \overline{a_1, \ldots, a_s}].$$

  Also ist $a_s = 2a_0$ und $a_i = a_{s-i}$ für $i = 1, \ldots, s-1$.

- $\Leftarrow$: Sei x wie angegeben. Nach Satz 5.27 existieren $s, t \in \mathbb{Q}$ mit $x = s + \sqrt{t}$. Mit den Bezeichnungen von oben ist $\epsilon_0^{-1} = [\overline{a_1, \ldots, a_d, 2a_0}]$ und

$$-\epsilon_0^* = \sigma = [\overline{2a_0, a_d, \ldots, a_1}] = [2a_0, \epsilon_0^{-1}] = 2a_0 + \epsilon_0.$$

  Dies zeigt

$$s - \sqrt{t} = x^* = a_0 + \epsilon_0^* = -a_0 - \epsilon_0 = -x = -s - \sqrt{t}$$

  und $s = 0$. Wegen $2a_0 = a_{d+1} \ge 1$ ist $t > 1$. □

Bemerkung 5.29. Ist $0 < x = [a_0, \ldots] < 1$, so gilt $x^{-1} = [0, a_0, a_1, \ldots] >$. Ist $x = \sqrt{r}$ für ein $r \in \mathbb{Q}$, so kann man Satz 5.28 auf x^{-1} anwenden und erhält damit auch den Kettenbruch für x.

Beispiel 5.30. Sei $n = d^2 + 1$ mit $d \in \mathbb{N}$. Dann gilt

$$\sqrt{n} = d + \frac{1}{\sqrt{n} + d} = d + \frac{1}{2d + \frac{1}{\sqrt{n}+d}} = [d, \overline{2d}].$$

Speziell gilt $\sqrt{2} = [1, \overline{2}]$, $1 + \sqrt{2} = [\overline{2}]$ und $\sqrt{5} = [2, \overline{4}]$. Andererseits ist $\sqrt{14} = [3, \overline{1, 2, 1, 6}]$.

Satz 5.31 (Pells Gleichung)**.** *Sei $n \in \mathbb{N}$ keine Quadratzahl und $P := \{(p,q) \in \mathbb{N}^2 : p^2 - nq^2 = 1\}$. Dann gilt $P \neq \varnothing$. Ist $(p_1, q_1) \in P$ mit p_1 möglichst klein, so gilt*

$$P = \big\{(p,q) \in \mathbb{N}^2 : \exists k \in \mathbb{N} : p + \sqrt{n}q = (p_1 + \sqrt{n}q_1)^k\big\}.$$

Beweis. Sei $\sqrt{n} = [a_0, \overline{a_1, \ldots, a_d}]$ der Kettenbruch aus Satz 5.28 (die Struktur der Periode wird nicht benötigt). Sei e ein gerades Vielfaches von d. Für $\beta := (\sqrt{n} - a_0)^{-1} = [\overline{a_1, \ldots, a_e}]$ gilt $\sqrt{n} = [a_0, a_1, \ldots, a_e, \beta]$. Aus Lemma 5.15 folgt

$$\sqrt{n} = \frac{\beta p_e + p_{e-1}}{\beta q_e + q_{e-1}} = \frac{p_e + p_{e-1}(\sqrt{n} - a_0)}{q_e + q_{e-1}(\sqrt{n} - a_0)}.$$

Multiplizieren mit dem Nenner ergibt

$$nq_{e-1} + (q_e - q_{e-1}a_0)\sqrt{n} = p_e - p_{e-1}a_0 + p_{e-1}\sqrt{n}.$$

Da $\sqrt{n}$ irrational ist, sind 1 und $\sqrt{n}$ linear unabhängig über $\mathbb{Q}$. Man kann also Koeffizienten vergleichen:

$$nq_{e-1} = p_e - p_{e-1}a_0, \qquad q_e - q_{e-1}a_0 = p_{e-1}.$$

Dies zeigt

$$p_{e-1}^2 - nq_{e-1}^2 = (q_e - q_{e-1}a_0)p_{e-1} - (p_e - p_{e-1}a_0)q_{e-1} = p_{e-1}q_e - p_e q_{e-1} \overset{5.17}{=} (-1)^e = 1,$$

d. h. $(p_{e-1}, q_{e-1}) \in P$. Sei nun $(p_1, q_1) \in P$ mit p_1 minimal. Seien $k, s, t \in \mathbb{N}$ mit

$$(p_1 + \sqrt{n}q_1)^k = s + \sqrt{n}t.$$

Dann gilt auch

$$s^2 - nt^2 = (s + \sqrt{n}t)(s + \sqrt{n}t)^* = (p + \sqrt{n}q)^k((p + \sqrt{n}q)^*)^k = (p^2 - nq^2)^k = 1^k = 1,$$

d. h. $(s,t) \in P$. Angenommen es gibt eine Lösung $(p,q) \in \mathbb{N}^2$ mit $p + \sqrt{n}q \neq (p_1 + \sqrt{n}q_1)^k$ für alle $k \in \mathbb{N}$. Dann existiert ein $k \in \mathbb{N}$ mit $(p_1 + \sqrt{n}q_1)^k < p + \sqrt{n}q < (p_1 + \sqrt{n}q_1)^{k+1}$. Es folgt

$$1 = (p_1 + \sqrt{n}q_1)^k(p_1 - \sqrt{n}q_1)^k < (p + \sqrt{n}q)(p_1 - \sqrt{n}q_1)^k < p_1 + \sqrt{n}q_1.$$

Es existieren $s, t \in \mathbb{Z}$ mit $(p + \sqrt{n}q)(p_1 - \sqrt{n}q_1)^k = s + \sqrt{n}t$. Wie oben ist $s^2 - nt^2 = 1$. Im Fall $t < 0$ ist $0 < (s + \sqrt{n}t)^{-1} = s - \sqrt{n}t < 1$ und $s < 0$. Dann wäre aber $s + \sqrt{n}t < 0$. Also ist $t > 0$. Im Fall $s < 0$ wäre $-s + \sqrt{n}t = -(s + \sqrt{n}t)^{-1} < 0$ mit $-s, t > 0$. Also ist $s, t \in \mathbb{N}$ und $(s,t) \in P$. Dies widerspricht der Minimalität von p_1. Damit folgt die zweite Behauptung. □

Bemerkung 5.32. Wie im Beweis sei d die Periodenlänge des Kettenbruchs von $\sqrt{n}$ und $e = \mathrm{kgV}(2, d)$. Man kann zeigen, dass das Paar $(p,q) \in P$ mit minimalem p durch (p_{e-1}, q_{e-1}) gegeben ist. Alle weiteren Paare in P treten ebenfalls als Näherungsbrüche auf (ohne Beweis).

Beispiel 5.33.

(i) Je länger die Periode des Kettenbruchs zu $\sqrt{n}$ ist, desto größer werden die Paare (p,q) mit $p^2 - nq^2 = 1$. Für $\sqrt{2} = [1, \overline{2}]$ funktioniert jeder zweite Näherungsbruch, also

$$(p,q) \in \{(3,2), (17,12), (99,70), \ldots\}.$$

Für $\sqrt{61} = [7, \overline{1, 4, 3, 1, 2, 2, 1, 3, 4, 1, 14}]$ ist die kleinste Lösung

$$(p,q) = (1766319049, 226153980).$$

(ii) (HERON-*Verfahren*) Für $n \in \mathbb{N}$ ist $\sqrt{n}$ die Seitenlänge eines Quadrats Q mit Flächeninhalt n. Wir nähern Q durch Rechtecke mit Flächeninhalt n an. Im ersten Schritt wählt man die Seitenlängen $x_1 := 1$ und $y_1 := n$. Sind die Seitenlängen $x_k < y_k$ bereits bestimmt, so erhält man eine bessere Seitenlänge durch den Mittelwert $x_{k+1} := \frac{x_k+y_k}{2}$. Die andere Seitenlänge muss $y_{k+1} := \frac{n}{x_{k+1}}$ sein. Für $n = 2$ erhält man einige der Näherungsbrüche für $\sqrt{2}$:

$$x_i = 1, \frac{3}{2}, \frac{12}{17}, \frac{577}{408}.$$

Dieses Verfahren ergibt sich aus dem NEWTON-*Verfahren* zur Nullstellenbestimmung von $f(x) = x^2 - n$.

6 Quadratische Zahlkörper

Bemerkung 6.1.

(i) Wir werden die eindeutige Primfaktorzerlegung von $\mathbb{Z}$ auf gewisse Teilringe R von $\mathbb{C}$ ausdehnen. Wie bei Restklassenringen sei $R^\times$ stets die Menge der invertierbaren Elemente von R.

(ii) Für $d \in \mathbb{Q}$ mit $\sqrt{d} \notin \mathbb{Q}$ hatten wir in Bemerkung 5.26 den Körper $\mathbb{Q}(\sqrt{d})$ eingeführt. Sei $d = \frac{r}{s}$ mit $r, s \in \mathbb{Z}$. Dann ist $\sqrt{d} = \frac{\sqrt{rs}}{s}$ und $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{rs})$. Man kann also stets $d \in \mathbb{Z}$ annehmen. Wegen $\sqrt{de^2} = \sqrt{d}e$ kann man außerdem annehmen, dass d quadratfrei ist, d. h. d ist nicht durch das Quadrat einer Primzahl teilbar. Man nennt $\mathbb{Q}(\sqrt{d})$ einen *quadratischen Zahlkörper*. Im Fall $d > 0$ bzw. $d < 0$ spricht man von *reell-quadratischen* bzw. *imaginär-quadratischen* Zahlkörpern.

Definition 6.2. Für $d \in \mathbb{Z}$ quadratfrei sei

$$\begin{aligned} S &\colon \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}, && a + b\sqrt{d} \mapsto 2a, \\ N &\colon \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}, && a + b\sqrt{d} \mapsto a^2 - b^2 d \end{aligned}$$

die *Spur* bzw. *Norm*.

Bemerkung 6.3.

(i) Im Fall $d < 0$ ist $N(x) = x\overline{x} = |x|^2$ für $x \in \mathbb{Q}(\sqrt{d})$.

(ii) Für $x = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ gilt

$$x^2 - S(x)x + N(x) = a^2 + b^2 d + 2ab\sqrt{d} - 2a(a + b\sqrt{d}) + a^2 - b^2 d = 0.$$

Lemma 6.4. *In jedem quadratischen Zahlkörper $\mathbb{Q}(\sqrt{d})$ gilt $S(x + y) = S(x) + S(y)$ und $N(xy) = N(x)N(y)$ für $x, y \in \mathbb{Q}(\sqrt{d})$.*

Beweis. Die Gleichung $S(x+y) = S(x)+S(y)$ ist trivial. Außerdem ist $N(xy) = xy(xy)^* = xyx^*y^* = xx^*yy^* = N(x)N(y)$ nach Bemerkung 5.26. $\square$

Definition 6.5. Man nennt $x \in \mathbb{Q}(\sqrt{d})$ *ganz-algebraisch*, falls $S(x), N(x) \in \mathbb{Z}$ gilt. Sei $\mathbb{Z}_d$ die Menge der ganz-algebraischen Zahlen in $\mathbb{Q}(\sqrt{d})$.

Bemerkung 6.6. Nach Bemerkung 6.3 ist eine ganz-algebraische Zahl x Nullstelle des normierten ganzzahligen Polynoms $X^2 - S(x)x + N(x)$.

Satz 6.7. *Für $d \in \mathbb{Z} \setminus \{0, 1\}$ quadratfrei gilt*

$$\mathbb{Z}_d = \begin{cases} \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{d}}{2} & \textit{falls } d \equiv 1 \pmod 4, \\ \mathbb{Z} + \mathbb{Z}\sqrt{d} & \textit{sonst.} \end{cases}$$

Insbesondere ist $\mathbb{Z}_d$ ein Ring.

Beweis. Zunächst gilt offensichtlich $\mathbb{Z}+\mathbb{Z}\sqrt{d} \subseteq \mathbb{Z}_d$. Sei umgekehrt $x = a+b\sqrt{d} \in \mathbb{Z}_d$. Aus $S(x) = 2a \in \mathbb{Z}$ und $N(x) = a^2 - b^2 d \in \mathbb{Z}$ folgt $(2b)^2 d = S(x)^2 - 4N(x) \in \mathbb{Z}$ und $2b \in \mathbb{Z}$, da d quadratfrei ist. Sei also $x = \frac{a_1+b_1\sqrt{d}}{2}$ mit $a_1, b_1 \in \mathbb{Z}$. Wegen $N(x) = \frac{a_1^2-b_1^2 d}{4} \in \mathbb{Z}$ gilt $a_1^2 \equiv b_1^2 d \pmod 4$ mit $d \not\equiv 0 \pmod 4$. Ist $d \equiv 2, 3 \pmod 4$, so müssen a_1 und b_1 gerade sein, denn $a_1^2 \equiv 0, 1 \pmod 4$. Ggf. ist $x \in \mathbb{Z} + \mathbb{Z}\sqrt{d}$. Sei nun $d \equiv 1 \pmod 4$. Ist a_1 ungerade, so muss auch b_1 ungerade sein. In diesem Fall ist

$$a + b\sqrt{d} = \frac{a_1 - b_1}{2} + b_1\frac{1+\sqrt{d}}{2} \in \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{d}}{2}.$$

Umgekehrt gilt hier auch $\mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{d}}{2} \subseteq \mathbb{Z}_d$.

Für die zweite Behauptung muss nur die Abgeschlossenheit bzgl. Multiplikation im Fall $d \equiv 1 \pmod 4$ gezeigt werden:

$$\Big(a_1 + b_1\frac{1+\sqrt{d}}{2}\Big)\Big(a_2 + b_2\frac{1+\sqrt{d}}{2}\Big) = a_1a_2 + b_1b_2\frac{d-1}{4} + (a_1b_1 + a_2b_1 + b_1b_2)\frac{1+\sqrt{d}}{2}. \qquad \square$$

Definition 6.8. Man nennt $\mathbb{Z}_d$ den *Ganzheitsring* von $\mathbb{Q}(\sqrt{d})$. Die Elemente von $\mathbb{Z}_{-1}$ bzw. $\mathbb{Z}_{-3}$ nennt man *Gauß-Zahlen* bzw. Eisenstein-*Zahlen*.

Lemma 6.9. *Für $d \in \mathbb{Z} \setminus \{0, 1\}$ quadratfrei gilt*

$$x \in \mathbb{Z}_d^\times \iff N(x) = \pm 1.$$

Beweis. Für $x = a + b\sqrt{d} \in \mathbb{Z}_d^\times$ gilt $N(x) \in \mathbb{Z}$ und $N(x)^{-1} = N(x^{-1}) \in \mathbb{Z}$. Dies geht nur für $N(x) = \pm 1$. Sei umgekehrt $N(x) = \pm 1$. Aus $x^{-1} = \frac{1}{N(x)}(a - b\sqrt{d})$ folgt $S(x^{-1}) = \pm S(x) \in \mathbb{Z}$ und $N(x^{-1}) = N(x) \in \mathbb{Z}$. Also ist $x \in \mathbb{Z}_d^\times$. $\square$

Satz 6.10. *Für $d < 0$ quadratfrei gilt*

$$\mathbb{Z}_d^\times = \begin{cases} \langle \mathrm{i} \rangle = \{\pm 1, \pm \mathrm{i}\} & \textit{falls } d = -1, \\ \langle \frac{1+\sqrt{-3}}{2} \rangle = \{\pm 1, \pm\frac{1\pm\sqrt{-3}}{2}\} & \textit{falls } d = -3, \\ \langle -1 \rangle = \{\pm 1\} & \textit{sonst.} \end{cases}$$

Für $d > 1$ gilt $|\mathbb{Z}_d^\times| = \infty$.

Beweis. Selbstverständlich gilt in allen Fällen $\pm 1 \in \mathbb{Z}_d^\times$. Sei $x = a + b\sqrt{d} \in \mathbb{Z}_d^\times$. Nach Lemma 6.9 ist $a^2 - b^2 d = N(x) = \pm 1$. Im Fall $b = 0$ ist $x = a = \pm 1$. Sei also $b \neq 0$. Sei zunächst $d < 0$. Dann ist $\frac{1}{4}|d| \le a^2 + b^2|d| = 1$ und $|d| \le 4$. Da d quadratfrei ist, erhält man $d \in \{-1, -2, -3\}$. Im Fall $d = -1$ sind $a, b \in \mathbb{Z}$ und es folgt $a, b \in \{\pm 1\}$. Im Fall $d = -2$ ist $b \in \mathbb{Z}$ und damit $b = 0$. Sei schließlich $d = -3$ und $a = a_1/2$ sowie $b = b_1/2$ mit $a_1, b_1 \in \mathbb{Z}$. Aus $a_1^2 + 3b_1^2 = 1$ folgt $a_1, b_1 \in \{\pm 1\}$. Dies ergibt die angegebenen sechs Elemente. Es handelt sich um die Gruppe der sechsten Einheitswurzeln, die von $\frac{1+\sqrt{-3}}{2}$ erzeugt wird.

Sei jetzt $d > 1$. Nach der Pellschen Gleichung existieren unendlich viele $a, b \in \mathbb{Z}$ mit $a^2 - b^2 d = 1$. Die Behauptung folgt daher aus Lemma 6.9. $\square$

Definition 6.11. Sei $R \subseteq \mathbb{C}$ ein Teilring.

- Für $a, b \in R$ schreiben wir (wie üblich) $a \mid b$, falls ein $c \in R$ mit $ac = b$ existiert. Man sagt dann: a *teilt* b, a ist ein *Teiler* von b usw. Außerdem sei $a \equiv b \pmod{c}$, falls $c \mid a - b$. Die Menge der Vielfachen von a sei $Ra = \{ra : r \in R\}$. Die *Restklassen* nach a haben die Form $b + Ra$.
- Wie in Definition 1.9 definiert man die Menge der gemeinsamen Teiler $\mathrm{gT}(a, b)$ für $a, b \in R$. Besteht $\mathrm{gT}(a, b)$ nur aus invertierbaren Elementen, so nennt man a und b *teilerfremd*. Man nennt $g \in \mathrm{gT}(a, b)$ einen *größten gemeinsamen Teiler* von a, b, falls $x \mid g$ für alle $x \in \mathrm{gT}(a, b)$ gilt.
- Man nennt $a, b \in R$ *assoziiert*, falls $a \mid b \mid a$ gilt.
- Man nennt $p \in R \setminus (R^\times \cup \{0\})$ ein *Primelement*, falls für alle $a, b \in R$ gilt: $p \mid ab \Rightarrow p \mid a \vee p \mid b$ (vgl. Lemma 2.3).

Bemerkung 6.12.

(i) Für $a, b, c, d, e \in R \subseteq \mathbb{C}$ gelten die üblichen Rechenregeln:
  - $\pm 1 \mid a \mid 0$,
  - $0 \mid a \iff a = 0$,
  - $a \mid b \mid c \implies a \mid c$,
  - $a \mid b, c \implies a \mid (bd + ce)$.

(ii) Die Assoziiertheit ist eine Äquivalenzrelation auf R. Sind $a, b \in R$ assoziiert, so existieren $r, s \in R$ mit $ar = b$ und $bs = a$. Es folgt $a(1 - rs) = a - ars = a - bs = a - a = 0$. Im Fall $a = 0$ ist auch $b = 0$. Anderenfalls ist $rs = 1$ und $r \in R^\times$. Gilt umgekehrt $ar = b$ mit $r \in R^\times$, so auch $br^{-1} = a$ und man erhält $a \mid b \mid a$. Also sind a, b genau dann assoziiert, wenn ein $r \in R^\times$ mit $ar = b$ existiert.

(iii) Im Gegensatz zu $\mathbb{Z}$ existieren größte gemeinsame Teiler nicht immer und selbst wenn sie existieren, sind sie nur bis auf Assoziiertheit eindeutig bestimmt (in $\mathbb{Z}$ hatten wir zusätzlich $\mathrm{ggT} \ge 0$ gefordert, was in $\mathbb{C}$ keinen Sinn ergibt).

(iv) Das nächste Lemma rechtfertigt die Bezeichnung „Primelement“.

Lemma 6.13. *Sei $R \subseteq \mathbb{C}$ ein Teilring und $p \in R$ ein Primelement. Existieren $a, b \in R$ mit $p = ab$, so ist $a \in R^\times$ oder $b \in R^\times$.*

Beweis. Nach Definition ist p ein Teiler von a oder b, sagen wir $p \mid a$. Wegen $a \mid p$ sind a und p assoziiert. Nach Bemerkung 6.12 existiert $r \in R^\times$ mit $p = ar$. Es folgt $a(b-r) = 0$. Wegen $p \neq 0 \neq a$ gilt $b = r \in R^\times$. □

Lemma 6.14. *Sei $R \subseteq \mathbb{C}$ ein Teilring. Seien $p_1, \ldots, p_s, q_1, \ldots, q_t \in R$ Primelemente mit $p_1 \ldots p_s = q_1 \ldots q_t$. Dann ist $s = t$ und bei geeigneter Nummerierung ist p_i zu q_i assoziiert für $i = 1, \ldots, s$.*

Beweis. Induktion nach s: Im Fall $s = 0$ ist $q_1 \ldots q_t = 1$ und $q_1 \in R^\times$. Da Primelemente nicht invertierbar sind, gilt $t = 0$. Sei nun $s \geq 1$ und die Behauptung für $s - 1$ bereits bewiesen. Aus $p_s \mid p_1 \ldots p_s = q_1 \ldots q_t$ folgt $p_s \mid q_i$ für ein $i \in \{1, \ldots, t\}$, sagen wir $i = t$. Sei also $e \in R$ mit $p_s e = q_t$. Nach Lemma 6.13 gilt $e \in R^\times$. Insbesondere sind p_s und q_t assoziiert. Es folgt

$$(p_1 \ldots p_{s-1} - q_1 \ldots q_{t-1} e) p_s = p_1 \ldots p_s - q_1 \ldots q_t = 0.$$

Wegen $p_s \neq 0$ ist $p_1 \ldots p_{s-1} = q_1 \ldots (q_{t-1} e)$. Nach Induktion ist $s = t$ und bei geeigneter Nummerierung ist p_i zu q_i bzw. zu $q_{t-1} e$ assoziiert für $i = 1, \ldots, s-1$. Dies zeigt die Behauptung. □

Definition 6.15. Ein Teilring $R \subseteq \mathbb{C}$ heißt

- *faktoriell*[10], falls jedes Element aus $R \setminus (R^\times \cup \{0\})$ ein Produkt von Primelementen ist.
- *euklidisch*, falls eine Abbildung $H \colon R \to \mathbb{N}_0$ mit folgender Eigenschaft existiert: Für alle $a, b \in R$ mit $b \neq 0$ existieren $q, r \in R$ mit $a = qb + r$ und $H(r) < H(b)$ (Division mit Rest).

Bemerkung 6.16.

(i) Sei $R \subseteq \mathbb{C}$ faktoriell und $P \subseteq R$ ein Repräsentantensystem für die Äquivalenzklassen assoziierter Primelemente (zum Beispiel die Primzahlen in $R = \mathbb{Z}$). Nach Lemma 6.14 besitzt jedes $x \in R \setminus \{0\}$ eine eindeutige *Primfaktorzerlegung*

$$x = e \prod_{p \in P} p^{\nu_p(x)}$$

mit $e \in R^\times$ und $\nu_p(x) \in \mathbb{N}_0$ für $p \in P$. Für $x, y \in R \setminus \{0\}$ gilt $x \mid y$ genau dann, wenn $\nu_p(x) \leq \nu_p(y)$ für alle $p \in P$. Für $x_1, \ldots, x_n \in R \setminus \{0\}$ setzt man

$$\operatorname{ggT}(x_1, \ldots, x_n) := \prod_{p \in P} p^{\min\{\nu_p(x_1), \ldots, \nu_p(x_n)\}},$$
$$\operatorname{kgV}(x_1, \ldots, x_n) := \prod_{p \in P} p^{\max\{\nu_p(x_1), \ldots, \nu_p(x_n)\}}.$$

(ii) In jedem euklidischen Ring $R \subseteq \mathbb{C}$ lässt sich ein größter gemeinsamer Teiler für $a, b \in R \setminus \{0\}$ mit dem erweiterten euklidischen Algorithmus bestimmen:

- Setze $(x_0, y_0, z_0) := (1, 0, a)$, $(x_1, y_1, z_1) := (0, 1, b)$ und $k := 0$.
- Solange $z_{k+1} \neq 0$ wiederhole:

$$(x_{k+2}, y_{k+2}, z_{k+2}) := (x_k - x_{k+1} q_{k+1}, y_k - y_{k+1} q_{k+1}, r_{k+1}),$$

  wobei $z_k = q_{k+1} z_{k+1} + r_{k+1}$ mit $H(r_{k+1}) < H(z_{k+1})$.

[10] oder *ZPE-Ring* (**Z**erlegung **P**rimelemente **e**indeutig) bzw. im Englischen *UFD* (unique factorization domain)

- Für $z_{k+1} = 0$ ist $z_k = x_k a + y_k b$ ein ggT von a und b.

Wegen $H(r_{k+1}) < H(z_{k+1})$ gilt $z_{k+1} = 0$ nach endlich vielen Schritten. Wie in Satz 1.11 zeigt man $\mathrm{gT}(a,b) = \mathrm{gT}(z_k, 0)$. Allerdings ist nicht klar, wie man in der Praxis die Division mit Rest ausführt.

Lemma 6.17. *In jedem euklidischen Ring $R \subseteq \mathbb{C}$ kann man die Funktion H so wählen, dass für alle $a, b \in R$ mit $b \neq 0$ gilt:*

(i) $H(a) \le H(ab)$.

(ii) *Ist $a \neq 0$, so gilt $H(a) = H(ab) \iff b \in R^\times$.*

(iii) $H(a) = H(1) \iff a \in R^\times$.

Beweis. Sei
$$H'(a) := \min_{b \in R \setminus \{0\}} H(ab)$$
für $a \in R$. Dann gilt $H'(a) \le H(a1) = H(a)$. Für $a, b \in R$ mit $b \neq 0$ existiert ein $c \in R \setminus \{0\}$ mit $H'(b) = H(bc)$. Wegen $bc \neq 0$ existieren $q, r \in R$ mit $a = qbc + r$ und $H'(r) \le H(r) < H(bc) = H'(b)$. Für $q' = qc$ gilt also $a = q'b + r$ und $H'(r) < H'(b)$. Also ist R bzgl. H' euklidisch.

(i) Sei $c \in R$ mit $H'(ab) = H(abc)$. Dann gilt $H'(a) \le H(a(bc)) = H'(ab)$.

(ii) Ist $b \in R^\times$, so folgt $H'(a) \le H'(ab) \le H'(abb^{-1}) = H'(a)$ aus (i). Sei umgekehrt $H'(a) = H'(ab)$. Division mit Rest liefert $q, r \in R$ mit $a = q(ab) + r$ und $H'(r) < H'(ab)$. Also ist $H'(a(1 - qb)) = H'(r) < H'(a)$ und $qb = 1$ nach (i). Dies zeigt $b \in R^\times$.

(iii) Folgt aus (ii) mit $a = 1$. □

Satz 6.18. *Euklidische Ringe sind faktoriell.*

Beweis. Sei R euklidisch mit H wie in Lemma 6.17. Wir zeigen durch Induktion nach $H(x)$, dass jedes $x \in R \setminus (R^\times \cup \{0\})$ ein Produkt von Primelementen ist. Sei $p \in R \setminus R^\times$ ein Teiler von x, sodass $H(p)$ möglichst klein ist (notfalls $p = x$). Seien $a, b \in R$ mit $p \mid ab$. Angenommen p ist zu a und zu b teilerfremd. Nach dem erweiterten euklidischen Algorithmus existieren $\alpha, \beta, \gamma, \delta \in R$ mit $\alpha p + \beta a = 1 = \gamma p + \delta b$. Dann wäre aber
$$p \mid \beta\delta ab + \beta\gamma ap + \alpha\delta bp + \alpha\gamma p^2 = (\alpha p + \beta a)(\gamma p + \delta b) = 1.$$
Sei also o. B. d. A. $q \in \mathrm{gT}(a, p) \setminus R^\times$. Aus $q \mid p \mid x$ folgt $H(q) = H(p)$. Nach Lemma 6.17 sind p und q assoziiert und daher $p \mid q \mid a$. Dies zeigt, dass p ein Primelement ist. Sei $y \in R$ mit $x = py$. Nach Lemma 6.17 gilt $H(y) < H(x)$. Nach Induktion ist y ein Produkt von Primelementen und somit auch x. □

Lemma 6.19. *Sei $d \in \mathbb{Z} \setminus \{0, 1\}$ quadratfrei. Existiert für jedes $x \in \mathbb{Q}(\sqrt{d})$ ein $a \in \mathbb{Z}_d$ mit $|N(x - a)| < 1$, so ist R euklidisch.*

Beweis. Sei $R := \mathbb{Z}_d$ und $H(a) := |N(a)|$ für $a \in R$. Für $a, b \in R$ mit $b \neq 0$ existiert $q \in R$ mit $|N(\frac{a}{b} - q)| < 1$. Mit $r := a - bq \in R$ folgt
$$H(r) = |N(a - bq)| = |N(b)| \Big| N\Big(\frac{a}{b} - q\Big) \Big| < |N(b)| = H(b).$$ □

Satz 6.20. *Für $d \in \{-11,-7,-3,-2,-1,2,3,5,6,7,13,17,21,29\}$ ist $\mathbb{Z}_d$ euklidisch.*

Beweis. Wir wenden Lemma 6.19 an. Sei $x+y\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ mit $x, y \in \mathbb{Q}$ gegeben. Für $d \in \{-2,-1,2,3\}$ wählen wir $a, b \in \mathbb{Z}$ mit $|x-a|, |y-b| \le \frac{1}{2}$. Dann gilt

$$\left|N\big((x+y\sqrt{d})-(a+b\sqrt{d})\big)\right| = \left|(x-a)^2 - d(y-b)^2\right| \le \frac{1}{4}\big(|d|+1\big)$$

und die Behauptung folgt (für $d = 3$ ist die Ungleichung strikt). Sei nun $d \in \{-11,-7,-3,5\}$. Dann kann man a, b mit

$$\left|N\Big(\Big(x+y\sqrt{d}\Big)-\Big(a+b\frac{1+\sqrt{d}}{2}\Big)\Big)\right| = \left|\Big(x-a-\frac{b}{2}\Big)^2 - d\Big(y-\frac{b}{2}\Big)^2\right| \le \frac{1}{4}+\frac{|d|}{16} < 1$$

wählen. Für die restlichen Werte benötigen wir eine Fallunterscheidung:

(i) $d \in \{6,7\}$: Sei

$$\begin{aligned} |x-a| &\le \frac{1}{2} && \text{falls} && |y-b|^2 < \frac{1}{d}, \\ \frac{1}{2} \le |x-a| &\le 1 && \text{falls} && \frac{1}{d} < |y-b|^2 < \frac{5}{4d}, \\ 1 \le |x-a| &\le \frac{3}{2} && \text{falls} && \frac{5}{4d} < |y-b|^2 \le \frac{1}{4}. \end{aligned}$$

Dann gilt

$$|(x-a)^2 - d(y-b)^2| < \begin{cases} d\frac{1}{d} = 1 & \text{falls } |y-b|^2 < \frac{1}{d}, \\ \frac{5}{4} - \frac{1}{4} = 1 & \text{falls } \frac{1}{d} < |y-b|^2 < \frac{5}{4d}, \\ \frac{9}{4} - \frac{5}{4} = 1 & \text{falls } \frac{5}{4d} < |y-b|^2 \le \frac{1}{4}. \end{cases}$$

(ii) $d \in \{13,17,21,29\}$: Anstelle von $|x-a|$ und $|y-b|$ kann man hier $|x-a-\frac{b}{2}|$ und $|y-\frac{b}{2}|$ wie im Fall $d \in \{6,7\}$ wählen. Die Abschätzungen gelten dann genauso, da man zusätzlich $|y-\frac{b}{2}| \le \frac{1}{4}$ erreichen kann. □

Beispiel 6.21.

(i) Wir zeigen, dass $\mathbb{Z}_{-5} = \mathbb{Z} + \sqrt{-5}\mathbb{Z}$ nicht faktoriell ist (und damit auch nicht euklidisch). Es gilt $2 \mid 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$. Wegen $N(2) = 4$ und $N(1 \pm \sqrt{-5}) = 6$ kann 2 nicht $1 \pm \sqrt{-5}$ teilen. Daher ist 2 kein Primelement. Nehmen wir an, es gibt eine Faktorisierung $2 = xy$ mit $x, y \in \mathbb{Z}_{-5}$. Wegen $N(a+b\sqrt{-5}) = a^2 + 5b^2 \ne 2$ für alle $a, b \in \mathbb{Z}$ muss $N(x) = 1$ oder $N(y) = 1$ gelten. Also ist $x \in \mathbb{Z}_{-5}^\times$ oder $y \in \mathbb{Z}_{-5}^\times$. Dies zeigt, dass sich 2 nicht als Produkt von Primelementen schreiben lässt.

(ii) Man kann zeigen, dass $\mathbb{Z}_d$ bzgl. $H(a) = |N(a)|$ genau dann euklidisch ist, falls

$$d \in \{-11,-7,-3,-2,-1,2,3,5,6,7,11,13,17,19,21,29,33,37,41,57,73\}.$$

Für $d < 0$ gibt es generell keine weiteren euklidischen Ringe $\mathbb{Z}_d$. Andererseits sind $\mathbb{Z}_{14}$ und $\mathbb{Z}_{69}$ euklidisch und man vermutet, dass es unendlich viele weitere euklidische Ringe mit $d > 0$ gibt.

(iii) Heegner gezeigt, dass $\mathbb{Z}_d$ für negative d genau dann faktoriell ist, falls

$$-d \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$$

(*Heegner-Zahlen*). Insbesondere gibt es faktorielle Ringe, die nicht euklidisch sind. Damit lässt sich begründen, warum

$$e^{\pi\sqrt{163}} = 262537412640768743{,}99999999999925\ldots$$

fast eine ganze Zahl ist (ohne Beweis).

(iv) Man nennt $x \in \mathbb{C}$ *algebraisch*, falls x Nullstelle eines nicht-konstanten Polynoms mit Koeffizienten in $\mathbb{Q}$ ist. Da sich diese Polynome abzählen lassen, existieren nur abzählbar viele algebraische Zahlen. Es gibt daher überabzählbar viele Zahlen, die nicht algebraisch sind. Sie nennt man *transzendent*. Nach dem Satz von Lindemann ist $\pi \approx 3{,}14$ transzendent.[11] Für eine transzendente Zahl $x \in \mathbb{C}$ erhält man nach Aufgabe 40 einen euklidischen Ring

$$\mathbb{Z}[x] := \Big\{\sum_{i=0}^{n} a_i x^i : n \in \mathbb{N}, a_0, \ldots, a_n \in \mathbb{Z}\Big\}.$$

Satz 6.22. *Für jedes Primelement $\pi \in \mathbb{Z}_{-1}$ gilt genau eine der folgenden Aussagen:*

(i) *π ist zu $1 + \mathrm{i}$ assoziiert.*

(ii) *π ist zu einer Primzahl $p \equiv 3 \pmod 4$ assoziiert.*

(iii) *$\pi\overline{\pi} = p \equiv 1 \pmod 4$ für eine Primzahl p und π ist nicht zu $\overline{\pi}$ assoziiert.*

Beweis. Sei $R := \mathbb{Z}_{-1}$. Wegen $\pi \notin R^\times$ ist $\pi \mid \pi\overline{\pi} = |\pi|^2 \geq 2$. Daher teilt π einen Primteiler p von $|\pi|^2$. Teilt π auch $q \in \mathbb{P} \setminus \{p\}$, so teilt π auch $\mathrm{ggT}(p, q) = 1$ und man erhält den Widerspruch $\pi \in R^\times$. Also ist p die einzige durch π teilbare Primzahl. Man kann somit die Primelemente in R bestimmen, indem man die Primzahlen in Primelemente zerlegt. Jedes $\pi \in R$ mit $|\pi|^2 \in \mathbb{P}$ ist wegen Lemma 6.13 ein Primelement in R. Insbesondere ist $1 + \mathrm{i} \in R$ ein Primelement und $2 = -\mathrm{i}(1 + \mathrm{i})^2$ ist die Primfaktorzerlegung von 2 (man sagt: 2 ist *verzweigt*).

Sei nun $p \equiv 3 \pmod 4$ und $\sigma, \tau \in R$ mit $p = \sigma\tau$. Dann ist

$$|\sigma\tau|^2 = p^2. \tag{6.1}$$

Wegen $a^2 + b^2 \not\equiv 3 \pmod 4$ für alle $a, b \in \mathbb{Z}$ hat die Gleichung $a^2 + b^2 = p$ keine ganzzahligen Lösungen. Daher ist σ oder τ invertierbar und p ein Primelement in R (man sagt: p ist *träge*).

Sei schließlich $p \equiv 1 \pmod 4$ und $q := (p - 1)/2 \in 2\mathbb{Z}$. Nach Wilson (Aufgabe 22) ist

$$-1 \equiv (p-1)! \equiv \prod_{k=1}^{q} k(p-k) \equiv (-1)^q (q!)^2 \equiv (q!)^2 \pmod p.$$

Dies zeigt $p \mid (q!)^2 + 1 = (q! - \mathrm{i})(q! + \mathrm{i})$. Wäre p ein Primelement in R, so wäre $p = \bar{p} \mid q! \pm \mathrm{i}$ und

$$0 \not\equiv 2q! = (q! + \mathrm{i}) + (q! - \mathrm{i}) \equiv 0 \pmod p.$$

Also ist p kein Primelement und nach (6.1) existiert ein Primteiler $\pi \mid p$ mit $\pi\overline{\pi} = p$. O. B. d. A. sei $\pi \mid q! + \mathrm{i}$. Angenommen π und $\overline{\pi}$ sind assoziiert. Dann wären π und $\overline{\pi}$ Teiler von $q! \pm \mathrm{i}$ und daher auch Teiler von $2 = \mathrm{i}((q! - \mathrm{i}) - (q! + \mathrm{i}))$. Wir wissen aber bereits, dass jedes Primelement nur eine Primzahl teilt. Daher sind π und $\overline{\pi}$ nicht assoziiert (man sagt: p ist *zerlegt*). $\square$

[11] Siehe Anhang in Algebra-Skript

Satz 6.23 (Girard)**.** *Genau dann lässt sich $n \in \mathbb{N}$ als Summe von zwei ganzzahligen Quadraten schreiben, wenn die Vielfachheit jeder Primzahl $p \equiv 3 \pmod 4$ in der Primfaktorzerlegung von n gerade ist. Insbesondere ist jede Primzahl $p \equiv 1 \pmod 4$ Summe zweier Quadrate.*

Beweis (Dedekind).

$\Rightarrow$: Sei $n = a^2+b^2 = (a+b\mathrm{i})(a-b\mathrm{i})$ mit $a, b \in \mathbb{Z}$. Nach Satz 6.22 erhält man die Primfaktorzerlegung von $a + b\mathrm{i} \in \mathbb{Z}_{-1}$ wie folgt

$$a+b\mathrm{i} = e(1+\mathrm{i})^{\delta_2} \prod_{\substack{p\in\mathbb{P} \\ p\equiv 3 \pmod 4}} p^{\delta_p} \prod_{\substack{p\in\mathbb{P} \\ p\equiv 1 \pmod 4}} \pi_p^{\delta_p}\overline{\pi_p}^{\delta'_p}$$

mit $e \in \{\pm 1, \pm\mathrm{i}\}$ und $\delta_2, \delta_p, \delta'_p \in \mathbb{N}_0$. Daher ist

$$n = |a+b\mathrm{i}|^2 = 2^{\delta_2} \prod_{\substack{p\in\mathbb{P} \\ p\equiv 3 \pmod 4}} p^{2\delta_p} \prod_{\substack{p\in\mathbb{P} \\ p\equiv 1 \pmod 4}} p^{\delta_p+\delta'_p}$$

die Primfaktorzerlegung von n.

$\Leftarrow$: Nach Voraussetzung ist

$$n = 2^{\delta_2} \prod_{\substack{p\in\mathbb{P} \\ p\equiv 3 \pmod 4}} p^{2\delta_p} \prod_{\substack{p\in\mathbb{P} \\ p\equiv 1 \pmod 4}} p^{\delta_p} = |\alpha|^2$$

mit

$$\alpha = (1+\mathrm{i})^{\delta_2} \prod_{\substack{p\in\mathbb{P} \\ p\equiv 3 \pmod 4}} p^{\delta_p} \prod_{\substack{p\in\mathbb{P} \\ p\equiv 1 \pmod 4}} \pi_p^{\delta_p} \in \mathbb{Z}_{-1}.$$

Daher existieren $a, b \in \mathbb{Z}$ mit $\alpha = a + b\mathrm{i}$ und $a^2 + b^2 = |\alpha|^2 = n$. $\square$

Lemma 6.24. *Sei p eine Primzahl und $a \in \mathbb{F}_p$. Dann existieren $x, y \in \mathbb{F}_p$ mit $x^2 + y^2 = a$.*

Beweis. Für $p = 2$ wählt man $x := a$ und $y := 0$. Sei also p ungerade und $q := (p-1)/2$. Für $0 \le k, l \le q$ gilt

$$k^2 \equiv l^2 \pmod p \iff (k+l)(k-l) \equiv 0 \pmod p \iff k \equiv \pm k \pmod p \iff k = l,$$

da $\mathbb{F}_p$ ein Körper ist. Man hat also $q + 1$ paarweise verschiedene Reste modulo p. Analog sind auch $a - k^2$ für $k = 0, \dots, q$ paarweise verschieden modulo p. Wegen $2(q+1) = p+1 > p$ existieren $x, y \in \mathbb{Z}$ mit $x^2 \equiv a - y^2 \pmod p$ nach dem Schubfachprinzip. Also gilt $x^2 + y^2 = a$ in $\mathbb{F}_p$. $\square$

Satz 6.25 (Lagranges 4-Quadrate-Satz)**.** *Jede natürliche Zahl ist die Summe von (höchstens) vier Quadratzahlen.*

Beweis. Indem wir $0 = 0^2$ als Quadratzahl zulassen, können wir zeigen, dass jedes $n \in \mathbb{N}$ die Summe von (genau) vier Quadratzahlen ist. O. B. d. A. sei $n \ge 3$. Sei p ein Primteiler von n. Im Fall $p < n$ können wir durch Induktion nach n annehmen, dass p und n/p Summen von vier Quadraten sind. Wegen der *eulerschen Identität*

$$\begin{aligned} &(a_1^2+a_2^2+a_3^2+a_4^2)(b_1^2+b_2^2+b_3^2+b_4^2) = (a_1b_1+a_2b_2+a_3b_3+a_4b_4)^2 \\ &+(a_1b_2-a_2b_1+a_3b_4-a_4b_3)^2 + (a_1b_3-a_3b_1+a_4b_2-a_2b_4)^2 + (a_1b_4-a_4b_1+a_2b_3-a_3b_2)^2 \end{aligned} \tag{6.2}$$

ist dann auch n eine Summe von vier Quadraten. Sei also $n = p \in \mathbb{P}$. Nach Satz 6.23 dürfen wir $p \equiv 3 \pmod 4$ voraussetzen. Nach Lemma 6.24 existieren $x, y \in \mathbb{Z}$ mit $x^2 + y^2 \equiv 0 \pmod p$. Indem man x bzw. y notfalls durch $-x$ bzw. $-y$ ersetzt, kann man $0 \le x, y \le \frac{p-1}{2}$ annehmen. Dann gilt $x^2 + y^2 < \frac{p^2}{2} < p^2$. Insbesondere ist die Gleichung $x_1^2 + x_2^2 + x_3^2 + x_4^2 = hp$ für ein $h < p$ lösbar. Sei h minimal mit dieser Eigenschaft. Nehmen wir $h > 1$ an. Sei zunächst h gerade. Dann ist die Anzahl der ungeraden Quadrate x_i^2 gerade (möglicherweise 0). Bei geeigneter Nummerierung gilt $2 \mid x_1 \pm x_2$ und $2 \mid x_3 \pm x_4$. Es folgt

$$\Big(\frac{x_1 + x_2}{2}\Big)^2 + \Big(\frac{x_1 - x_2}{2}\Big)^2 + \Big(\frac{x_3 + x_4}{2}\Big)^2 + \Big(\frac{x_3 - x_4}{2}\Big)^2 = \frac{1}{2}\big(x_1^2 + x_2^2 + x_3^2 + x_4^2\big) = \frac{h}{2}p$$

im Widerspruch zur Wahl von h. Also ist $h \ge 3$ ungerade. Seien $y_1, \ldots, y_4 \in \mathbb{Z}$ mit $y_i \equiv x_i \pmod h$ und $|y_i| \le \frac{h-1}{2}$ für $i = 1, \ldots, 4$. Im Fall $(y_1, \ldots, y_4) = (0, \ldots, 0)$ ist $h^2 \mid x_1^2 + \ldots + x_4^2 = hp$ und $h \mid p$. Dann wäre aber $h \ge p$. Also gilt $0 < y_1^2 + \ldots + y_4^2 < h^2$ und $y_1^2 + \ldots + y_4^2 \equiv x_1^2 + \ldots + x_4^2 \equiv 0 \pmod h$. Also existiert ein $1 \le k < h$ mit $y_1^2 + \ldots + y_4^2 = kh$. Wegen (6.2) gilt $hp \cdot kh = z_1^2 + \ldots + z_4^2$ mit

$$\begin{aligned}
z_1 &= x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv hp \equiv 0 \pmod h,\\
z_2 &= x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3 \equiv x_1x_2 - x_2x_1 + x_3x_4 - x_4x_3 \equiv 0 \pmod h,\\
z_3 &= x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4 \equiv x_1x_3 - x_3x_1 + x_4x_2 - x_2x_4 \equiv 0 \pmod h,\\
z_4 &= x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2 \equiv x_1x_4 - x_4x_1 + x_2x_3 - x_3x_2 \equiv 0 \pmod h.
\end{aligned}$$

Damit erhält man $kp = \big(\frac{z_1}{h}\big)^2 + \ldots + \big(\frac{z_4}{h}\big)^2$ im Widerspruch zur Wahl von h. □

Bemerkung 6.26. Es gibt einige verwandte Quadrat-Sätze, die wir ohne Beweis angeben:

(i) (LEGENDRES 3-*Quadrate-Satz*) Genau dann ist $n \in \mathbb{N}$ eine Summe von drei Quadraten, wenn n *nicht* die Form $4^a(8b + 7)$ mit $a, b \in \mathbb{N}_0$ hat. Zum Beispiel ist 7 nicht die Summe von drei Quadraten. Eine Beweisrichtung ist leicht (Aufgabe 43), aber die andere Richtung ist schwieriger als der 4-Quadrate-Satz.

(ii) (WARING-Problem) Für jedes $k \in \mathbb{N}$ existiert ein $w_k \in \mathbb{N}$, sodass jede natürliche Zahl die Summe von höchstens w_k nicht-negativen k-ten Potenzen ist. Nach dem 4-Quadrate-Satz kann man $w_2 = 4$ wählen. Außerdem gilt $w_3 = 9$, $w_4 = 19$ und allgemein wird vermutet, dass

$$w_k = \Big\lfloor \frac{3^k}{2^k} \Big\rfloor + 2^k - 2$$

für $k \ge 2$ das kleinste w_k ist (vgl. Aufgabe 38). Man vermutet, dass jede natürliche Zahl die Summe von vier *ganzzahligen* Kubikzahlen ist. Darüber hinaus wird vermutet, dass bis auf endlich viele Ausnahmen jede natürliche Zahl die Summe von vier nicht-negativen Kubikzahlen ist.

(iii) (MORDELL-Problem) Jede Zahl $n \equiv 4, 5 \pmod 9$ ist nicht die Summe von drei ganzzahligen Kubikzahlen, denn $a^3 \equiv -1, 0, 1 \pmod 9$. Man weiß nicht, ob alle anderen Zahlen die Summe von drei Kubikzahlen sind. Dies hat man bis $n \le 113$ überprüft. Der letzte ausstehende Fall $n = 42$ wurde 2019 gelöst:

$$42 = (-80538738812075974)^3 + 80435758145817515^3 + 12602123297335631^3.$$

(iv) Aus dem Beweis von Satz 6.23 und der eindeutigen Primfaktorzerlegung in $\mathbb{Z}_{-1}$ folgt, dass sich jede Primzahl $p \equiv 1 \pmod 4$ nur auf eine Weise als Summe von Quadraten schreiben lässt (bis auf Reihenfolge der Quadrate). Die Anzahl der möglichen Zerlegungen einer natürlichen Zahl n als Summe von vier Quadraten ist durch JACOBIs *Formel*

$$\left|\{(a,b,c,d) \in \mathbb{Z}^4 : a^2+b^2+c^2+d^2=n\}\right| = 8 \sum_{4 \nmid d \mid n} d$$

gegeben. Für $n = 28$ erhält man

$$\sum_{4 \nmid d \mid 28} d = 1+2+7+14 = 24.$$

Also gibt es $8 \cdot 24 = 192$ Möglichkeiten 28 als Summe von vier Quadraten zu schreiben. Allerdings entstehen all diese Möglichkeiten durch Permutation von Vorzeichenwahl aus

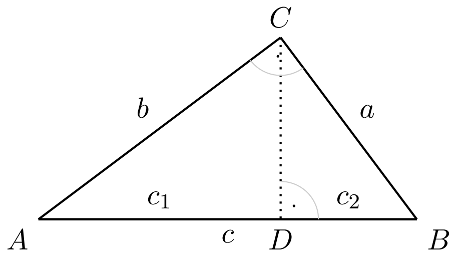
$$28 = 5^2+1^2+1^2+1^2 = 4^2+2^2+2^2+2^2 = 3^2+3^2+3^2+1^2.$$

7 Fermats letzter Satz

Bemerkung 7.1. Wir besprechen in diesem Kapitel zwei Spezialfälle des berühmten letzten Satz von Fermat. Dabei spielt der euklidische Ring der Eisenstein-Zahlen $\mathbb{Z}_{-3}$ eine Rolle.

Satz 7.2 (PYTHAGORAS)**.** *Ein Dreieck mit den Seitenlängen a, b und c ist genau dann rechtwinklig, wenn (bei geeigneter Beschriftung) $a^2 + b^2 = c^2$ gilt.*

Beweis. Alle Beweise setzen gewisse geometrische Postulate voraus, die auf EUKLIDs *Elemente* zurückgehen. Sei ABC ein rechtwinkliges Dreieck mit den Seiten a, b, c:



Die Dreiecke ABC und ADC haben neben dem rechten Winkel auch den Winkel an A gemeinsam. Sie sind daher ähnlich. Analog sind auch ABC und DBC ähnlich. Für die Seitenlängen gilt daher $\frac{a}{c} = \frac{c_2}{a}$ und $\frac{b}{c} = \frac{c_1}{b}$. Es folgt

$$a^2 + b^2 = cc_2 + cc_1 = c(c_1 + c_2) = c^2.$$

Seien nun a, b, c die Seitenlängen eines beliebigen Dreiecks Δ, sodass $a^2 + b^2 = c^2$ gilt. Sicher existiert ein rechtwinkliges Dreieck Δ' mit den Seitenlängen a, b, c', wobei c' die größte Seite ist. Nach dem ersten Teil des Beweises gilt $(c')^2 = a^2 + b^2 = c^2$ und somit $c' = c$. Also sind Δ und Δ' kongruent. Mit Δ' ist auch Δ rechtwinklig. $\square$

Definition 7.3. Man nennt $(a, b, c) \in \mathbb{N}^3$ ein *pythagoreisches Tripel*, falls $a^2 + b^2 = c^2$.

Satz 7.4 (Euklid). *Jedes pythagoreische Tripel hat die Form*

$$d(2st, t^2 - s^2, t^2 + s^2) \qquad \text{bzw.} \qquad d(t^2 - s^2, 2st, t^2 + s^2)$$

wobei $d, s, t \in \mathbb{N}$ mit $s < t$. Umgekehrt liefert jede Wahl dieser Parameter ein pythagoreisches Tripel. Insbesondere gibt es unendlich viele pythagoreische Tripel.

Beweis. Sei (a, b, c) ein pythagoreisches Tripel und $d := \operatorname{ggT}(a, b)$. Dann ist d^2 ein Teiler von $a^2 + b^2 = c^2$. Nach der eindeutigen Primfaktorzerlegung ist d ein Teiler von c. Folglich ist auch $\frac{1}{d}(a, b, c)$ ein pythagoreisches Tripel. Wir können daher $\operatorname{ggT}(a, b) = 1$ annehmen. Insbesondere ist a oder b ungerade. Sind beide ungerade, so ergibt sich der Widerspruch $c^2 = a^2 + b^2 \equiv 2 \pmod 4$. O. B. d. A. sei also $a = 2k$ und b ungerade. Dann ist auch c ungerade und man erhält

$$\frac{c+b}{2}\frac{c-b}{2} = \frac{c^2 - b^2}{4} = \frac{a^2}{4} = k^2. \tag{7.1}$$

Sei $e \in \mathbb{N}$ ein gemeinsamer Teiler von $\frac{c+b}{2}$ und $\frac{c-b}{2}$. Dann teilt e auch $\frac{c+b}{2} + \frac{c-b}{2} = c$ sowie $\frac{c+b}{2} - \frac{c-b}{2} = b$. Folglich teilt e^2 auch $c^2 - b^2 = a^2$. Wegen $\operatorname{ggT}(a, b) = 1$ ist daher $e = 1$, d. h. $\frac{c+b}{2}$ und $\frac{c-b}{2}$ sind teilerfremd. Jeder Primfaktor von k teilt also entweder den ersten oder den zweiten Faktor in (7.1). Dies liefert $s, t \in \mathbb{N}$ mit $s < t$ und

$$\frac{c+b}{2} = t^2, \qquad \frac{c-b}{2} = s^2, \qquad st = k.$$

Wir berechnen

$$\begin{aligned} a &= 2k = 2st, \\ b &= \frac{c+b}{2} - \frac{c-b}{2} = t^2 - s^2, \\ c &= \frac{c+b}{2} + \frac{c-b}{2} = t^2 + s^2. \end{aligned}$$

Sind umgekehrt $d, s, t \in \mathbb{N}$ mit $s < t$ gegeben, so ist $(a, b, c) := d(2st, t^2 - s^2, t^2 + s^2) \in \mathbb{N}^3$ mit

$$a^2 + b^2 = d^2(4s^2t^2 + (t^2 - s^2)^2) = d^2(t^4 + 2s^2t^2 + s^4) = d^2(t^2 + s^2)^2 = c^2. \qquad \square$$

Beispiel 7.5. Für $(d, s, t) \in \{(1, 1, 2), (1, 2, 3)\}$ erhält man die pythagoreischen Tripel $(3, 4, 5)$ und $(5, 12, 13)$. Für $(d, s, t) \in \{(1, 1, 3), (2, 1, 2)\}$ erhält man jeweils $(6, 8, 10)$. Man kann die Zahlen d, s, t in Satz 7.4 eindeutig machen, indem man zusätzlich $\operatorname{ggT}(s, t) = 1$ und $s \not\equiv t \pmod 2$ fordert.

Satz 7.6 (Fermats „letzter“ Satz). *Für $n \geq 3$ existiert kein Tripel $(a, b, c) \in \mathbb{N}^3$ mit $a^n + b^n = c^n$.*

Bemerkung 7.7.

(i) Angenommen $a, b, c \in \mathbb{Z}$ erfüllen $a^n + b^n = c^n$. Ist n gerade oder $a, b, c < 0$, so gilt auch $|a|^n + |b|^n = |c|^n$. In allen anderen Fällen kann man notfalls c mit a oder b vertauschen, um $|a|^n + |b|^n = |c|^n$ zu erreichen. Fermats letzter Satz (kurz FLT) zeigt, dass mindestens eine der Zahlen a, b oder c Null sein muss. In $\mathbb{Z}^3$ gibt es daher nur *triviale* Lösungen. Das Gleiche gilt offenbar auch über $\mathbb{Q}$ (multipliziere mit gemeinsamen Nenner).

(ii) Ist Satz 7.6 für n bewiesen, so auch für nk mit $k \in \mathbb{N}$, denn jede Lösung $a^{nk} + b^{nk} = c^{nk}$ für nk liefert eine Lösung $(a^k)^n + (b^k)^n = (c^k)^n$ für n. Man braucht Satz 7.6 daher „nur“ für $n = 4$ und ungerade Primzahlen zu beweisen. Fermat hat seinen Satz nur für $n = 4$ bewiesen. Dies ist vermutlich der elementarste Fall.

Satz 7.8 (Fermat)**.** *Es existiert kein Tripel* $(a, b, c) \in \mathbb{N}^3$ *mit* $a^4 + b^4 = c^4$.

Beweis. Nehmen wir etwas allgemeiner an, dass $(a, b, c) \in \mathbb{N}^3$ mit $a^4 + b^4 = c^2$ existieren (dies schließt die gegebene Gleichung ein wegen $c^4 = (c^2)^2$). Sei dabei c so klein wie möglich. Dann gilt $\mathrm{ggT}(a, b) = 1$, denn anderenfalls könnte man wie im Beweis von Satz 7.4 durch $\mathrm{ggT}(a, b)$ teilen. Da (a^2, b^2, c) ein pythagoreisches Tripel ist, existieren $s, t \in \mathbb{N}$ mit $s < t$ und o. B. d. A. $(a^2, b^2, c) = (2st, t^2 - s^2, t^2 + s^2)$. Nun ist auch (b, s, t) ein pythagoreisches Tripel mit $\mathrm{ggT}(b, s) \mid \mathrm{ggT}(b, 2st) = \mathrm{ggT}(b, a^2) = 1$. Da a gerade ist, ist b ungerade. Nach Satz 7.4 existieren also $u, v \in \mathbb{N}$ mit $(b, s, t) = (v^2 - u^2, 2uv, v^2 + u^2)$. Wegen $\mathrm{ggT}(a, b) = 1$ ist auch $\mathrm{ggT}(s, t) = 1$. Dabei ist $s = 2uv$ gerade und t ist ungerade. Die Primfaktorzerlegung von $a^2 = 2st$ zeigt $s = 2x^2$ und $t = y^2$ mit $x, y \in \mathbb{N}$ und $\mathrm{ggT}(x, y) = 1$. Schließlich gilt auch $\mathrm{ggT}(u, v) \mid \mathrm{ggT}(b, s) = 1$. Die Gleichung $x^2 = uv$ liefert daher $p, q \in \mathbb{N}$ mit $u = p^2$ und $v = q^2$. Insgesamt erhält man $p^4 + q^4 = u^2 + v^2 = t = y^2$ mit $y \le y^2 = t \le t^2 < t^2 + s^2 = c$. Dies widerspricht der Wahl von (a, b, c). □

Bemerkung 7.9. Nach Bemerkung 7.7 und Satz 7.8 genügt es FLT für jede ungerade Primzahl $n = p$ zu beweisen. Die Idee ist die Summe $a^p + b^p$ in ein Produkt zu verwandeln und anschließend mit der Primfaktorzerlegung von c^p zu vergleichen. Sei dazu $\zeta := e^{2\pi \mathrm{i}/p} \in \mathbb{C}$. Da p ungerade ist, sind $-\zeta, -\zeta^2, \ldots, -\zeta^p = -1$ die Nullstellen des normierten Polynoms $X^p + 1$, d. h.

$$X^p + 1 = \prod_{i=1}^{p} (X + \zeta^i).$$

Wir substituieren $\frac{a}{b}$ für X und multiplizieren anschließend mit b^p:

$$a^p + b^p = \prod_{i=1}^{p} (a + \zeta^i b). \tag{7.2}$$

Die Faktoren auf der rechten Seite liegen im Ring

$$R := \mathbb{Z}[\zeta] := \{a_2\zeta^{p-2} + a_3\zeta^{p-3} + \ldots + a_p : a_2, \ldots, a_p \in \mathbb{Z}\}.$$

Wir beschränken uns ab jetzt auf $p = 3$. Es gilt dann $\zeta = \frac{1}{2}(-1 + \sqrt{-3})$ und $R = \mathbb{Z}_{-3}$ ist euklidisch nach Satz 6.20. Für $\alpha = a + b\zeta \in R$ ist

$$N(\alpha) = |\alpha|^2 = (a + b\zeta)(a + b\zeta^2) = a^2 + b^2 - ab.$$

Wir betrachten $\lambda := 1 - \zeta \in R$. Wegen $N(\lambda) = 3$ ist λ ein Primelement. Aus $3 = \lambda\bar{\lambda} \equiv 0 \pmod{\lambda}$ und $\zeta \equiv 1 \pmod{\lambda}$ folgt $R/R\lambda \cong \mathbb{F}_3$.

Lemma 7.10. *Für* $\alpha \in R = \mathbb{Z}_{-3}$ *mit* $\lambda \nmid \alpha$ *gilt* $\alpha^3 \equiv \pm 1 \pmod{\lambda^4}$.

Beweis. Indem man notfalls α durch $-\alpha$ ersetzt, kann man $\alpha \equiv 1 \pmod{\lambda}$ annehmen. Sei $\beta \in R$ mit $\alpha - 1 = \beta\lambda$. Dann gilt

$$\begin{aligned} \alpha - \zeta &= (\alpha - 1) + \lambda = \lambda(\beta + 1), \\ \alpha - \zeta^2 &= (\alpha - \zeta) + (\zeta - \zeta^2) = \lambda(\beta + 1) + \zeta\lambda = \lambda(\beta - \zeta^2). \end{aligned}$$

Es folgt

$$\alpha^3 - 1 = (\alpha - 1)(\alpha - \zeta)(\alpha - \zeta^2) = \lambda^3\beta(\beta + 1)(\beta - \zeta^2).$$

Wegen $\zeta^2 \equiv 1 \pmod{\lambda}$ liegen β, $\beta + 1$ und $\beta - \zeta^2$ in verschiedenen Restklassen modulo λ. Eine der Zahlen muss daher durch λ teilbar sein. Dies zeigt die Behauptung. $\square$

Satz 7.11 (Euler)**.** *Es gibt kein Tripel $(a, b, c) \in \mathbb{N}^3$ mit $a^3 + b^3 = c^3$.*

Beweis. Sei $R := \mathbb{Z}_{-3}$. Wir nehmen allgemeiner an, dass $\alpha, \beta, \gamma \in R \setminus \{0\}$ und $\epsilon \in R^\times$ mit $\alpha^3 + \beta^3 = \epsilon\gamma^3$ existieren. O. B. d. A. seien α, β und γ (paarweise) teilerfremd. Sei zunächst $\lambda \mid \alpha\beta$. Da λ ein Primelement ist, gilt o. B. d. A. $\lambda \mid \alpha$ und $\lambda \nmid \beta$ sowie $\lambda \nmid \gamma$. Nach Lemma 7.10 ist dann $\pm\epsilon \equiv \epsilon\gamma^3 = \alpha^3 + \beta^3 \equiv \pm 1 \pmod{\lambda^2}$ und $\lambda^2 \mid 1 \pm \epsilon$. Im Fall $\epsilon \neq \mp 1$ wäre $3 = |\lambda^2| \leq |1 \pm \epsilon| \leq 2$ nach der Dreiecksungleichung. Also ist $\epsilon = \mp 1$ und $\beta^3 + (\pm\gamma)^3 = (-\alpha)^3$. Durch Vertauschen von α und γ kann man also $\lambda \nmid \alpha\beta$ annehmen.

Unter allen solchen Gegenbeispielen wählen wir γ, sodass

$$t := \nu(\gamma) := \max\{n \in \mathbb{N}_0 : \lambda^n \mid \gamma\}$$

möglichst klein ist. Im Fall $t = 0$ existieren $e, f \in \{\pm 1\}$ mit

$$\pm\epsilon \equiv \epsilon\gamma^3 = \alpha^3 + \beta^3 \equiv e + f \pmod{\lambda^4}$$

nach Lemma 7.10. Offenbar ist $e = f$ und $\lambda^4 \mid \epsilon \pm 2$. Dies liefert den Widerspruch $9 = |\lambda^4| \leq |\epsilon \pm 2| \leq 5$. Im Fall $t = 1$ ist

$$0 \not\equiv \epsilon\gamma^3 = \alpha^3 + \beta^3 \equiv \pm 2 \pmod{\lambda^4}$$

und $\lambda \mid \epsilon\gamma^3 + (\pm 2 - \epsilon\gamma^3) = \pm 2$. Dies ergibt den Widerspruch $3 = N(\lambda) \mid N(2) = 4$. Also ist $t \geq 2$ und $\nu(\gamma^3) = 3t \geq 6$.

Gleichung 7.2 wird zu

$$(\alpha + \beta)(\alpha + \beta\zeta)(\alpha + \beta\zeta^2) = \epsilon\gamma^3. \tag{7.3}$$

Es folgt $\nu(\alpha + \beta) \geq 2$, $\nu(\alpha + \beta\zeta) \geq 2$ oder $\nu(\alpha + \beta\zeta^2) \geq 2$. O. B. d. A. sei $\nu(\alpha + \beta) \geq 2$ (anderenfalls ersetze man β durch $\beta\zeta$ bzw. $\beta\zeta^2$). Wegen $\lambda \nmid \beta$ ist dann

$$\nu(\alpha + \beta\zeta) = \nu(\alpha + \beta - \beta(1 - \zeta)) = \nu(\alpha + \beta - \beta\lambda) = 1,$$
$$\nu(\alpha + \beta\zeta^2) = \nu(\alpha + \beta - \beta\lambda(1 + \zeta)) = \nu(\alpha + \beta + \beta\lambda\zeta^2) = 1.$$

Dies zeigt $\nu(\alpha + \beta) = 3t - 2 \geq 4$. Sei $\delta \in R$ ein Primelement, welches nicht zu λ assoziiert ist. Ist δ ein gemeinsamer Teiler von $\alpha + \beta$ und $\alpha + \beta\zeta$, so teilt δ auch $\beta(1 - \zeta) = \beta\lambda$. Es folgt $\delta \mid \beta$ und $\delta \mid \alpha$ im Widerspruch zu $\mathrm{ggT}(\alpha, \beta) \in R^\times$. Analog sieht man, dass δ höchstens eine der Zahlen $\alpha + \beta$, $\alpha + \beta\zeta$ und $\alpha + \beta\zeta^2$ teilen kann. Die Primfaktorzerlegung von (7.3) liefert daher $\alpha_1, \beta_1, \rho \in R$ und $\epsilon_1, \epsilon_2, \epsilon_3 \in R^\times$ mit

$$\alpha + \beta = \epsilon_1\lambda^{3t-2}\rho, \qquad \alpha + \beta\zeta = \epsilon_2\lambda\alpha_1^3, \qquad \alpha + \beta\zeta^2 = \epsilon_3\lambda\beta_1^3$$

und $\lambda \nmid \rho\alpha_1\beta_1$. Es folgt

$$0 = (\alpha + \beta) + (\alpha + \beta\zeta)\zeta + (\alpha + \beta\zeta^2)\zeta^2 = \epsilon_1\lambda^{3t-2}\rho^3 + \epsilon_2\lambda\alpha_1^3\zeta + \epsilon_3\lambda\beta_1^3\zeta^2.$$

Wir setzen $\gamma_1 := \lambda^{t-1}\rho$. Dann existieren $\mu_1, \mu_2 \in R^\times$ mit

$$\alpha_1^3 + \mu_1\beta_1^3 = \mu_2\gamma_1^3.$$

Wegen $t \geq 2$ ist $\lambda \mid \gamma_1$ und daher $0 \equiv \pm\mu_2\gamma_1^3 \equiv 1 \pm \mu_1 \pmod{\lambda^2}$ nach Lemma 7.10. Wie oben folgt $\mu_1 = \mp 1$. Also ist

$$\alpha_1^3 + (\mp\beta_1)^3 = \mu_2\gamma_1^3$$

mit $\nu(\gamma_1) = t - 1$ im Widerspruch zur Wahl von γ. $\square$

Bemerkung 7.12.

(i) Legendre und Dirichlet bewiesen FLT für $p = 5$.

(ii) Sei $p > 2$ eine beliebige Primzahl und $\zeta = e^{2\pi \mathrm{i}/p}$. Für $1 \leq k, l \leq q := \frac{p-1}{2}$ gilt

$$2k \equiv \pm 2l \pmod{p} \overset{3.6}{\iff} k \equiv \pm l \pmod{p} \iff k = l.$$

Wegen

$$(X^{p-1} + \ldots + X + 1)(X - 1) = X^p - 1 = \prod_{k=1}^{p} (X - \zeta^k)$$

folgt

$$p = \prod_{k=1}^{p-1} (1 - \zeta^k) = \prod_{k=1}^{q} (1 - \zeta^{2k})(1 - \zeta^{-2k}) = \prod_{k=1}^{q} (\zeta^k - \zeta^{-k})(\zeta^{-k} - \zeta^k) = (-1)^q \prod_{k=1}^{q} (\zeta^k - \zeta^k)^2.$$

Also ist $\sqrt{(-1)^q p} = \prod_{k=1}^{q} (\zeta^k - \zeta^k) \in \mathbb{Z}[\zeta] = R$. Dies zeigt $\mathbb{Z}_p \subseteq R$, falls $p \equiv 1 \pmod{4}$ und $\mathbb{Z}_{-p} \subseteq R$ sonst. Im ersten Fall ist $|R^\times| = \infty$ nach Satz 6.10. Dies gilt auch im zweiten Fall für $p > 3$ nach Dirichlets *Einheitensatz*.

(iii) Lamé hatte geglaubt den Beweis von Satz 7.11 für alle $p > 2$ führen zu können. Liouville wies aber daraufhin, dass $R = \mathbb{Z}[\zeta]$ für $p > 19$ nicht mehr faktoriell ist.

(iv) Als Alternative zeigte Kummer, dass zumindest alle *Ideale* in R eine eindeutige Faktorisierung in Primideale besitzen (Ringe mit dieser Eigenschaft heißen *Dedekind-Ringe*). Mittels der *Klassenzahl* lässt sich genau messen, wie weit R von einem faktoriellen Ring entfernt ist. Kummer bewies FLT für *reguläre* Primzahlen p, d. h. die Klassenzahl von R ist nicht durch p teilbar. Diese Primzahlen $p > 2$ lassen sich äquivalent dadurch charakterisieren, dass die Zähler der Bernoulli-*Zahlen* $B_2, B_4, \ldots, B_{p-3}$ nicht durch p teilbar sind. Die Bernoulli-Zahlen treten als Koeffizienten der Potenzreihe

$$\frac{X}{\exp(X) - 1} = \sum_{n=0}^{\infty} \frac{B_n}{n!} X^n$$

auf und lassen sich durch die Rekursionsformel

$$\sum_{k=0}^{n-1} \binom{n}{k} B_k = 0$$

mit dem Startwert $B_0 = 1$ berechnen. Es gilt $B_1 = -\frac{1}{2}$, $B_2 = \frac{1}{6}$ und $B_{2n+1} = 0$ für $n \geq 1$ (Der *Nenner* von B_{2n} ist das Produkt aller Primzahlen q mit $q - 1 \mid 2n$ nach Clausen und von Staudt). Damit gilt FLT für $p \leq 31$. Leider hat Jensen gezeigt, dass es unendlich viele *irreguläre* Primzahlen gibt (wobei $p = 37$ die kleinste ist).

(v) Betrachtet man $a^3 + b^3 = c^3$ modulo 9, so sieht man $p \mid abc$ (dies entspricht der Behauptung $t \geq 1$ im Beweis von Satz 7.11). Für $p > 3$ ist diese Schlussweise nicht möglich. Man unterscheidet daher zwischen dem *ersten Fall* ($p \nmid abc$) und dem *zweiten Fall* ($p \mid abc$). Im ersten Fall sind die Hauptideale in der Faktorisierung

$$(c)^p = \prod_{i=1}^{p} (a + b\zeta)$$

aus (7.2) teilerfremd. Jedes der Ideale $(a + b\zeta^i)$ ist daher die p-te Potenz eines Ideals. Ist p regulär, so ist $(a + b\zeta^i)$ sogar die p-te Potenz eines Hauptideals. Dies erlaubt eine ähnliche Argumentation wie in Satz 7.11. Germain hat den ersten Fall für alle Primzahlen p bewiesen, für die auch $2p+1$ eine Primzahl ist (sogenannte *Germain-Primzahlen*).

(vi) Faltings bewies, dass bei festem p nur höchstens endlich viele teilerfremde Lösungen (a, b, c) existieren können.

(vii) 1993 legte Wiles einen 100-seitigen Beweis für FLT in voller Allgemeinheit vor. Dieser enthielt jedoch eine Lücke, die Wiles zusammen mit Taylor ein Jahr später schließen konnte. Im Beweis interpretiert man FLT als elliptische Kurve (Definition 10.32) und benutzt modulare Formen.

8 Das quadratische Reziprozitätsgesetz

Bemerkung 8.1. In Satz 3.8 und Satz 3.11 haben wir gelernt wie man lineare Gleichung bzw. Gleichungssystem in Restklassenringen löst. Um quadratische Gleichungen zu lösen, muss man zunächst klären, welche Restklassen eine Quadratwurzel besitzen. Wir werden mit dem Jacobi-Symbol ein äußerst einfaches Kriterium hierfür herleiten.

Definition 8.2. Sei p eine Primzahl und $n \in \mathbb{Z} \setminus p\mathbb{Z}$. Man nennt n einen *quadratischen Rest* modulo p, falls ein $k \in \mathbb{Z}$ mit $n \equiv k^2 \pmod{p}$ existiert. Anderenfalls nennt man n einen *quadratischen Nichtrest* modulo p. Für $n \in \mathbb{Z}$ definiert man das *Legendre-Symbol*

$$\left(\frac{n}{p}\right) := \begin{cases} 1 & \text{falls } n \text{ ein quadratischer Rest modulo } p \text{ ist,} \\ -1 & \text{falls } n \text{ ein quadratischer Nichtrest modulo } p \text{ ist,} \\ 0 & \text{falls } p \mid n \end{cases}$$

von n *nach* p.

Beispiel 8.3. Offenbar gilt $\left(\frac{n}{2}\right) \equiv n \pmod{2}$. Man kann sich daher auf ungerade Primzahlen konzentrieren. Für $m \equiv n \pmod{p}$ ist außerdem $\left(\frac{n}{p}\right) = \left(\frac{m}{p}\right)$. Somit kann man $0 < n < p$ annehmen.

Lemma 8.4 (Euler-Kriterium). *Für jede ungerade Primzahl p und $n \in \mathbb{Z}$ gilt*

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

Beweis. O. B. d. A. sei $p \nmid n$. Wegen $n^{p-1} \equiv 1 \pmod{p}$ (Euler-Fermat) ist $n^{\frac{p-1}{2}} \in \{1, -1\}$, denn die Gleichung $x^2 = 1$ hat im Körper $\mathbb{F}_p$ nur die Lösungen ± 1. Sei $\zeta \in \mathbb{F}_p^\times$ eine Primitivwurzel. Ist $\left(\frac{n}{p}\right) = 1$, so gilt $n = \zeta^{2i}$ für ein $i \in \mathbb{Z}$. Es folgt $n^{\frac{p-1}{2}} = \zeta^{p-1} = 1$. Sei umgekehrt $n = \zeta^i$ mit $\gamma^{i\frac{p-1}{2}} = n^{\frac{p-1}{2}} = 1$. Nach Lemma 4.13 ist $p - 1 = \operatorname{ord}_p(\gamma) \mid i\frac{p-1}{2}$. Da p ungerade ist, folgt $2 \mid i$ und $n = \zeta^i$ ist ein Quadrat. $\square$

Beispiel 8.5 (1. Ergänzungssatz)**.** Aus dem Euler-Kriterium folgt

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{falls } p \equiv 1 \pmod 4, \\ -1 & \text{falls } p \equiv -1 \pmod 4 \end{cases} \tag{8.1}$$

und $\left(\frac{n}{3}\right) \equiv n \pmod 3$. Für $n, m \in \mathbb{Z}$ folgt außerdem $\left(\frac{nm}{p}\right) = \left(\frac{n}{p}\right)\left(\frac{m}{p}\right)$. Es genügt also $\left(\frac{p}{q}\right)$ für Primzahlen p und q zu berechnen.

Lemma 8.6 (2. Ergänzungssatz)**.** *Für jede ungerade Primzahl p gilt*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \textit{falls } p \equiv \pm 1 \pmod 8, \\ -1 & \textit{falls } p \equiv \pm 3 \pmod 8. \end{cases}$$

Beweis. Für $p' := (p-1)/2$, $r := \lfloor p'/2 \rfloor$ und $s := \lfloor (p'-1)/2 \rfloor$ gilt

$$\begin{aligned}(p'!)^2 &\equiv (-1)^{p'} \prod_{k=1}^{p'} k(p-k) \equiv (-1)^{p'}(p-1)! \equiv (-1)^{p'}\big(1 \cdot 3 \cdot \ldots \cdot (p-2)\big)\big(2 \cdot 4 \cdot \ldots \cdot (p-1)\big) \\ &\equiv (-2)^{p'}(p'!)\big(1 \cdot 3 \cdot \ldots \cdot (p-2)\big) \overset{8.4}{\equiv} (-1)^{p'}\left(\frac{2}{p}\right)(p'!)\big(1 \cdot 3 \cdot \ldots \cdot (2s+1)\big)\big((p-2)\ldots(p-2r)\big) \\ &\equiv (-1)^{p'+r}(p'!)\left(\frac{2}{p}\right)\big(1 \cdot 3 \cdot \ldots \cdot (2s+1)\big)(2 \cdot 4 \cdot \ldots \cdot 2r) \equiv (-1)^{p'+r}(p'!)^2\left(\frac{2}{p}\right) \pmod p.\end{aligned}$$

Dies zeigt $\left(\frac{2}{p}\right) = (-1)^{p'+r}$. Eine einfache Fallunterscheidung ergibt $p' + r \equiv 0 \pmod 2 \iff p \equiv \pm 1 \pmod 8$. Gleichzeitig gilt

$$\frac{p^2-1}{8} \equiv 0 \pmod 2 \overset{3.6}{\iff} (p-1)(p+1) \equiv p^2 - 1 \equiv 0 \pmod{16} \iff p \equiv \pm 1 \pmod 8. \qquad \square$$

Definition 8.7. Sei $p \in \mathbb{P}$ ungerade und $a \in \mathbb{Z}$. Dann existiert genau ein $r \in \mathbb{Z}$ mit $a \equiv r \pmod p$ und $|r| \le \frac{p-1}{2}$. Im Fall $r > 0$ (bzw. $r < 0$) nennen wir a einen *positiven* (bzw. *negativen*) Rest modulo p.

Lemma 8.8 (Gauss)**.** *Sei $p \in \mathbb{P}$ ungerade und $p \nmid a \in \mathbb{Z}$. Sei μ die Anzahl der negativen Reste modulo p unter dem Zahlen $a, 2a, \ldots, \frac{p-1}{2}a$. Dann gilt $\left(\frac{a}{p}\right) = (-1)^\mu$.*

Beweis. Sei $p' := \frac{p-1}{2}$. Seien $-p' \le r_1, \ldots, r_\mu \le -1$ bzw. $1 \le s_1, \ldots, s_{p'-\mu} \le p'$ die negativen bzw. positiven Reste unter den Zahlen $a, 2a, \ldots, p'a$ (wegen $p \nmid a$ ist kein Rest 0). Wegen $ka \not\equiv la \pmod p$ für $1 \le k < l \le p'$ sind die r_i und die s_i untereinander paarweise verschieden. Nehmen wir $-r_i = s_j$ an. Dann existieren $1 \le k, l \le p'$ mit $-ka \equiv -r_i \equiv s_j \equiv la \pmod p$. Aus $(k+l)a \equiv 0 \pmod p$ und $0 \le k + l \le 2p' = p - 1$ folgt der Widerspruch $k = l$. Dies zeigt $\{-r_1, \ldots, -r_\mu, s_1, \ldots, s_{p'-\mu}\} = \{1, \ldots, p'\}$ und

$$(p')! = (-1)^\mu r_1 \ldots r_\mu s_1 \ldots s_{p'-\mu} \equiv (-1)^\mu \prod_{k=1}^{p'} ka \equiv (-1)^\mu a^{p'}(p')! \pmod p.$$

Mit der Euler-Kriterium ergibt sich $\left(\frac{a}{p}\right) \equiv a^{p'} \equiv (-1)^\mu \pmod p$. $\square$

Lemma 8.9. *Sei $p \in \mathbb{P}$ ungerade und $a \in \mathbb{Z}$ ungerade mit $p \nmid a$. Dann gilt*

$$\left(\frac{a}{p}\right) = (-1)^{\sum\limits_{k=1}^{(p-1)/2} \left\lfloor \frac{ka}{p} \right\rfloor}.$$

Beweis. Wir benutzen die Bezeichnungen aus dem Beweis von Lemma 8.8. Für $1 \le k \le p'$ gilt $ka = \left\lfloor \frac{ka}{p} \right\rfloor p + r$ mit $r \in \{p + r_1, \ldots, p + r_\mu, s_1, \ldots, s_{p'-\mu}\}$ (Division mit Rest). Aufsummieren ergibt

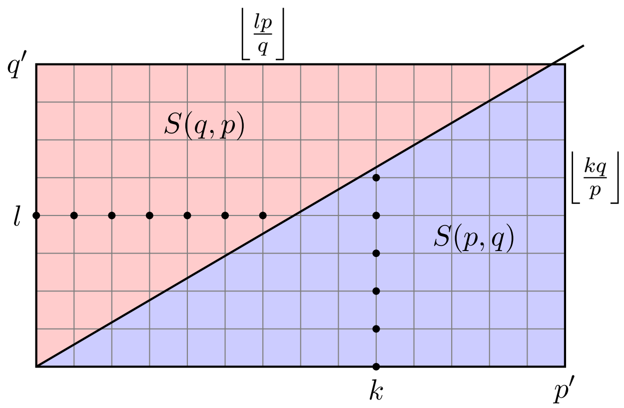
$$a\binom{p'+1}{2} = \sum_{k=1}^{p'} ka = p \sum_{k=1}^{p'} \left\lfloor \frac{ka}{p} \right\rfloor + \sum_{i=1}^{\mu} (p + r_i) + \sum_{j=1}^{p'-\mu} s_j = p \sum_{k=1}^{p'} \left\lfloor \frac{ka}{p} \right\rfloor + \mu p + \binom{p'+1}{2}.$$

Da a und p ungerade sind, ist $\mu \equiv \sum_{k=1}^{p'} \left\lfloor \frac{ka}{p} \right\rfloor \pmod 2$ und die Behauptung folgt aus Lemma 8.8. $\square$

Satz 8.10 (Quadratisches Reziprozitätsgesetz)**.** *Für verschiedene ungerade Primzahlen p und q gilt*

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

Beweis (Eisenstein). Wie zuvor sei $p' := \frac{p-1}{2}$ und $q' := \frac{q-1}{2}$. Wir zählen die Punkte mit ganzzahligen Koordinaten innerhalb des Rechtecks $(0, p/2) \times (0, q/2) \subseteq \mathbb{R}^2$ auf zwei Weisen. Offensichtlich gibt es genau $p'q'$ solche Punkte, nämlich (x, y) mit $1 \le x \le p'$ und $1 \le x \le q'$. Auf der Diagonale $y = \frac{q}{p}x$ liegen keine Punkte, denn sonst wäre $pa = qb$ mit $a, b \in \mathbb{N}$ und $a < q$ sowie $b < p$. Unterhalb der Diagonalen verteilen sich die Punkte auf die senkrechten Geraden $(k, *)$. Die Anzahl der Punkte auf dieser Gerade ist $\left\lfloor \frac{kq}{p} \right\rfloor$. Insgesamt liegen $S(p, q) := \sum_{k=1}^{p'} \left\lfloor \frac{kq}{p} \right\rfloor$ Punkte unterhalb der Diagonalen. Ein analoges Argument mit den waagerechten Geraden $(*, k)$ ergibt genau $S(q, p)$ Punkte oberhalb der Diagonalen.



Dies zeigt $S(p, q) + S(q, p) = p'q'$. Mit Lemma 8.9 folgt

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{S(p,q)+S(q,p)} = (-1)^{p'q'}. \qquad \square$$

Bemerkung 8.11.

(i) Nach dem Reziprozitätsgesetz gilt

$$\left(\frac{p}{q}\right) = \begin{cases} -\left(\frac{q}{p}\right) & \text{falls } p \equiv q \equiv -1 \pmod 4, \\ \left(\frac{q}{p}\right) & \text{sonst.} \end{cases} \tag{8.2}$$

Auf diese Weise lässt sich $\left(\frac{n}{p}\right)$ für beliebiges $n \in \mathbb{Z}$ berechnen, sofern man die Primfaktorzerlegung von n und allen kleineren Zahlen kennt. Wir zeigen im Folgenden wie man auf die (aufwendige) Primfaktorzerlegung verzichten kann.

(ii) Man kennt über 300 Beweise für das Reziprozitätsgesetz. [12]

Definition 8.12. Sei $n \in \mathbb{Z}$. Sei $a \in \mathbb{N}$ ungerade mit Primfaktorzerlegung $a = p_1 \dots p_k$ (der Fall $a = 1$ mit $k = 0$ ist zugelassen). Man nennt

$$\left(\frac{n}{a}\right) := \left(\frac{n}{p_1}\right) \dots \left(\frac{n}{p_k}\right)$$

das *Jacobi-Symbol* von n *nach* a.[13]

Bemerkung 8.13. Das Jacobi-Symbol setzt das Legendre-Symbol fort. Ist n ein quadratischer Rest modulo a, so ist n auch ein quadratischer Rest modulo p_i für jeden Primteiler p_i von a. Ggf. gilt $\left(\frac{n}{a}\right) = 1$. Die Umkehrung ist jedoch falsch. Zum Beispiel ist -1 kein quadratischer Rest modulo 9, aber $\left(\frac{-1}{9}\right) = \left(\frac{-1}{3}\right)\left(\frac{-1}{3}\right) = 1$. Die Rechenregeln für das Legendre-Symbol übertragen sich auf das Jacobi-Symbol wie folgt.

Satz 8.14. *Für $n, m \in \mathbb{Z}$ und ungerade $a, b \in \mathbb{N}$ gilt:*

(i) $n \equiv m \pmod a \Longrightarrow \left(\frac{n}{a}\right) = \left(\frac{m}{a}\right)$.

(ii) $\left(\frac{nm}{a}\right) = \left(\frac{n}{a}\right)\left(\frac{m}{a}\right)$ *und* $\left(\frac{n}{ab}\right) = \left(\frac{n}{a}\right)\left(\frac{n}{b}\right)$.

(iii) $\left(\frac{-1}{a}\right) = \begin{cases} 1 & \textit{falls } a \equiv 1 \pmod 4, \\ -1 & \textit{falls } a \equiv -1 \pmod 4. \end{cases}$

(iv) $\left(\frac{2}{a}\right) = \begin{cases} 1 & \textit{falls } a \equiv \pm 1 \pmod 8, \\ -1 & \textit{falls } a \equiv \pm 3 \pmod 8. \end{cases}$

(v) $\left(\frac{a}{b}\right) = \begin{cases} -\left(\frac{b}{a}\right) & \textit{falls } a \equiv b \equiv -1 \pmod 4, \\ \left(\frac{b}{a}\right) & \textit{sonst.} \end{cases}$

Beweis. Seien $a = p_1 \dots p_k$ und $b = q_1 \dots q_l$ die Primfaktorzerlegungen von a und b.

(i) Nach Beispiel 8.3 ist $\left(\frac{n}{a}\right) = \left(\frac{n}{p_1}\right) \dots \left(\frac{n}{p_k}\right) = \left(\frac{m}{p_1}\right) \dots \left(\frac{m}{p_k}\right) = \left(\frac{m}{a}\right)$.

[12] siehe `https://www.mathi.uni-heidelberg.de/~flemmermeyer/qrg_proofs.html`

[13] Das allgemeinere *Kronecker-Symbol* lässt auch gerade Nenner zu, wobei jedoch die Eigenschaft $n \equiv m \pmod a \Longrightarrow \left(\frac{n}{a}\right) = \left(\frac{m}{a}\right)$ verloren geht.

(ii) Nach Beispiel 8.5 ist

$$\left(\frac{nm}{a}\right) = \left(\frac{nm}{p_1}\right) \cdots \left(\frac{nm}{p_k}\right) = \left(\frac{n}{p_1}\right)\left(\frac{m}{p_1}\right) \cdots \left(\frac{n}{p_k}\right)\left(\frac{m}{p_k}\right) = \left(\frac{n}{a}\right)\left(\frac{m}{a}\right).$$

Die zweite Gleichung folgt direkt aus der Definition.

(iii) Für $r := |\{1 \le i \le k : p_i \equiv -1 \pmod 4\}|$ gilt

$$a - 1 \equiv (-1)^r - 1 \equiv 2r \equiv \sum_{i=1}^{k} (p_i - 1) \pmod 4.$$

Dies zeigt $\frac{a-1}{2} \equiv \sum_{i=1}^k \frac{p_i - 1}{2} \pmod 2$ nach Lemma 3.6. Aus (8.1) folgt

$$\left(\frac{-1}{a}\right) = \left(\frac{-1}{p_1}\right) \cdots \left(\frac{-1}{p_k}\right) = \prod_{i=1}^{k} (-1)^{\frac{p_i-1}{2}} = (-1)^{\sum_{i=1}^k \frac{p_i-1}{2}} = (-1)^{\frac{a-1}{2}}.$$

(iv) Für $r := |\{1 \le i \le k : p_i \equiv \pm 3 \pmod 8\}|$ gilt

$$a^2 - 1 \equiv 9^r - 1 \equiv 8r \equiv \sum_{i=1}^{k} (p_i^2 - 1) \pmod{16}$$

und $\frac{a^2-1}{8} \equiv \sum_{i=1}^k \frac{p_i^2 - 1}{8} \pmod 2$. Aus Lemma 8.6 folgt

$$\left(\frac{2}{a}\right) = \left(\frac{2}{p_1}\right) \cdots \left(\frac{2}{p_k}\right) = \prod_{i=1}^{k} (-1)^{\frac{p_i^2-1}{8}} = (-1)^{\sum_{i=1}^k \frac{p_i^2-1}{8}} = (-1)^{\frac{a^2-1}{8}}.$$

(v) O. B. d. A. sei $\mathrm{ggT}(a,b) = 1$, denn anderenfalls sind beide Seiten 0. Wie in (iii) gilt

$$\begin{aligned}\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) &\overset{\text{(ii)}}{=} \prod_{i=1}^{k}\prod_{j=1}^{l} \left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right) = \prod_{i=1}^{k}\prod_{j=1}^{l} (-1)^{\frac{p_i-1}{2}\frac{q_j-1}{2}} \\ &= (-1)^{\sum_{i=1}^k \frac{p_i-1}{2} \sum_{j=1}^l \frac{q_j-1}{2}} = (-1)^{\frac{a-1}{2}\frac{b-1}{2}}.\end{aligned}$$

□

Bemerkung 8.15. Sei $n \in \mathbb{Z}$ und $a \in \mathbb{N}$ ungerade. Folgender Algorithmus berechnet $\left(\frac{n}{a}\right)$:

(1) Setze $\epsilon := 1$.

(2) Solange $a > 1$ wiederhole:

- Reduziere n modulo a, sodass $|n| \le \frac{a-1}{2}$.
- Falls $n = 0$, dann gebe 0 aus. Ende.
- Falls $n < 0$, dann
  - ersetze n durch $-n$ (nun ist $n \in \mathbb{N}$),
  - falls $a \equiv -1 \pmod 4$, dann multipliziere ϵ mit -1.
- Solange $4 \mid n$, teile n durch 4.

- Falls $2 \mid n$, dann
  - teile n durch 2 (nun ist n ungerade),
  - falls $a \equiv \pm 3 \pmod 8$, dann multipliziere ϵ mit -1.
- Vertausche n und a.
- Falls $n \equiv a \equiv -1 \pmod 4$, dann multipliziere ϵ mit -1.

(3) Ausgabe: ϵ.

Die Laufzeit ist wie beim euklidischen Algorithmus logarithmisch in der Eingabe (Aufgabe 5). Die Bedingung $a \equiv 1 \pmod 4$ (bzw. $a \equiv \pm 1 \pmod 8$) lässt sich an den letzten beiden (bzw. drei) Dezimalziffern von a ablesen, denn $4 \mid 100$ (bzw. $8 \mid 1000$).

Beispiel 8.16. Wegen

$$\begin{aligned}\left(\frac{12346}{7787}\right) &= \left(\frac{-3408}{7787}\right) = -\left(\frac{3408}{7787}\right) = -\left(\frac{852}{7787}\right) = -\left(\frac{213}{7787}\right) = -\left(\frac{7787}{213}\right) = -\left(\frac{-94}{213}\right)\\ &= -\left(\frac{94}{213}\right) = \left(\frac{47}{213}\right) = \left(\frac{213}{47}\right) = \left(\frac{-22}{47}\right) = -\left(\frac{22}{47}\right) = -\left(\frac{11}{47}\right) = \left(\frac{47}{11}\right) = \left(\frac{3}{11}\right)\\ &= -\left(\frac{11}{3}\right) = -\left(\frac{-1}{3}\right) = \left(\frac{1}{3}\right) = 1\end{aligned}$$

ist 12346 ein quadratischer Rest modulo der Primzahl 7787.

Bemerkung 8.17. Im Folgenden benutzen wir das Jacobi-Symbol zur Konstruktion von Primzahltest für Mersenne- und Fermat-Primzahlen. In Bemerkung 2.13 haben wir den Primteiler $641 = 5 \cdot 2^7 + 1$ von $F_5 = 2^{2^5} + 1$ nachgewiesen.

Satz 8.18 (Lucas)**.** *Sei $n \ge 2$. Für jeden Primteiler p von F_n gilt $2^{n+2} \mid p - 1$.*

Beweis. Sicher ist $p > 2$. Aus $2^{2^n} \equiv -1 \pmod p$ folgt daher $2^{n+1} = \operatorname{ord}_p(2) \mid p - 1$. Wegen $p \equiv 1 \pmod{2^{n+1}}$ ist $p \equiv 1 \pmod 8$ und $\left(\frac{2}{p}\right) = 1$ nach dem zweiten Ergänzungssatz. Das Euler-Kriterium zeigt $2^{\frac{p-1}{2}} = 1 \pmod p$, d. h. $2^{n+1} = \operatorname{ord}_p(2) \mid \frac{p-1}{2}$. Also ist 2^{n+2} ein Teiler von $p - 1$. □

Satz 8.19 (Pépin-Test)**.** *Sei $n \in \mathbb{N}$. Genau dann ist F_n eine Primzahl, wenn $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$ gilt.*

Beweis. Sei $F_n \in \mathbb{P}$. Nach den Euler-Kriterium und dem Reziprozitätsgesetz gilt

$$3^{(F_n-1)/2} \equiv \left(\frac{3}{F_n}\right) \equiv \left(\frac{F_n}{3}\right) \equiv \left(\frac{4^{2^{n-1}} + 1}{3}\right) \equiv \left(\frac{2}{3}\right) \equiv -1 \pmod{F_n}.$$

Sei umgekehrt $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$ und p ein Primteiler von F_n. Aus $3^{F_n-1} \equiv 1 \pmod p$ folgt $2^{2^n} = F_n - 1 = \operatorname{ord}_p(3) \mid p - 1$. Dies zeigt $F_n \le p \le F_n$, d. h. $F_n = p \in \mathbb{P}$. □

Satz 8.20. *Sei $p \equiv 3 \pmod 4$ eine Germain-Primzahl (d. h. $2p + 1 \in \mathbb{P}$). Dann ist $2p + 1 \mid M_p$. Insbesondere ist $M_p \notin \mathbb{P}$ falls $p > 3$.*

Beweis. Sei $q := 2p + 1 \in \mathbb{P}$. Nach Fermat-Euler ist

$$M_p(M_p + 2) = (2^p - 1)(2^p + 1) = 2^{q-1} - 1 \equiv 0 \pmod{q}.$$

Nehmen wir $q \mid M_p + 2$ an. Dann gilt

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

Aus dem zweiten Ergänzungssatz folgt $2p + 1 = q \equiv \pm 3 \pmod 8$ und $p \equiv 1 \pmod 4$ im Widerspruch zur Voraussetzung. Also ist $q \mid M_p$. Im Fall $p > 3$ ist $q < M_p \notin \mathbb{P}$. $\square$

Beispiel 8.21. Aus Satz 8.20 folgt $M_p \notin \mathbb{P}$ für $p = 11, 23, 83, 131, \ldots$.

Satz 8.22. *Sei $p \in \mathbb{P}$ ungerade und d ein Teiler von M_p. Dann gilt $d \equiv \pm 1 \pmod 8$ und $d \equiv 1 \pmod p$.*

Beweis. O. B. d. A. sei $d \in \mathbb{P} \setminus \{2\}$. Aus $2^p \equiv 1 \pmod d$ folgt $1 \neq \mathrm{ord}_d(2) \mid p$ und $p = \mathrm{ord}_d(2) \mid \varphi(d) = d - 1$. Also gilt $d \equiv 1 \pmod p$. Wegen $p > 2$ existiert ein $k \in \mathbb{N}$ mit $d - 1 = 2kp$. Aus dem Euler-Kriterium folgt

$$\left(\frac{2}{d}\right) \equiv 2^{\frac{d-1}{2}} \equiv 2^{kp} \equiv 1 \pmod{d}.$$

Der zweite Ergänzungssatz liefert $d \equiv \pm 1 \pmod 8$. $\square$

Beispiel 8.23. Als Primteiler von M_{13} kommt nach Satz 8.22 nur 79 in Frage, denn $\sqrt{M_{13}} < 91$. Allerdings ist $79 \nmid M_{13}$ und M_{13} muss eine Primzahl sein.

Definition 8.24. Die LUCAS-*Folge* ist durch $L_0 := 4$, $L_{k+1} := L_k^2 - 2$ für $k \geq 0$ definiert.

Bemerkung 8.25.

(i) Im Folgenden betrachten wir den euklidischen Ring $\mathbb{Z}_3 = \mathbb{Z} + \mathbb{Z}\sqrt{3}$ (Satz 6.20) mit $\omega := 2 + \sqrt{3}$. Wegen $N(\omega) = \omega\omega^* = (2 + \sqrt{3})(2 - \sqrt{3}) = 1$ ist ω invertierbar. Offenbar gilt $\omega + \omega^* = 4 = L_0$. Sei induktiv $\omega^{2^k} + (\omega^*)^{2^k} = L_k$ gezeigt. Dann ist

$$L_{k+1} = L_k^2 - 2 = \omega^{2^{k+1}} + 2(\omega\omega^*)^{2^k} + (\omega^*)^{2^{k+1}} - 2 = \omega^{2^{k+1}} + (\omega^*)^{2^{k+1}}.$$

Also gilt $\omega^{2^k} + (\omega^*)^{2^k} = L_k$ für alle $k \in \mathbb{N}_0$.

(ii) Für eine Primzahl q sei $\mathbb{Z}_3 q = \mathbb{Z}q + \mathbb{Z}q\sqrt{3}$. Man zeigt leicht, dass die Restklassen modulo $\mathbb{Z}_3 q$ den Ring

$$R_q := \mathbb{Z}_3/\mathbb{Z}_3 q = \mathbb{F}_q + \mathbb{F}_q\sqrt{3}$$

bilden. Die Abbildung $\mu\colon \mathbb{Z}_3 \to R_q$, $x \mapsto x + \mathbb{Z}_3 q$ ist offensichtlich ein Ringhomomorphismus, d. h. $\mu(x \overset{+}{\cdot} y) = \mu(x) \overset{+}{\cdot} \varphi(y)$ für alle $x, y \in \mathbb{Z}_3$. Wir benutzen im Folgenden, dass $\mathrm{Ker}(\mu) \cap \mathbb{Z} = q\mathbb{Z}$. Da 0 nicht invertierbar ist, gilt $|R_q^\times| \leq |R| - 1 = q^2 - 1$. Wie im Beweis von Euler-Fermat zeigt man $x^{|R_q^\times|} = 1$ für alle $x \in R_q^\times$. Insbesondere ist die Ordnung von x durch $q^2 - 1$ beschränkt (vgl. Lemma 4.13).

Satz 8.26 (LUCAS-LEHMER-Test)**.** *Sei $p \in \mathbb{P} \backslash \{2\}$. Genau dann ist M_p eine Primzahl, wenn $M_p \mid L_{p-2}$.*

Beweis.

$\Leftarrow$: Sei $kM_p = L_{p-2} = \omega^{2^{p-2}} + (\omega^*)^{2^{p-2}}$ für ein $k \in \mathbb{Z}$ mit den Bezeichnungen aus Bemerkung 8.25. Dann folgt

$$\omega^{2^{p-1}} = (kM_p - (\omega^*)^{2^{p-2}})\omega^{2^{p-2}} = kM_p\omega^{2^{p-2}} - 1.$$

Nehmen wir $M_p \notin \mathbb{P}$ an. Für den kleinsten Primteiler q von M_p gilt dann $q^2 \leq M_p$. Mit M_p ist auch q ungerade. Wegen $\mu(M_p) = 0 \in R_q$ gilt

$$\mu(\omega^{2^{p-1}}) = \mu(M_p)\mu(k\omega^{2^{p-2}}) - \mu(1) = -1 \in R_q \setminus \{1\}.$$

Also hat ω die Ordnung 2^p in R_q. Bemerkung 8.25 liefert den Widerspruch $2^p \leq q^2 - 1 \leq M_p - 1 = 2^p - 2$.

$\Rightarrow$: Sei $p = 2k + 1$ und $q := M_p \in \mathbb{P}$. Dann gilt $M_p = 2^p - 1 = 2 \cdot 4^k - 1 \equiv 1 \pmod 3$. Nach dem Euler-Kriterium und dem Reziprozitätsgesetz gilt

$$3^{\frac{q-1}{2}} \equiv \left(\frac{3}{q}\right) \equiv -\left(\frac{q}{3}\right) \equiv -\left(\frac{1}{3}\right) \equiv -1 \pmod q.$$

Mit dem zweiten Ergänzungssatz ist

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

Zusammen ergibt sich

$$6^{\frac{q-1}{2}} \equiv 2^{\frac{q-1}{2}} 3^{\frac{q-1}{2}} \equiv -1 \pmod q. \tag{8.3}$$

Insbesondere ist $\mu(6) \in R_q^\times$. In R_q gilt außerdem

$$(3 + \sqrt{3})^q \overset{3.5}{\equiv} 3^q + \sqrt{3}^q \overset{4.8}{\equiv} 3 + \sqrt{3} \cdot 3^{\frac{q-1}{2}} \equiv 3 - \sqrt{3} \pmod q$$

Wegen $(3 + \sqrt{3})^2 = 9 + 3 + 6\sqrt{3} = 6\omega$ folgt

$$6 = (3 + \sqrt{3})(3 - \sqrt{3}) \equiv (3 + \sqrt{3})^{q+1} = (6\omega)^{\frac{q+1}{2}} \equiv 6\omega(6\omega)^{\frac{q-1}{2}} \overset{(8.3)}{\equiv} -6\omega^{\frac{q+1}{2}} \pmod q.$$

Wegen $\mu(6) \in R_q^\times$ darf man durch 6 teilen und erhält $\omega^{\frac{q+1}{2}} \equiv -1 \pmod q$. Aus $\omega\omega^* = 1$ folgt schließlich

$$L_{p-2} \overset{8.25}{=} \omega^{2^{p-2}} + (\omega^*)^{2^{p-2}} = \omega^{\frac{q+1}{4}} + (\omega^*)^{\frac{q+1}{4}} \equiv \left(\omega^{\frac{q+1}{2}} + 1\right)(\omega^*)^{\frac{q+1}{4}} \equiv 0 \pmod q. \qquad \square$$

Beispiel 8.27. In der Praxis genügt es die Lucas-Folge modulo M_p zu berechnen. Für $p = 17$ ist beispielsweise:

k	0	1	2	3	4	5	6	7
$L_k \pmod{M_{17}}$	4	14	194	37634	95799	119121	66179	53645
k	8	9	10	11	12	13	14	15
$L_k \pmod{M_{17}}$	122218	126220	70490	69559	99585	78221	130559	0

Wegen $L_{15} \equiv 0 \pmod{M_{17}}$ ist $M_{17} \in \mathbb{P}$.

9 Dirichlets Primzahlsatz

Bemerkung 9.1. Bekanntlich existieren unendlich viele ungerade Primzahlen p, d. h. $p \equiv 1 \pmod 2$. In Satz 2.9 haben wir bewiesen, dass unendlich viele Primzahlen die Form $p \equiv 3 \pmod 4$ haben. Dirichlet bewies 1837, dass für teilerfremde natürliche Zahlen a, d unendlich viele Primzahlen $p \equiv a \pmod d$ existieren. Sein Beweis benutzt tiefliegende Eigenschaften der Riemannschen ζ-Funktion und man glaubte lange, dass es keinen „elementaren" Beweis (d. h. ohne Funktionentheorie) geben kann. Ein solcher Beweis wurde erst 1949 von Selberg gefunden. Da Selbergs Beweis deutlich länger und technischer ist, verfolgen wir einen analytischen Ansatz, der mit elementaren Eigenschaften des komplexen Logarithmus auskommt (inspiriert von Chapman). Es werden lediglich Kenntnisse der Analysis 1 im Umfang von Forsters Buch „Analysis 1" benötigt.

Definition 9.2. Für $s \in \mathbb{R}$ mit $s > 1$ definieren wir die *Riemannsche ζ-Funktion*

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Bemerkung 9.3. Wegen

$$\sum_{n=1}^{\infty} \frac{1}{n^s} \le 1 + \frac{1}{2^s} + \frac{1}{2^s} + 4\frac{1}{4^s} + \ldots = \sum_{n=0}^{\infty} 2^{n(1-s)} = \frac{1}{1-2^{1-s}} < \infty$$

konvergiert $\zeta(s)$ für $s > 1$. Für $s = 1$ erhält man hingehen die harmonische Reihe $\sum_{n=1}^{\infty} \frac{1}{n} = \infty$.

Lemma 9.4. *Für $s > 1$ gilt $\frac{1}{s-1} < \zeta(s) < \frac{s}{s-1}$. Insbesondere ist*

$$\lim_{s \to 1} (s-1)\zeta(s) = 1. \tag{9.1}$$

Beweis. Für $n \in \mathbb{N}$ gilt $\frac{1}{n+1} < \int_n^{n+1} x^{-n} \mathrm{d}x < \frac{1}{n}$ (Stichwort: Treppenfunktion). Summieren über n ergibt

$$\zeta(s) - 1 = \sum_{n=2}^{\infty} \frac{1}{n^s} < \int_1^{\infty} x^{-s} \mathrm{d}x < \zeta(s).$$

Wir berechnen

$$\int_1^{\infty} x^{-s} \mathrm{d}x = \lim_{n \to \infty} \int_1^n x^{-s} \mathrm{d}x = -\lim_{n \to \infty} \frac{x^{-s+1}}{s-1}\Big|_1^n = \frac{1}{s-1}.$$

Daraus folgt leicht die Behauptung. $\square$

Satz 9.5. *Sei A eine endliche abelsche Gruppe und $\hat{A} := \mathrm{Hom}(A, \mathbb{C}^\times)$ die Menge der Homomorphismen $A \to \mathbb{C}^\times$. Dann gilt:*

(i) Durch punktweise Multiplikation ist $\hat{A}$ eine abelsche Gruppe der Ordnung $|A|$, die unter komplexer Konjugation abgeschlossen ist.

(ii) Für $B \le A$ ist die Einschränkungsabbildung $\hat{A} \to \hat{B}$ ein Epimorphismus. Insbesondere besitzt jedes $\lambda \in \hat{B}$ genau $|A : B|$ Fortsetzungen nach A.

(iii) Für $\lambda, \mu \in \hat{A}$ gilt die erste Orthogonalitätsrelation

$$\sum_{a \in A} \lambda(a)\overline{\mu(a)} = \begin{cases} |A| & \textit{falls } \lambda = \mu, \\ 0 & \textit{falls } \lambda \neq \mu. \end{cases}$$

(iv) Für $a, b \in A$ gilt die zweite Orthogonalitätsrelation

$$\sum_{\lambda \in \hat{A}} \lambda(a)\overline{\lambda(b)} = \begin{cases} |A| & \textit{falls } a = b, \\ 0 & \textit{falls } a \neq b. \end{cases}$$

Beweis.

(i) Für $\lambda, \mu \in \hat{A}$ ist $\lambda\mu \in \hat{A}$ mit $(\lambda\mu)(a) := \lambda(a)\mu(a)$ für $a \in A$. Offenbar wird $\hat{A}$ auf diese Weise zu einer abelschen Gruppe. Nach dem Hauptsatz über endliche abelsche Gruppen existieren $a_1, \ldots, a_n \in A$ mit $A = \langle a_1 \rangle \oplus \ldots \oplus \langle a_n \rangle$. Sei $d_i := |\langle a_i \rangle|$ für $i = 1, \ldots, n$. Für $\lambda \in \hat{A}$ gilt $\lambda(a_i)^{d_i} = \lambda(a_i^{d_i}) = \lambda(1) = 1$, d. h. $\lambda(a_i)$ ist eine d_i-te Einheitswurzel. Insbesondere gibt es höchstens d_i Möglichkeiten für $\lambda(a_i)$. Da λ durch die Bilder von $a_1, \ldots, a_n$ eindeutig bestimmt ist, folgt $|\hat{A}| \leq d_1 \ldots d_n = |A|$. Jedes Element in A lässt sich eindeutig in der Form $a_1^{k_1} \ldots a_n^{k_n}$ mit $0 \leq k_i \leq d_i - 1$ für $i = 1, \ldots, n$ schreiben. Sei $\zeta_i \in \mathbb{C}$ eine d_i-te Einheitswurzel. Dann definiert

$$\lambda(a_1^{k_1} \ldots a_n^{k_n}) := \zeta_1^{k_1} \ldots \zeta_n^{k_n}$$

einen Homomorphismus $A \to \mathbb{C}^\times$. Unterschiedliche Wahlen der ζ_i definieren verschiedenen λ. Dies zeigt $|\hat{A}| \geq |A|$. Für $\lambda \in \hat{A}$ ist auch $\overline{\lambda} \in \hat{A}$ mit $\overline{\lambda}(a) := \overline{\lambda(a)}$ für $a \in A$.

(ii) Die Einschränkung $\Gamma\colon \hat{A} \to \hat{B}$, $\lambda \mapsto \lambda_{|B}$ ist offenbar ein Homomorphismus. Für $\lambda \in \mathrm{Ker}(\Gamma)$ gilt $B \leq \mathrm{Ker}(\lambda)$. Nach dem Homomorphiesatz lässt sich λ als Element von $\widehat{A/B}$ auffassen. Umgekehrt definiert jedes $\hat{\lambda} \in \widehat{A/B}$ durch $a \mapsto \hat{\lambda}(aB)$ ein Element aus $\mathrm{Ker}(\Gamma)$. Aus (i) folgt $|\mathrm{Ker}(\Gamma)| = |\widehat{A/B}| = |A/B|$. Nach dem Homomorphiesatz ist

$$|\Gamma(A)| = |\hat{A} : \mathrm{Ker}(\Gamma)| = \frac{|A|}{|A/B|} = |B| = |\hat{B}|,$$

d. h. Γ surjektiv. Die zweite Aussage folgt, da das Urbild von λ eine Nebenklasse nach $\mathrm{Ker}(\Gamma)$ ist.

(iii) Im Fall $\lambda = \mu$ ist $\lambda(a)\overline{\mu(a)} = |\lambda(a)|^2 = 1$, da $\lambda(a)$ eine Einheitswurzel ist. Wir können daher $\lambda \neq \mu$ annehmen. Dann existiert ein $b \in A$ mit $\lambda(b)\overline{\mu(b)} \neq 1$. Aus

$$\lambda(b)\overline{\mu(b)} \sum_{a \in A} \lambda(a)\overline{\mu(a)} = \sum_{a \in A} \lambda(ab)\overline{\mu(ab)} = \sum_{a \in A} \lambda(a)\overline{\mu(a)}$$

folgt die Behauptung.

(iv) Da die Werte von $\lambda \in \hat{A}$ Einheitswurzeln sind, gilt $\overline{\lambda(a)} = \lambda(a^{-1})$. Wir können daher $b = 1$ annehmen. Für $a = 1$ ist die Behauptung trivial. Sei also $a \neq 1$ und $B := \langle a \rangle$. Nach (ii) gilt

$$\sum_{\lambda \in \hat{A}} \lambda(a) = |A/B| \sum_{\mu \in \hat{B}} \mu(a).$$

Sei $k := |B|$ und $\zeta \in \mathbb{C}^\times$ eine primitive k-te Einheitswurzel. Der Beweis von (i) zeigt

$$\sum_{\mu \in \hat{B}} \mu(a) = 1 + \zeta + \ldots + \zeta^{k-1} = \frac{1 - \zeta^k}{1 - \zeta} = 0. \qquad \square$$

Definition 9.6. Im Folgenden sei stets $d \geq 2$ eine natürliche Zahl. Eine Funktion $\chi\colon \mathbb{Z} \to \mathbb{C}$ heißt *Dirichlet-Charakter* modulo d, falls für alle $a, b \in \mathbb{Z}$ gilt

- $\chi(a) = 0 \iff \mathrm{ggT}(a, d) > 1$,
- $\chi(ab) = \chi(a)\chi(b)$,
- $\chi(a + d) = \chi(a)$.

Die Menge der Dirichlet-Charaktere modulo d sei Ψ_d. Die zu χ gehörige *L-Reihe* ist durch

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

für $s \in \mathbb{R}$ mit $s > 1$ definiert.

Bemerkung 9.7.

(i) Sei $A := (\mathbb{Z}/d\mathbb{Z})^\times$. Durch Einschränkung erhält man einen Monomorphismus $\Gamma\colon \Psi_d \to \hat{A} = \mathrm{Hom}(A, \mathbb{C}^\times)$. Da sich jeder Homomorphismus $\lambda \in \hat{A}$ durch $\lambda(n) := 0$ für $\mathrm{ggT}(n, d) > 1$ zu einem Dirichlet-Charakter fortsetzen lässt, ist Γ ein Isomorphismus. Insbesondere ist $|\Psi_d| = |\hat{A}| = |A| = \varphi(d)$ nach Satz 9.5.

(ii) Mit $\chi \in \Psi_d$ ist auch $\overline{\chi} \in \Psi_d$ nach Satz 9.5. Im Fall $\chi = \overline{\chi}$ nennen wir χ *reell*. Ggf. gilt $\chi(\mathbb{Z}) \subseteq \{0, \pm 1\}$. Der *triviale* Dirichlet-Charakter χ_0 mit den Werten 0 und 1 ist reell.

(iii) Für $\chi \in \Psi_d$ und $s > 1$ gilt

$$\sum_{n=1}^{\infty} \frac{|\chi(n)|}{n^s} \leq \zeta(s).$$

Daher ist $L(s, \chi)$ absolut konvergent.

Lemma 9.8 (Euler-Produkt)**.** *Für jeden Dirichlet-Charakter χ und $s > 1$ gilt*

$$L(s, \chi) = \prod_{p \in \mathbb{P}} \frac{1}{1 - \chi(p)p^{-s}}. \tag{9.2}$$

Beweis. Sei $\mathbb{P}_N := \{p \in \mathbb{P} : p \leq N\} = \{p_1, \ldots, p_t\}$. Sei Z_N die Menge der natürlichen Zahlen, deren Primfaktoren in $\mathbb{P}_N$ liegen. Nach dem Cauchy-Produkt für absolut konvergente Reihen gilt

$$\prod_{p \in \mathbb{P}_N} \frac{1}{1 - \chi(p)p^{-s}} = \prod_{i=1}^{t} \sum_{k=0}^{\infty} \frac{\chi(p_i^k)}{p_i^{ks}} = \sum_{k=0}^{\infty} \sum_{k_1 + \ldots + k_t = k} \frac{\chi(p_1^{k_1} \cdots p_t^{k_t})}{(p_1^{k_1} \cdots p_t^{k_t})^s} = \sum_{n \in Z_N} \frac{\chi(n)}{n^s},$$

wobei die Reihenfolge der Zahlen in Z_N auf Grund der absoluten Konvergenz keine Rolle spielt. Die Behauptung folgt mit $N \to \infty$. $\square$

Beispiel 9.9. Offensichtlich gilt auch $\zeta(s) = \prod_{p \in \mathbb{P}} \frac{1}{1 - p^{-s}}$ für $s > 1$. Für den trivialen Dirichlet-Charakter $\chi_0 \in \Psi_d$ ergibt sich

$$L(s, \chi_0) = \prod_{\substack{p \in \mathbb{P} \\ p \nmid d}} \frac{1}{1 - p^{-s}} = \zeta(s) \prod_{\substack{p \in \mathbb{P} \\ p \mid d}} \frac{p^s - 1}{p^s}$$

und

$$\lim_{s\to 1} L(s,\chi_0)(s-1) = \lim_{s\to 1} \zeta(s)(s-1) \lim_{s\to 1} \prod_{p\,|\,d} \frac{p^s-1}{p^s} \overset{(9.1)}{=} \frac{\varphi(d)}{d}. \tag{9.3}$$

Insbesondere ist $\lim_{s\to 1} L(s,\chi_0) = \infty$. Wir werden sehen, dass sich nicht-triviale Dirichlet-Charaktere anders verhalten.

Satz 9.10. *Für $s > 1$ gilt*

$$\prod_{\chi\in\Psi_d} L(s,\chi) \geq 1. \tag{9.4}$$

Beweis. Nach (9.2) gilt

$$P := \prod_{\chi\in\Psi_d} L(s,\chi) = \prod_{\substack{p\in\mathbb{P}\\ p\nmid d}} \prod_{\chi\in\Psi_d} \frac{1}{1-\chi(p)p^{-s}}$$

(beachte $|\Psi_d| = \varphi(d) < \infty$). Sei e die Ordnung von $p + d\mathbb{Z} \in (\mathbb{Z}/d\mathbb{Z})^\times$ und $f := \varphi(d)/e$. Nach Satz 9.5(ii) (angewendet auf $\langle p + d\mathbb{Z}\rangle \leq (\mathbb{Z}/d\mathbb{Z})^\times$) durchlaufen die Zahlen $\{\chi(p) : \chi \in \Psi_d\}$ alle e-ten Einheitswurzeln und jede Einheitswurzel tritt genau f-mal auf. Für eine primitive e-te Einheitswurzel $\omega \in \mathbb{C}$ gilt $X^e - 1 = \prod_{k=1}^{e}(X-\omega^k)$. Dies zeigt

$$\prod_{\chi\in\Psi_d} \frac{1}{1-\chi(p)p^{-s}} = \Big(\prod_{k=1}^{e} \frac{p^s}{p^s-\omega^k}\Big)^f = \frac{p^{sef}}{(p^{se}-1)^f} > 1.$$

Somit ist $P \geq 1$. □

Lemma 9.11 (Abelsche Summation)**.** *Seien $a_1,\ldots,a_n,b_1,\ldots,b_n \in \mathbb{C}$ und $A_k := \sum_{i=1}^{k} a_i$. Dann gilt*

$$\sum_{k=1}^{n} a_k b_k = A_n b_n + \sum_{k=1}^{n-1} A_k(b_k - b_{k+1}). \tag{9.5}$$

Beweis. Induktion nach n: Für $n = 1$ ist $\sum_{k=1}^{n} a_k b_k = A_1 b_1$. Sei nun $n \geq 1$. Dann gilt

$$\begin{aligned}\sum_{k=1}^{n} a_k b_k &= A_{n-1}b_{n-1} + \sum_{k=1}^{n-2} A_k(b_k-b_{k+1}) + a_n b_n = \sum_{k=1}^{n-1} A_k(b_k-b_{k+1}) + A_{n-1}b_n + a_n b_n\\ &= A_n b_n + \sum_{k=1}^{n-1} A_k(b_k-b_{k+1}).\end{aligned}$$ □

Folgerung 9.12. *Seien $a_1, a_2, \ldots \in \mathbb{C}$, sodass die Partialsummen $A_n := \sum_{k=1}^{n} a_k$ beschränkt sind. Sei $b_1, b_2, \ldots \in \mathbb{R}$ eine monoton fallende Nullfolge. Dann konvergiert $\sum_{n=1}^{\infty} a_n b_n$.*

Beweis. Sei $|A_n| \leq C$ für alle $n \in \mathbb{N}$. Für $n \leq m$ gilt

$$\Big|\sum_{k=n}^{m} a_k b_k\Big| \overset{(9.5)}{\leq} |A_m - A_{n-1}|b_m + \sum_{k=n}^{m-1} |A_k - A_{n-1}|\underbrace{(b_k - b_{k+1})}_{\geq 0} \leq 2Cb_n.$$

Wegen $\lim_{n\to\infty} b_n = 0$ bilden die Partialsummen $\sum_{k=1}^{n} a_k b_k$ eine Cauchyfolge. □

Definition 9.13. Stetigkeit und Differenzierbarkeit von komplexen Funktionen $f\colon \mathbb{C} \to \mathbb{C}$ definiert man wie im Reellen:

- Wir sagen f *konvergiert* im Punkt $z \in \mathbb{C}$ gegen $a \in \mathbb{C}$, falls

$$\forall \epsilon > 0\,\exists \delta > 0\,\forall w \in \mathbb{C} \setminus \{z\} : |z - w| < \delta \Longrightarrow |f(z) - a| < \epsilon.$$

  Ggf. schreiben wir $\lim_{w \to z} f(w) = a$.

- Man nennt f *stetig* im Punkt $z \in \mathbb{C}$, falls $\lim_{w \to z} f(w) = f(z)$ gilt. Ist f in jedem Punkt des Definitionsbereichs stetig, so heißt f *stetig*.

- Man nennt f *differenzierbar* (oder *holomorph*) im Punkt $z \in \mathbb{C}$, falls

$$f'(z) := \lim_{w \to z} \frac{f(z) - f(w)}{z - w}$$

  existiert. Ggf. nennt man $f'(z)$ die *Ableitung* von f in z. Ist f in jedem Punkt des Definitionsbereichs differenzierbar, so heißt f *differenzierbar* (oder *holomorph*).

Bemerkung 9.14. Ist f differenzierbar in z, so ist f auch stetig in z. Die üblichen Ableitungsregeln gelten für komplexe Funktionen genau wie im Reellen. Insbesondere ist $(fg)' = f'g + fg'$ (Produktregel) und $(f \circ g)' = (f' \circ g)g'$ (Kettenregel) für differenzierbare Funktionen $f, g\colon \mathbb{C} \to \mathbb{C}$.

Beispiel 9.15. Bekanntlich ist die *Exponentialfunktion*

$$\exp\colon \mathbb{C} \to \mathbb{C}^\times, \qquad z \mapsto \sum_{n=0}^{\infty} \frac{z^n}{n!}$$

differenzierbar mit $\exp' = \exp$. Für $z \in \mathbb{C}$ gilt $\exp(z) = e^z$, wobei $e := \exp(1) \approx 2{,}718$ die *eulersche Zahl* ist. Die Einschränkung $\exp\colon \mathbb{R} \to \mathbb{R}_{>0}$ ist surjektiv und streng monoton steigend. Sie besitzt mit dem *natürlichen Logarithmus* $\ln\colon \mathbb{R}_{>0} \to \mathbb{R}$ eine differenzierbare Umkehrfunktion.

Bemerkung 9.16. Aus dem Cauchy-Produkt absolut konvergenter Reihen folgt

$$\exp(z + w) = \exp(z) \exp(w)$$

für $z, w \in \mathbb{C}$. Induktiv erhält man $\exp(z_1 + \ldots + z_n) = \exp(z_1) \ldots \exp(z_n)$ für $z_1, \ldots, z_n \in \mathbb{C}$. Aus der Stetigkeit von exp folgt

$$\exp\Big(\sum_{k=1}^{\infty} z_k\Big) = \prod_{k=1}^{\infty} \exp(z_k) \tag{9.6}$$

für jede konvergente Reihe $\sum_{k=1}^{\infty} z_k$.

Satz 9.17. *Sei $\chi \in \Psi_d \setminus \{\chi_0\}$. Dann ist $L(s, \chi)$ auf $[1, \infty)$ stetig mit $L(1, \chi) \neq 0$.*

Beweis (Monsky). Für $n \in \mathbb{N}$ und $s \geq 1$ sei $a_n := \chi(n)$ und $b_n := \frac{1}{n^s}$. Nach der ersten Orthogonalitätsrelation (Satz 9.5) gilt

$$A_d := \sum_{n=1}^{d} a_n = \sum_{n=1}^{d} \chi(n)\chi_0(n) = 0$$

und es folgt

$$|A_k| \leq \sum_{n=d\lfloor k/d \rfloor+1}^{k} |\chi(n)| \leq d$$

für alle $k \in \mathbb{N}$. Der Beweis von Folgerung 9.12 zeigt

$$\Big|L(s,\chi) - \sum_{n=1}^{N-1} \frac{\chi(n)}{n^s}\Big| \leq \Big|\sum_{n=N}^{\infty} a_n b_n\Big| \leq \frac{2d}{N^s} \leq \frac{2d}{N}.$$

Daher konvergieren die Partialsummen von $L(s,\chi)$ gleichmäßig gegen $L(s,\chi)$ für $s \geq 1$. Insbesondere ist $L(s,\chi)$ stetig auf $[0,\infty)$.

Nehmen wir nun $L(1,\chi) = 0$ an.

Fall 1: $\overline{\chi} \neq \chi$.
Für $f\colon \mathbb{R}_{\geq 1} \to \mathbb{R}$, $x \mapsto x^{-1} - x^{-s}$ gilt

$$f'(x) \leq 0 \iff sx^{-s-1} - x^{-2} \leq 0 \iff x \geq s^{\frac{1}{s-1}} =: t,$$

wobei $t = 1$ für $s = 1$. Daher ist f für $x \geq t$ monoton fallend.[14] Insbesondere ist $b_n := f(n) = \frac{1}{n} - \frac{1}{n^s}$ eine monoton fallende Nullfolge für $n \geq t$. Nach dem Mittelwertsatz, angewendet auf $g\colon \mathbb{R} \to \mathbb{R}$, $s \mapsto n^{-s}$, existiert $1 \leq \xi_n \leq s$ mit

$$b_n = g(1) - g(s) = g'(\xi_n)(1-s) = \frac{\ln(n)}{n^{\xi_n}}(s-1).$$

Mit b_n ist auch $\frac{\ln(n)}{n^{\xi_n}}$ eine monoton fallende Nullfolge für $n \geq t$. Nach Folgerung 9.12 konvergiert

$$\gamma(s) := \sum_{n=1}^{\infty} a_n \frac{\ln(n)}{n^{\xi_n}}$$

für alle $s \geq 1$ (die endlichen vielen Summanden $n \leq t$ haben keinen Einfluss auf die Konvergenz). Der Beweis von Folgerung 9.12 zeigt (wie für $L(s,\chi)$), dass die Partialsummen gleichmäßig konvergieren und $\gamma(s)$ somit stetig auf $[0,\infty)$ ist. Insgesamt ist

$$L(s,\chi) = L(s,\chi) - L(1,\chi) = -\sum_{n=1}^{\infty} a_n b_n = (1-s)\gamma(s) \tag{9.7}$$

für $s \geq 1$.

Nach Voraussetzung gilt $L(1,\overline{\chi}) = \overline{L(1,\chi)} = 0$. Das Produkt $P(s) := \prod_{\psi \in \Psi_d} L(s,\psi)$ aus (9.4) lässt sich aufspalten in $P(s) = L(s,\chi_0)L(s,\chi)L(s,\overline{\chi})Q(s)$. Die Stetigkeit von $L(s,\psi)$ für alle $\psi \neq \chi_0$ zeigt $\lim_{s\to 1} Q(s) < \infty$. Nach (9.7) und (9.3) ist andererseits

$$\lim_{s\to 1} L(s,\chi_0)L(s,\chi)L(s,\overline{\chi}) = \lim_{s\to 1} L(s,\chi_0)(1-s) \lim_{s\to 1}(1-s)\gamma(s)\overline{\gamma(s)} = 0.$$

Also ist auch $\lim_{s\to 1} P(s) = 0$ im Widerspruch zu (9.4).

Fall 2: $\overline{\chi} = \chi$.
Für $0 \leq x < 1$ und $n \in \mathbb{N}$ ist $\frac{x^n}{1-x^n} \leq \frac{x^n}{1-x}$. Daher konvergiert

$$f(x) := \sum_{n=1}^{\infty} \chi(n) \frac{x^n}{1-x^n}$$

[14] es gilt $t = (1 + (s-1))^{\frac{1}{s-1}} \leq e$

absolut für $0 \le x < 1$. Es gilt

$$-f(x) = \frac{1}{1-x}L(1,\chi) - f(x) = \sum_{n=1}^{\infty} a_n \underbrace{\left(\frac{1}{n(1-x)} - \frac{x^n}{1-x^n}\right)}_{=:b_n}$$

mit

$$\begin{aligned}(1-x)(b_n - b_{n+1}) &= \frac{1}{n} - \frac{1}{n+1} - \frac{x^n}{1+x+\ldots+x^{n-1}} + \frac{x^{n+1}}{1+x+\ldots+x^n} \\ &= \frac{1}{n(n+1)} - \frac{x^n}{(1+x+\ldots+x^{n-1})(1+x+\ldots+x^n)}.\end{aligned}$$

Aus der Ungleichung zwischen arithmetischen und geometrischen Mittel folgt

$$\frac{1-x^n}{1-x} = 1+x+\ldots+x^{n-1} \ge nx^{\frac{1}{n}\binom{n}{2}} = nx^{\frac{n-1}{2}} \ge nx^{n/2} \ge nx^n.$$

Damit erhält man $b_n \ge 0$ und

$$(1-x)(b_n - b_{n+1}) \ge \frac{1}{n(n+1)} - \frac{x^n}{n(n+1)x^n} = 0,$$

d. h. $1 = b_1 \ge b_2 \ge \ldots \ge 0$. Abelsche Summation ergibt

$$\Big|\sum_{k=1}^{n} a_k b_k\Big| \le db_n + d\sum_{k=1}^{n-1}(b_k - b_{k+1}) = db_1 = d.$$

Insbesondere ist $f(x)$ beschränkt auf $[0,1)$. Wegen $\frac{x^n}{1-x^n} = \sum_{k=1}^{\infty} x^{kn}$ gilt

$$\begin{aligned}\Big|\sum_{n=1}^{N} \chi(n)\frac{x^n}{1-x^n} - \sum_{n=1}^{N}\Big(\sum_{k\mid n}\chi(k)\Big)x^n\Big| &= \Big|\sum_{n=1}^{N}\chi(n)\sum_{k=\lfloor N/n\rfloor+1}^{\infty} x^{kn}\Big| \le \sum_{n=1}^{N}\frac{x^{n\lfloor N/n\rfloor+n}}{1-x^n} \\ &\le \frac{1}{1-x}\sum_{n=1}^{N} x^N = \frac{Nx^N}{1-x} \xrightarrow{N\to\infty} 0.\end{aligned}$$

Dies zeigt

$$f(x) = \sum_{n=1}^{\infty}\underbrace{\Big(\sum_{k\mid n}\chi(k)\Big)}_{=:c_n}x^n.$$

Da χ reell ist, gilt $\chi(k) \in \{0, \pm 1\}$ für alle $k \in \mathbb{N}$. Für jede Primzahl p folgt $c_{p^r} = 1+\chi(p)+\ldots+\chi(p)^r \ge 0$. Mit der Primfaktorzerlegung $n = p_1^{r_1}\ldots p_t^{r_t}$ ergibt sich

$$c_n = c_{p_1^{r_1}} \ldots c_{p_t^{r_t}} \ge 0.$$

Wegen $d \ge 2$ besitzt d einen Primteiler p. Dann gilt $c_{p^r} = 1$ und $f(x) \ge \sum_{r=1}^{\infty} x^{p^r}$. Folglich ist $\lim_{x\to 1} f(x) = \infty$ im Widerspruch zu Beschränktheit von $f(x)$. $\square$

Beispiel 9.18. Mit elementarer Analysis gilt

$$\begin{aligned}L(2,\chi_0) &= 1 + \frac{1}{9} + \frac{1}{25} + \ldots = \zeta(2) - \frac{1}{4}\zeta(2) = \frac{\pi^2}{8} \qquad (\chi_0 \in \Psi_2), \\ L(1,\chi) &= 1 - \frac{1}{3} + \frac{1}{5} \mp \ldots = \frac{\pi}{4} \qquad (\chi \in \Psi_4 \setminus \{\chi_0\}), \\ L(3,\chi) &= 1 - \frac{1}{27} + \frac{1}{125} \mp \ldots = \frac{\pi^3}{32} \qquad (\chi \in \Psi_4 \setminus \{\chi_0\}).\end{aligned}$$

Aus der Partialbruchzerlegung des Cotangens mit $x = \frac{1}{3}$ bzw. $x = \frac{1}{6}$ folgt außerdem

$$L(1,\chi) = 1 + \sum_{n=1}^{\infty}\Big(\frac{1}{3n+1} - \frac{1}{3n-1}\Big) = \frac{1}{3}\pi\cot(\pi/3) = \frac{\pi}{3\sqrt{3}} \qquad (\chi \in \Psi_3 \setminus \{\chi_0\}),$$
$$L(1,\chi) = 1 + \sum_{n=1}^{\infty}\Big(\frac{1}{6n+1} - \frac{1}{6n-1}\Big) = \frac{1}{6}\pi\cot(\pi/6) = \frac{\pi}{2\sqrt{3}} \qquad (\chi \in \Psi_6 \setminus \{\chi_0\}).$$

Definition 9.19. Eine nichtleere Teilmenge $Z \subseteq \mathbb{C}$ heißt *konvex*, falls für alle $x, y \in Z$ die Verbindungsstrecke $\{\lambda x + (1-\lambda)y : 0 \le \lambda \le 1\}$ zwischen x und y in Z liegt.

Lemma 9.20. *Sei $Z \subseteq \mathbb{C}$ konvex und $f\colon Z \to \mathbb{C}$ differenzierbar mit $f'(z) = 0$ für alle $z \in Z$. Dann ist f konstant.*

Beweis. Seien $x, y \in Z$. Die reelle Funktion

$$g\colon [0,1] \to \mathbb{R}, \qquad \lambda \mapsto f\big(\lambda x + (1-\lambda)y\big) + \overline{f\big(\lambda x + (1-\lambda)y\big)} = 2\Re\big(f(\lambda x + (1-\lambda)y)\big)$$

ist wohldefiniert (da Z konvex ist) und erfüllt

$$g'(\lambda) = (x-y)f'\big(\lambda x + (1-\lambda)y\big) + \overline{(x-y)f'\big(\lambda x + (1-\lambda)y\big)} = 0$$

für alle $0 \le \lambda \le 1$ nach der Kettenregel. Aus dem Mittelwertsatz folgt, dass g konstant ist. Insbesondere ist $\Re(f(x)) = \frac{1}{2}g(1) = \frac{1}{2}g(0) = \Re(f(y))$. Analog zeigt man $\Im(f(x)) = \Im(f(y))$. Also ist f auf Z konstant. □

Bemerkung 9.21. Nach Analysis lässt sich jedes $z \in \mathbb{C}^\times$ in eindeutig *Polarkoordinaten*

$$z = re^{\mathrm{i}\varphi} = r(\cos\varphi + \mathrm{i}\sin\varphi)$$

mit $r = |z| > 0$ und $-\pi < \varphi \le \pi$ schreiben. Daher ist die Einschränkung

$$\exp\colon \{z \in \mathbb{C} : -\pi < \Im(z) \le \pi\} \to \mathbb{C}^\times$$

bijektiv.

Definition 9.22. Der *Hauptzweig* des komplexen *Logarithmus* ist durch

$$\log\colon \mathbb{C}^\times \to \mathbb{C}, \qquad re^{\mathrm{i}\varphi} \mapsto \ln(r) + \mathrm{i}\varphi \qquad (r > 0,\ -\pi < \varphi \le \pi)$$

definiert.

Bemerkung 9.23. Für $z = re^{\mathrm{i}\varphi} \in \mathbb{C}$ gilt

$$\exp(\log(z)) = \exp(\ln(r) + \mathrm{i}\varphi) = re^{\mathrm{i}\varphi} = z. \tag{9.8}$$

Andererseits ist $\log(\exp(2\pi\mathrm{i})) = \log(1) = \ln(1) = 0 \ne 2\pi\mathrm{i}$.

Lemma 9.24.

(i) Der komplexe Logarithmus ist auf $D := \mathbb{C} \setminus \mathbb{R}_{\le 0}$ differenzierbar mit $\log'(z) = \frac{1}{z}$ für $z \in D$.

(ii) *Für $z \in \mathbb{C}^\times$ mit $|z| < 1$ gilt* $\log(1-z) = -\sum_{n=1}^\infty \frac{z^n}{n}$.

Beweis.

(i) Nach Analysis ist $\ln\colon \mathbb{R}_{>0} \to \mathbb{R}$ differenzierbar mit $\ln'(x) = 1/x$ für $x > 0$. Sei $z = re^{\mathrm{i}\varphi} \in D$ mit $r > 0$ und $-\pi < \varphi < \pi$. Sei $z_k := r_k e^{\mathrm{i}\varphi_k} \in D$ eine Folge mit $\lim_{k\to\infty} z_k = z$ und $-\pi < \varphi_k < \pi$ für $k \in \mathbb{N}$. Dann existiert ein $\epsilon > 0$ mit $|\varphi - \varphi_k| < 2\pi - \epsilon$ für alle $k \in \mathbb{N}$. Wegen

$$|r - r_k| = \big||z| - |z_k|\big| \le |z - z_k| \xrightarrow{k\to\infty} 0$$

gilt $\lim_{k\to\infty} r_k = r$. Aus

$$\cos(\varphi - \varphi_k) + \mathrm{i}\sin(\varphi - \varphi_k) = e^{\mathrm{i}(\varphi - \varphi_k)} = \frac{r_k}{r}\frac{z}{z_k} \xrightarrow{k\to\infty} 1$$

und $|\varphi - \varphi_k| < 2\pi - \epsilon$ folgt $\lim_{k\to\infty} \varphi_k = \varphi$ (arccos ist stetig). Dies zeigt

$$\lim_{k\to\infty} \log(z_k) = \lim_{k\to\infty} (\ln(r_k) + \mathrm{i}\varphi_k) = \ln(r) + \mathrm{i}\varphi = z,$$

d. h. log ist stetig auf D. Nehmen wir nun $z_k \ne z$ für $k \in \mathbb{N}$ an. Als Umkehrfunktion der eingeschränkten Exponentialfunktion ist log injektiv. Insbesondere gilt $\log(z_k) \ne \log(z)$. Dies zeigt

$$\lim_{k\to\infty} \frac{\log(z) - \log(z_k)}{z - z_k} \overset{(9.8)}{=} \frac{1}{\lim\limits_{k\to\infty} \frac{\exp(\log(z)) - \exp(\log(z_k))}{\log(z) - \log(z_k)}} = \frac{1}{\exp'(\log(z))} = \frac{1}{\exp(\log(z))} = \frac{1}{z}$$

für alle $z \in D$.

(ii) Nach (i) ist die Funktion $f(z) := \log(1-z)$ auf der konvexen Menge $Z := \{z \in \mathbb{C} : |z| < 1\}$ differenzierbar mit $f'(z) = -\log'(1-z) = -\frac{1}{1-z}$ für $z \in Z$. Wegen

$$\sum_{n=1}^\infty \frac{|z|^n}{n} \le \sum_{n=1}^\infty |z|^n = \frac{|z|}{1 - |z|} < \infty$$

konvergiert die Reihe $g(z) := -\sum_{n=1}^\infty \frac{z^n}{n}$ absolut für $z \in Z$. Nach Analysis gilt

$$g'(z) = -\sum_{n=1}^\infty z^{n-1} = -\frac{1}{1-z} = f'(z).$$

Nach Lemma 9.20 existiert eine Konstante C mit $f(z) = g(z) + C$ und $C = f(0) - g(0) = 0$. $\square$

Bemerkung 9.25. Aus Lemma 9.24 folgt

$$\log\Big(\frac{1}{1-z}\Big) = \log\Big(\frac{1-z}{1-z}\Big) - \log(1-z) = \log(1) - \log(1-z) = \sum_{n=1}^\infty \frac{z^n}{n} \tag{9.9}$$

für $|z| < 1$.

Satz 9.26 (Dirichlets Primzahlsatz). *Für alle teilerfremden Zahlen $a, d \in \mathbb{N}$ gilt*

$$\sum_{\substack{p \in \mathbb{P} \\ p \equiv a \pmod d}} \frac{1}{p} = \infty.$$

Insbesondere existieren unendlich viele Primzahlen $p \equiv a \pmod d$.

Beweis. O. B. d. A. sei $d \geq 2$. Nach Satz 9.17 existiert ein $t > 1$ mit $L(s, \chi) \neq 0$ für alle $\chi \in \Psi_d$ und $1 < s < t$ (beachte $L(s, \chi_0) \geq 1$ für alle $s > 1$). Im Folgenden sei stets $1 < s < t$. Für $\chi \in \Psi_d$ gilt

$$\sum_{p\in\mathbb{P}}\sum_{k=2}^{\infty}\frac{|\chi(p^k)|}{kp^{ks}} \leq \sum_{p\in\mathbb{P}}\sum_{k=2}^{\infty}(p^{-s})^k = \sum_{p\in\mathbb{P}}\frac{p^{-2s}}{1-p^{-s}} = \sum_{p\in\mathbb{P}}\frac{1}{p^s(p^s-1)} \leq \sum_{n=2}^{\infty}\Big(\frac{1}{n-1}-\frac{1}{n}\Big) = 1.$$

Nach der zweiten Orthogonalitätsrelation (Satz 9.5) ist

$$\sum_{\psi\in\Psi_d}\overline{\chi(a)}\chi(p) = \begin{cases}|\Psi_d| = \varphi(d) & \text{falls } p \equiv a \pmod d,\\ 0 & \text{sonst.}\end{cases}$$

Dies zeigt

$$f(s) := \sum_{\chi\in\Psi_d}\overline{\chi(a)}\sum_{p\in\mathbb{P}}\sum_{k=1}^{\infty}\frac{\chi(p^k)}{kp^{ks}} = \sum_{p\in\mathbb{P}}\sum_{\chi\in\Psi_d}\overline{\chi(a)}\Big(\frac{\chi(p)}{p^s}+\sum_{k=2}^{\infty}\frac{\chi(p^k)}{kp^{ks}}\Big) \leq \varphi(d)\sum_{p\equiv a \pmod d}\frac{1}{p^s}+C$$

für eine Konstante C (da Ψ_d nach Satz 9.5 unter komplexer Konjugation abgeschlossen ist, ist $f(s) \in \mathbb{R}$). Es genügt daher $\lim_{s\to 1} f(s) = \infty$ zu zeigen. Wegen $|\chi(p)p^{-s}| < 1$ gilt

$$\exp\Big(\sum_{p\in\mathbb{P}}\sum_{k=1}^{\infty}\frac{\chi(p^k)}{kp^{ks}}\Big) \overset{(9.6)+(9.9)}{=} \prod_{p\in\mathbb{P}}\exp\Big(\log\Big(\frac{1}{1-\chi(p)p^{-s}}\Big)\Big) \overset{(9.8)}{=} \prod_{p\in\mathbb{P}}\frac{1}{1-\chi(p)p^{-s}} \overset{(9.2)}{=} L(s,\chi).$$

Für $\chi \neq \chi_0$ ist also $\lim_{s\to 1}\sum_{p\in\mathbb{P}}\sum_{k=1}^{\infty}\frac{\chi(p^k)}{kp^{ks}}$ beschränkt. Wegen $\mathrm{ggT}(a, d) = 1$ ist andererseits $\chi_0(a) = 1$ und $\lim_{s\to 1}\sum_{p\in\mathbb{P}}\sum_{k=1}^{\infty}\frac{\chi_0(p^k)}{kp^{ks}} = \infty$ nach Beispiel 9.9. Dies zeigt $\lim_{s\to 1} f(s) = \infty$. □

Bemerkung 9.27.

(i) Seien $a, d \in \mathbb{N}$ teilerfremd. Man kann zeigen, dass sich die Primzahlen „gleichmäßig“ auf die primen Restklassen verteilen, d. h.

$$\lim_{n\to\infty}\frac{|\{p \in \mathbb{P}_n : p \equiv a \pmod d\}|}{\pi(n)} = \frac{1}{\varphi(d)}.$$

(ii) In der Funktionentheorie setzt man die Riemannsche ζ-Funktion zu einer holomorphen Funktion auf $\mathbb{C} \setminus \{1\}$ fort. Sie besitzt dann die sogenannten trivialen Nullstellen $-2k$ für $k \in \mathbb{N}$. Der Gaußsche Primzahlsatz

$$\lim_{n\to\infty}\frac{\pi(n)\ln(n)}{n} = 1$$

ist äquivalent zu $\zeta(s) \neq 0$ für $\Re(s) = 1$ und lässt sich daher mit Funktionentheorie beweisen. Auch hier gibt es „elementare“ Beweise von Erdős, Selberg und anderen.

(iii) Die *Riemannsche Vermutung* besagt, dass alle nicht-trivialen Nullstellen von ζ den Realteil $\frac{1}{2}$ haben. Dies ist eines der größten ungelösten Probleme der Mathematik. Man weiß, dass es unendlich viele solche Nullstellen gibt. Die Nullstelle mit dem kleinsten positiven Imaginärteil ist $\approx \frac{1}{2} + 14{,}347\,\mathrm{i}$. Ein Beweis der Riemannschen Vermutung würde die folgende Verbesserung des Gaußschen Primzahlsatz implizieren:

$$\Big|n - \sum_{p\in\mathbb{P}_n}\log(p)\Big| < \frac{\sqrt{n}\ln(n/\ln(n))^2}{8\pi} \qquad (n \geq e^{78}).$$

10 Kryptologie

Bemerkung 10.1.

(i) Lange Zeit galt die Zahlentheorie als reine Spielerei. Die ersten wichtigen Anwendungen außerhalb der Mathematik ergaben sich in der Kryptologie und Codierungstheorie mit dem Beginn des Computerzeitalters in den 1970er Jahren. Die *Kryptologie* beschäftigt sich mit dem Verschlüsseln (*Kryptographie*) und Entschlüsseln (*Kryptoanalyse*) von vertraulichen Nachrichten. Die Codierungstheorie beschäftigt sich mit der Fehlererkennung und -korrektur bei der Übertragung digitaler Daten über einen störungsanfälligen Kanal.[15]

(ii) Nachrichten jeglicher Form (Text, Ton, Bilder, ...) können bekanntlich in Form von Dezimal- oder Binärzahlen digitalisiert werden. Da man Nachrichten in Blöcke aufteilen kann, können wir annehmen, dass solche Zahlen beschränkt sind.

(iii) *Kerckhoffs' Prinzip* besagt, dass die Sicherheit einer Verschlüsselungsmethode nicht von der Geheimhaltung des Algorithmus, sondern nur von der Geheimhaltung des Schlüssels abhängen sollte. Daher sind gängige Verfahren frei verfügbar (ohne Patent) und gut untersucht.

(iv) Ein grundlegendes Werkzeug der Kryptographie ist eine *Ein-Weg-Funktion*. Dies ist eine algorithmisch leicht zu berechnende injektive Funktion, deren Umkehrabbildung jedoch nur sehr schwer berechenbar ist. Der folgende Algorithmus zeigt, dass die Potenzabbildung in einer Gruppe effizient berechenbar ist.

Satz 10.2 (Binäre Exponentiation)**.** *Sei G eine Gruppe, $g \in G$ und $n \in \mathbb{N}$. Der folgende Algorithmus berechnet $g^n \in G$:*

Initialisierung: $h := g$, $x := g$ *und* $m := n$.
Solange $m > 0$, *wiederhole:*
  Falls $m \equiv 1 \pmod 2$, *berechne* $h := hx$.
  Berechne $x := x^2$.
  Berechne $m := \lfloor m/2 \rfloor$.
Ausgabe: $h = g^n$.

Beweis. Sei $n = \sum_{i=0}^{k} b_i 2^i$ die Binärdarstellung von n, wobei $b_k = 1$. Die Schleife wird $(k+1)$-mal durchlaufen mit folgenden Werten:

m	n	$\sum_{i=1}^{k} b_i 2^{i-1}$	$\sum_{i=2}^{k} b_i 2^{i-2}$	$\cdots$	$b_k = 1$	0
h	1	g^{b_0}	$g^{2b_1+b_0}$	$\cdots$	$g^{2^{k-1}b_{k-1}+\ldots+b_0}$	g^n
x	g	g^2	g^4	$\cdots$	g^{2^k}	$g^{2^{k+1}}$

$\square$

Bemerkung 10.3. Der naive Algorithmus zur Berechnung von g^n benötigt $n-1$ Multiplikation ($g \to g^2 \to g^3 \to \ldots \to g^n$), während die binäre Exponentation nur höchstens $2k = 2\lfloor \log_2(n) \rfloor$ Multiplikation benötigt (für $h = 1$ ist die Berechnung von $h := 1x$ trivial, während im letzten Durchlauf die Berechnung von $x := x^2$ überflüssig ist).

[15] Siehe Algebra-Skript

Beispiel 10.4.

(i) Bei Arithmetik in Restklassenringen modulo einer Zahl n ist es sinnvoll nach jeder Operation modulo n zu reduzieren. Zum Beispiel gilt

$$2^{27} = 2^{16+8+2+1} = 4^{8+4+1}2 = (-1)^{4+2}4 \cdot 2 \equiv 8 \pmod{17}.$$

(ii) Die binäre Exponentation ist nicht in jedem Fall ist effizienteste Methode zur Potenzierung. Zum Beispiel benötigt die binäre Exponentation von $g^{15} = gg^2g^4g^8$ sechs Multiplikationen, obwohl es auch mit fünf geht:

$$g \to g^2 \to g^3 = gg^2 \to g^5 = g^2g^3 \to g^{10} = (g^5)^2 \to g^{15} = g^{10}g^5.$$

Das Konstruieren solcher sogenannten *Additionsketten* ist jedoch aufwendig und in der Praxis selten lohnenswert.

Definition 10.5. Sei $G = \langle g \rangle$ eine zyklische Gruppe der Ordnung n. Der *diskrete Logarithmus* ist die Umkehrfunktion des Potenzierens $\log\colon G \to \mathbb{Z}/n\mathbb{Z}$, $g^k \mapsto k + n\mathbb{Z}$.

Bemerkung 10.6. Die Berechnung des diskreten Logarithmus hängt von der gegebenen Darstellung der Gruppe G ab. In $G = (\mathbb{Z}/n\mathbb{Z}, +) = \langle g + n\mathbb{Z} \rangle$ lässt sich der Logarithmus von $h + n\mathbb{Z}$ leicht berechnen, indem man mit $g^{-1} + n\mathbb{Z}$ multipliziert ($g^{-1} + n\mathbb{Z}$ lässt sich effizient mit dem erweiterten euklidischen Algorithmus berechnen). Im Allgemeinen ist die Berechnung von log schwierig, d. h. Potenzieren ist eine Ein-Weg-Funktion. Anstatt alle n Potenzen von g zu berechnen, kommt der folgende Algorithmus mit $2\sqrt{n}$ Multiplikationen aus (das ist in der Praxis immer noch viel).

Satz 10.7 (Babystep-Giantstep-Algorithmus)**.** *Sei $G = \langle g \rangle$ eine Gruppe der Ordnung n und $h \in G$. Der folgende Algorithmus berechnet $k + n\mathbb{Z}$ mit $g^k = h$:*

Initialisierung: $m := \lceil \sqrt{n} \rceil$.
Berechne und speichere: $P := \{1 = g^0, g^1, g^2, \ldots, g^m\}$ (*Babysteps*).
Für $i = 0, \ldots, m$:
    Berechne $x := hg^{-mi}$ (*Giantsteps*).
    Gilt $x = g^j \in P$, *so halte an.*
Ausgabe: $k + n\mathbb{Z} = mi + j + n\mathbb{Z}$.

Beweis. Offenbar existieren $0 \le i, j \le m$ mit $k = mi + j$. Der Algorithmus bricht ab, wenn $hg^{-mi} = x = g^j$ gilt, d. h. $h = g^{mi+j} = g^k$. □

Beispiel 10.8. Sei $G = \langle 3 + 101\mathbb{Z} \rangle = (\mathbb{Z}/101\mathbb{Z})^\times$ und $h = 4 + 101\mathbb{Z}$. Dann ist $m = \lceil \sqrt{101} \rceil = 11$. Wir berechnen die Babysteps (alle Werte modulo 101):

i	0	1	2	3	4	5	6	7	8	9	10	11
g^i	1	3	9	27	-20	41	22	-35	-4	-12	-36	-7

Wegen $7 \cdot 29 = 203 \equiv 1 \pmod{101}$ ist $g^{-11} \equiv -7^{-1} \equiv -29 \pmod{101}$. Damit berechnen wir die Giantsteps:

i	0	1	2	3	4	5
hg^{-mi}	4	-15	31	10	13	27

Wegen $27 \equiv g^3 \pmod{101}$ erhalten wir $k = 5 \cdot 11 + 3 = 58$ mit $g^k = h$. Insgesamt haben wir 15 Multiplikationen benötigt, während der naive Ansatz 57 Multiplikationen erfordert hätte.

Bemerkung 10.9. Beim Babystep-Giantstep-Algorithmus erkauft man sich einen Zeitvorteil mit erhöhten Speicherbedarf, um die Menge P zu speichern (*Time-Memory Tradeoff*). Der folgende Algorithmus reduziert die Berechnung des diskreten Logarithmus auf den Fall, in dem n eine Primzahl ist. Ist also $|G|$ ein Produkt von „kleinen“ Primzahlen, so hat man eine Chance $\log(h)$ zu berechnen.

Satz 10.10 (POHLIG-HELLMAN-Algorithmus)**.** *Sei $G = \langle g \rangle$ eine Gruppe der Ordnung $n = p_1^{a_1} \dots p_s^{a_s}$ (Primfaktorzerlegung). Sei $h \in G$. Der folgende Algorithmus berechnet $k + n\mathbb{Z}$ mit $g^k = h$:*

Für $i = 1, \dots, s$:
- *Setze $x := g^{n/p_i}$, $y := g^{n/p_i^{a_i}}$, $z := h^{n/p_i^{a_i}}$ und $l_0 := 0$.*
- *Für $j = 0, \dots, a_i - 1$:*
  - *Berechne $w := (y^{-l_j} z)^{p_i^{a_i-1-j}}$.*
  - *Bestimme $0 \leq r_j < p_i$ mit $x^{r_j} = w$ (z. B. mit Satz 10.7).*
  - *Berechne $l_{j+1} := l_j + p_i^j r_j$.*
- *Setze $k_i := l_{a_i}$.*

Bestimme k mit $k \equiv k_i \pmod{p_i^{a_i}}$ für $i = 1, \dots, s$ (chinesischer Restsatz).
Ausgabe: $k + n\mathbb{Z}$.

Beweis. Wir betrachten die i-te Iteration und setzen zur besseren Übersicht $p^a := p_i^{a_i}$. Nach Konstruktion hat x Ordnung p. Für $j = 0$ ist $w = z^{p^{a-1}} \in \langle x \rangle$. Daher existiert genau ein r_0 mit $0 \leq r_0 < p$ und $y^{p^{a-1} r_0} = x^{r_0} = w = z^{p^{a-1}}$, d. h. $(y^{-r_0} z)^{p^{a-1}} = 1$. Man setzt dann $l_1 := r_0$. Für $j = 1$ gilt wieder $w = (y^{-r_0} z)^{p^{a-2}} \in \langle x \rangle$. Nehmen wir nun induktiv an, dass im j-ten Schritt ein r_j mit $0 \leq r_j < p$ und $y^{p^{a-1} r_j} = x^{r_j} = w = (x^{-l_j} z)^{p^{a-1-j}}$ existiert. Dann gilt

$$(y^{-l_{j+1}} z)^{p^{a-1-j}} = (y^{-(l_j + p^j r_j)} z)^{p^{a-1-j}} = 1.$$

Dies garantiert, dass r_{j+1} existiert. Für $j = a - 1$ gilt schließlich $y^{p^{a-1} r_j} = x^{r_j} = w = y^{-l_j} z$. Mit $k_i := l_a = l_j + p^{a-1} r_j$ ist dann $y^{k_i} = z$. Wir setzen $y_i := y$ und $z_i := z$.

Da $p_1^{a_1}, \dots, p_s^{a_s}$ paarweise teilerfremd sind, lässt sich k mit dem chinesischen Restsatz berechnen. Sei $q_i := n/p_i^{a_i}$ für $i = 1, \dots, s$. Nach dem euklidischen Algorithmus existieren $b_1, \dots, b_s \in \mathbb{Z}$ mit $b_1 q_1 + \dots + b_s q_s = 1$. Dann gilt

$$g^k = g^{k b_1 q_1 + \dots + k b_s q_s} = y_1^{b_1 k_1} \dots y_s^{b_1 k_s} = z_1^{b_1} \dots z_s^{b_s} = h^{b_1 q_1 + \dots + b_s q_s} = h. \qquad \square$$

Beispiel 10.11. Sei $G := \langle 2 + 101\mathbb{Z} \rangle = (\mathbb{Z}/101\mathbb{Z})^\times$ und $h := 57 + 101\mathbb{Z}$. Es gilt $|G| = \varphi(101) = 100 = 2^2 5^2$. Mit den Bezeichnungen aus obigen Beweis ist $x_1 = g^{50} = -1 + 101\mathbb{Z}$, denn dies ist das einzige Element der Ordnung 2 in G. Wegen $10^2 \equiv -1 \pmod{101}$ ist $y_1 = 10 + 101\mathbb{Z}$. Weiter gilt

$$z_1 = 57^{25} \equiv (-44)^{16+8+1} \equiv 17^{8+4}(-44) \equiv \dots \equiv 10 \pmod{101}.$$

Wir können sofort $k_1 = 1$ ablesen ohne die innere Schleife zu durchlaufen.

Für $p_2 = 5$ erhält man $y_2 = g^4 = 16 + 101\mathbb{Z}$ und

$$\begin{aligned} x_2 = y_2^5 &= 16^4 16 \equiv (-13)16 \equiv -6 \pmod{101}, \\ z_2 &= 57^4 \equiv 17^2 \equiv -14 \pmod{101}, \\ w &= z_2^5 \equiv (-6)^2(-14) \equiv \dots \equiv 1 \pmod{101}. \end{aligned}$$

Also gilt $l_1 = r_0 = 0$. Im nächsten Schritt ($j = 1$) ist $w = z_2$. Wegen $(-6)^3 \equiv -14 \pmod{101}$ gilt $k_2 = l_2 = 5 \cdot 3 = 15$. Für $k = 65$ gilt schließlich $k \equiv 1 \pmod 4$ und $k \equiv 15 \pmod{25}$. Also ist $2^{65} \equiv 57 \pmod{101}$.

Bemerkung 10.12.

(i) Eine *Hash-Funktion* ist eine leicht zu berechnende Funktion $h\colon A \to B$, sodass Urbilder $f^{-1}(b)$ für $b \in B$ nur sehr schwer berechenbar sind. In der Praxis ist $|B| < |A|$, sodass h im Gegensatz zu Ein-Weg-Funktionen nicht injektiv sein kann. Dennoch möchte man, dass *Kollisionen* $f(a) = f(a')$ mit $a \neq a'$ in der Praxis nicht auftreten. Aufgrund des *Geburtstagsparadoxons* treten Kollisionen überraschend häufig auf (die Wahrscheinlichkeit, dass von 23 Personen zwei am gleichen Tag Geburtstag haben, ist größer als 50%).

(ii) Hash-Funktionen werden beispielsweise für den Abgleich von Passwörtern bei Logins benutzt. Anstatt ein Passwort a im Klartext zu speichern, speichert man nur den Hashwert (Fingerabdruck) $h(a)$ in einer Datenbank. Wird beim Login ein Passwort a' eingegeben, so prüft man $h(a') = h(a)$. Mit den Hashwerten aus der Datenbank kann ein Angreifer nichts anfangen. Um das Ausprobieren von häufig verwendeten Passwörtern (Wörterbuch-Angriff) zu unterbinden, kann man vor dem „Hashen“ die Passwörter mit einem *Salt*, also einer zufälligen Zeichenfolge erweitern.

(iii) Im Alltag benutzen wir Hash-Funktionen oft unbewusst, zum Beispiel beim Abgleich von Telefonnummern (ein Blick auf die letzten Ziffern genügt). Der kryptographisch unsichere Algorithmus (Kollisionen sind bekannt) *MD5* (Message-digest) wird benutzt, um Dateien auf Fehler zu prüfen (etwa nach einem Download). Er wandelt eine Eingabe beliebiger Länge in eine Folge von 16 Bytes um (es gibt also $2^{128} \approx 10^{38}$ mögliche Hashwerte). Als derzeit kollisionsresistent und kryptographisch sicher gilt der Algorithmus *SHA-2*.

(iv) Bei *symmetrischen* Krypto-Systemen wird zum Verschlüsseln und Entschlüsseln der gleiche Schlüssel benutzt (der Algorithmus kann sich jedoch unterscheiden). Es stellt sich die Frage wie sich beide Parteien vor der Nachrichtenübertragung auf einen geheimen Schlüssel einigen. Eine Lösung dieses scheinbar einfachen Problems wurde erst in den 70er Jahren von Diffie, Hellman und Merkle entwickelt. Es verwendet den diskreten Logarithmus als Ein-Weg-Funktion.

Satz 10.13 (DHM-Schlüsselaustausch)**.** *Euler und Gauß wählen öffentlich eine Gruppe $G = \langle g \rangle$. Euler wählt geheim $a \in \mathbb{N}$ und schickt g^a an Gauß. Gauß wählt geheim $b \in \mathbb{N}$ und schickt g^b an Euler. Beide können nun $(g^a)^b = g^{ab} = (g^b)^a$ als geheimen Schlüssel verwenden.*

Beweis. Trivial. □

Bemerkung 10.14.

(i) Nach dem Pohlig-Hellman-Algorithmus hängt die Sicherheit des DHM-Schlüsselaustauschs von der Primfaktorzerlegung von $|G|$ ab. In der Praxis wählt man eine Germain-Primzahl $p > 10^{100}$, d. h. $n := 2p + 1$ ist ebenfalls eine Primzahl (man nennt dann n eine *sichere* Primzahl). Für $G = (\mathbb{Z}/n\mathbb{Z})^\times$ gilt $|G| = \varphi(n) = 2p$, sodass Satz 10.10 immer noch die Berechnung des diskreten Logarithmus modulo p erfordert.

(ii) Der DHM-Schlüsselaustausch schützt nicht vor sogenannten *Man-in-the-Middle-Angriffen*, bei denen ein Angreifer, sagen wir Fermat, den Datenaustausch der Parteien manipulieren kann. Fermat empfängt g^a von Euler und g^b von Gauß, aber schickt g^c an beide. Euler berechnet den Schlüssel g^{ac}, während Gauß g^{bc} als Schlüssel berechnet. Fermat verfügt über beide Schlüssel und kann daher die weitere Kommunikation entschlüsseln. Darauf kommen wir in Bemerkung 10.25 zurück.

(iii) Der DHM-Schlüsselaustausch setzt voraus, dass man große (sichere) Primzahlen zufällig generieren kann. Dazu benutzt man Zufallszahlengeneratoren und effiziente Primzahltests. Echte Zufallszahlen lassen sich nicht deterministisch generieren. In der Praxis genügend aber sogenannte *Pseudozufallszahlen*.

(iv) (Linearer Kongruenzgenerator) Gegeben seien natürliche Zahlen $a, b < n$, wobei n möglichst groß ist. Man generiert einen Startwert (*seed*) $x_0 \in \mathbb{N}$ (zum Beispiel aus der Systemzeit oder aus Rauschen analoger Geräte). Die rekursive Folge

$$x_{i+1} := ax_i + b \pmod n$$

mit $i \in \mathbb{N}$ liefert Pseudozufallszahlen. Auf diesem Algorithmus basiert der Befehl `rand()` in den Programmiersprachen C und C++. Für ernsthafte kryptographische Anwendungen sind die erzeugten Zahlen aber nicht zufällig genug. Man kann den Algorithmus auf viele Arten variieren zum Beispiel, indem man nicht-lineare Funktionen in mehr als zwei Parametern benutzt. Abhängig von den gewählten Parametern wird sich die Folge in jedem Fall aber früher oder später wiederholen.

Beispiel 10.15. Sei $n = 1000$, $x_0 := 387$ und $x_{i+1} := 19x_i + 397 \pmod n$. Dies liefert die Folge:

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
x_i	387	750	647	690	507	30	967	770	27	910	687	687	450	947	390	807

Die Folge wiederholt sich erstmals nach 100 Gliedern, d. h. $x_{100} = x_0$.

Bemerkung 10.16. Sei $n \in \mathbb{N}$ eine zufällig erzeugte Zahl mit 100 Dezimalziffern. Durch eine geeignete Wahl der letzten Dezimalziffer können wir $\mathrm{ggT}(n, 30) = 1$ annehmen (Aufgabe 21). Es gibt $\frac{\varphi(30)}{30}(10^{101} - 10^{100}) = \frac{6}{5}10^{100}$ solche Zahlen. Nach dem Gaußschen Primzahlsatz gibt es

$$\pi(10^{101}) - \pi(10^{100}) \approx \frac{10^{101}}{101 \ln(10)} - \frac{10^{100}}{100 \ln(10}$$

Primzahlen mit 100 Dezimalziffern. Die Wahrscheinlichkeit, dass n eine Primzahl ist, beträgt also ca.

$$\frac{25}{3 \cdot 101 \ln(10)} - \frac{1}{6 \cdot 20 \ln(100)} \approx 0{,}016.$$

Dies kann man mit dem Miller-Rabin-Test prüfen. Hat man eine große Primzahl p gefunden, so kann man mit dem folgenden Test verifizieren, ob $2p + 1$ eine sichere Primzahl ist.

Satz 10.17 (Pocklington-Test). *Sei $p \in \mathbb{P}$ und $n = 2p + 1$. Genau dann ist $n \in \mathbb{P}$, wenn ein $a \in \mathbb{N}$ mit $a^{2p} \equiv 1 \pmod n$ und $a^2 \not\equiv 1 \pmod n$ existiert.*

Beweis. Ist $n \in \mathbb{P}$, so erfüllt jede Primitivwurzel a die angegebenen Bedingungen. Nehmen wir umgekehrt an, dass die Bedingungen für a gelten. Dann ist $p \mid \mathrm{ord}_n(a) \mid \varphi(n)$. Ist n keine Primzahl, so ist $\varphi(n)$ ein Produkt von Zahlen $\leq \frac{1}{3}n < p$. $\square$

Beispiel 10.18. Wir beschreiben einige symmetrische Krypto-Systeme:

(i) (Caesar-Verschlüsselung) Gegeben ist ein Nachrichtentext t aus lateinischen Buchstaben (A, $B, \ldots, Z$) und eventuell Leerzeichen. Der Schlüssel ist eine Zahl $1 \leq s \leq 25$. Zum Verschlüsseln wird jeder Buchstabe in t um s im Alphabet verschoben, modulo 26 (Leerzeichen können ignoriert werden). Besonders praktisch ist die Wahl $s = \frac{26}{2} = 13$, weil hier Verschlüsseln und Entschlüsseln identisch ist (*ROT13*). Da es nur 25 mögliche Schlüssel gibt, ist das Verfahren äußerst unsicher. In der Praxis genügt es die ersten Buchstaben der verschlüsselten Nachricht zu betrachten, um Schlüssel auszuschließen.

(ii) (Substitutionsverschlüsselung) Wieder ist ein Nachrichtentext t mit Buchstaben eines Alphabets A gegeben (A könnte Groß- und Kleinbuchstaben, Umlaute, Satzzeichen oder Sonderzeichen beinhalten). Der Schlüssel ist eine Permutation $\pi\colon A \to A$. Bei der Verschlüsselung wird jeder Buchstabe $a \in A$ in t durch $\pi(a)$ ersetzt. Obwohl es hier eine große Anzahl möglicher Schlüssel gibt (nämlich $|A|! \ge 26! \approx 4 \cdot 10^{26}$), können verschlüsselte Nachrichten durch eine Häufigkeitsanalyse entschlüsselt werden. In deutschen Texten tritt beispielsweise der Buchstabe e häufiger als andere Buchstaben auf. Man kann also Rückschlüsse ziehen, an welchen Stellen sich im Klartext ein e befinden könnte.

(iii) (One-Time-Pad) Gegeben ist eine Nachricht im Binärformat $t = (t_1, \ldots, t_n)$ mit $t_1, \ldots, t_n \in \{0, 1\}$. Der Schlüssel hat ebenfalls Binärformat $s = (s_1, \ldots, s_n)$ mit $s_1, \ldots, s_n \in \{0, 1\}$. Verschlüsselt wird durch Addition in $\mathbb{F}_2$:[16]

$$\tilde{t} := t + s = (t_1 + s_1, \ldots, t_n + s_n).$$

Wegen $\tilde{t} + s = t + (s + s) = t$ sind Ver- und Entschlüsseln identische Verfahren. Wegen $t_i + s_i = 0 \Leftrightarrow t_i = s_i$ kann man aus $t_i + s_i$ keinerlei Rückschlüsse auf t_i ziehen ($t_i = 0$ und $t_i = 1$ sind gleichwahrscheinlich). Daher ist das Verfahren absolut sicher, aber unpraktikabel, da der Schlüssel genauso viel Speicher wie die Nachricht benötigt. Wird s benutzt, um eine weitere Nachricht $\tilde{r} = r + s$ zu verschlüsseln (entgegen des Namens), so kann ein Angreifer $\tilde{t} + \tilde{r} = t + r$ berechnen. Mit Häufigkeitsanalysen kann man Rückschlüsse auf t und r ziehen.

(iv) (Advanced Encryption Standard, AES) Eine Nachricht im Binärformat wird aufgeteilt in Blöcke von je 16 Bytes. Jedes der 16 Bytes besteht aus acht Bits und kann daher als Element des Körper $\mathbb{F}_{2^8}$ repräsentiert werden. Jeder Block wird als 4×4-Matrix $A = (a_{ij}) \in \mathbb{F}_{2^8}^{4\times 4}$ interpretiert. Der Algorithmus benutzt eine Bijektion $f\colon \mathbb{F}_{2^8} \to \mathbb{F}_{2^8}$ mit

$$f(x) = \begin{cases} ax^{-1} + b & \text{falls } x \ne 0, \\ b & \text{falls } x = 0 \end{cases}$$

für gewisse $a, b \in \mathbb{F}_{2^8}^\times$. Weiterhin ist eine Matrix $M \in \mathrm{GL}(4, 8)$ gegeben. Der Schlüssel $s = s_1$ ist ebenfalls ein Block von 16 Bytes. Die Matrix A wird nun in 10 Runden wie folgt manipuliert:

Für $i = 1, \ldots, 10$:

Ersetze A durch

$$M \begin{pmatrix} f(a_{11}) & f(a_{12}) & f(a_{13}) & f(a_{14}) \\ f(a_{22}) & f(a_{23}) & f(a_{24}) & f(a_{21}) \\ f(a_{33}) & f(a_{34}) & f(a_{31}) & f(a_{32}) \\ f(a_{44}) & f(a_{41}) & f(a_{42}) & f(a_{43}) \end{pmatrix} \oplus s_i.$$

Erzeuge s_{i+1} aus s_i.

Hierbei beschreibt $\oplus$ die elementweise Bit-Addition der entsprechenden Matrixeinträge. Die Erzeugung von s_{i+1} aus s_i hängt vom gewählten Modus ab. Im einfachsten und unsichersten Modus (Electronic Code Book, ECB) ist $s_{i+1} = s_i = s_1$. Auf die anderen Modi gehen wir nicht im Detail

[16] In der Informatik spricht man vom XOR-Operator, der ein „Entweder oder“ ausführt.

ein (mathematisch uninteressant). Da f nur 256 Werte annimmt, werden diese explizit gespeichert, um die Anwendung von f zu beschleunigen. Bei der Entschlüsslung wird das Verfahren rückwärts ausgeführt.

Der Algorithmus erfüllt die von Shannon eingeführten Kriterien *Diffusion* (selbst kleine Änderung der Eingabe sollten größere Änderungen der Ausgabe bewirken) und *Konfusion* (zwischen Eingabe, Schlüssel und Ausgabe sollte keine einfache, z. B. lineare Beziehung bestehen).

AES ist ein weitverbreiteter Krypto-Standard, der sogar auf Hardware-Ebene implementiert ist.[17] Der Algorithmus wird zum Beispiel für WLAN-Kommunikation eingesetzt (WPA2).

Bemerkung 10.19. Wir kommen nun zu *asymmetrischen* Krypto-Systemen, bei denen zum Ver- und Entschlüsseln unterschiedliche Schlüssel verwenden werden. Damit können einander unbekannte Parteien kommunizieren, ohne zuvor einen Schlüssel ausgetauscht zu haben. Das erste Verfahren basiert wieder auf dem diskreten Logarithmus.

Satz 10.20 (ELGAMAL-Verfahren)**.** *Sei $G = \langle g\rangle$ eine Gruppe der Ordnung n. Euler wählt geheim einen* privaten *Schlüssel $d \in \mathbb{N}$ und gibt den* öffentlichen *Schlüssel $h := g^d$ bekannt. Gauß möchte eine Nachricht $t \in G$ an Euler schicken. Dazu wählt er eine Zufallszahl $k \in \mathbb{N}$ und verschickt das Paar $(g^k, h^k t)$. Euler entschlüsselt die Nachricht mit $t = (g^k)^{-d} h^k t$.*

Beweis. Die Behauptung folgt aus $(g^k)^d = (g^d)^k = h^k$. □

Satz 10.21 (RSA-Verfahren[18])**.** *Euler wählt geheim zwei verschiedene Primzahlen p, q und setzt $n := pq$. Der öffentliche Schlüssel von Euler besteht aus n und einer weiteren zu $\varphi(n)$ teilerfremden Zahl e (oft wählt man die Fermat-Primzahl $e = 2^{2^4} + 1 = 65537$). Der private Schlüssel von Euler ist $d \in \mathbb{N}$ mit $de \equiv 1 \pmod{\varphi(n)}$. Gauß möchte eine Nachricht $t < n$ an Euler schicken. Er verschlüsselt seine Nachricht als $\tilde{t} := t^e \pmod n$. Euler kann durch $t \equiv \tilde{t}^d \pmod n$ entschlüsseln.*

Beweis. Sei $a \in \mathbb{Z}$ mit $de = 1 + a\varphi(n)$. Nach Euler-Fermat gilt $\tilde{t}^d \equiv t^{de} \equiv t(t^{\varphi(n)})^a \equiv t \pmod n$. Wegen $t < n$ ist t durch die Restklasse $\tilde{t}^d + n\mathbb{Z}$ eindeutig bestimmt. □

Bemerkung 10.22. Das RSA-Verfahren wird an vielen Stellen für die Kommunikation im Internet genutzt (HTTPS, SSH, PGP, VPN etc.). Die Sicherheit basiert auf der Schwierigkeit der Primfaktorzerlegung von n, wenn p und q genügt groß sind. Ohne Kenntnis von p und q kann man weder $\varphi(n)$ noch d aus n und e berechnen. Außerdem kennt man keinen schnellen Algorithmus zur Berechnung der (diskreten) e-ten Wurzel aus $\tilde{t}$. Kennt man $\varphi(n) = (p-1)(q-1) = n - p - q + 1$, so kann man p und q als Lösung der quadratischen Gleichung $X^2 + (\varphi(n) - n - 1)X + n = 0$ bestimmen.

[17] Unter anderen in den meisten Intel i3, i5 und i7 Prozessoren

[18] Benannt nach RIVEST, SHAMIR und ADLEMAN

Beispiel 10.23. Die Seite `https://www.uni-hannover.de` benutzt den öffentlichen 2048-bit Schlüssel:

$$
\begin{aligned}
n = {} & 80409729020175958416756576209636997107230954204530745496259958765504450237823179\\
& 46561632329522754965271046574853851349673374084363450099777281296457067064507439\\
& 56176563384533851106410986353692839865946702914876875636580409962216287798998276\\
& 65844688974539265194324488012624252238123419484862944566381071145365892978719157\\
& 26049612921467415859662011505094403114129370528910494566048308399881902465282666\\
& 97286741413900129860255294665119080802030528133808354115327889235773371455487445\\
& 51859948344067491402559082615153816705680957149227400676127581978616964716256953\\
& 37772678974623853724849569150073041086608225485909645052886256117120018221192647\\
& 41011605033755571165375097731952989542102157180321716440117385673147891283233890\\
& 97743042788667586045863826029554623077159601221066678267135423041517167794004247\\
& 54360589201191230946407014136178783718752334220120685024486586451796457818330838\\
& 98365472234891716647496250801882470415987624658991379703365228665719509557328047\\
& 00077318060602574835322553556048031856131403920197084007609298210413848235821432\\
& 34209898031637800790351360153430371471039730049220618082585515358687599357387181\\
& 64609306021972433318394035956161479465720626055354947315137055607140703046593366\\
& 1822177053643541304295153526113 79\\
e = {} & 65537
\end{aligned}
$$

Satz 10.24. *Beim RSA-Verfahren lassen sich p und q effizient aus n, e und d berechnen.*

Beweis. Wir orientieren uns am Beweis von Satz 4.27. O. B. d. A. seien p und q ungerade. Sei $a \in \{2, \ldots, n-1\}$ zufällig und gleichverteilt gewählt. Im Fall $\mathrm{ggT}(a, n) \neq 1$ gilt $\mathrm{ggT}(a, n) \in \{p, q\}$ und man kann p (bzw. q) mit dem euklidischen Algorithmus berechnen. Sei also $\mathrm{ggT}(a, n) = 1$. Dann gilt $\mathrm{ord}_n(a) \mid \varphi(n) = (p-1)(q-1)$. Die Wahrscheinlichkeit, dass $\mathrm{ord}_n(a)$ ungerade ist, beträgt höchstens $\frac{1}{4}$. Indem wir genügend viele Zufallszahlen wählen, können wir $2 \mid \mathrm{ord}_n(a)$ annehmen. Nach Konstruktion gilt $b := de - 1 \equiv 0 \pmod{\varphi(n)}$ und $a^b \equiv 1 \pmod{n}$. Sei $b = 2^k m$ mit $2 \nmid m$. Wegen $2 \mid \mathrm{ord}_n(a)$ existiert ein $l < k$ mit $a^{2^l m} \not\equiv 1 \pmod{n}$ und $a^{2^{l+1} m} \equiv 1 \pmod{n}$. Wie im Beweis von Satz 4.27 zeigt man, dass $a^{2^l m} \not\equiv -1 \pmod{n}$ mit Wahrscheinlichkeit $\geq \frac{3}{4}$ gilt. Dies können wir annehmen. Nun gilt

$$n \mid a^{2^{l+1} m} - 1 = (a^{2^l m} - 1)(a^{2^l m} + 1).$$

Da n weder $a^{2^l m} - 1$ noch $a^{2^l m} + 1$ teilen kann, ist $\mathrm{ggT}(a^{2^l m} - 1, n) \in \{p, q\}$. Die Behauptung folgt mit dem euklidischen Algorithmus. $\square$

Bemerkung 10.25.

(i) Benutzt Euler zur Berechnung von $\tilde{t}^d$ die binäre Exponentation, so kann ein *Seitenkanal*-Angreifer die Binärdarstellung von d aus einer Laufzeitmessung bestimmen (für jede 1 in der Binärdarstellung wird eine zusätzliche Multiplikation benötigt). Um das zu verhindern, benutzt man Algorithmen zum Potenzieren, die nicht von der Binärdarstellung des Exponenten abhängen (Aufgabe 50).

(ii) Beim RSA-Verfahren kann ein Man-in-the-Middle-Angreifer die verschlüsselten Nachrichten zwar nicht lesen, aber beliebig manipulieren, denn er benötigt dafür nur den öffentlichen Schlüssel. Abhilfe schaffen sogenannte *Signaturen*. Sei (n', e') der öffentliche Schlüssel von Gauß und d' der private Schlüssel. Zunächst berechnet Gauß einen ganzzahligen Hashwert $h(t)$ seiner geheimen Nachricht t. Anschließend übermittelt er neben der verschlüsselten Nachricht $\tilde{t} = t^e \pmod{n}$ auch die Signatur $s(t) := h(t)^{d'} \pmod{n'}$. Euler kann sowohl t als auch $h(t) = s(t)^{e'} \pmod{n'}$

berechnen und vergleichen (die Hash-Funktion h sei öffentlich bekannt). Ein Angreifer kann weder t aus $h(t)$ bestimmen, noch $s(t')$ für eine manipulierte Nachricht t' berechnen. Auf diese Weise kann Euler verifizieren, dass die Nachricht wirklich von Gauß stammt. Durch die Schwierigkeit des diskreten Logarithmus gibt Gauß mit $s(t)$ seinen privaten Schlüssel nicht preis.

(iii) Ein Angreifer könnte versuchen sich mit dem eigenen öffentlichen Schlüssel als Euler auszugeben. Um sicher zu gehen, dass öffentliche RSA-Schlüssel den richtigen Personen oder Webseiten zugeordnet sind, verwendet man *Zertifikate*. Dafür muss Euler bei einer Zertifizierungsstelle wie beispielsweise der LUH[19] persönlich seinen Ausweis vorlegen. Die LUH bürgt mit der Ausgabe des Zertifikats, dass der öffentliche Schlüssel korrekt zugeordnet ist. Gauß kann Eulers Zertifikat nur überprüfen, wenn er der LUH vertraut. Dies ist durch ein Netz an verbundenen Zertifizierungsstellen gegeben. Zum Beispiel wird das Zertifikat der LUH von der höheren Stelle *GEANT OV RSA CA 4* ausgegeben. Diese wiederum erhält ihr Zertifikat vom *Wurzelzertifikat USERTrust RSA Certification Authority*, dem alle gängigen Betriebssysteme vertrauen.

(iv) Ähnlich wie beim DHM-Schlüsselaustausch muss man auch beim RSA-Verfahren darauf achten, dass $p-1$ und $q-1$ nicht in „zu kleine" Primzahlen zerfallen. Dies veranschaulicht der folgende Algorithmus.

Satz 10.26 (Pollards $p-1$-Methode)**.** *Der folgende Algorithmus findet Teiler einer Zahl $n \in \mathbb{N}$.*

Wähle eine Schranke $S \in \mathbb{N}$.
Berechne das Produkt q aller Primzahlpotenzen kleiner S.
Wähle zufällig $a \in \{2, \dots, n-1\}$.
Berechne $d := \operatorname{ggT}(a^q - 1, n)$.
Gilt $1 < d < n$, so hat man einen echten Teiler von n gefunden.
Anderenfalls wähle ein neues a oder passe S an.

Beweis. Es gibt eigentlich nichts zu beweisen, aber wir begründen die Motivation des Algorithmus. Angenommen n besitzt einen Primteiler p, sodass $p-1$ ein Produkt von Primzahlpotenzen $< S$ ist. Dann gilt $a^q \equiv 1 \pmod p$ für alle $a < p$ nach Euler-Fermat. Ist sogar $a^q \equiv 1 \pmod n$ (also $d = n$), so ist $\operatorname{ord}_n(a)$ „zu klein" oder n zerfällt in lauter Primteiler p, sodass $p-1$ ein Produkt von Primzahlpotenzen $< S$ ist. Diese Situation kann man durch Anpassen von a bzw. S verändern. □

Satz 10.27 (Pollards ρ-Methode)**.** *Sei $n \in \mathbb{N}$ und $x_0 = y_0 \in \mathbb{N}$ ein beliebiger Startwert. Sei $f\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ eine möglichst zufällige Funktion.*

Für $i \in \mathbb{N}$:
  Berechne $x_i := f(x_{i-1}) \pmod n$ und $y_i := f(f(y_{i-1}))$.
  Gilt $1 < \operatorname{ggT}(x_i - y_i, n) < n$, so kennt man einen Teiler von n.

Beweis. Die Folge (x_i) muss sich nach endlich vielen Schritten wiederholen. Es gibt also $i < j$ mit $x_i \equiv x_j \pmod n$. Für jeden (Prim)teiler $p \nmid n$ gilt ebenfalls $x_i \equiv x_j \pmod p$. Die Idee des Algorithmus ist, dass sich die Folge $(x_i \pmod p)_i$ möglicherweise schon eher wiederholt, sodass $x_i \equiv x_j \pmod p$ und $x_i \not\equiv x_j \pmod n$ gilt. In diesem Fall liefert $\operatorname{ggT}(x_i - x_j, n)$ einen echten Teiler von n. Wir überlegen uns, dass man nicht alle Differenzen $x_i - x_j$ betrachten muss. Sei dafür $\delta := j - i$. Dann gilt $x_i \equiv x_{i+\delta} \pmod p$ und $x_k \equiv x_{k+\delta} \pmod p$ für alle $k \geq i$. Für $k := m\delta \geq i$ gilt nun $x_k \equiv x_{2k} \equiv y_k \pmod p$. □

[19] LUH-Nutzerzertifikate

Beispiel 10.28.

(i) Sei $n := 9701$, $x_0 = y_0 = 2$ und $f(x) := x^2 + 3 \pmod{n}$. Dann gilt

$$\begin{array}{c|cccc} i & 0 & 1 & 2 & 3 \\ \hline x_i & 2 & 7 & 52 & 2707 \\ y_i & 2 & 52 & 3597 & 7424 \end{array}$$

und $\operatorname{ggT}(7424 - 2707, n) = 89$.

(ii) Mit Pollards ρ-Methode wurde der kleinste Primzahl der 8. Fermat-Zahl

$$F_8 = 2^{2^8} + 1 \equiv 0 \pmod{1238926361552897}.$$

gefunden.

Satz 10.29 (Quadratisches Sieb). *Sei $n \in \mathbb{N}$ und $p_1, \ldots, p_r$ „kleine" Primzahlen. Wähle Zahlen $x_1, \ldots, x_m$ mit der Eigenschaft $x_i^2 \equiv \prod_{j=1}^r p_j^{a_{ij}} \pmod{n}$ für $i = 1, \ldots, m$ und gewisse $a_{ij} \in \mathbb{N}_0$. Sei $A := (a_{ji} + 2\mathbb{Z})_{ij} \in \mathbb{F}_2^{r \times m}$. Angenommen es existiert ein $v = (v_i) \in \mathbb{F}_2^m \setminus \{0\}$ mit $Av = 0$. Sei*

$$x := x_1^{v_i} \ldots x_m^{v_m} \pmod{n},$$
$$y := \prod_{i=1}^r p_i^{\frac{1}{2}(a_{i1}v_1 + \ldots + a_{im}v_m)} \pmod{n}.$$

Dann gilt $\operatorname{ggT}(x - y, n) \neq 1$ *oder* $\operatorname{ggT}(x + y, n) \neq 1$.

Beweis. Nach Voraussetzung ist $\sum_{j=1}^m a_{ij}v_j = (Av)_i \equiv 0 \pmod{2}$ für $i = 1, \ldots, r$. Daher ist $y \in \mathbb{N}$. Außerdem gilt

$$x^2 \equiv x_1^{2v_1} \ldots x_m^{2v_m} \equiv \prod_{i=1}^m \prod_{j=1}^r p_j^{a_{ij}v_i} = \prod_{j=1}^r p_j^{\sum_{i=1}^m a_{ij}v_i} \equiv y^2 \pmod{n}.$$

Es folgt $(x + y)(x - y) = x^2 - y^2 \equiv 0 \pmod{n}$. □

Bemerkung 10.30. Mit dem Heron-Verfahren kann man $\sqrt{n}$ berechnen (insbesondere kann man prüfen, ob n eine Quadratzahl ist, vgl. Aufgabe 47). Es bietet sich an, die x_i oberhalb von $\sqrt{n}$ zu wählen, denn dann ist $x_i^2 - n$ „klein" und kann leicht faktorisiert werden. Ist r klein genug, so genügen Probedivisionen (gelingt das nicht, so hat $x_i^2 - n$ nicht die gewünschte Form). Für $m > r$ lässt sich $Av = 0$ stets (mit dem Gauß-Algorithmus) lösen, d. h. der Algorithmus ist erfolgreich sofern man genügend viele x_i findet. Für „große" Zahlen n bis ca. 100 Dezimalstellen ist das quadratische Sieb das schnellste bekannte Faktorisierungsverfahren. Für noch größere Zahlen benutzt man das *Zahlkörpersieb*. Dies ist ein ähnlicher Algorithmus im Ganzheitsring eines Zahlkörpers. Liegen die Primzahlen p und q beim RSA-Verfahren nah beieinander, so kann es passieren, dass man beim quadratischen Sieb auf $x = x_i = \frac{p+q}{2}$ stößt. Mit $y := \frac{|p-q|}{2}$ gilt dann $x^2 - y^2 = pq = n$ und $\{x + y, x - y\} = \{p, q\}$.

Beispiel 10.31.

(i) Sei $n = 101069$ und $\{p_1, p_2, p_3\} = \{2, 5, 11\}$. Mit $\lceil \sqrt{n} \rceil = 318$ finden wir folgende Zerlegungen:

$$318^2 - n = 5 \cdot 11,$$
$$320^2 - n = 11^3,$$
$$337^2 - n = 2^2 \cdot 5^5.$$

Also ist

$$A = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

mit der Lösung $v = (1, 1, 1)$. Wir setzen $x = 318 \cdot 320 \cdot 337 \equiv 30729 \pmod{n}$ und $y = 2 \cdot 5^3 \cdot 11^2 = 30250$. Dies liefert $\mathrm{ggT}(x + y, n) = 211$ und $\mathrm{ggT}(x - y, n) = 479$.

(ii) 1994 hat man eine als RSA-129 bekannte 129-stellige Zahl mit dem quadratischen Sieb in die folgenden Primzahlen faktorisiert:

$$3490529510847650949147849619903898133417764638493387843990820577$$
$$32769132993266709549961988190834461413177642967992942539798288533$$

Definition 10.32. Sei K ein Körper und $a_1, \ldots, a_5 \in K$. Man nennt

$$\mathcal{E}(a_1, \ldots, a_5) := \left\{(x, y) \in K^2 : y^2 + a_1xy + a_2y = x^3 + a_3x^2 + a_4x + a_5\right\}$$

eine *elliptische Kurve*.[20]

Lemma 10.33. *Im Fall* $\mathrm{Char}\, K \notin \{2, 3\}$ *lässt sich jede elliptische Kurve durch eine affine Transformation in die* Weierstraß-Normalform

$$\mathcal{E}(a, b) := \left\{(x, y) \in K^2 : y^2 = x^3 + ax + b\right\}$$

mit $a, b \in K$ *überführen.*

Beweis. Für $y \in K$ sei $\widetilde{y} := y + \frac{1}{2}a_1x + \frac{1}{2}a_2$ (wohldefiniert wegen $\mathrm{Char}\, K \neq 2$). Dann gilt

$$(x, y) \in \mathcal{E}(a_1, \ldots, a_5) \iff \widetilde{y}^2 = y^2 + a_1xy + a_2y + \frac{1}{4}a_1^2x^2 + \frac{1}{4}a_2^2 + \frac{1}{2}a_1a_2x = x^3 + a'x^2 + b'x + c'$$

mit gewissen $a', b', c' \in K$. Mit der affinen Transformation $\widetilde{x} := x + \frac{1}{3}a'$ erhält man $\widetilde{y}^2 = \widetilde{x}^3 + a\widetilde{x} + b$ mit gewissen $a, b \in K$. $\square$

Bemerkung 10.34. Wir betrachten im Folgenden ausschließlich elliptische Kurven in Weierstraß-Normalform.

Definition 10.35. Sei $\mathcal{E} = \mathcal{E}(a, b)$ eine elliptische Kurve. Sei $O = (\infty, \infty)$ ein neues Symbol und $\mathcal{E}^+ := \mathcal{E} \cup \{O\}$. Für $P \in \mathcal{E}^+$ sei $P + O := P =: O + P$. Für $P = (x_1, y_2) \in \mathcal{E}$, $Q = (x_2, y_2) \in \mathcal{E}$ sei $P + Q = (x_3, y_3) = \left(d^2 - x_1 - x_2,\ d(x_1 - x_3) - y_1\right)$ mit

$$d := \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{falls } P \neq Q, \\ \frac{3x_1^2 + a}{2y_1} & \text{falls } P = Q. \end{cases}$$

Lemma 10.36. *Sei* $\mathcal{E}$ *eine elliptische Kurve. Dann gilt* $P + Q \in \mathcal{E}^+$ *für alle* $P, Q \in \mathcal{E}^+$.

[20] Die Gleichung selbst beschreibt keine Ellipse, aber Gleichungen dieser Form treten bei Kurvenintegralen von Ellipsen auf.

Beweis. O. B. d. A. sei $P = (x_1, y_1) \neq O$ und $Q = (x_2, y_2) \neq O$. Sei zunächst $x_1 \neq x_2$ und $d = \frac{y_2 - y_1}{x_2 - x_1} \in K$. Wir betrachten das normierte Polynom

$$\alpha := X^3 + aX + b - \big(d(X - x_1) + y_1\big)^2 \in K[X].$$

Offenbar gilt $\alpha(x_1) = \alpha(x_2) = 0$. Polynomdivision liefert ein $x_3 \in K$ mit $\alpha = (X - x_1)(X - x_2)(X - x_3)$. Ein Koeffizientenvergleich von X^2 zeigt $d^2 = x_1 + x_2 + x_3$, d. h. $x_3 = d^2 - x_1 - x_2$. Für $y_3 := d(x_1 - x_3) - y_1$ gilt

$$y_3^2 = \big(d(x_3 - x_1) + y_1\big)^2 = x_3^3 + ax_3 + b - \alpha(x_3) = x_3^3 + ax_3 + b.$$

Dies zeigt $P + Q = (x_3, y_3) \in \mathcal{E}^+$.

Sei nun $x_1 = x_2$. Dann gilt $y_1^2 = y_2^2$, d. h. $y_1 = \pm y_2$. Ist $y_1 = -y_2$, so liefert die Definition $P + Q = O$, indem man $\frac{1}{0} = \infty$ interpretiert. Sei schließlich $P = Q$ und $y_1 \neq 0$. Dann ist $d = \frac{3x_1^2 + a}{2y_1} \in K$. Die (formale) Ableitung von α (wie oben) ist

$$\alpha' = 3X^2 + a - 2d\big(d(X - x_1)^2 + y_1\big).$$

Wegen $\alpha'(x_1) = 3x_1^2 + a - 2y_1 d = 0$ ist x_1 eine doppelte Nullstelle von α. Daher existiert ein $x_3 \in K$ mit $\alpha = (X - x_1)^2(X - x_3)$. Ein Koeffizientenvergleich von X^2 zeigt $x_3 = d^2 - 2x_1$. Für $y_3 := d(x_1 - x_3) - y_1$ gilt wie zuvor $y_3^2 = x_3^3 + ax_3 + b$. Also ist auch in diesem Fall $P + Q = (x_3, y_3) \in \mathcal{E}^+$. □

Bemerkung 10.37. Es liegt nahe zu vermuten, dass $\mathcal{E}^+$ eine abelsche Gruppe ist. Offensichtlich ist O ein neutrales Element und $(x, -y)$ ist invers zu $(x, y) \in \mathcal{E}$. Man sieht außerdem leicht, dass $P + Q = Q + P$ für alle $P, Q \in \mathcal{E}^+$ gilt. Die Assoziativität hingegen ist keineswegs klar und gilt nur unter einer Zusatzannahme. Zum Beispiel ist $(0, 0), (1, 1) \in \mathcal{E}(0, 0)$ und $(0, 0) + (1, 1) = (0, 0)$ im Widerspruch zu $(1, 1) \neq O$.

Definition 10.38. Eine elliptische Kurve $\mathcal{E}(a, b)$ heißt *singulär*, falls $4a^3 + 27b^2 = 0$.

Bemerkung 10.39.

(i) Man kann zeigen, dass eine elliptische Kurve $\mathcal{E}(a, b)$ genau dann singulär ist, wenn das Polynom $X^3 + aX + b \in K[X]$ eine mehrfache Nullstelle besitzt.[21] Ist $\mathcal{E}$ nicht-singulär, so ist $\mathcal{E}^+$ tatsächlich eine abelsche Gruppe. Der Beweis der Assoziativität kann entweder mit einer langwierigen Rechnung[22] oder mit algebraischer Geometrie geführt werden.

(ii) Zu jedem $x \in K$ existiert höchstens ein $y \in K$ mit $(x, y), (x, -y) \in \mathcal{E}$. Für endliche Körper K gilt daher $|\mathcal{E}^+| = |\mathcal{E}| + 1 \leq 2|K| + 1$. Hasse bewies die stärkere Abschätzung

$$|K| - 2\sqrt{|K|} + 1 \leq |\mathcal{E}^+| \leq |K| + 2\sqrt{|K|} + 1.$$

Ein Element der Ordnung 2 in $\mathcal{E}^+$ hat die Form $(x, 0)$, wobei x eine Nullstelle von $X^3 + aX + b$ ist. Es kann daher höchstens drei solche Elemente geben. Man kann zeigen, dass $\mathcal{E}^+$ ein direktes Produkt von höchstens zwei zyklischen Gruppen ist. Oft ist $\mathcal{E}^+$ selbst zyklisch.

[21] siehe Diskriminante in Algebra-Skript

[22] siehe [Zwegers, *An Elementary Approach to the Group Law on Elliptic Curves*, 2024, arXiv:2401.02346v2]

(iii) Man kann den DHM-Schlüsselaustausch oder das Elgamal-Verfahren mit dem diskreten Logarithmus in $\mathcal{E}^+$ formulieren. Durch die Parameter K, a und b hat man deutlich mehr Möglichkeiten als im Restklassenring $\mathbb{Z}/n\mathbb{Z}$. Heuristisch kann dadurch ein gutes Sicherheitsniveau bei kürzerer Schlüssellänge erreichen. Bitcoin[23] nutzt zum Beispiel $\mathcal{E}(0,7) = \{(x,y) : y^2 = x^3 + 7\}$ über $K = \mathbb{F}_p$ mit

$$\begin{aligned} p &= 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1 \\ &= 115792089237316195423570985008687907853269984665640564039457584007908834671663 \in \mathbb{P}. \end{aligned}$$

Hier ist $\mathcal{E}^+$ zyklisch mit Primzahlordnung

$$\begin{aligned} |\mathcal{E}^+| &= 115792089237316195423570985008687907852837564279074904382605163141518161494337 \\ &= p - 432420386565659656852420866390673177326. \end{aligned}$$

Man vergleiche die Parametergrößenordnung mit Beispiel 10.23.

(iv) Shor hat effiziente Algorithmen für den diskreten Logarithmus und zur Faktorisierung von Zahlen auf Quantencomputern entwickelt. Sollten in Zukunft leistungsfähige Quantencomputer zur Verfügung stehen, so werden gängige asymmetrische Verschlüsselungsverfahren unsicher (symmetrische Verfahren wie AES sind davon bisher nicht betroffen). In der *Post-Quantum-Kryptographie* entwickelt man daher Alternativen. Sie basieren zum Beispiel auf Gittern, Linearen Codes oder Entscheidungsproblemen in endlich erzeugten (nicht-abelschen) Gruppen.

Beispiel 10.40. Sei $\mathcal{E} = \mathcal{E}(1,2)$ über $K = \mathbb{F}_{11}$. Wegen $4 + 27 \cdot 2^2 \equiv 2 \pmod{11}$ ist $\mathcal{E}$ nicht singulär. Man berechnet

$$\mathcal{E} = \bigl\{(1,\pm2),(2,\pm1),(4,\pm2),(5,0),(6,\pm2),(7,0),(8,\pm4),(9,\pm5),(10,0)\bigr\}$$

und $|\mathcal{E}^+| = 16$. Da es drei Elemente der Ordnung 2 gibt, ist $\mathcal{E}^+$ nicht zyklisch. Wegen

$$2(4,2) = \bigl(d^2 + 3, d(4 - x_3) - 2\bigr) = (8,4) \qquad \Bigl(d = \frac{3 \cdot 5 + 1}{4} = 4\Bigr)$$

besitzt $\mathcal{E}^+$ mit $(4,2)$ ein Element der Ordnung 8. Daher gilt $\mathcal{E}^+ \cong \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Aufgaben

Aufgabe 1 (2 Punkte)**.** Konstruieren Sie die 11-adische Entwicklung von 123456789.

Aufgabe 2 ($2 + 2$ Punkte)**.** Wir betrachten das Nim-Spiel aus Beispiel 1.6.

(a) Es seien drei Stapel mit jeweils 45, 33, 24 Münzen gegeben. Prüfen Sie, welcher der Spieler den Sieg erzwingen kann und geben Sie eine entsprechende Zugfolge an.

(b) Wer kann mit der Ausgangsposition $(m_1, m_2, m_3) = (1, 2k, 2k+1)$ oder $(1, 2k, 2k-1)$ gewinnen?

Aufgabe 3 ($2 + 2 + 2 + 2 + 3$ Punkte)**.** Die *Fibonacci-Zahlen* sind rekursiv definiert durch $f_1 := 1$, $f_2 := 1$ und $f_{n+2} := f_{n+1} + f_n$ für $n \in \mathbb{N}$.

(a) Zeigen Sie $f_1 + f_3 + \ldots + f_{2n+1} = f_{2n+2}$ für $n \geq 0$.

[23]siehe `https://en.bitcoin.it/wiki/Secp256k1`

(b) Zeigen Sie $1 + f_1 + f_2 + \ldots + f_n = f_{n+2}$ für $n \geq 1$.

(c) Für welche n ist f_n durch 3 teilbar?

(d) Für welche n ist f_n durch 4 teilbar?

(e) Beweisen Sie

$$f_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right)$$

für $n \in \mathbb{N}$.

Aufgabe 4 (3 Punkte)**.** Berechnen Sie $\operatorname{ggT}(813, 1329)$ und finden Sie $a, b \in \mathbb{Z}$ mit

$$813a + 1329b = \operatorname{ggT}(813, 1329).$$

Aufgabe 5 (3 Punkte)**.** (Lamé) Wie groß müssen $a, b \in \mathbb{N}$ mindestens sein, damit der euklidische Algorithmus zur Berechnung von $\operatorname{ggT}(a, b)$ genau $k \in \mathbb{N}$ Iterationen durchläuft?
Hinweis: Die Lösung führt auf eine bekannte Zahlenfolge.

Aufgabe 6 (Münzproblem)**.** Angenommen Sie besitzen beliebig viele Münzen im Wert von a und b Euro, wobei $a, b \in \mathbb{N}$ teilerfremd seien. Zeigen Sie:

(a) Sie können den Betrag $ab - a - b$ Euro nicht exakt (d. h. ohne Wechselgeld) bezahlen.

(b) Sie können jeden ganzen Eurobetrag größer als $ab - a - b$ bezahlen.

Aufgabe 7 (2 Punkte)**.** Zeigen Sie, dass es unendlich viele Primzahlen der Form $6n - 1$ gibt.

Aufgabe 8 (2 + 2 + 2 Punkte)**.** Für $n \in \mathbb{N}_0$ sei $F_n := 2^{2^n} + 1$ die n-te Fermat-Zahl. Zeigen Sie:

(a) $\prod_{k=0}^{n-1} F_k = F_n - 2$ für $n \in \mathbb{N}_0$.

(b) $\operatorname{ggT}(F_n, F_m) = 1$ für $n \neq m$.

(c) Geben Sie mit Hilfe von (b) einen neuen Beweis für $|\mathbb{P}| = \infty$.

Aufgabe 9 (2 Punkte)**.** Sei $b \in \mathbb{N}$, sodass mindestens ein Primteiler von b mit Vielfachheit 1 auftritt. Sei $a \in \mathbb{N}$ keine Potenz von b. Zeigen Sie, dass $\log_b(a)$ irrational ist.

Aufgabe 10 (2 + 3 Punkte)**.**

(a) Berechnen Sie $\operatorname{kgV}(10.403, 10.807)$.

(b) Zeigen Sie $\operatorname{ggT}(a^n - 1, a^m - 1) = a^{\operatorname{ggT}(n,m)} - 1$ für $a, n, m \in \mathbb{N}$.

Aufgabe 11 (3 Punkte)**.** Bestimmen Sie die Primfaktorzerlegung von 42!. Wie viele Nullen stehen am Ende der Dezimalentwicklung von 42!?

Aufgabe 12 (3 Punkte)**.** Angenommen es gibt 8-Euroscheine und Sie besitzen beliebig viele 5- und 8-Euroscheine. Zeigen Sie, dass Sie jeden genügend großen natürlichen Eurobetrag zahlen können.

Aufgabe 13 ($2+2+2$ Punkte)**.** Beweisen Sie:

(a) $\pi(n^2) \geq n$ für $n \in \mathbb{N} \setminus \{1\}$.

(b) Ist p_n die n-te Primzahl (also $p_1 = 2$, $p_2 = 3$, usw.), so gilt $p_n \leq n^2$ für $n \geq 2$.

(c) Ist $n! = m^k \geq 2$ für $n, m, k \in \mathbb{N}$, so gilt $k = 1$.

Aufgabe 14 (2 Punkte)**.** Sei $n \in \mathbb{N}$ durch alle Zahlen von $1, \ldots, 200$ teilbar außer zwei aufeinanderliegende Zahlen $d, d+1$. Bestimmen Sie d.

Aufgabe 15 (3 Punkte)**.** Bestimmen Sie die kleinste natürliche Zahl n mit der Eigenschaft

$$\forall p \in \mathbb{P} : p \mid n \iff (p-1) \mid n.$$

Aufgabe 16 ($2+2$ Punkte)**.** Seien $p, q \in \mathbb{P} \setminus \{3, 5\}$. Zeigen Sie:

(a) $p^2 \equiv q^2 \pmod{24}$.

(b) $p^4 \equiv 1 \pmod{240}$.

Aufgabe 17 ($2+2+2$ Punkte)**.**

(a) Lösen Sie die Gleichung $47x \equiv 27 \pmod{89}$ in $\mathbb{Z}$.

(b) Lösen Sie das System

$$\begin{aligned} x &\equiv 11 \pmod{37}, \\ 2x &\equiv 13 \pmod{41}. \end{aligned}$$

Aufgabe 18 (3 Punkte)**.** Fünf Piraten und ein Affe stranden auf einer einsamen Insel. Am ersten Tag sammeln Sie n Kokosnüsse. In der folgenden Nacht wacht ein Pirat auf, um sich seinen Anteil zu sichern. Er teilt den Haufen der Kokosnüsse in fünf gleichgroße Teile, wobei eine Kokosnuss übrig bleibt, die er dem Affen schenkt. Danach bringt er einen der fünf Teile in ein Geheimversteck und legt sich wieder schlafen. Kurze Zeit später wacht auch der zweite Pirat auf, um die gleiche Prozedur durchzuführen (wieder bleibt eine Nuss für den Affen übrig). Im weiteren Verlauf der Nacht führen auch die übrigen drei Piraten diese Prozedur durch. Am nächsten Morgen wird der verbleibende Haufen zu gleichen Teilen an die fünf Piraten verteilt, wobei diesmal keine Nuss übrig bleibt. Wie groß war n mindestens?

Aufgabe 19 (3 Punkte)**.** Zeigen Sie, dass es 48 aufeinander folgende natürliche Zahlen gibt, die alle einen quadratischen Teiler haben.
Hinweis: Chinesischer Restsatz.

Aufgabe 20 (2 Punkte)**.** Prüfen Sie, ob die ISBN 123456789X gültig ist.

Aufgabe 21 ($2+2+2+2+2$ Punkte)**.** Sei $n \in \mathbb{N}$. Zeigen Sie:

(a) Genau dann ist n durch 2^k (bzw. 5^k) teilbar, wenn die aus den letzten k Dezimalziffern gebildete Zahl durch 2^k (bzw. 5^k) teilbar ist.

(b) Genau dann ist n durch 3 (bzw. 9) teilbar, wenn die *Quersumme* von n durch 3 (bzw. 9) teilbar ist. (Die Quersumme ist die Summe der Dezimalziffern.)

(c) Genau dann ist n durch 11 teilbar, wenn die alternierende Summe der Dezimalziffern von n durch 11 teilbar ist. Es spielt keine Rolle, ob man die Summe von links oder rechts beginnt. Beispiel: $n = 253 \to 2 - 5 + 3 = 0 \Longrightarrow 7 \mid 253$.

(d) Sei $n = 10a + b$. Genau dann ist n durch 7 teilbar, wenn $a - 2b$ durch 7 teilbar ist. Beispiel: $1452 \to 145 - 4 = 141 \to 14 - 2 = 12 \not\equiv 0 \pmod 7$.

(e) Finden Sie eine Teilbarkeitsregel für 13.

Aufgabe 22 (3 Punkte)**.** (Wilson) Sei $2 \leq n \in \mathbb{N}$. Zeigen Sie, dass n genau dann eine Primzahl ist, wenn

$$(n-1)! \equiv -1 \pmod n$$

gilt.

Aufgabe 23 ($2+2$ Punkte)**.**

(a) Bestimmen Sie alle $n \in \mathbb{N}$ mit $\varphi(n) = 14$.

(b) Bestimmen Sie die Primfaktorzerlegung von 626.257.
Hinweis: $\varphi(626.257) = 624.640$.

Aufgabe 24 ($3+3$ Punkte)**.** Seien p und $q = 2p - 1$ Primzahlen und $n := pq$. Sei $a \in \mathbb{N}$ ein quadratischer Rest, aber keine vierte Potenz modulo q. Sei a kein quadratischer Rest modulo p.

(a) Zeigen Sie, dass der Miller-Rabin-Test mit der Basis a nicht erkennt, dass n keine Primzahl ist.

(b) Konstruieren Sie ein p, sodass die angegebenen Eigenschaften für $a = 2$ erfüllt sind.

Aufgabe 25 ($3+1$ Punkte)**.** Sei $n \in \mathbb{N}$ und $a_1 + n\mathbb{Z}, \ldots, a_r + n\mathbb{Z}$ ein Erzeugendensystem für $(\mathbb{Z}/n\mathbb{Z})^\times$. Zeigen Sie:

(a) Der Miller-Rabin-Test mit $a_1, \ldots, a_r$ liefert eine deterministische Antwort (keine Wahrscheinlichkeit).

(b) Es genügt den Miller-Rabin-Test mit Primzahlen $a_1, \ldots, a_r$ durchzuführen.

Aufgabe 26 (2 Punkte)**.** Sei $(G, \cdot)$ eine abelsche Gruppe und $f, F \colon \mathbb{N} \to G$. Zeigen Sie, dass die folgenden Aussagen äquivalent sind:

(a) $F(n) = \prod_{d \mid n} f(d)$ für alle $n \in \mathbb{N}$.

(b) $f(n) = \prod_{d \mid n} F(n/d)^{\mu(d)}$ für alle $n \in \mathbb{N}$.

Aufgabe 27 (2 Punkte)**.** Sei $s > 1$ reell. Zeigen Sie

$$\Big(\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}\Big)^{-1} = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Bemerkung: Beide Reihen konvergieren absolut.

Aufgabe 28 $(2 + 2 + 3$ Punkte$)$**.**

(a) Berechnen Sie $(45 + 101\mathbb{Z})^{-1}$ in $(\mathbb{Z}/101\mathbb{Z})^\times$.

(b) Bestimmen Sie alle Erzeuger von $(\mathbb{Z}/22\mathbb{Z})^\times$.

(c) Bestimmen Sie die Anzahl der Elemente in $(\mathbb{Z}/2200\mathbb{Z})^\times$ mit Ordnung 5.

Aufgabe 29 (3 Punkte)**.** Überprüfen Sie mit dem kleinen Satz von Fermat, ob 341 eine Primzahl ist.

Aufgabe 30 (2 Punkte)**.**

(a) Zeigen Sie, dass 7 die kleinste Primitivwurzel modulo 71 ist.

(b) Zeigen Sie, dass 4 für keine Primzahl eine Primitivwurzel ist.

Aufgabe 31 $(2 + 2 + 2$ Punkte$)$**.** Zeigen Sie:

(a) Für $n \geq 3$ gilt $5^{2^{n-3}} \equiv 1 + 2^{n-1} \pmod{2^n}$.

(b) Für $n \geq 2$ gilt $\operatorname{ord}_{2^n}(5) = 2^{n-2}$.

(c) Für $n \in \mathbb{N}$ gilt $(\mathbb{Z}/2^n\mathbb{Z})^\times = \{\pm 5^k + 2^n\mathbb{Z} : k = 1, \dots, 2^{n-2}\}$.

Aufgabe 32 (3 Punkte)**.** Sei $p > 2$ eine Primzahl und $a \in \mathbb{Z}$ mit $\operatorname{ord}_{p^2}(a) = \varphi(p^2)$. Zeigen Sie $\operatorname{ord}_{p^m}(a) = \varphi(p^m)$ für alle $m \in \mathbb{N}$.

Aufgabe 33 $(2 + 3$ Punkte$)$**.**

(a) Bestimmen Sie die Periode der Dezimalbruchentwicklung von $\frac{1}{43}$.

(b) Bestimmen Sie die Periodenlänge von $\frac{3}{814}$.

Aufgabe 34 (2 Punkte)**.** Bestimmen Sie die (unendliche) 3-adische Entwicklung von $\frac{3}{5}$ gemäß Satz 5.2. *Hinweis:* Erinnern Sie sich an die Methode des schriftlichen Dividierens aus der Schule.

Aufgabe 35 (3 Punkte)**.** Bestimmen Sie einen Näherungsbruch $\frac{a}{b}$ für $\sqrt[3]{2}$ mit $b \leq 1000$ und $|\sqrt[3]{2} - a/b| < \frac{1}{1001b}$.

Aufgabe 36 $(2 + 2 + 2$ Punkte$)$**.**

(a) Bestimmen Sie den Kettenbruch von $\frac{1+\sqrt{7}}{2}$.

(b) Schreiben Sie den Kettenbruch $[2, 1, \overline{2, 3}]$ als Lösung einer quadratischen Gleichung.

(c) Bestimmen Sie die Lösungen der Pellschen Gleichung $x^2 - 7y^2 = 1$.

Aufgabe 37 (3 Punkte)**.** (Schlacht von Hastings) Harolds Mannen standen nach alter Gewohnheit dichtgedrängt in 13 gleichgroßen Quadraten aufgestellt, und wehe dem Normannen, der es wagte, in eine solche Phalanx einbrechen zu wollen. (...) Als aber Harold selbst auf dem Schlachtfeld erschien, formten die Sachsen ein einziges gewaltiges Quadrat mit ihrem König an der Spitze. Wie groß soll die Armee Harolds II. gewesen sein?

Aufgabe 38 (2 Punkte)**.** Sei $k \in \mathbb{N}$ und $q := \lfloor 3^k/2^k \rfloor$. Zeigen Sie, dass sich $2^k q - 1$ nicht als Summe von $q + 2^k - 3$ nicht-negativen k-ten Potenzen schreiben lässt.

Aufgabe 39 (2 Punkte)**.** Sei $\omega := \frac{1+\sqrt{-3}}{2} \in \mathbb{Z}_{-3}$. Prüfen Sie, ob $3 + 7\omega$ ein Primelement in $\mathbb{Z}_{-3}$ ist.

Aufgabe 40 (2 Punkte)**.** Sei $x \in \mathbb{C}$ transzendent. Zeigen Sie, dass

$$\mathbb{Z}[x] := \Big\{ \sum_{i=0}^{n} a_i x^i : n \in \mathbb{N}, a_0, \ldots, a_n \in \mathbb{Z} \Big\} \subseteq \mathbb{C}$$

ein euklidischer Ring ist.
Hinweis: Betrachten Sie, dass kleinste n mit $a_n \neq 0$.

Aufgabe 41 (2 Punkte)**.** Zeigen Sie, dass $\mathbb{Z}_{10}$ nicht faktoriell ist.

Aufgabe 42 (2 Punkte)**.** Schreiben Sie 941 als Summe von zwei Quadratzahlen.

Aufgabe 43 (2 Punkte)**.** Sei $n = 4^a(8b + 7) \in \mathbb{N}$ mit $a, b \in \mathbb{N}_0$. Zeigen Sie, dass n nicht die Summe von drei Quadratzahlen ist.

Aufgabe 44 (2+2 Punkte)**.** Seien $a, b \in \mathbb{Z}$ und $p \in \mathbb{P}\backslash\{2\}$. Beschreiben Sie mit dem Legendre-Symbol, wann die quadratische Gleichung

$$x^2 + ax + c \equiv 0 \pmod{p}$$

eine Lösung $x \in \mathbb{Z}$ besitzt. Untersuchen Sie damit, ob $x^2 + x + 10 \equiv 0 \pmod{101}$ eine Lösung besitzt.

Aufgabe 45 (3 Punkte)**.** Berechnen Sie die Jacobi-Symbole $\left(\frac{444}{97}\right)$, $\left(\frac{201}{91}\right)$ und $\left(\frac{551}{437}\right)$.

Aufgabe 46 (3 Punkte)**.** Für welche Primzahlen p ist 3 ein quadratischer Rest modulo p?

Aufgabe 47 (2 Punkte)**.** Um zu verifizieren, ob $n \in \mathbb{N}$ eine Quadratzahl ist, kann man prüfen ob n ein quadratischer Rest modulo vorgegebenen Zahlen $p_1, \ldots, p_r$ ist (dies geht effizient mit Hilfe des Jacobi-Symbols). Untersuchen Sie, mit welcher Wahrscheinlichkeit dieser Algorithmus eine korrekte Antwort liefert.

Aufgabe 48 (2 Punkte)**.** Wir wollen mit dem RSA-Verfahren eine Massen-E-Mail $m \in \mathbb{N}$ an $k \geq e$ viele Empfänger mit den öffentlichen Schlüsseln $(e, n_1), \ldots, (e, n_k)$ schicken ($m < n_1, \ldots, n_k$). Ist das eine gute Idee?
Hinweis: Chinesischer Restsatz.

Aufgabe 49 ($2 + 2$ Punkte)**.**

(a) Verschlüsseln Sie die Nachricht $t = 14$ mit dem RSA-Verfahren bzgl. des öffentlichen Schlüssels $(n, e) = (209, 13)$, d. h. berechnen Sie $\tilde{t}$ mit den Bezeichnungen aus Satz 10.21.

(b) Entschlüsseln Sie die Nachricht $\tilde{t} = 100$ mit Hilfe des privaten Schlüssels $d = 11$.

Aufgabe 50 (3 Punkte)**.** (Montgomery-Leiter) Sei $G = \langle g \rangle$ eine Gruppe und $n = \sum_{i=0}^{k} b_i 2^i \in \mathbb{N}$ (Binärdarstellung) mit $b_k = 1$. Zeigen Sie, dass der folgende Algorithmus g^n mit $2k$ Multiplikationen berechnet:

Initialisierung: $x := g$, $y := g^2$.
Für $i = k - 1, k - 2, \ldots, 0$:
  Falls $b_i \equiv 0 \pmod 2$, berechne $y := xy$ und $x := x^2$.
  Falls $b_i \equiv 1 \pmod 2$, berechne $x := xy$ und $y := y^2$.
Ausgabe: $x = g^n$.

Anhang

Primzahlen ≤ 1000:

2	3	5	7	11	13	17	19	23	29	31	37
41	43	47	53	59	61	67	71	73	79	83	89
97	101	103	107	109	113	127	131	137	139	149	151
157	163	167	173	179	181	191	193	197	199	211	223
227	229	233	239	241	251	257	263	269	271	277	281
283	293	307	311	313	317	331	337	347	349	353	359
367	373	379	383	389	397	401	409	419	421	431	433
439	443	449	457	461	463	467	479	487	491	499	503
509	521	523	541	547	557	563	569	571	577	587	593
599	601	607	613	617	619	631	641	643	647	653	659
661	673	677	683	691	701	709	719	727	733	739	743
751	757	761	769	773	787	797	809	811	821	823	827
829	839	853	857	859	863	877	881	883	887	907	911
919	929	937	941	947	953	967	971	977	983	991	997

Kleinste Primitivwurzel modulo p:

p	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59
	1	2	2	3	2	2	3	2	5	2	3	2	6	3	5	2	2

p	61	67	71	73	79	83	89	97	101	103	107	109	113	127	131	137	139
	2	2	7	5	3	2	3	5	2	5	2	6	3	3	2	3	2

Primitive pythagoreische Tripel:

a	b	c	a	b	c	a	b	c
3	4	5	5	12	13	6	8	10
7	24	25	8	15	17	9	40	41
10	24	26	11	60	61	12	35	37
13	84	85	14	48	50	15	112	113
16	30	34	16	63	65	17	144	145
18	80	82	19	180	181	20	21	29
20	99	101	21	220	221	22	120	122
23	264	265	24	70	74	24	143	145
25	312	313	26	168	170	27	364	365
28	45	53	28	195	197	29	420	421
30	224	226	31	480	481	32	126	130
32	255	257	33	56	65	33	544	545
34	288	290	35	612	613	36	77	85
36	323	325	37	684	685	38	360	362
39	80	89	39	760	761	40	42	58
40	198	202	40	399	401	44	117	125
48	55	73	48	286	290	51	140	149
52	165	173	56	90	106	56	390	394
57	176	185	60	91	109	60	221	229
64	510	514	65	72	97	66	112	130
68	285	293	69	260	269	72	154	170
72	646	650	75	308	317	76	357	365
78	160	178	84	187	205	85	132	157
87	416	425	88	105	137	88	234	250
93	476	485	95	168	193	96	110	146
96	247	265	102	280	298	104	153	185

Jacobi-Symbol $\left(\frac{p}{q}\right)$ für $p, q \leq 20$ (p indiziert die Zeilen):

	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
2	0	−	0	−	0	+	0	+	0	−	0	−	0	+	0	+	0	−	0
3	−	0	+	−	0	−	−	0	+	+	0	+	+	0	+	−	0	−	−
4	0	+	0	+	0	+	0	+	0	+	0	+	0	+	0	+	0	+	0
5	−	−	+	0	+	−	−	+	0	+	−	−	+	0	+	−	−	+	0
6	0	0	0	+	0	−	0	0	0	−	0	−	0	0	0	−	0	+	0
7	+	+	+	−	+	0	+	+	−	−	+	−	0	−	+	−	+	+	−
8	0	−	0	−	0	+	0	+	0	−	0	−	0	+	0	+	0	−	0
9	+	0	+	+	0	+	+	0	+	+	0	+	+	0	+	+	0	+	+
10	0	+	0	0	0	−	0	+	0	−	0	+	0	0	0	−	0	−	0
11	−	−	+	+	+	+	−	+	−	0	−	−	−	−	+	−	−	+	+
12	0	0	0	−	0	−	0	0	0	+	0	+	0	0	0	−	0	−	0
13	−	+	+	−	−	−	−	+	+	−	+	0	+	−	+	+	−	−	−
14	0	−	0	+	0	0	0	+	0	+	0	+	0	−	0	−	0	−	0
15	+	0	+	0	0	+	+	0	0	+	0	−	+	0	+	+	0	−	0
16	0	+	0	+	0	+	0	+	0	+	0	+	0	+	0	+	0	+	0
17	+	−	+	−	−	−	+	+	−	−	−	+	−	+	+	0	+	+	−
18	0	0	0	−	0	+	0	0	0	−	0	−	0	0	0	+	0	−	0
19	−	+	+	+	−	−	−	+	−	−	+	−	+	+	+	+	−	0	+
20	0	−	0	0	0	−	0	+	0	+	0	−	0	0	0	−	0	+	0

Kleinste Lösung der Pellschen Gleichung $p^2 - nq^2 = 1$.

n	p	q	n	p	q	n	p	q
2	3	2	3	2	1	5	9	4
6	5	2	7	8	3	8	3	1
10	19	6	11	10	3	12	7	2
13	649	180	14	15	4	15	4	1
17	33	8	18	17	4	19	170	39
20	9	2	21	55	12	22	197	42
23	24	5	24	5	1	26	51	10
27	26	5	28	127	24	29	9801	1820
30	11	2	31	1520	273	32	17	3
33	23	4	34	35	6	35	6	1
37	73	12	38	37	6	39	25	4
40	19	3	41	2049	320	42	13	2
43	3482	531	44	199	30	45	161	24
46	24335	3588	47	48	7	48	7	1
50	99	14	51	50	7	52	649	90
53	66249	9100	54	485	66	55	89	12
56	15	2	57	151	20	58	19603	2574
59	530	69	60	31	4	61	1766319049	226153980
62	63	8	63	8	1	65	129	16
66	65	8	67	48842	5967	68	33	4
69	7775	936	70	251	30	71	3480	413
72	17	2	73	2281249	267000	74	3699	430
75	26	3	76	57799	6630	77	351	40
78	53	6	79	80	9	80	9	1
82	163	18	83	82	9	84	55	6
85	285769	30996	86	10405	1122	87	28	3
88	197	21	89	500001	53000	90	19	2
91	1574	165	92	1151	120	93	12151	1260
94	2143295	221064	95	39	4	96	49	5
97	62809633	6377352	98	99	10	99	10	1

Stichwortverzeichnis