Zahlentheorie

Steffen Roch

SS 2016

Inhaltsverzeichnis

Einleitung Die Zahlentheorie ist

- ursprünglich die Wissenschaft von den natürlichen (ganzen) Zahlen,
- neben der Geometrie eine der ältesten mathematischen Theorien,
- extrem reizvoll: es gibt zahlreiche außerordentlich einfache Fragestellungen, die oft außerordentlich schwer zu beantworten sind,

Einige Beispiele
Die Goldbachsche Vermutung (1742): Jede gerade Zahl > 2 ist als Summe zweier Primzahlen darstellbar; jede ungerade Zahl > 5 ist als Summe dreier Primzahlen darstellbar.
(bekannt: gilt für jede hinreichend große Zahl $n > 3^{3^{15}}$)

Großer Satz von Fermat (etwa 1650 – 1993): Falls $m > 2$, so gibt es keine natürlichen Zahlen $x, y, z \geq 1$ mit $x^m + y^m = z^m$.

lange Zeit nur Spezialfälle:	$m = 3, 4, 5$
Kummer:	m reguläre Primzahl
(≈ 1980) Faltings:	nur für endlich viele m lösbar
(1993) Andrew Wiles:	vollständige Lösung

Der Primzahlsatz Sei $\pi(n)$ die Anzahl der Primzahlen $\leq n$. Dann gilt

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

Vermutet von Gauß, bewiesen ca. 100 Jahre später durch Hadamard/ de la Valleé Poussin.

Eine kleine Auswahl weiterer Mathematiker, die wesentlich zur Entwicklung der Zahlentheorie beigetragen haben:

Pythagoras	(Zahlenmystik, $3^2 + 4^2 = 5^2$)
Euklid	(Euklidscher Algorithmus, unendlich viele Primzahlen)
Diophant	(Auflösung von Gleichungen in ganzen Zahlen)
Fermat	(Großer Satz von Fermat, Fermatsche Primzahlen)
Euler	(analytische Methoden, 4 Quadrate)
Gauß	(erstes zusammenfassendes Werk über Zahlentheorie, quadratisches Reziprozitätsgesetz)

Dirichlet, Kummer, Tschebyschew, Riemann, Dedekind, Hensel, Hasse, Minkowski, Hilbert, Artin ... 20. Jhd.

Literatur Eine Suche im Internet bringt zahlreiche Texte mit dem Titel "Elementare Zahlentheorie" oder "Elementary number theory". Bei der Ausarbeitung des Skriptes waren mir folgende Texte hilfreich:

Krätzel	Zahlentheorie (MfL 19),
Koch/Pieper	Zahlentheorie (Studienbücherei),
Ireland/Rosen	A classical Introduction to Modern Number Theory,
Stein	Elementary Number Theory: Primes, Congruences, and Secrets.

1 Teilbarkeit und Primzahlen

1.1 Teilbarkeit

Wir bezeichnen mit

$\mathbb{N}$ die Menge der natürlichen Zahlen $\{1, 2, \dots\}$,
$\mathbb{Z}$ die Menge der ganzen Zahlen $\{0, \pm 1, \dots\}$,
$\mathbb{Q}$ die Menge der rationalen Zahlen.

In $\mathbb{N}$ sind Addition und Multiplikation uneingeschränkt ausführbar, in $\mathbb{Z}$ außerdem noch die Subtraktion; in $\mathbb{Q}$ kann auch die Division (außer durch 0) uneingeschränkt ausgeführt werden.

Seien $a, b \in \mathbb{Z}$. Die Zahl b heißt *Vielfaches* von a, falls es eine Zahl $c \in \mathbb{Z}$ gibt so, dass $b = a \cdot c$. Ist b Vielfaches von a, so heißt a *Teiler* von b. Wir notieren dies mit $a \mid b$.

Beispiele: $3 \mid (-6)$, $37 \mid 111$, $28 \nmid 96$.

Einfache Eigenschaften: Für alle $a, b, c \in \mathbb{Z}$ gilt

- $a \mid a$, $(-a) \mid a$ („Reflexivität“)
  $\big($denn: $a = 1 \cdot a = (-1) \cdot (-a)\big)$
- $1 \mid a$, $-1 \mid a$
  (gleiche Begründung)
- $a \mid b, b \mid c \Rightarrow a \mid c$ („Transitivität“)
  (denn: $b = d_1 a, c = d_2 b \Rightarrow c = d_1 d_2 a$)
- $a \mid b, b \mid a \Rightarrow a = b$ oder $a = -b$
- $a \mid b, a \mid c \Rightarrow a \mid (b + c)$
  (denn $b = b_1 a, c = c_1 a \Rightarrow b + c = (b_1 + c_1)a$)

- $a \mid 0$.

Die Zahlen ± 1 heißen *Einheiten*; es sind die einzigen ganzen Zahlen, die jede andere ganze Zahl teilen (und es sind die einzigen ganzen Zahlen, die in $\mathbb{Z}$ invertierbar sind). Eine natürliche Zahl n heißt *Primzahl*, wenn $n \neq 1$ und wenn die einzigen natürlichen Teiler von n die Zahl 1 und die Zahl selbst sind. Natürliche Zahlen, die weder Primzahlen noch 1 sind, heißen *zusammengesetzt*.

1.2 Der größte gemeinsame Teiler

Gegeben seien Zahlen $b_1, \ldots, b_k \in \mathbb{Z}$. Eine Zahl a heißt *gemeinsamer Teiler* dieser Zahlen, falls

$$a \mid b_1, \ldots, a \mid b_k.$$

Sind nicht alle Zahlen $b_1, \ldots, b_k$ gleich Null, so gibt es unter den gemeinsamen Teilern dieser Zahlen einen größten (dieser ist notwendig positiv). Dieser heißt der *größte gemeinsame Teiler* von $b_1, \ldots, b_k$. Sind alle b_i gleich 0, so definieren wir 0 als ihren größten gemeinsamen Teiler. Zwei Zahlen heißen *teilerfremd*, wenn ihr größter gemeinsamer Teiler gleich 1 ist.

Eine Zahl c heißt *gemeinsames Vielfaches* der Zahlen $b_1, \ldots, b_k \in \mathbb{Z}$ falls

$$b_1 \mid c, \ldots, b_k \mid c.$$

Sind alle b_i ungleich 0, so gibt es unter allen gemeinsamen Vielfachen dieser Zahlen ein kleinstes positives. Dieses heißt das *kleinste gemeinsame Vielfache* von $b_1, \ldots, b_k$. Ist eine der Zahlen b_i gleich 0, so definieren wir 0 als ihr kleinstes gemeinsame Vielfache.
Symbolisch schreiben wir:

$$a = \mathrm{ggT}(b_1, \ldots, b_k) \qquad \text{und} \qquad c = \mathrm{kgV}(b_1, \ldots, b_k).$$

Beispiele

- Suchen $\mathrm{ggT}\,(32, -8, 12)$. Die gemeinsamen Teiler dieser Zahlen sind $\{1, 2, 4, -1, -2, -4\}$. Also ist $\mathrm{ggT}\,(32, -8, 12) = 4$.

- Suchen $\mathrm{kgV}\,(3, -2, -5)$. Die gemeinsamen Vielfachen dieser Zahlen sind $\{0, \pm 30, \pm 60, \pm 90, \ldots\}$. Somit ist $\mathrm{kgV}\,(3, -2, -5) = 30$.

Wir geben zunächst eine andere Charakterisierung des größten gemeinsamen Teilers der ganzen Zahlen $a_1, \ldots, a_k$ an. Dazu betrachten wir die Menge $R(a_1, \ldots, a_k)$ aller Zahlen, die aus diesen Zahlen durch (wiederholte) Addition bzw. Subtraktion entstehen. Man sieht leicht ein, dass sich jede Zahl aus $R(a_1, \ldots, a_k)$ darstellen lässt als

$$m_1 a_1 + m_2 a_2 + \cdots + m_k a_k \quad \text{mit } m_i \in \mathbb{Z} \tag{1}$$

und dass umgekehrt jede Zahl dieser Gestalt zu $R(a_1, \ldots, a_k)$ gehört. Aus der Darstellung (1) folgt sofort, dass Summe und Produkt zweier Zahlen aus $R(a_1, \ldots, a_k)$ wieder zu $R(a_1, \ldots, a_k)$ gehören. Die Menge $R(a_1, \ldots, a_k)$ ist also ein *kommutativer Ring*.

Satz 1.1 *Seien nicht alle a_i gleich 0. Dann ist die kleinste positive Zahl in $R(a_1, \ldots, a_k)$ der größte gemeinsame Teiler von $a_1, \ldots, a_k$.*

Zum Beweis benutzen wir eine wichtige Eigenschaft der ganzen Zahlen:

Division mit Rest: Seien $a, b \in \mathbb{Z}$ und $b > 0$. Dann gibt es eindeutig bestimmte Zahlen $m \in \mathbb{Z}$ und $r \in \{0, \ldots, b-1\}$ so, dass $a = b \cdot m + r$. Die Zahl r heißt der *Rest* von a bei Division durch b.

Beweis von Satz 1.1. Da nicht alle a_i gleich 0 sind und da mit a auch $-a$ zu $R(a_1, \ldots, a_k)$ gehört, gibt es in $R(a_1, \ldots, a_k)$ positive Zahlen. Sei d die kleinste positive Zahl in $R(a_1, \ldots, a_k)$. Wir teilen jede der Zahlen a_i mit Rest durch d:

$$a_i = d \cdot m_i + r_i \qquad \text{mit } m_i \in \mathbb{Z} \text{ und } 0 \le r_i < d.$$

Wegen der Ringeigenschaft von $R(a_1, \ldots, a_k)$ ist $r_i \in R(a_1, \ldots, a_k)$. Da d die kleinste positive Zahl in $R(a_1, \ldots, a_k)$ ist, kann r_i nur 0 sein. Also gilt $d \mid a_i$ für alle i, d. h. d ist ein gemeinsamer Teiler von $a_1, \ldots, a_k$.

Weiter: d lässt sich darstellen als

$$d = m_1 a_1 + \cdots + m_k a_k \quad \text{mit gewissen } \; m_i \in \mathbb{Z}.$$

Hätten nun die $a_1, \ldots, a_k$ einen größeren gemeinsamen Teiler d' als d, so wäre $d' \mid d$, ein Widerspruch. Also ist tatsächlich $d = \mathrm{ggT}(a_1, \ldots, a_k)$. ∎

Folgerung 1.2 *Seien $a_1, \ldots, a_k \in \mathbb{Z}$. Dann gibt es Zahlen $m_1, \ldots, m_k \in \mathbb{Z}$ so, dass*

$$\mathrm{ggT}(a_1, \ldots, a_k) = m_1 a_1 + \cdots + m_k a_k.$$

Beispiel. $\mathrm{ggT}(5, 11) = 1$ lässt sich schreiben als $1 = 6 \cdot 11 - 13 \cdot 5$. (Wir haben die Koeffizienten 6 und -13 durch Probieren gefunden. Später werden wir sehen, wie man die Zahlen $m_1, \ldots, m_k$ algorithmisch bestimmen kann.) ■

Folgerung 1.3 *Seien $a_1, \ldots, a_k \in \mathbb{Z}$ und $d \in \mathbb{N}$. Dann gilt*

$$\mathrm{ggT}(da_1, \ldots, da_k) = d \cdot \mathrm{ggT}(a_1, \ldots, a_k).$$

Beweis. Die Elemente der Ringe $R(da_1, da_2, \ldots, da_k)$ und $R(a_1, \ldots, a_k)$ entsprechen einander auf eindeutige Weise: Ist $m_1a_1 + \cdots + m_ka_k \in R(a_1, \ldots, a_n)$, so ist

$$d(m_1a_1 + \cdots + m_ka_k) = m_1(da_1) + \cdots + m_k(da_k) \in R(da_1, \ldots, da_k),$$

und umgekehrt. (Die Abbildung $a \mapsto da$ ist also eine Isomorphie des Ringes $R(a_1, \ldots, a_k)$ auf $R(da_1, da_2, \ldots, da_k)$.) Also entsprechen auch die kleinsten positiven Elemente dieser Ringe einander, und sie gehen durch Multiplikation mit $d > 0$ auseinander hervor. ■

Folgerung 1.4 *Ist ab durch d teilbar und $\mathrm{ggT}(a, d) = 1$, so ist b durch d teilbar.*

Beweis. Ist b positiv, so ist b der größte gemeinsame Teiler von ab und db. Wegen Folgerung 1.3 ist nämlich

$$\mathrm{ggT}(ab, db) = b \cdot \mathrm{ggT}(a, d) = b.$$

Außerdem ist d ein gemeinsamer Teiler von ab und db. Da jeder gemeinsame Teiler den größten gemeinsamen Teiler teilt (Folgerung 1.2), folgt die Behauptung. Für $b = 0$ ist die Aussage offensichtlich, und für negatives b folgt sie wie oben. ■

Satz 1.5 *Ein Produkt $a_1 \ldots a_k$ ganzer Zahlen ist genau dann durch eine Primzahl p teilbar, wenn mindestens einer der Faktoren durch p teilbar ist.*

Beweis. Sei zunächst $k = 2$. Da p als positive Teiler nur 1 und p besitzt, gilt entweder $\mathrm{ggT}(a_1, p) = p$ oder $\mathrm{ggT}(a_1, p) = 1$. Im ersten Fall hat man $p \mid a_1$, im zweiten wegen Folgerung 1.4 $p \mid a_2$.
Im allgemeinen Fall können wir so argumentieren. Aus $p \mid a_1 \ldots a_k$ folgt $p \mid a_1$ oder $p \mid a_2 \ldots a_k$. Im ersten Fall sind wir fertig, im zweiten finden wir

$p \mid a_2$ oder $p \mid a_3 \dots a_n$. Wir fahren so fort und gelangen nach endlich vielen Schritten zur Aussage des Satzes. ∎

Ü1 Seien $a, b \in \mathbb{Z}$. Dann gilt:

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

Ü2 Seien a, b teilerfremd. Dann gilt

$$\mathrm{kgV}(a, b) = ab.$$

1.3 Der Euklidische Algorithmus

Der Euklidische Algorithmus ist ein Verfahren zur Ermittlung des größten gemeinsamen Teilers zweier Zahlen a_1, $a_2 \in \mathbb{N}$: Dazu dividieren wir a_1 durch a_2 mit Rest:

$$a_1 = q_1 a_2 + a_3, \quad 0 \leq a_3 < a_2.$$

Ist $a_3 \neq 0$, so wiederholen dies mit a_2 und a_3:

$$a_2 = q_2 a_3 + a_4, \quad 0 \leq a_4 < a_3,$$

und fahren so fort. Die erhaltene Folge der Reste $a_2, a_3, a_4 \dots$ ist streng monoton fallend und nicht negativ; also gibt es irgendwann einen Rest, der gleich 0 ist und bei dem dieses Verfahren abbricht, etwa

$$\begin{aligned} a_{n-1} &= q_{n-1} a_n + a_{n+1}, \quad 0 < a_{n+1} < a_n \\ a_n &= q_n a_{n+1}. \end{aligned}$$

Satz 1.6 *Die Zahl a_{n+1} ist der größte gemeinsame Teiler von a_1 und a_2.*

Beweis. Sei $d := \mathrm{ggT}(a_1, a_2)$. Wir erhalten aus der erster Gleichung $d \mid a_3$, aus der zweiten Gleichung $d \mid a_4$, u.s.w. Schließlich erhalten wir aus der vorletzten Gleichung $d \mid a_{n+1}$.

Umgekehrt: Aus der letzten Gleichung folgt $a_{n+1} \mid a_n$, aus der vorletzten $a_{n+1} \mid a_{n-1}, \dots$ u.s.w. Schließlich folgt aus der zweiten Gleichung $a_{n+1} \mid a_2$ und aus der ersten $a_{n+1} \mid a_1$.

Wir sehen also: a_{n+1} ist ein gemeinsamer Teiler von a_1 und a_2, und wegen $d \mid a_{n+1}$ gilt $d = a_{n+1}$. ∎

Beispiel. Wir suchen $\mathrm{ggT}\,(111, 77)$. Der Euklidische Algorithmus liefert

$$\begin{aligned} 111 &= 1 \cdot 77 + 34 \\ 77 &= 2 \cdot 34 + 9 \\ 34 &= 3 \cdot 9 + 7 \\ 9 &= 1 \cdot 7 + 2 \\ 7 &= 3 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 \end{aligned}$$

Also ist $\mathrm{ggT}(111, 77) = 1$. ■

Mit Hilfe des Euklidischen Algorithmus gewinnt man durch Rückwärtsrechnen auch eine Darstellung von $\mathrm{ggT}\,(a_1, a_2)$ in der Form $\mathrm{ggT}\,(a_1, a_2) = m_1 a_1 + m_2 a_2$. Wir zeigen dies nur am obigen Beispiel:

$$\begin{aligned} 1 &= 7 - 3 \cdot 2 \\ 1 &= 7 - 3(9 - 7) = 4 \cdot 7 - 3 \cdot 9 \\ 1 &= 4 \cdot (34 - 3 \cdot 9) - 3 \cdot 9 = 4 \cdot 34 - 15 \cdot 9 \\ 1 &= 4 \cdot 34 - 15(77 - 2 \cdot 34) = 34 \cdot 34 - 15 \cdot 77 \\ 1 &= 34(111 - 77) - 15 \cdot 77 = 34 \cdot 111 - 49 \cdot 77 \end{aligned}$$

Also ist $\quad 1 = \mathrm{ggT}(111, 77) = 34 \cdot 111 - 49 \cdot 77.$

Ü3 Gesucht ist $\mathrm{ggT}\,(234, 377)$ sowie eine Darstellung dieser Zahl in der Form $m_1 \cdot 234 + m_2 \cdot 377$.

Ü4 Gesucht ist $\mathrm{ggT}\,(2541, 3042, 3249)$.

1.4 Primfaktorzerlegung

Ziel dieses Abschnittes ist ein Beweis des Hauptsatzes der elementaren Zahlentheorie.

Satz 1.7 (Existenz und Eindeutigkeit der Primfaktorzerlegung)
Jede natürliche Zahl größer als Eins ist entweder selbst eine Primzahl, oder sie lässt sich auf eindeutige Weise als Produkt von Primzahlen darstellen.

Beweis. Wir müssen zeigen:

(a) Jede natürliche Zahl $a > 1$ lässt sich als Produkt von Primzahlen darstellen.

(b) Diese Darstellung ist eindeutig.

Zu (a)**.** Die Zahl a ist entweder eine Primzahl (dann sind wir fertig) oder zusammengesetzt. Dann gibt es unter allen Teilern von a größer als 1 einen kleinsten; etwa p_1:

$$a = p_1 \cdot a_1.$$

Dieser ist eine Primzahl (klar); außerdem ist $a_1 < a$. Wir wiederholen diese Überlegung mit a_1: Ist a_1 Primzahl, sind wir fertig; andernfalls gibt es eine Primzahl p_2 und eine Zahl $a_2 < a_1$ mit

$$a_1 = p_2 a_2.$$

Wir fahren so fort: da $a > a_1 > a_2 > \cdots > 1$, muss a_k für irgendein k selbst Primzahl sein. Damit haben wir eine Zerlegung von a in Primfaktoren gefunden.

Zu (b) Angenommen, es gibt Zahlen, die 2 verschiedene Zerlegungen in Primfaktoren gestatten. Unter diesen gibt es eine kleinste, etwa a, und es seien $a = p_1 \dots p_k$ und $a = q_1 \dots q_l$ zwei Zerlegungen dieser Zahl in Primfaktoren. Wegen

$$a = p_1 \dots p_k = q_1 \dots q_l \tag{2}$$

gilt $p_1 \mid q_1 \dots q_l$. Nach Satz 1.5 muss p_1 eine der Zahlen q_i teilen, etwa $p_1 \mid q_1$. Dann ist aber $p_1 = q_1$ (beides sind ja Primzahlen). Teilt man nun Gleichung (2) durch $p_1 (= q_1)$, so erhält man die Zahl

$$a/p_1 = p_2 \dots p_k = q_2 \dots q_l,$$

welche kleiner als a ist und ebenfalls zwei verschiedene Zerlegungen besitzt. Dies steht im Widerspruch zur Wahl von a. ∎

Wie findet man die Primfaktorzerlegung? Genauso wie im ersten Teil des Beweises:

$$\begin{aligned} 21420 &= 2 \cdot 10710 \\ &= 2 \cdot 2 \cdot 5355 \\ &= 2 \cdot 2 \cdot 3 \cdot 1785 \\ &= 2 \cdot 2 \cdot 3 \cdot 3 \cdot 595 \\ &= 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 \cdot 119 \\ &= 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 \cdot 7 \cdot 17 \end{aligned}$$

oder kürzer, $21420 = 2^2 \cdot 3^3 \cdot 5 \cdot 7 \cdot 17$.
Wir werden im weiteren stets die Schreibweise

$$a = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_k^{a_k} \quad (\text{mit } a_i \in \mathbb{N}, \quad p_i \neq p_j)$$

für die Primfaktorzerlegung verwenden.

Folgerung 1.8 *Jede ganze Zahl $a \neq 0$ lässt sich eindeutig darstellen als*

$$a = e p_1^{a_1} \cdot \ldots \cdot p_k^{a_k},$$

wobei die p_i voneinander verschiedene natürliche Primzahlen und die a_i positive natürliche Zahlen sind und e eine Einheit (also ± 1) ist.

Ü5 Man bestimme den g.g.T. und das k.g.V. gegebener Zahlen unter Benutzung ihrer Primfaktorzerlegungen.

Ü6 Man zeige: Für natürliche Zahlen a, b gilt

$$\mathrm{ggT}(a,b) \cdot \mathrm{kgV}(a,b) = a \cdot b.$$

Ü7 Man zeige: $\sqrt{2}$ und $\sqrt{2} + \sqrt{3}$ sind irrational.

1.5 Über die Menge der Primzahlen

1.5.1 Bestimmung von Primzahlen

Die Bestimmung der Primzahlen unterhalb einer gegebenen Zahl n kann im Prinzip erfolgen mittels des „**Sieb des Eratosthenes**“. Man schreibt dazu alle Zahlen von 2 bis n auf. Die kleinste Zahl 2 lassen wir stehen und streichen jedes Vielfache von 2 weg. Die nächste nicht gestrichene Zahl ist 3; man streicht alle Vielfachen davon weg. Die nächste nicht gestrichene Zahl ist 5; jedes Vielfache davon wird gestrichen u.s.w. Für $n = 50$ findet man beispielsweise

	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~~

Übrig bleiben die Primzahlen bis 50. Warum kann man nach den Vielfachen von 7 aufhören? An welcher Stelle kann man aufhören, wenn man die Primzahlen zwischen 1 und $n \in \mathbb{N}$ bestimmen möchte?

1.5.2 Wie viele Primzahlen gibt es?

Satz 1.9 (Euklid) *Es gibt unendlich viele Primzahlen.*

Beweis 1 (Euklid) Angenommen, es gäbe nur endlich viele Primzahlen, etwa $p_1, \ldots, p_n$. Die Zahl

$$a := p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$$

ist durch keine der Zahlen p_k teilbar, da sie bei Teilung durch jede von ihnen den Rest 1 lässt. Die Zahl a ist aber nach dem Hauptsatz entweder selbst Primzahl, oder sie läßt sich in Primfaktoren zerlegen, die dann sicher von den p_k verschieden sind. Es gibt also neben den p_k weitere Primzahlen. ■

Beweis 2 (Kummer) Angenommen, es gibt nur die Primzahlen $p_1 < p_2 \cdots < p_n$. Bilden $N := p_1 \cdot \ldots \cdot p_n$. Die Zahl $N-1$ hat einen Primfaktor (Hauptsatz), der (nach Konstruktion von N) auch in N steckt. Also sind N und $N-1$ durch die gleiche Primzahl teilbar. Dann teilt diese Primzahl auch $N-(N-1) = 1$, was unmöglich ist. ■

Beweis 3 Wir bezeichnen die n. Primzahl mit p_n. Euler zeigte, dass die Reihe

$$\sum \frac{1}{p_n} = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \cdots$$

divergiert. Hieraus folgt insbesondere, dass es unendlich viele Primzahlen gibt. (Gäbe es nur endlich viele Primzahlen, wäre diese Reihe eine endliche Summe und würde konvergieren). Zum Vergleich: Wir wissen, dass

$$\sum_{n=1}^{\infty} \frac{1}{n} \quad \text{divergiert (harmonische Reihe) und}$$

$$\sum_{n=1}^{\infty} \frac{1}{n^2} \quad \text{konvergiert.}$$

In diesem Sinn gibt es also „wesentlich mehr“ Primzahlen als Quadratzahlen. ■

Auf ähnliche Weise kann man sogar noch ein viel stärkeres Resultat über Primzahlen in arithmetischen Folgen beweisen:

Satz 1.10 (Dirichlet) *Seien a und b teilerfremd. Dann gibt es unendlich viele Primzahlen der Gestalt $am + b$ mit $m \in \mathbb{N}$.*

Den Beweis von Euler und einen Beweis des Satzes von Dirichlet finden Sie z.B. in Koch, Pieper (Kapitel 6). Wir beschränken uns auf den (wesentlich einfacheren) Beweis eines Spezialfalles des Satzes von Dirichlet.

Satz 1.11 *Es gibt unendlich viele Primzahlen der Form* $4m + 3$.

Beweis. Angenommen, es gibt nur endlich viele Primzahlen der Form $4m+3$, etwa $p_0 = 3, p_1, p_2, \ldots, p_n$. Wir betrachten die Zahl

$$N := 4p_1p_2 \ldots p_n + 3.$$

Nun ist jede ungerade Primzahl von der Form $4m+1$ oder $4m+3$. Wären in der Primfaktorzerlegung von N ausschließlich Primfaktoren der Form $4m+1$ enthalten, hätte auch N diese Form (warum?), was offenbar nicht der Fall ist. Die Zahl N hat also wenigstens einen Primteiler q der Form $4m + 3$. Es muss daher q eine der Primzahlen $3, p_1, p_2, \ldots, p_n$ sein.

Wäre $q = 3$, so wäre N und dann auch $N - 3 = 4p_1p_2 \ldots p_n$ durch 3 teilbar. Das ist unmöglich, da dann eine der Primzahlen $p_1, \ldots, p_n$ durch 3 teilbar wäre (Satz 1.5).

Wäre q eine der Zahlen p_i mit $i > 0$, so würde aus $q \mid N$ folgen, dass $p_i \mid N$ und somit auch

$$p_i \mid N - 4p_1p_2 \ldots p_n = 3,$$

was ebenfalls unmöglich ist. Dieser Widerspruch zeigt, dass die Annahme falsch war, d.h. es gibt unendlich viele Primzahlen der Form $4m + 3$. ∎

Es gibt also unendlich viele Primzahlen. Bekannt sind aber nur endlich viele davon; die größte aktuell bekannte Primzahl ist $2^{74.207.281} - 1$, eine Zahl mit 22.338.618 Stellen, die im Januar 2016 gefunden wurde. Diese Zahl ist eine sogenannte Mersenne-Primzahl. *Mersenne-Primzahlen* sind Primzahlen der Form $M_n := 2^n - 1$ mit $n > 1$ (man beachte, dass M_n nur dann eine Primzahl sein kann, wenn n eine Primzahl ist).

Mersenne-Primzahlen stehen in engem Zusammenhang mit vollkommenen Zahlen. Eine natürliche Zahl heißt *vollkommen*, wenn sie gleich der Summe ihrer echten Teiler ist (wie die Zahlen $6 = 1 + 2 + 3$, 28, 496 und 8128). Schon Euklid wußte, dass die Zahl $2^{n-1}(2^n - 1)$ vollkommen ist, wenn $2^n - 1$ eine Primzahl ist ($n = 2$ liefert die vollkommene Zahl 6). Rund 2000 Jahre später wurde von Euler die Umkehrung für *gerade* vollkommene Zahlen gezeigt: jede gerade vollkommene Zahl ist von der Form $2^{n-1}(2^n - 1)$ mit einer Primzahl $2^n - 1$. Es ist unbekannt, ob es auch ungerade vollkommene Zahlen gibt.

1.5.3 Verteilung der Primzahlen

Sei $\pi(x)$ die Anzahl der Primzahlen kleiner oder gleich x. Der folgende Satz wurde 1792 von Gauß vermutet und ca. 100 Jahre später von Hadamard und de la Valleé Poussin bewiesen.

Satz 1.12 (Primzahlsatz)

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

Die Funktion π wächst also wie $n/\ln n$. Bessere Annäherungen an $\pi(x)$ erhält man durch Benutzung „höhere Funktionen“ wie den *Integrallogarithmus*:

$$\mathrm{Li}\,(x) := \int_2^x \frac{dt}{\ln t}.$$

Dann gilt ähnlich zum Primzahlsatz

$$\lim_{n\to\infty} \frac{\pi(n)}{\mathrm{Li}\,(n)} = 1.$$

Man kann zeigen, dass die Annäherung von $\pi(x)$ durch $\mathrm{Li}\,(x)$ deutlich besser ist als die durch die elementare Funktion $x/\ln x$, wie auch folgende Tabelle nahelegt:

n	$\pi(n) =$	$n/\ln n \approx$	$\mathrm{Li}\,(n) \approx$
10^3	168	145	178
10^6	78498	72382	78628
10^9	50.847.534	48.254.942	50.849.235
10^{16}	279.238.341.033.925	$\rightarrow$ diese Zahl	$\rightarrow$ diese Zahl
		-7.804.289.844.393	+ 3.214.632

Außerdem gilt mit gewissen Konstanten a_1, a_2

$$|\pi(x) - \mathrm{Li}\,(x)| \leq a_1\, x\, e^{-a_2\sqrt{\ln x}}$$

(de la Valleé Poussin), und man vermutet, dass sogar

$$|\pi(x) - \mathrm{Li}\,(x)| \leq a\sqrt{x}\ln x$$

mit einer Konstanten a gilt. Letzteres kann man zeigen unter Benutzung einer anderen Vermutung, der wohl berühmtesten noch „ungeknackten“ Hypothese

der Mathematik (eines der sieben Millenium-Probleme, für deren Lösung jeweils 1 Million Dollar ausgesetzt wurden):

Die Riemannsche Vermutung *Alle Nullstellen der Zetafunktion*

$$\zeta(z) = \sum_{n=1}^{\infty} \frac{1}{n^z} \qquad (z \neq 1) \tag{3}$$

liegen auf der Geraden $\operatorname{Re} z = 1/2$.

Zum Verständnis: Wie man leicht sieht, konvergiert die Reihe in (3) für $\operatorname{Re} z > 1$ absolut. Für die übrigen komplexen Zahlen ungleich 1 kann man die Zetafunktion durch analytische Fortsetzung definieren.

1.5.4 Primzahlzwillinge

Sind sowohl p als auch $p+2$ Primzahlen, so nennt man das Paar $(p, p+2)$ einen *Primzahlzwilling*. Beispiele sind $(5, 7)$, $(11, 13)$ und $(17, 19)$. Bis heute ist unbekannt, ob es endlich oder unendlich viele Primzahlzwillinge gibt. Man kann aber z. B. zeigen, dass die Reihe

$$\sum \left(\frac{1}{p} + \frac{1}{p+2} \right),$$

in der p alle Primzahlen durchläuft, für die $p+2$ ebenfalls Primzahl ist, *konvergiert*. Es gibt also in diesem Sinn wesentlich weniger Primzahlzwillinge als Primzahlen. Das größte derzeit bekannte Paar von Primzahlzwillingen (wikipedia 2016) ist

$$3756801695685 \cdot 2^{666669} \pm 1;$$

das sind Zahlen mit 200.700 Ziffern. Zum Vergleich: der Rekordhalter aus dem Jahr 1985 war

$$107.570.463 \cdot 10^{2250} \pm 1,$$

eine 2259 stellige Zahl.

Die oben betrachteten Primzahlzwillinge haben den Abstand 2 voneinander. Allgemeiner kann man Primzahlpaare betrachten, deren Abstand voneinander höchstens k ist. Lange Zeit war offen, ob es für *irgendein* $k \geq 2$ unendlich viele solcher Paare gibt. Es erregte daher große Aufmerksamkeit, als Yitang Zhang von der University of New Hampshire im Mai 2013 bewies,

dass es unendlich viele Primzahlpaare gibt, deren Abstand voneinander maximal 70.000.000 ist. Inzwischen konnte die Zahl 70.000.000 auf nur 246 herabgesetzt werden (Polymath-Projekt). Ein weiteres Reduzieren dieser Zahl auf 2 würde beweisen, dass es unendlich viele Primzahlzwillinge gibt; Experten halten dies mit dem von Zhang entdeckten Ansatz aber für unmglich (wikipedia 2016).

1.6 Teilbarkeitstheorie in Hauptidealringen

Eine natürliche und recht allgemeine Heimat findet die Teilbarkeitstheorie in Hauptidealringen. Zunächst einige Begriffe. Sei R ein kommutativer Ring mit Eins e. Ein Element $x \in R \setminus \{0\}$ heißt ein *Nullteiler*, wenn es ein $y \in R \setminus \{0\}$ mit $xy = 0$ gibt. Ist R nullteilerfrei, so heißt R ein *Integritätsbereich*. In Integritätsbereichen darf durch Nichtnullelemente gekürzt werden: Sei $ax = ay$ und $a \neq 0$. Dann folgt $a(x - y) = 0$. Wegen $a \neq 0$ muss $x - y = 0$ sein. Also ist $x = y$.

1.6.1 Hauptidealringe

Sei R ein kommutativer Ring mit Eins e und $a \in R$. Dann bildet die Menge Ra aller Elemente ra mit $r \in R$ ein Ideal in R, welches wir mit (a) bezeichnen. R heißt ein *Hauptidealring*, wenn r nullteilerfrei (also ein Integritätsbereich) ist und wenn jedes seiner Ideale von der Gestalt (a) mit einem $a \in R$ ist.

Beispiele. (a) $\mathbb{Z}$ ist ein Hauptidealring.

Sei I ein Ideal in $\mathbb{Z}$. Ist $I = \{0\}$, so ist $I = (0)$. Sei also $I \neq \{0\}$. Liegt $a \neq 0$ in I, dann auch $-a$. Es gibt also positive Zahlen in I. Sei p die kleinste positive Zahl in I. Wir zeigen, dass $I = (p)$.

Wegen $p \in I$ ist die Inklusion $(p) \subseteq I$ klar. Angenommen, es gibt ein $b \in I \setminus (p)$. Dann können wir b schreiben als

$$b = kp + r \quad \text{mit } 0 < r \leq p - 1.$$

Dann wäre $r \in I$, und es gäbe in I eine positive Zahl kleiner als p. Dieser Widerspruch zeigt, dass $I \subseteq (p)$.

(b) Ist R ein Körper, so ist der Ring $R[x]$ der Polynome mit Koeffizienten in R ein Hauptidealring. Zur Vorbereitung überlegen wir uns, dass man in $R[x]$ ein Analogon der Division mit Rest hat.

Lemma 1.13 *Seien $f, g \in R[x]$ und $g \neq 0$ (d.h. g ist nicht das Nullpolynom). Dann gibt es Polynome q, r mit*

$$f = qg + r \quad \textit{und} \quad \deg r < \deg g \quad \textit{oder} \quad r = 0.$$

Beweis. Seien $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ mit $a_n \neq 0$ und $g(x) = b_m x^m + b_{m-1}x^{m-1} + \ldots + b_1 x + b_0$ mit $b_m \neq 0$. Dann ist also $\deg f = n$ und $\deg g = m$. Für $m = 0$ ist die Behauptung klar. Falls $\deg f < \deg g$, wählen wir $q = 0$ und $r = f$.

Sei also $\deg f \geq \deg g$. Wir bilden

$$f_1(x) := f(x) - a_n b_m^{-1} x^{n-m} g(x). \tag{4}$$

Dann ist $\deg f_1 < \deg f$. Ist sogar $\deg f_1 < \deg g$, so sind wir fertig, und (4) ist die gesuchte Darstellung. Andernfalls wiederholen wir diese Prozedur:

$$\begin{aligned} f_2(x) &= f_1(x) - q_2(x)g(x) \quad \text{mit} \quad \deg f_2 < \deg f_1, \\ &\vdots \\ f_{s+1}(x) &= f_s(x) - q_{s+1}\, g(x) \quad \text{mit} \quad \deg f_{s+1} < \deg f_s, \end{aligned}$$

und zwar so lange, bis $\deg f_{s+1} < \deg g$. Dann setzen wir $r := f_{s+1}$, $q_1 := a_n b_m^{-1} x^{n-m}$ und $q := q_1 + \ldots + q_{s+1}$ und erhalten

$$\begin{aligned} f(x) &= f_1(x) + q_1(x)g(x) \\ &= f_2(x) + q_2(x)g(x) + q_1(x)g(x) \\ &\quad\vdots \\ &= f_{s+1}(x) + \big(q_{s+1}(x) + \ldots + q_2(x) + q_1(x)\big)g(x), \end{aligned}$$

also $f = qg + r$ mit $\deg r < \deg g$. ∎

Nun können wir die Aussage dieses Beispiels leicht zeigen: Sei $I \neq \{0\}$ ein Ideal in $R[x]$. Wir wählen ein Polynom $d \neq 0$ von minimalem Grad aus I. Ist nun $f \in I$, so gibt es $q, r \in R[x]$ mit

$$f = qd + r \quad \text{mit} \quad \deg r < \deg d \text{ oder } r = 0.$$

Nun ist $r \in I$, und da d bereits minimalen Grad hat, muss $r = 0$ sein. Es ist also $f \in (d)$ und daher $I = (d)$. ∎

In beiden Beispielen beruht der Beweis der Hauptidealeigenschaft auf einer Variante der „Division mit Rest“. Man definiert daher allgemein: Ein Integritätsbereich R heißt ein *Euklidischer Ring*, wenn es eine Abbildung $h : R \setminus \{0\} \to \mathbb{N}_0$ gibt mit folgender Eigenschaft: Für beliebige $a, b \in R$ mit $a \neq 0$ gibt es $q, r \in R$ so, dass

$$b = qa + r \quad \text{mit} \quad h(r) < h(b) \text{ oder } r = 0. \tag{5}$$

Satz 1.14 *Euklidische Ringe sind Hauptidealringe.*

Beweis. Sei R Euklidischer Ring und $I \neq \{0\}$ ein Ideal von R. Wir wählen ein $d \in I$ so, dass $h(d)$ minimal wird. Ist nun $a \in I$, so gibt es $q, r \in R$ mit

$$a = qd + r \quad \text{mit} \quad h(r) < h(d) \text{ oder } r = 0.$$

Nun ist $r \in I$, und da $h(d)$ bereits minimal ist, folgt $r = 0$. Also ist $a \in (d)$ und $I = (d)$. ∎

Beispiele für Euklidische Ringe. (a) $\mathbb{Z}$ mit $h(d) = |d|$.

(b) $R[x]$ mit einem Körper R und $h(d) = \deg d$.

(c) der Ring $\mathbb{Z}+i\mathbb{Z} \subseteq \mathbb{C}$ der ganzen Gaußschen Zahlen mit $h(d_1+id_2) := d_1^2 + d_2^2 = |d_1+id_2|^2$. Wir überlegen uns dies: Seien $a = a_1+ia_2$, $b = b_1+ib_2 \in \mathbb{Z}+i\mathbb{Z}$ und $a \neq 0$. Wir schreiben

$$b/a = k_1 + ik_2 \quad \text{mit} \quad k_1, k_2 \in \mathbb{Q}$$

und bestimmen $q_1, q_2 \in \mathbb{Z}$ so, dass $|k_1 - q_1| \leq 1/2$, $|k_2 - q_2| \leq 1/2$. Sei $q := q_1 + iq_2$. Dann ist

$$\left| \frac{b}{a} - q \right|^2 = (k_1 - q_1)^2 + (k_2 - q_2)^2 \leq 1/2,$$

also $|b - aq|^2 \leq \frac{1}{2}|a|^2$ und somit $h(b - aq) \leq \frac{1}{2}h(a) < h(a)$. Mit $r := b - aq$ erhalten wir schließlich

$$b = qa + r \quad \text{mit} \quad h(r) < h(a). \qquad \blacksquare$$

1.6.2 Der größte gemeinsame Teiler

Sei R ein Integritätsbereich mit Eins e. Mit $G(R)$ bezeichnen wir die Menge aller invertierbaren Elemente von R. Die Elemente von $G(R)$ heißen auch *Einheiten* von R. Zwei Elemente $a, b \in R$ heißen *assoziiert*, wenn es ein $u \in G(R)$ mit $a = ub$ gibt. Assoziiert sein ist eine Äquivalenzrelation.

Ein Element $a \in R$ heißt *Teiler* von $b \in R$, wenn es ein $c \in R$ mit $b = ac$ gibt. Offenbar sind e, a und die zu e oder a assoziierten Elemente stets Teiler von a. Diese nennen wir die *trivialen* Teiler. Ein Element $a \in R \setminus \{0\}$ heißt *unzerlegbar* oder *irreduzibel*, wenn $a \notin G(R)$ und wenn a nur die trivialen Teiler besitzt.

Schließlich heißt $a \in R \setminus \{0\}$ ein *Primelement*, wenn $a \notin G(R)$ und wenn aus $a \mid bc$ mit $b, c \in R$ folgt $a \mid b$ oder $a \mid c$.

Beispiele. (a) Für $R = \mathbb{Z}$ ist $G(R) = \{-1, 1\}$, und die unzerlegbaren Elemente sind gerade die natürlichen Primzahlen und ihre Entgegengesetzten: $\pm 2, \pm 3, \pm 5, \ldots$. Dies sind auch genau die Primelemente von $\mathbb{Z}$ (dies folgt aus Satz 1.5 und dem folgenden Lemma). In diesem Fall fallen also die Begriffe „unzerlegbar“ und „Primelement“ zusammen.
(b) Wir betrachten $R = \mathbb{Z} + \sqrt{-3}\,\mathbb{Z} = \{c \in \mathbb{C} : c = z_1 + i\sqrt{3}z_2 \text{ mit } z_1, z_2 \in \mathbb{Z}\}$. Dann ist $G(R) = \{1, -1\}$, und es ist

$$3 = (0 + \sqrt{-3} \cdot 1)(0 + \sqrt{-3}(-1)) \text{ zerlegbar und}$$
$$2 \text{ unzerlegbar (über Beträge einzusehen),}$$

aber 2 ist kein Primelement: Es ist nämlich $4 = (1 + \sqrt{-3})(1 - \sqrt{-3})$ und $2 \mid 4$, aber 2 teilt weder $1 + \sqrt{-3}$ noch $1 - \sqrt{-3}$. Im allgemeinen fallen also die Begriffe „unzerlegbar“ und „Primelement“ *nicht* zusammen. ∎

Lemma 1.15 *Primelemente sind unzerlegbar.*

Beweis. Sei p ein Primelement und $p = ab$. Dann gilt $p \mid a$ oder $p \mid b$. Sei z.B. $a = px$. Dann folgt $p = pxb$ und $p(e - xb) = 0$. Aus der Nullteilerfreiheit folgt $xb = e$, d.h. b liegt in $G(R)$, und a und p sind assoziiert. ∎

Seien $a_1, \ldots, a_n \in R$. Ein Element $d \in R$ heißt ein *größter gemeinsamer Teiler* von $a_1, \ldots, a_n$, wenn gilt

(1) $d \mid a_i$ für alle $i = 1, \ldots, n$ (d.h. d ist ein gemeinsamer Teiler).

(2) Falls $t \mid a_i$ für alle $i = 1, \ldots, n$, dann gilt auch $t \mid d$.

Satz 1.16 (Satz vom größten gemeinsamen Teiler) *Sei R ein Hauptidealring und $a_1, \ldots, a_n \in R$. Dann gilt*

(a) Es gibt einen größten gemeinsamen Teiler von $a_1, \ldots, a_n$.
(b) Je zwei größte gemeinsame Teiler von $a_1, \ldots, a_n$ sind assoziiert. (In diesem Sinn ist der größte gemeinsame Teiler also eindeutig bestimmt.)
(c) d ist größter gemeinsamer Teiler von $a_1, \ldots, a_n$ genau dann, wenn d ein gemeinsamer Teiler von $a_1, \ldots, a_n$ ist und wenn Elemente $x_1, \ldots, x_n \in R$ existieren mit $d = x_1a_1 + \ldots + x_na_n$.

Beweis. Sei D der Durchschnitt aller Ideale von R, die $a_1, \ldots, a_n$ enthalten. Dann ist D ein Ideal von R und, da R ein Hauptidealring ist, von der Gestalt $D = (d)$ mit einem $d \in R$. Wegen $a_i \in (d)$ gibt es Elemente $k_i \in R$ mit $a_i = k_id$, d.h. d ist ein gemeinsamer Teiler von $a_1, \ldots, a_n$.

Sei $V := \{\sum_{i=1}^n x_ia_i : x_i \in R\}$. V ist ein Ideal von R. Aus $a_i \in (d)$ folgt $V \subseteq (d)$. Andererseits ist $a_i \in V$ für alle i und somit $D = (d) \subseteq V$ nach Definition von D. Es ist also $V = (d)$. Insbesondere lässt sich d darstellen als $\sum_{i=1}^n x_ia_i$ mit $x_i \in R$.

Wir zeigen, dass jedes Element d mit diesen beiden Eigenschaften (d.h. d ist gemeinsamer Teiler und $d = \sum_{i=1}^n x_ia_i$) ein größter gemeinsamer Teiler von $a_1, \ldots, a_n$ ist. Sei t ein gemeinsamer Teiler von $a_1, \ldots, a_n$. Dann gibt es $f_i \in R$ mit $a_i = tf_i$, und es ist

$$d = \sum_{i=1}^n x_ia_i = t\sum_{i=1}^n x_if_i, \quad \text{also } t \mid d.$$

Somit ist d ein größter gemeinsamer Teiler von $a_1, \ldots, a_n$. Damit sind (a) und die Implikation $\Leftarrow$ in (c) bewiesen.

Wir zeigen (b). Sind d, d' größte gemeinsame Teiler von $a_1, \ldots, a_n$, so folgt $d \mid d'$ und $d' \mid d$, d.h. es gibt Elemente $a, b \in R$ mit $d' = ad$ und $d = bd'$. Hieraus folgt $d = abd$, d.h. $ab = e$. Dann sind a, b Einheiten, und d und d' sind assoziiert.

Wir zeigen die Implikation $\Rightarrow$ in (c). Ist d' ein größter gemeinsamer Teiler von $a_1, \ldots, a_n$, so ist er nach (b) zu dem oben konstruierten d assoziiert. Da d in der Form $\sum_{i=1}^n x_ia_i$ darstellbar ist, ist es auch d'. ∎

Zwei Elemente $a, b \in R$ heißen *teilerfremd*, wenn ihr größter gemeinsamer Teiler in $G(R)$ liegt. (Diese Eigenschaft ist offenbar unabhängig von der Wahl des größten gemeinsamen Teilers.)

Satz 1.17 *Sei R ein Hauptidealring und $p \in R \setminus \{0\}$. Dann gilt:*

$$p \text{ ist Primelement } \Leftrightarrow p \text{ ist unzerlegbar.}$$

Beweis. Die Implikation $\Rightarrow$ gilt allgemein und wurde in Lemma 1.15 gezeigt. Wir zeigen $\Leftarrow$. Sei p unzerlegbar und $p \mid ab$. Sei d ein größter gemeinsamer Teiler von a und p. Da p unzerlegbar ist, gibt es nur zwei Möglichkeiten:
Fall 1: d ist assoziiert zu p. Dann ist $d = up$ mit $u \in G(R)$ und $a = xd$ mit $x \in R$ und folglich $a = xup$, also $p \mid a$.
Fall 2: $d \in G(R)$. Dann ist e ein größter gemeinsamer Teiler von a und p und nach Satz 1.16 können wir e schreiben als $e = x_1 p + x_2 a$ mit $x_1, x_2 \in R$. Dann ist $b = x_1 pb + x_2 ab$. Wegen $p \mid ab$ ist die rechte Seite durch p teilbar. Also ist $p \mid b$. ∎

In Euklidischen Ringen kann der größte gemeinsame Teiler zweier Elemente mit dem Euklidischen Algorithmus bestimmt werden. Seien $a_1, a_2 \in R \setminus \{0\}$ und $h(a_1) \geq h(a_2)$. Wir bestimmen der Reihe nach Elemente $q_1, q_2, \ldots$ und $r_1, r_2, \ldots \in R$ so, dass

$$\begin{aligned}
a_1 &= a_2 q_1 + r_1 && \text{mit } h(r_1) < h(a_2), \quad r_1 \neq 0 \\
a_2 &= r_1 q_2 + r_2 && \text{mit } h(r_2) < h(r_1), \quad r_2 \neq 0 \\
r_1 &= r_2 q_3 + r_3 && \text{mit } h(r_3) < h(r_2), \quad r_3 \neq 0 \\
&\vdots \\
r_{k-1} &= r_k q_{k+1} + r_{k+1} && \text{mit } h(r_{k+1}) < h(r_k), \quad r_{k+1} \neq 0 \\
r_k &= r_{k+1} q_{k+2}.
\end{aligned}$$

Das Verfahren muss abbrechen, da $h(a_2) > h(r_1) > h(r_2) > \ldots \geq 0$. Aus diesen Gleichungen ergibt sich

$$r_{k+1} \mid r_k \Rightarrow r_{k+1} \mid r_{k-1} \Rightarrow \ldots \Rightarrow r_{k+1} \mid a_2 \Rightarrow r_{k+1} \mid a_1,$$

also ist r_{k+1} ein gemeinsamer Teiler von a_1, a_2. Wiederholtes Einsetzen liefert

$$r_{k+1} = r_{k-1} - r_k q_{k+1} = \ldots = a_1 x_1 + a_2 x_2$$

mit $x_1, x_2 \in R$. Nach Satz 1.16 ist r_{k+1} der größte gemeinsame Teiler. ∎

Beispiel. In $R = \mathbb{Z} + \mathbb{Z}i$ suchen wir einen größten gemeinsamen Teiler von $2 + 4i$ und $5 + 5i$. Es ist $h(5 + 5i) = 50$, $h(2 + 4i) = 20$ und

$$\begin{aligned}
5 + 5i &= (2 + 4i) \cdot 1 + (3 + i) && \text{mit } h(3 + i) = 10 < 20, \\
2 + 4i &= (3 + i)(1 + i).
\end{aligned}$$

Somit ist $3+i$ ein größter gemeinsamer Teiler. (Diese Zerlegungen kann man wie oben beschrieben finden: Es ist

$$\frac{5+5i}{2+4i} = \frac{(5+5i)(2-4i)}{20} = \frac{30-10i}{20} = \frac{3}{2} - \frac{1}{2}i,$$

und 1 ist eine zu $\frac{3}{2} - \frac{1}{2}i$ nächstgelegene Zahl in $\mathbb{Z} + \mathbb{Z}i$.) ∎

1.6.3 Zerlegung in Primelemente

Wir streben nun eine Verallgemeinerung des Satzes der eindeutigen Primfaktorzerlegung an. Dazu benötigen wir

Lemma 1.18 (Teilerkettensatz) *Sei R ein Hauptidealring. Ist in einer Folge $a_1, a_2, a_3, \ldots$ in R jedes Element a_{i+1} ein nicht-trivialer Teiler von a_i, so kann diese Folge nur endlich viele Elemente enthalten.*

Beweis. Sei $a_1, a_2, a_3, \ldots$ eine Folge in R mit $a_{i+1} \mid a_i$. Dann ist offenbar $(a_i) \subseteq (a_{i+1})$ für alle $i \in \mathbb{N}$.

Wir zeigen, dass $A := \bigcup_{i=1}^{\infty}(a_i)$ ein Ideal in R ist. Seien $a, b \in A$ und $r \in R$. Dann ist $a \in (a_i)$ und $b \in (a_j)$ mit gewissen i, j. O.B.d.A. sei $i \leq j$. Dann ist $a \in (a_i) \subseteq (a_j)$ und somit

$$a + b \in (a_j) \subseteq A.$$

Weiter ist $ra \in (a_i) \subseteq A$, d.h. A ist ein Ideal.

Da R Hauptidealring ist, gibt es ein $a \in R$ mit $A = (a)$. Wegen $a \in A$ gibt es ein i mit $a \in (a_i)$. Für alle $j \geq i$ gilt dann

$$(a) \subseteq (a_i) \subseteq (a_j) \subseteq A \subseteq (a),$$

d.h. von der Stelle i an sind alle Ideale (a_j) gleich. Aus $(a_i) = (a_{i+1})$ folgt aber $a_i \mid a_{i+1}$ und $a_{i+1} \mid a_i$, d.h. a_{i+1} ist ein trivialer Teiler von a_i. ∎

Satz 1.19 (Eindeutige Primelementzerlegung) *Sei R ein Hauptidealring. Dann lässt sich jede Nichteinheit $a \in R \setminus \{0\}$ als Produkt $a = p_1 \ldots p_m$ von Primelementen darstellen. Ist $a = q_1 \ldots q_n$ eine weitere Zerlegung von a in ein Produkt aus Primelementen, so ist $m = n$, und bei geeigneter Nummerierung ist p_i zu q_i assoziiert.*

Beweis. *Existenz*: Angenommen, a habe keine Zerlegung in Primelemente. Dann ist a kein Primelement, sondern zusammengesetzt, etwa $a = a_1 b_1$, und wenigstens eines der Elemente a_1, b_1 besitzt auch keine Zerlegung in Primelemente, etwa a_1. Wir wiederholen diese Überlegung und erhalten eine unendliche Kette $\ldots a_2 \mid a_1 \mid a$ echter Teiler, im Widerspruch zum Teilerkettensatz.

Eindeutigkeit: Wir führen den Beweis durch Induktion nach m. Sei $m = 1$, $a = p_1$ und $a = q_1 \ldots q_n$. Da p_1 Primelement ist, ist p_1 unzerlegbar. Also ist $n = 1$ und $q_1 = p_1$.

Wir nehmen nun an, die zu zeigende Aussage gelte für alle Produkte von weniger als m Primelementen und betrachten $a = p_1 \ldots p_m = q_1 \ldots q_n$. Da p_1 Primelement ist, folgt $p_1 \mid q_i$ für ein i, etwa $p_1 \mid q_1$. Da auch q_1 Primelement ist, sind p_1 und q_1 zueinander assoziiert: $q_1 = u p_1$ mit $u \in G(R)$. Folglich ist

$$a = p_1 \ldots p_m = u p_1 q_2 \ldots q_n$$

und daher $p_2 \ldots p_m = u q_2 \ldots q_n$. Aus der Induktionsannahme folgt die Behauptung. ∎

Integritätsbereiche, in denen der Satz von der eindeutigen Primelementzerlegung gilt, heißen auch *faktorielle* oder *ZPE-Ringe*.

$\mathbb{Z}, \mathbb{Z} + i\mathbb{Z}$	$\Rightarrow$	Euklidische	$\Rightarrow$	Hauptideal-	$\Rightarrow$	ZPE-
$K[x]$ mit K Körper		Ringe		ringe		Ringe.

Offen bleibt damit die ZPE-Eigenschaft für Ringe wie $\mathbb{Z}[x]$ oder $\mathbb{R}[x, y]$, die keine Hauptidealringe sind (man betrachte die Ideale $\mathrm{Id}(5, x)$ in $\mathbb{Z}[x]$ oder $\mathrm{Id}(x, y)$ in $\mathbb{R}[x, y]$).

1.6.4 Primelementzerlegung in Polynomringen

Wie wir am Ende des vorigen Abschnittes gesehen haben, ist für einige wichtige Ringe die ZPE-Eigenschaft noch unklar. Wir zeigen in diesem Abschnitt folgenden Satz, der diese Fälle klärt.

Satz 1.20 (Gauß) *Ist R ein ZPE-Ring, dann ist auch $R[x]$ ein ZPE-Ring.*

Da $\mathbb{Z}$ und $\mathbb{R}[x]$ als Euklidische Ringe ZPE-Ringe sind, folgt mit diesem Satz die ZPE-Eigenschaft von $\mathbb{Z}[x]$ und $(\mathbb{R}[x])[y] = \mathbb{R}[x, y]$ und die vieler weiterer Ringe.

Im weiteren sei R ein ZPE-Ring. In der Algebra wird gezeigt, dass man jedem Integritätsbereich auf natürliche Weise einen Quotientenkörper zuordnen kann (ähnlich, wie man $\mathbb{Z}$ den Körper $\mathbb{Q}$ zuordnet). Wir bezeichnen den

Quotientenkörper von R mit K. Schließlich sei vermerkt, dass man in R größte gemeinsame Teiler hat, die man (wie in $\mathbb{Z}$) aus der Primelementzerlegung gewinnen kann.

Ein Polynom $p(x) = \sum_{i=0}^{n} a_i x^i \in R[x] \setminus \{0\}$ heißt *primitiv*, wenn jeder größte gemeinsame Teiler von $a_0, \ldots, a_n$ eine Einheit ist.

Satz 1.21 (Gauß) *Sind $f, g \in R[x]$ primitiv, so ist auch fg primitiv.*

Beweis. Sei $f(x) = \sum_{i=0}^{m} a_i x^i$, $g(x) = \sum_{j=0}^{n} b_j x^j$ mit $a_m, b_n \neq 0$. Dann ist

$$f(x)g(x) = \sum_{i=0}^{n} \sum_{j=0}^{n} a_i b_j x^i x^j = \sum_{k=0}^{m+n} \sum_{i=0}^{k} (a_i b_{k-i}) x^k.$$

Sei p ein Primelement von R. Da $\mathrm{ggT}(a_0, \ldots, a_n)$ eine Einheit ist, ist klar, dass p nicht alle Koeffizienten von f teilt. Ebenso teilt p nicht alle Koeffizienten von g. Sei

$$s := \max\{i : p \text{ teilt nicht } a_i\}, \quad r := \max\{j : p \text{ teilt nicht } b_j\}.$$

Wir betrachten nun den Koeffizienten von fg bei $r + s$. Dieser ist

$$\sum_{i=0}^{r+s} a_i b_{r+s-i} = a_0 b_{r+s} + a_1 b_{r+s-1} + \ldots + a_{r+s} b_0.$$

Da p weder a_s noch b_r teilt, teilt p auch nicht $a_s b_r$. Die übrigen Summanden in dieser Summe sind aber durch p teilbar. Somit ist dieser Koeffizient von fg nicht durch p teilbar. ∎

Lemma 1.22 *Jedes Polynom $f \in K[x] \setminus \{0\}$ lässt sich schreiben als $f = rg$ mit $r \in K$ und mit einem primitiven Polynom $g \in R[x]$. Diese Darstellung ist eindeutig bis auf Einheiten von R.*

Beweis. *Existenz*: Sei $f(x) = \sum_{i=0}^{m} \frac{b_i}{a_i} x^i$ mit $a_i, b_i \in R$ und $a_i \neq 0$. Mit $a := \prod_{i=1}^{m} a_i$ ist klar, dass $af \in R[x]$. Weiter: Ist b ein größter gemeinsamer Teiler der Koeffizienten von af, so ist

$$af = bg \quad \text{bzw.} \quad f = \frac{b}{a} g$$

mit einem primitiven Polynom $g \in R[x]$.

Eindeutigkeit: Sei $f = r_1 g_1 = r_2 g_2$ mit $r_1, r_2 \in K$ und primitiven Polynomen $g_1, g_2 \in R[x]$. Dann gibt es ein $t \in R \setminus \{0\}$ (ein „gemeinsamer Nenner“ von r_1, r_2) so, dass $tr_1, tr_2 \in R$. Es ist also

$$tf = tr_1 g_1 = tr_2 g_2.$$

Da g_1 und g_2 primitiv sind, sind tr_1 und tr_2 größte gemeinsame Teiler der Koeffizienten von tf. Folglich sind tr_1 und tr_2 assoziiert. Hieraus folgt die Behauptung. ∎

Lemma 1.23 *Sei $f \in R[x]$ ein primitives Polynom und seien $a, b \in R$ mit $a \neq 0$. Dann gilt*

$$\frac{b}{a} f \in R[x] \quad \Leftrightarrow \quad a \mid b \text{ in } R.$$

Beweis. Wir zeigen die Implikation $\Rightarrow$. Sei $\frac{b}{a} f \in R[x]$ und c ein größter gemeinsamer Teiler der Koeffizienten von $\frac{b}{a} f$. Dann ist $\frac{b}{a} f = cg$ mit einem primitiven Polynom $g \in R[x]$. Da f und g primitiv sind, folgt aus der Eindeutigkeitsaussage in Lemma 1.22, dass $\frac{b}{a}$ zu c assoziiert ist. Es gibt also ein $u \in G(R)$ mit $\frac{b}{a} = uc$ bzw. $b = uca$. Somit ist a Teiler von b. Die umgekehrte Implikation ist klar. ∎

Satz 1.24 *Besitzt ein Polynom aus $R[x]$ in $K[x]$ eine Zerlegung in Polynome positiven Grades, so gibt es bereits in $R[x]$ eine solche Zerlegung mit Faktoren gleichen Grades.*

Beweis. Sei $f \in R[x]$ und $f = g_1 g_2$ mit $g_1, g_2 \in K[x]$. Wir wenden Lemma 1.22 auf die Polynome g_1, g_2 an und finden Elemente $a_1, a_2 \in R \setminus \{0\}$, $b_1, b_2 \in R$ und primitive Polynome $h_1, h_2 \in R[x]$ mit

$$g_1 = \frac{b_1}{a_1} h_1, \quad g_2 = \frac{b_2}{a_2} h_2 \quad \text{und somit} \quad f = \frac{b_1 b_2}{a_1 a_2} h_1 h_2.$$

Dies ist ein Polynom in $R[x]$, und $h_1 h_2$ ist primitiv nach Satz 1.21. Nach Lemma 1.23 ist $a_1 a_2 \mid b_1 b_2$. Somit ist f in $R[x]$ in Faktoren vom gleichen Grad wie g_1, g_2 zerlegbar. ∎

Wir können nun die Primelemente in $R[x]$ charakterisieren.

Satz 1.25 *Die Primelemente von $R[x]$ sind genau die Primelemente von R (betrachtet als Polynome nullten Grades) und alle primitiven unzerlegbaren Polynome positiven Grades.*

Beweis. Ist $f \in R[x]$ und a ein größter gemeinsamer Teiler der Koeffizienten von f, so ist $f = ag$ mit einem primitiven Polynom g. Alle Elemente von $R[x]$ außer den im Satz genannten sind daher zerlegbar und können keine Primelemente sein.

Es verbleibt daher zu zeigen, dass die im Satz genannten Elemente tatsächlich Primelemente sind. Wir tun dies für die primitiven unzerlegbaren Polynome positiven Grades.

Sei $f \in R[x]$ ein solches Polynom. Nach Satz 1.24 ist f auch in $K[x]$ unzerlegbar. Da $K[x]$ ein Hauptidealring ist, ist f ein Primelement in $K[x]$ (Satz 1.17). Mithin gilt: Sind $g, h \in R[x]$ und ist f Teiler von gh in $R[x]$, so ist f Teiler von g oder h, jedoch zunächst in $K[x]$.

Sei z.B. $f \mid g$ in $K[x]$. Dann gibt es ein $\tilde{g} \in K[x]$ mit $g = \tilde{g}f$. Lemma 1.22, angewandt auf $\tilde{g}$, liefert Elemente $a \in R \setminus \{0\}$ und $b \in R$ sowie ein primitives Polynom $p \in R[x]$ mit

$$\tilde{g} = \frac{b}{a}p, \quad \text{also} \quad g = \frac{b}{a}pf.$$

Nach Voraussetzung und Satz 1.21 ist pf primitiv. Aus Lemma 1.23 folgt dann $\frac{b}{a} \in R$. Also ist $\frac{b}{a}p \in R[x]$, und f teilt g in $R[x]$. Somit ist f ein Primelement. ∎

Beweis von Satz 1.20. Sei $f \in R[x] \setminus \{0\}$. Da $K[x]$ als Euklidischer Ring ein ZPE-Ring ist, können wir f in Primelemente p_i von $K[x]$ zerlegen: $f = p_1 \dots p_n$. Mit Lemma 1.22 finden wir $a_i \in R \setminus \{0\}$, $b_i \in R$ sowie primitive Polynome $q_i \in R[x]$, die offenbar unzerlegbar sind, so dass $p_i = \frac{b_i}{a_i}q_i$. Mithin ist

$$f = \frac{b_1 \dots b_n}{a_1 \dots a_n}\, q_1 \dots q_n \in R[x].$$

Da $q_1 \dots q_n$ wieder primitiv ist (Satz 1.21), ist $c := \frac{b_1 \dots b_n}{a_1 \dots a_n} \in R$ (Lemma 1.23). Da R ein ZPE-Ring ist, folgt $c = r_1 \dots r_m$ mit gewissen Primelementen r_i von R. Zusammengefasst ist

$$f = r_1 \dots r_m\, q_1 \dots q_n,$$

und nach Satz 1.25 sind alle Faktoren Primelemente von $R[x]$. Damit ist die Existenz einer Primelementzerlegung gesichert. Die Eindeutigkeit der Primelementzerlegung (bis auf Einheiten) macht man sich wie in Satz 1.19 klar. ∎

Das folgende Kriterium ist hilfreich bei der Bestimmung der unzerlegbaren Polynome.

Satz 1.26 (Eisenstein-Kriterium) *Sei* $f(x) = a_0 + a_1 x + \ldots + a_n x^n \in \mathbb{Z}[x]$ *primitiv. Wenn es eine Primzahl* p *gibt mit*

$$p \mid a_0,\ p \mid a_1,\ \ldots,\ p \mid a_{n-1}$$

und so, dass weder a_n *durch* p *noch* a_0 *durch* p^2 *teilbar sind, so ist* f *irreduzibel in* $\mathbb{Z}[x]$.

Beispiel. $f(x) = x^3 - 4$ ist irreduzibel über $\mathbb{Q}$. Ersetzt man nämlich x durch $y + 1$, erhält man $(y+1)^3 - 4 = y^3 + 3y^2 + 3y - 3$, und dies ist irreduzibel über $\mathbb{Z}$ nach dem Eisenstein-Kriterium mit $p = 3$. ∎

2 Kongruenzen

2.1 Rechnen mit Kongruenzen

Seien a, b ganze Zahlen und $m > 1$. Man sagt, dass

$$a \textit{ kongruent zu } b \textit{ modulo } m$$

ist, falls a und b bei Division durch m den gleichen Rest lassen bzw. (was dasselbe ist) falls $a - b$ durch m teilbar ist. In diesem Fall schreibt man

$$a \equiv b\ (m) \quad \text{oder} \quad a \equiv b \bmod m.$$

Beispielsweise ist $128 \equiv 33\ (5)$, $17 \equiv -2\ (19)$, $91 \equiv 0\ (13)$ und $28 \not\equiv 36\ (7)$.

Satz 2.1 *Kongruenz modulo m ist eine Äquivalenzrelation.*

Beweis. Die *Reflexivität* $a \equiv a\ (m)$ folgt aus $a - a = 0$ und $m \mid 0$.
Die *Symmetrie* $a \equiv b\ (m) \Rightarrow b \equiv a\ (m)$ folgt aus $a - b = km \Rightarrow b - a = (-k)m$.
Die *Transitivität* $a \equiv b\ (m),\ b \equiv c\ (m) \Rightarrow a \equiv c\ (m)$ ergibt sich schließlich aus

$$a - b = k_1 m, \quad b - c = k_2 m \quad \Rightarrow \quad (a - b) + (b - c) = k_1 m + k_2 m,$$

also $a - c = (k_1 + k_2)m$. ∎

Der folgende Satz klärt das Rechnen mit Kongruenzen.

Satz 2.2 *Seien $a_1 \equiv b_1\ (m)$ und $a_2 \equiv b_2\ (m)$. Dann gilt*

$$a_1 \pm a_2 \equiv b_1 \pm b_2\ (m) \qquad \textit{und} \qquad a_1 \cdot a_2 \equiv b_1 \cdot b_2\ (m).$$

Beweis *Addition*: Addition von $a_1 - b_1 = c_1 \cdot m$ und $a_2 - b_2 = c_2 \cdot m$ liefert

$$a_1 + a_2 - b_1 - b_2 = (c_1 + c_2)m, \quad \text{also} \quad a_1 + a_2 \equiv b_1 + b_2\ (m).$$

Multiplikation: Es ist

$$\begin{aligned} a_1 a_2 - b_1 b_2 &= a_1 a_2 - b_1 a_2 + b_1 a_2 - b_1 b_2 \\ &= (a_1 - b_1)a_2 + b_1(a_2 - b_2) \\ &= c_1 m a_2 + b_1 c_2 m \\ &= (c_1 a_2 + b_1 c_2)m, \end{aligned}$$

also $a_1a_2 \equiv b_1b_2\ (m)$. ∎

Beispiele: (a) Wir suchen den Rest von $86 \cdot 738 \cdot 9150$ bei Division durch 7. Es ist

$$86 \equiv 2\ (7), \quad 738 \equiv 3\ (7), \quad 9150 \equiv 1\ (7)$$

und somit nach Satz 2.2 $86 \cdot 738 \cdot 9150 \equiv 2 \cdot 3 \cdot 1 \equiv 6\ (7)$.

(b) Wir suchen den Rest von $3 + 12 \cdot 40 + 8 \cdot 40^2 + 5 \cdot 40^3$ bei Division durch 13. Wegen $40 \equiv 1\ (13)$ ist

$3 + 12 \cdot 40 + 8 \cdot 40^2 + 5 \cdot 40^3 \equiv 3 + 12 \cdot 1 + 8 \cdot 1^2 + 5 \cdot 1^3 \equiv 28 \equiv 2\ (13)$. ∎

Achtung: Division von Kongruenzen ist problematisch, wie einfache Beispiele zeigen: Es ist zwar $3 \equiv 6\ (3)$; formales Dividieren durch 3 liefert aber $1 \equiv 2\ (3)$, was offenbar falsch ist!

Satz 2.3 *Ist* $da \equiv db\ (m)$ *und zusätzlich* $\mathrm{ggT}(d, m) = 1$, *so ist auch* $a \equiv b\ (m)$.

Beweis. Nach Voraussetzung ist $m \mid da - db$ bzw. $m \mid d(a-b)$. Aus Folgerung 1.4 ergibt sich $m \mid a - b$, also $a \equiv b\ (m)$. ∎

Bevor wir uns weiter mit Kongruenzen befassen, sehen wir uns zunächst einige Anwendungen an.

2.2 Fermat-Zahlen

Die Zahlen $F_m := 2^{2^m} + 1$ mit $m \in \mathbb{N}$ heißen *Fermat-Zahlen*. Die ersten von ihnen sind

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65537,$$

und diese fünf Zahlen sind Primzahlen! Fermat hatte vermutet, dass alle Fermat-Zahlen Primzahlen sind. Euler konnte zeigen, dass dies falsch ist. Genauer zeigte er, dass bereits F_5 durch 641 teilbar und daher keine Primzahl ist. Das kann man wie folgt einsehen:

$$2^{16} = (2^8)^2 = (256)^2 = 65536 \equiv 154\ (641),$$
$$2^{32} = (154)^2 = 23766 \equiv -1\ (641).$$

Somit ist $F_5 = 2^{32} + 1 \equiv 0\ (641)$. Noch weniger wird bei folgender Überlegung gerechnet: Es ist

$$641 = 640 + 1 = 5 \cdot 2^7 + 1, \quad \text{also} \quad 5 \cdot 2^7 \equiv -1\ (641),$$
$$641 = 625 + 16 = 5^4 + 2^4, \quad \text{also} \quad 5^4 \equiv -2^4\ (641).$$

Wir potenzieren erste Kongruenz mit 4 und erhalten $5^4 \cdot 2^{28} \equiv 1\ (641)$. Mit der zweiten Kongruenz gelangen wir zu $-2^4 \cdot 2^{28} \equiv 1\ (641)$ bzw. $2^{32}+1 \equiv 0\ (641)$. ■

Warum interessiert man sich für Fermat-Zahlen, die gleichzeitig Primzahlen sind? Der junge Gauß hat entdeckt: *Ein reguläres n-Eck kann genau dann mit Zirkel und Lineal konstruiert werden, wenn n von der Gestalt*

$$n = 2^k p_1 p_2 \dots p_r$$

mit $k \geq 0$ und paarweise verschiedenen Fermatschen Primzahlen $p_1, \dots, p_r$ ist.
Zur Zeit sind keine weiteren Fermatschen Primzahlen außer den oben genannten bekannt. Man weiß auch nicht, ob es endlich oder unendlich viele von ihnen gibt und ob es endlich oder unendlich viele zusammengesetzte Fermat-Zahlen gibt.

2.3 Teilbarkeitskriterien

Ausgangspunkt: Jede natürliche Zahl besitzt eine eindeutige Darstellung in der Form

$$a_m \cdot 10^m + a_{m-1} \cdot 10^{m-1} + \dots + a_1 \cdot 10 + a_0 \tag{6}$$

mit $a_0, \dots, a_m \in \{0, 1, \dots, 9\}$ (Darstellung im Dezimalsystem). Anstelle der 10 kann man auch eine beliebige andere Basis $b > 1$ wählen:

$$a_m b^m + \dots + a_1 b + a_0 \quad \text{mit} \quad a_0, \dots, a_m \in \{0, 1, \dots, b-1\}.$$

2.3.1 Teilbarkeit durch 2, 4, 8

Wir betrachten (6) modulo 2, 4 bzw. 8. Wegen $10 \equiv 0\ (2)$, $100 \equiv 0\ (4)$ und $1000 \equiv 0\ (8)$ erhalten wir

$$a_m \cdot 10^m + \dots + a_1 \cdot 10 + a_0 \equiv \begin{cases} a_0 & (2) \\ a_1 \cdot 10 + a_0 & (4) \\ a_2 \cdot 100 + a_1 \cdot 10 + a_0 & (8). \end{cases}$$

Mit anderen Worten:
Eine Zahl lässt bei Division durch 2 denselben Rest wie ihre letzte Ziffer.
Eine Zahl lässt bei Division durch 4 denselben Rest wie die aus ihren letzten

2 Ziffern bestehende Zahl.
Eine Zahl lässt bei Division durch 8 denselben Rest wie die aus ihren letzten 3 Ziffern bestehende Zahl.

Beispiel. Die Zahl $\underbrace{44\ldots444}_{2016\text{Vieren}}$ ist durch 2 und 4 teilbar und lässt bei Division durch 8 den Rest 4. ■

2.3.2 Teilbarkeit durch 5, 25, 125

Wegen $10 \equiv 0\ (5)$, $100 \equiv 0\ (25)$ und $1000 \equiv 0\ (125)$ folgt wie vorher aus (6):

$$a_m \cdot 10^m + \ldots + a_1 \cdot 10 + a_0 \equiv \begin{cases} a_0 & (5) \\ a_1 \cdot 10 + a_0 & (25) \\ a_2 \cdot 100 + a_1 \cdot 10 + a_0 & (125), \end{cases}$$

Mit anderen Worten:
Eine Zahl lässt bei Division durch 5 denselben Rest wie ihre letzte Ziffer.
Eine Zahl lässt bei Division durch 25 denselben Rest wie die aus ihren letzten 2 Ziffern bestehende Zahl.
Eine Zahl lässt bei Division durch 125 denselben Rest wie die aus ihren letzten 3 Ziffern bestehende Zahl.

2.3.3 Teilbarkeit durch 3, 9

Wegen $10 \equiv 1\ (3)$ und $10 \equiv 1\ (9)$ ist

$$a_m \cdot 10^m + \ldots + a_1 \cdot 10 + a_0 \equiv \begin{cases} a_m + \ldots + a_0 & (3) \\ a_m + \ldots + a_0 & (9) \end{cases}$$

D.h. eine Zahl lässt bei Division durch 3 bzw. 9 denselben Rest wie ihre *Quersumme*.

Beispiel. Die Quersumme von $N = \underbrace{44\ldots4}_{44\text{Vieren}}$ ist $4 \cdot 44 = 176$. Davon die Quersumme ist 14, und davon die Quersumme ist 5. Daher ist der Rest von N bei Division durch 3 gleich 2 und bei Division durch 9 gleich 5.

2.3.4 Teilbarkeit durch 11

Es ist $10 \equiv -1\ (11)$, $\quad 10^2 \equiv 1\ (11)$, $\quad 10^3 \equiv -1\ (11)$ u.s.w., und daher

$$a_m \cdot 10^m + \ldots + a_1 \cdot 10 + a_0 \equiv (-1)^m \cdot a_m \pm \ldots + a_2 - a_1 + a_0\ (11).$$

Eine Zahl lässt also bei Division durch 11 denselben Rest wie ihre *alternierende Quersumme*.

Für eine weitere Regel schreibt man die zu untersuchende Zahl im Hunderter-System und benutzt, dass $100 \equiv 1\ (11)$:

$$a_m \cdot 100^m + \ldots + a_1 \cdot 100 + a_0 \equiv a_m + \ldots + a_1 + a_0\ (11)$$

wobei $a_m, \ldots, a_0 \in \{0, \ldots, 99\}$. Praktisch heisst das, die zu untersuchende Zahl (z.B. 123456789) von rechts beginnend in Zweiergruppen (z.B. 1 | 23 | 45 | 67 | 89) aufzuteilen und diese zu addieren (z.B. 1+23+45+67+89 = 225). Die zu untersuchende Zahl lässt bei Division durch 11 denselben Rest wie die so bestimmte Zahl (z.B. $123456789 \equiv 225 \equiv 5\ (11)$).

Neunerprobe, Elferprobe Wenigstens seit dem Mittelalter (Adam Ries' Wappen!) sind Rechenproben in Gebrauch, die auf den einfachen Teilbarkeitsregeln für 9 und 11 beruhen. Um etwa die Rechnung $455 \cdot 3217 = 1463735$ zu überprüfen, betrachtet man

$$\begin{aligned} \text{die Reste mod } 9: &\quad 5 \cdot 4 = 2 \quad \checkmark \\ \text{die Reste mod } 11: &\quad 4 \cdot 5 = 9 \quad \checkmark. \end{aligned}$$

Offenbar erhält man in beiden Rechnungen gleiche Reste. Dies heisst natürlich nicht zwingend, dass man richtig gerechnet hat. Stimmt die Neuner- oder Elferprobe jedoch nicht, ist mit Sicherheit etwas falsch.

Ü8 Man überprüfe die Rechnung $13 \cdot 28 \cdot 51 + 5 \cdot 213 - 17 \cdot 23 \cdot 35 = 5494$ modulo 9 und modulo 11!

Ü9 Warum sind die Moduln 2 und 5 wenig geeignet als Rechenproben?

2.3.5 Teilbarkeit durch weitere Primzahlen

Für weitere Teilbarkeitskriterien kann man benutzen, dass bestimmte Potenzen von 10 bei Division durch bestimmte Primzahlen die Reste ± 1 lassen. So ist z.B. $1000 - 1 = 999 = 27 \cdot 37$, also $10^3 \equiv 1\ (37)$, und es ist $1000 + 1 = 1001 = 7 \cdot 11 \cdot 13$, also $10^3 \equiv -1\ (7)$ und $10^3 \equiv -1\ (13)$. Um dies auszunutzen, unterteilt man die zu untersuchende Zahl rechts beginnend in Dreiergruppen (stellt sie also im 1000-er System dar). Addiert man diese Dreiergruppen, so lässt die resultierende Zahl bei Division durch 37 den gleichen Rest wie Ausgangszahl. Bildet man dagegen aus diesen Dreiergruppen eine Summe mit alternierenden Vorzeichen, so lässt die resultierende

Zahl bei Division durch 7, 11 bzw. 13 den gleichen Rest wie Ausgangszahl. Beispielsweise ist

$$\underbrace{11}_{+}\ \underbrace{014}_{+}\ \underbrace{023}_{+} \equiv 48 \equiv 11\ (37),$$

$$\underbrace{11}_{+}\ \underbrace{014}_{-}\ \underbrace{023}_{+} \equiv 20 \equiv \begin{cases} 6\ (7), \\ 9\ (11), \\ 7\ (13). \end{cases}$$

Obige Regeln für 7 oder 13 sind bereits mühsamer anzuwenden. Es gibt für diese Zahlen Teilbarkeitsregeln ganz anderer Art, die oft leichter benutzbar sind.

Satz 2.4 *Die Zahl* $10a+b$ *mit* $b \in \{0,\dots,9\}$ *ist genau dann durch* 7 *teilbar, wenn* $a-2b$ *durch* 7 *teilbar ist.*

Beweis. Nach Satz 2.3 ist $10a+b \equiv 0\ (7)$ äquivalent zu $20a+2b \equiv 0\ (7)$. Da $21a$ durch 7 teilbar ist, ist dies weiter äquivalent zu $-a+2b \equiv 0\ (7)$ bzw. $a-2b \equiv 0\ (7)$. ∎

Um etwa zu überprüfen, ob 864192 durch 7 teilbar ist, rechnet man

$$\begin{aligned} 86419 - 2\cdot 2 &= 86415, \\ 8641 - 2\cdot 5 &= 8631, \\ 863 - 2\cdot 1 &= 861, \\ 86 - 2\cdot 1 &= 84, \\ 8 - 2\cdot 4 &= 0. \end{aligned}$$

Das Ergebnis ist durch 7 teilbar, also ist es auch die Ausgangszahl.

Ü10 Man zeige, dass hierdurch jedoch kein Restgleichheitskriterium geliefert wird, d.h. man finde Zahlen $a \in \mathbb{N}$, $b \in \{0,\dots,9\}$ so, dass $10a+b$ und $a-2b$ unterschiedliche Reste bei Division durch 7 lassen!

Ü11 Die Zahl $10a+b$ mit $b \in \{0,\dots,9\}$ ist genau dann durch 13 teilbar, wenn $a+4b$ durch 13 teilbar ist.

Ü12 Man formuliere eine Teilbarkeitsregel für 7, falls die zu untersuchende Zahl im 8-er System gegeben ist!

2.4 Lineare Kongruenzen

Wir wollen nun lineare Kongruenzen $ax \equiv b\ (m)$ (mit gegebenen Zahlen a, b, m und gesuchtem x) lösen und sehen uns zuerst einige Beispiele an.

Beispiele (a) Betrachten $2x \equiv 1\ (3)$. Eine Lösung ist offenbar $x = 2$. Klar ist auch, dass $2 + 3 = 5$, $2 + 2 \cdot 3 = 8$,... weitere Lösungen sind.
Allgemein gilt: Ist x_0 eine Lösung von $ax \equiv b\ (m)$, so sind auch $x_0 \pm m$, $x_0 \pm 2m$,... Lösungen (es ist ja $a(x + m) = ax + am \equiv b\ (m)$). Wir wollen diese Lösungen nicht als wesentlich verschieden ansehen und fragen daher nur nach modulo m inkongruenten Lösungen.

(b) Lösungen von $3x \equiv 3\ (6)$ sind $x = 1$ und $x = 3$. Diese Lösungen sind modulo 6 nicht zueinander kongruent.

(c) Die Gleichung $5x \equiv 1\ (5)$ hat offenbar keine Lösung. ■

Satz 2.5 *Die lineare Kongruenz* $ax \equiv b\ (m)$ *ist genau dann lösbar, wenn* $\mathrm{ggT}\,(a, m) \mid b$. *In diesem Fall gibt es genau* $\mathrm{ggT}\,(a, m)$ *zueinander modulo* m *inkongruente Lösungen.*

Beweis. Im weiteren setzen wir $\mathrm{ggT}\,(a, m) =: d$.
Lösbarkeit: Sei zunächst $ax \equiv b\ (m)$ lösbar. Dann gibt es Zahlen k und x_0 so, dass $ax_0 - b = k \cdot m$ bzw. $b = ax_0 - km$. Da die rechte Seite durch d teilbar ist, ist auch b durch d teilbar.
Sei nun umgekehrt d ein Teiler von b, etwa $b = b' \cdot d$. Nach Folgerung 1.2 gibt es Zahlen u, v mit $d = u \cdot a + v \cdot m$. Damit folgt

$$b = b'(ua + vm) = a(b'u) + m(b'v), \quad \text{also} \quad a(b'u) \equiv b\ (m).$$

Eindeutigkeit: Sei zuerst $d = 1$, und seien x_1 und x_2 Lösungen der Kongruenz. Aus $ax_1 \equiv b\ (m)$ und $ax_2 \equiv b\ (m)$ folgt $a(x_1 - x_2) \equiv 0\ (m)$, und wegen Satz 2.3 darf durch a dividiert werden. Folglich ist $x_1 - x_2 \equiv 0\ (m)$ bzw. $x_1 \equiv x_2\ (m)$, d. h. die Lösung der Kongruenz ist eindeutig modulo m.

Sei nun $d > 1$ und $ax_1 \equiv b\ (m)$ sowie $ax_2 \equiv b\ (m)$. Dann ist wieder $a(x_1 - x_2) \equiv 0\ (m)$, d.h. es gibt ein $k \in \mathbb{Z}$ mit $a(x_1 - x_2) = km$. Mit $a' := a/d$ und $m' := m/d$ folgt $a'(x_1 - x_2) = km'$ bzw. $a'(x_1 - x_2) \equiv 0\ (m')$. Nun ist aber $\mathrm{ggT}\,(a', m') = 1$ nach Folgerung 1.3, also darf durch a' geteilt werden und wir erhalten

$$x_1 - x_2 \equiv 0\ (m') \quad \text{bzw.} \quad x_2 = x_1 + lm', \quad l \in \mathbb{Z}.$$

Ist also x_1 eine Lösung, so ist jede weitere Lösung von der Gestalt $x_1 + lm'$. Umgekehrt sind alle diese Zahlen Lösungen:

$$\begin{aligned} a(x_1 + lm') &= ax_1 + alm' = ax_1 + a'dlm' \\ &= ax_1 + a'lm \equiv b\ (m). \end{aligned}$$

Welche der Zahlen $x_1 + lm'$ liefern nun unterschiedliche Restklassen mod m? Die Antwort ist klar:

$$x_1,\ x_1 + m',\ x_1 + 2m',\ \ldots, x_1 + (d-1)m'.$$

(Die nächste Zahl wäre $x_1 + dm' = x_1 + m$. Diese ist aber wieder kongruent zu x_1 modulo m). Also gibt es genau $d = \mathrm{ggT}\,(a, m)$ modulo m inkongruente Lösungen. ∎

Beispiele. (a) Die Kongruenz $5x \equiv 2\ (16)$ hat wegen $\mathrm{ggT}\,(5, 16) = 1$ eine eindeutige Lösung modulo 16. Man kann diese leicht durch Probieren finden: Es ist ja

$$5x \equiv 2\ (16), \quad 5x \equiv 18\ (16), \quad 5x \equiv 34\ (16), \quad 5x \equiv 50\ (16).$$

In der letzten Kongruenz ist die Division durch 5 erlaubt; also ist $x \equiv 10\ (16)$ die Lösung.

(b) Für $6x \equiv 9\ (21)$ ist $\mathrm{ggT}\,(6, 21) = 3$ und $3 \mid 9$. Die Kongruenz ist also lösbar und hat genau 3 Lösungen, die modulo 21 inkongruent sind. Wir suchen eine Lösung von $6x \equiv 30\ (21)$ und finden sofort $x_1 = 5$. Weitere dazu modulo 21 inkongruente Lösungen sind dann $x_2 = 5 + 1 \cdot \frac{21}{3} = 12$ und $x_3 = 5 + 2 \cdot \frac{21}{3} = 19$. Lösungen sind also alle Zahlen $x \equiv 5\ (21)$, $x \equiv 12\ (21)$ und $x \equiv 19\ (21)$. ∎

Ü13 Lösen Sie:

$a)$	$7x \equiv 8\ (13)$,	$c)$	$4x \equiv 7\ (15)$,
$b)$	$7x \equiv 8\ (14)$,	$d)$	$4x \equiv 6\ (18)$.

2.5 Lineare diophantische Gleichungen

Diophantische Gleichungen sind Gleichungen, deren Lösungen nur in der Menge der ganzen (mitunter auch der rationalen) Zahlen gesucht werden. Die einfachsten diophantischen Gleichungen sind die linearen Gleichungen mit 2 Unbekannten:

$$ax + by = c \quad (\text{mit gegebenen } a,\ b,\ c \in \mathbb{Z} \text{ und gesuchten } x,\ y \in \mathbb{Z}). \qquad (7)$$

Weiter wollen wir $ab \neq 0$ annehmen. Lassen wir für x und y reelle Zahlen zu, so beschreiben die Lösungen von $ax + by = c$ eine Gerade in der Ebene. Die Suche nach ganzzahligen Lösungen dieser Gleichung ist daher gleichbedeutend mit der Suche nach Gitterpunkten, die auf dieser Geraden liegen.

Wann ist nun (7) lösbar, und wie findet man alle Lösungen? Offenbar muss notwendigerweise gelten:

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

Ist dies erfüllt, kann man $ax + by = c$ durch $d := \mathrm{ggT}\,(a, b)$ dividieren und erhält die neue Gleichung

$$a'x + b'y = c' \quad (\text{mit } a' := a/d,\ b' := b/d,\ c' := c/d)\,, \tag{8}$$

wobei nun $\mathrm{ggT}\,(a', b') = 1$. Ist $b' = \pm 1$, so können wir in Gleichung (8) für x eine beliebige ganze Zahl einsetzen und erhalten ein passendes ganzzahliges y. O.E.d.A. sei noch $b' > 1$. Dann betrachten wir Gleichung (8) modulo b':

$$a'x \equiv c'\ (b')$$

Wegen $\mathrm{ggT}\,(a', b') = 1$ ist diese Kongruenz modulo b' eindeutig lösbar: $x = x_0 + lb'$ mit $l \in \mathbb{Z}$. Wir setzen dies in Ausgangsgleichung (8) ein:

$$a'(x_0 + lb') + b'y = c' \quad \Rightarrow \quad b'y = c' - a'x_0 - a'lb'$$

und erhalten nach Division durch b'

$$y = \frac{c' - a'x_0}{b'} - a'l \qquad (\text{beachte, dass } \frac{c' - a'x_0}{b'} \text{ ganzzahlig ist}).$$

Als Lösungen erhalten wir also die Paare (x, y) mit

$$x = x_0 + lb', \quad y = \frac{c' - a'x_0}{b'} - a'l \quad \text{mit } l \in \mathbb{Z}.$$

Eine Probe zeigt, dass dies tatsächlich Lösungen sind. Da $y_0 := \frac{c' - a'x_0}{b'}$ gerade die zu x_0 gehörende Lösung von $ax+by = c$ ist, erhalten wir zusammengefasst:

Satz 2.6 *Die Gleichung (7) ist genau dann lösbar in $\mathbb{Z}$, wenn $\mathrm{ggT}\,(a, b) \mid c$. Ist dies erfüllt, und ist (x_0, y_0) irgendeine Lösung von (7), so werden alle weiteren Lösungen geliefert durch*

$$x = x_0 + lb', \quad y = y_0 - la' \quad \textit{mit } l \in Z. \tag{9}$$

Beispiele. (*a*) Die Gleichung $11x + 33y = 22$ ist wegen $11 \mid 22$ lösbar in $\mathbb{Z}$. Division durch 11 liefert die Gleichung $x + 3y = 2$. Offenbar ist $x = -1$, $y = 1$ eine spezielle Lösung dieser Gleichung. Die allgemeine Lösung der Ausgangsgleichung besteht daher aus allen Paaren $(x, y) = (-1 + 3l, 1 - l)$ mit $l \in \mathbb{Z}$.

(*b*) Die Gleichung $3x + 5y = 7$ ist wegen $1 \mid 7$ lösbar in $\mathbb{Z}$. Um eine Lösung zu finden, gehen wir wie oben beschrieben vor und betrachten diese Gleichung modulo 3: Aus $3x + 5y = 7$ wird dann $2y \equiv 1\ (3)$ und weiter $2y \equiv 4\ (3)$. In letzterer Kongruenz dürfen wir durch 2 dividieren und erhalten $y \equiv 2\ (3)$ bzw. $y = 2 + 3l$ mit $l \in \mathbb{Z}$.

Einsetzen in die Ausgangsgleichung ergibt $3x + 5(2 + 3l) = 7$, woraus $3x = -15l - 3$ und schließlich $x = -5l - 1$ mit $l \in \mathbb{Z}$ folgt. Lösungen sind also alle Paare $(x, y) = (-1 - 5l, 2 + 3l)$ mit $l \in \mathbb{Z}$. ■

Einen Weg zum Auffinden einer speziellen ganzzahligen Lösung der Gleichung

$$ax + by = c \quad \text{mit ggT}\,(a, b) = 1$$

eröffnet der Euklidischem Algorithmus. Mit diesem findet man Zahlen u, v so, dass

$$au + bv = 1.$$

Multiplikation mit c liefert $a(cu) + b(cv) = c$, d.h. $x = cu$, $y = cv$ ist eine spezielle Lösung der Gleichung. Die allgemeine Lösung erhält man dann aus Formel (9).

Ü14 Bestimmen Sie die ganzzahligen Lösungen folgender Gleichungen:

$$7x + 2y = 14,$$
$$8x + 4y = 3,$$
$$26x + 65y = 91.$$

2.6 Systeme linearer Kongruenzen

Wir betrachten nun Systeme linearer Kongruenzen, d.h. wir suchen alle Zahlen x, die gleichzeitig folgende Kongruenzen erfüllen:

$$\left.\begin{aligned} x &\equiv a_1\ (m_1), \\ x &\equiv a_2\ (m_2), \\ &\vdots \\ x &\equiv a_k\ (m_k). \end{aligned}\right\} \tag{10}$$

Satz 2.7 (Chinesischer Restsatz) *Sind die Module m_j* paarweise teilerfremd*, dann ist das System* (10) *eindeutig lösbar modulo $m = m_1 \cdot m_2 \cdot \ldots \cdot m_k$.*

Beweis. Wir können uns auf $k = 2$ beschränken. Der allgemeine Fall folgt mittels vollständiger Induktion.

Existenz der Lösung: Aus $x \equiv a_1(m_1)$ folgt $x = a_1 + l \cdot m_1$ mit $l \in \mathbb{Z}$. Wir müssen zeigen, dass man l so wählen kann, dass x auch die zweite Gleichung erfüllt. Einsetzen in die zweite Gleichung liefert

$$a_1 + lm_1 \equiv a_2 \ (m_2) \quad \text{bzw.} \quad lm_1 \equiv a_2 - a_1 \ (m_2).$$

Wegen $\mathrm{ggT}\,(m_1, m_2) = 1$ ist diese Kongruenz (eindeutig) lösbar nach Satz 2.5.

Eindeutigkeit der Lösung: Seien x_1, x_2 Lösungen von (10). Dann ist zunächst $x_1 \equiv a_1 \ (m_1)$ und $x_2 \equiv a_1 \ (m_1)$, also $x_1 - x_2 \equiv 0 \ (m_1)$. Somit ist $x_1 - x_2$ durch m_1 teilbar. Analog sieht man, dass $x_1 - x_2$ durch m_2 teilbar ist. Wegen $m = m_1 m_2$ und $\mathrm{ggT}\,(m_1, m_2) = 1$ folgt die Teilbarkeit von $x_1 - x_2$ durch m; es ist also tatsächlich $x_1 \equiv x_2 \ (m)$. ∎

Man sieht auch leicht, dass für jede Lösung x von (10) auch $x \pm m$ Lösung ist, d.h. die Lösungsmenge ist von Gestalt $\{x \in \mathbb{Z} : x \equiv b \ (m)\}$ mit einem geeigneten $b \in \mathbb{Z}$.

Beispiel. Man bestimme alle $x \in \mathbb{Z}$ mit $x \equiv 4 \ (5)$ und $x \equiv 3 \ (8)$. Die erste Kongruenz schreiben wir als $x - 4 = 5l$ mit $l \in \mathbb{Z}$; Einsetzen in die zweite Kongruenz liefert

$$5l + 4 \equiv 3 \ (8) \quad \text{bzw.} \quad 5l \equiv -1 \ (8).$$

Die Lösung der letzteren Gleichung lautet $l \equiv 3 \ (8)$, also ist $l = 3 + 8k$ mit $k \in \mathbb{Z}$. Mithin erhalten wir nacheinander $x = 4 + 5l = 4 + 5(3 + 8k)$ bzw. $x = 19 + 40k$ mit $k \in \mathbb{Z}$ bzw. $x \equiv 19 \ (40)$. ∎

Ü15 Man löse folgendes System von Kongruenzen

$$\begin{aligned} x &\equiv 2 \ (3), \\ x &\equiv 1 \ (4), \\ x &\equiv 1 \ (5). \end{aligned}$$

Ü16 Es seien m_i paarweise teilerfremde Zahlen > 1. Nach dem chinesischem Restsatz gibt es Zahlen $e_1, \ldots, e_k \in \mathbb{Z}$ so, dass

$$e_k \equiv 1 \ (m_k) \quad \text{und} \quad e_k \equiv 0 \ (m_j) \text{ für } j \neq k.$$

Man zeige, dass dann die Lösung des Systems (10) gegeben wird durch

$$x \equiv a_1 e_1 + a_2 e_2 + \ldots + a_k e_k \ (m).$$

Ü17 Man löse Ü15 nach der Methode von Ü16.

3 Restklassen

3.1 Rechnen mit Restklassen

Sei $m > 1$. Wir haben bereits gesehen, dass die Relation $a \equiv b\ (m)$ eine *Äquivalenzrelation* auf $\mathbb{Z}$ ist und somit eine Einteilung der Menge der ganzen Zahlen in Äquivalenzklassen definiert, die in diesem Zusammenhang auch *Restklassen* heißen. Wir bezeichnen mit $[a]_m$ die Äquivalenzklasse, die die Zahl a enthält. $[a]_m$ besteht also aus allen ganzen Zahlen, die bei Division durch m den gleichen Rest lassen wie a. Offenbar gibt es genau m verschiedene Restklassen modulo m:

$$[0]_m, [1]_m, \ldots, [m-1]_m.$$

Anstelle von etwa $[6]_7$ kann man natürlich auch $[-1]_7$ oder $[13]_7$ schreiben; jedes Element einer Restklasse kann diese repräsentieren.

Addition und Multiplikation von Restklassen werden erklärt durch

$$[a]_m + [b]_m := [a+b]_m \qquad \text{und} \qquad [a]_m \cdot [b]_m := [ab]_m.$$

Man überlegt sich leicht, dass diese Definitionen in der Tat unabhängig von der Wahl der Repräsentanten sind, d.h. aus $[a_1]_m = [a_2]_m$ und $[b_1]_m = [b_2]_m$ folgt $[a_1 + b_1]_m = [a_2 + b_2]_m$ und $[a_1 b_1]_m = [a_2 b_2]_m$.

Die von den ganzen Zahlen her bekannten Rechengesetze
– Assoziativität der Addition/Multiplikation,
– Kommutativität der Addition/Multiplikation,
– Distributivität
werden „vererbt“ und gelten auch für das Rechnen mit Restklassen. Weiter gilt für alle $a \in \mathbb{Z}$

$$[a]_m + [0]_m = [a]_m \qquad \text{und} \qquad [a]_m\,[1]_m = [a]_m,$$

d.h. $[0]_m$ ist das neutrale Element bzgl. der Addition (Nullelement) und $[1]_m$ das neutrale Element bzgl. der Multiplikation (Einselement). Schließlich gibt es zu jedem Element $[a]_m$ bzgl. der Addition ein Entgegengesetztes: $[a]_m + [-a]_m = [0]_m$. Zusammengefasst:

Satz 3.1 *Die Menge der Restklassen* mod m *bildet einen kommutativen Ring.*

Wir bezeichnen diesen Ring mit $\mathbb{Z}/m\mathbb{Z}$ (was man ringtheoretisch als Quotienten des Ringes $\mathbb{Z}$ nach seinem Ideal $m\mathbb{Z}$ verstehen kann).

Ü18 Man zeige, dass die Gruppe der Restklassen mod m bzgl. Addition zyklisch ist.

3.2 Prime Restklassen

Die Restklassen modulo m bilden bzgl. der Addition eine Gruppe. Wie sieht es mit der Multiplikation aus (wobei wir uns natürlich auf Restklassen ungleich $[0]_m$ beschränken)? Hier sind die entsprechenden Multiplikationstafeln modulo 5 und modulo 6:

$\cdot$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[1]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[2]_5$	$[2]_5$	$[4]_5$	$[1]_5$	$[3]_5$
$[3]_5$	$[3]_5$	$[1]_5$	$[4]_5$	$[2]_5$
$[4]_5$	$[4]_5$	$[3]_5$	$[2]_5$	$[1]_5$

$\cdot$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[1]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[2]_6$	$[2]_6$	$[4]_6$	$[0]_6$	$[2]_6$	$[4]_6$
$[3]_6$	$[3]_6$	$[0]_6$	$[3]_6$	$[0]_6$	$[3]_6$
$[4]_6$	$[4]_6$	$[2]_6$	$[0]_6$	$[4]_6$	$[2]_6$
$[5]_6$	$[5]_6$	$[4]_6$	$[3]_6$	$[2]_6$	$[1]_6$

Man überprüft schnell, dass wir modulo 5 eine Gruppe erhalten haben und modulo 6 nicht. Probleme bereiten offenbar die Restklassen von 2, 3, 4, die mit 6 gemeinsame Teiler haben. Schaut man sich nur die übrigen an, bekommt man wiede reine Gruppe:

$\cdot$	$[1]_6$	$[5]_6$
$[1]_6$	$[1]_6$	$[5]_6$
$[5]_6$	$[5]_6$	$[1]_6$

Eine Restklasse $[a]_m \neq [0]_m$ heißt *prim* modulo m, wenn $\mathrm{ggT}\,(a, m) = 1$ ist. Die Menge der primen Restklassen modulo m bezeichnen wir mit G_m.

Satz 3.2 *Die Menge G_m der primen Restklassen modulo m bildet bezüglich der Multiplikation eine Gruppe.*

Insbesondere ist für jede Primzahl p die Menge $\mathbb{Z}/p\mathbb{Z}$ der Restklassen modulo p ein Körper.

Beweis. (a) *Abgeschlossenheit bzgl. der Multiplikation*: Seien $[a]_m, [b]_m \in G_m$, d.h. es ist $\mathrm{ggT}\,(a,m) = \mathrm{ggT}\,(b,m) = 1$. Aus dem Satz über die Primfaktorzerlegung folgt $\mathrm{ggT}\,(ab,m) = 1$; also $[ab]_m \in G_m$.

(b) *Einselement*: Wegen $\mathrm{ggT}\,(1,m) = 1$ ist $[1]_m \in G_m$.

(c) *Inverses Element*: Sei $[a]_m \in G_m$. Nach Satz 2.5 hat die Gleichung $ax = 1\ (m)$ genau eine Lösung modulo m, d.h. es gibt genau eine Restklasse $[x]_m$ mit $[a]_m[x]_m = 1$. Hätte x einen gemeinsamen Teiler mit m, so könnte nicht $ax \equiv 1\ (m)$ sein. Somit ist $[x]_m \in G_m$. ∎

Ü19 Man bestimme die primen Restklassen modulo $m = 2, \ldots, 12$.

Ü20 Man stelle die Gruppentafeln für $G_7, G_8, G_9, G_{10}, G_{11}$ auf.

Ü21 Man löse die Kongruenzen $3x \equiv 5\ (8)$ und $2x \equiv 1\ (11)$ mit Hilfe dieser Gruppentafeln.

3.3 Die Eulersche Funktion

Die Anzahl der Elemente von G_m oder, anders gesagt, die Anzahl der zu m teilerfremden Zahlen zwischen 1 und m heißt *Eulersche Funktion* von m und wird mit $\varphi(m)$ bezeichnet.

Beispiele. (a) Zu 10 sind 1, 3, 7, 9 teilerfremd. Somit ist $\varphi(10) = 4$.

(b) Ist p eine Primzahl, so ist $\varphi(p) = p - 1$, da alle Zahlen $1, 2, \ldots, p-1$ zu p teilerfremd sind. ∎

Satz 3.3 *Sind a und b teilerfremde natürliche Zahlen, so ist*

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

Beweis. Für $a = 1$ ist nichts zu zeigen. Sei also $a > 1$. Wir bezeichnen mit $T(a)$ die Menge aller zu a teilerfremden natürlichen Zahlen kleiner als a. Unser Ziel ist es, eine Bijektion zwischen den Mengen $T(ab)$ und $T(a) \times T(b)$ herzustellen. Hieraus folgt dann, dass $T(ab)$ und $T(a) \times T(b)$ gleich viele Elemente haben, und dies ist gerade die Behauptung.

Sei $x \in T(ab)$. Dann ist x teilerfremd zu a und b. Seien r bzw. s die Reste von x bei Division durch a bzw. b. Diese sind ebenfalls teilerfremd zu a bzw. b, d.h. das Paar (r,s) gehört zu $T(a) \times T(b)$. Wir zeigen, dass die Abbildung

$\mu : x \mapsto (r, s)$ von $T(ab)$ nach $T(a) \times T(b)$ die gesuchte Bijektion ist.
Injektivität: Seien x, $y \in T(ab)$ mit $\mu(x) = \mu(y) =: (r, s)$. Dann lösen sowohl x als auch y die simultanen Kongruenzen

$$x \equiv r \ (a)$$
$$x \equiv s \ (b).$$

Nach dem Chinesischem Restsatz unterscheiden sich x und y um ein Vielfaches von ab. Folglich stimmen x und y überein.
Surjektivität: Sei $(r, s) \in T(a) \times T(b)$. Wir haben zu zeigen, dass es ein $x \in T(ab)$ mit $\mu(x) = (r, s)$ bzw. mit

$$x \equiv r \ (a)$$
$$x \equiv s \ (b)$$

gibt. Wegen $\mathrm{ggT}\,(a, b) = 1$ ist diese Kongruenz ist stets lösbar (Chinesischer Restsatz), und alle Lösungen lassen den gleichen Rest x bei Division durch ab. Die Zahl x gehört aber zu $T(ab)$ (hätte nämlich x mit ab einen gemeinsamen Teiler größer 1, dann auch mit a oder b, und dann hätte r oder s einen gemeinsamen Teiler mit a oder b). ■

Dieser Satz öffnet einen Weg zur Berechnung der Eulerschen Funktion.

Satz 3.4 *Sei $m = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ die Primfaktorzerlegung von m. Dann ist*

$$\varphi(m) = m \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right).$$

Beweis. Da $p_i^{a_i}$ und $p_j^{a_j}$ für $i \neq j$ teilerfremd sind, folgt aus Satz 3.3

$$\varphi(m) = \varphi(p_1^{a_1}) \varphi(p_2^{a_2}) \dots \varphi(p_k^{a_k}),$$

und es bleibt die Aufgabe, $\varphi(p^a)$ für Primzahlen p zu berechnen. Da von den p^a Zahlen $1, 2, \dots, p^a$ nur die durch p teilbaren Zahlen mit p^a einen Teiler gemeinsam haben, und da es p^{a-1} durch p teilbare Zahlen unter diesen gibt, ist

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

Zusammengefasst erhalten wir

$$\begin{aligned}\varphi(m) &= p_1^{a_1}\left(1-\frac{1}{p_1}\right)p_2^{a_2}\left(1-\frac{1}{p_2}\right)\ldots p_k^{a_k}\left(1-\frac{1}{p_k}\right)\\ &= \underbrace{p_1^{a_1}p_2^{a_2}\cdot\ldots\cdot p_k^{a_k}}_{=m}\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_k}\right).\end{aligned}$$

■

Beispielsweise ist

$$\begin{aligned}\varphi(121000) &= \varphi\big(2^3\cdot 5^3\cdot 11^2\big)\\ &= 121000\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right)\left(1-\frac{1}{11}\right)\\ &= 121000\cdot\frac{1}{2}\cdot\frac{4}{5}\cdot\frac{10}{11} \;=\; 44000.\end{aligned}$$

Satz 3.5 *Es ist* $\sum_{d|n}\varphi(d)=n$.

(Hier wird über alle Teiler von n summiert.)

Beweis. Wir betrachten die n rationalen Zahlen $\frac{1}{n},\frac{2}{n},\ldots,\frac{n}{n}$ und kürzen diese so weit wie möglich. Alle entstehenden Nenner sind Teiler von n. Eine Zahl d ist nur dann Nenner, wenn sie zum entsprechenden Zähler teilerfremd ist. Jeder Nenner d kommt also $\varphi(d)$ mal vor. Hieraus folgt die Behauptung. ■

Als Anwendung geben wir einen weiteren Beweis für die Unendlichkeit der Menge der Primzahlen. Angenommen, es gäbe nur n Primzahlen $p_1,\ldots,p_n$. Bilden $m := p_1\cdot\ldots\cdot p_n$. Da jede Zahl größer als 1 durch eine der Primzahlen $p_1,\ldots,p_n$ teilbar ist, folgt $\varphi(m)=1$. Andererseits ist nach Satz 3.4

$$\varphi(m)=(p_1-1)(p_2-1)\ldots(p_n-1)>1,$$

ein Widerspruch. ■

3.4 Der Satz von Euler/Fermat

Satz 3.6 (Euler/Fermat) *Ist* $\mathrm{ggT}\,(a,m)=1$, *so gilt*

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

Beweis. Es seien $n_1, \ldots, n_{\varphi(m)}$ die Elemente von G_m. Wegen $\mathrm{ggT}\,(a, m) = 1$ ist $[a]_m$ eines dieser Elemente. Wie betrachten die Elemente

$$[a]_m n_1, [a]_m n_2, \ldots, [a]_m n_{\varphi(m)}.$$

Da G_m eine Gruppe ist, sind dies wieder dieselben Elemente wie oben (möglicherweise in anderer Reihenfolge). Daher ist

$$n_1 \cdot \ldots \cdot n_{\varphi(m)} = [a]_m n_1 \cdot \ldots \cdot [a]_m n_{\varphi(m)}.$$

Hieraus folgt sofort $[1]_m = [a]_m^{\varphi(m)}$ bzw. $a^{\varphi(m)} \equiv 1\ (m)$. ∎

Ist p Primzahl, so ist $\varphi(p) = p - 1$. Als unmittelbare Folgerung des Satzes von Euler/Fermat erhalten wir

Folgerung 3.7 (Kleiner Satz von Fermat) *Ist p Primzahl und $p \nmid a$, so gilt*

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

Beispiel. Wir wollen zeigen, dass $42 \mid n^7 - n$ für alle $n \in \mathbb{N}$. Da $42 = 2 \cdot 3 \cdot 7$, müssen wir die Teilbarkeit von $n^7 - n$ durch 2, 3 und 7 zeigen. Dazu schreiben wir

$$n^7 - n = n(n^6 - 1).$$

Teilbarkeit durch 7: Falls 7 Teiler von n ist, ist alles klar. Ist 7 kein Teiler von n, dann ist nach Fermat $7 \mid n^6 - 1$.
Teilbarkeit durch 2: Eine der Zahlen n, $n^6 - 1$ ist gerade.
Teilbarkeit durch 3: Diese folgt z.B. mit Hilfe einer Fallunterscheidung

$$\begin{aligned} &n \equiv 0\ (3) \Rightarrow \text{ gut} \\ &n \equiv 1\ (3) \Rightarrow n^6 \equiv 1\ (3) \Rightarrow 3 \mid n^6 - 1 \\ &n \equiv 2\ (3) \Rightarrow n^2 \equiv 1\ (3) \Rightarrow n^6 \equiv 1\ (3). \end{aligned}$$

Alternativ kann man weiter faktorisieren:

$$n^7 - n = n(n^6 - 1) = n(n^3 - 1)(n^3 + 1) = n(n - 1)(n^2 + n + 1)(n^3 + 1).$$

Einer der Faktoren n, $n - 1$ und $n^3 + 1$ ist sicher durch 3 teilbar. ∎

Der Satz von Euler/Fermat kann auch zur Lösung von linearen Kongruenzen $ax \equiv b\ (m)$ mit $\mathrm{ggT}\,(a, m) = 1$ benutzt werden. Aus Euler/Fermat folgt nämlich

$$ax \equiv b \cdot a^{\varphi(m)}\ (m), \quad \text{also} \quad x \equiv b \cdot a^{\varphi(m)-1}\ (m).$$

Beispiel. Die Kongruenz $8x \equiv 3\ (15)$ hat als Lösung $x \equiv 3 \cdot 8^{\varphi(15)-1}\ (15)$. Mit $\varphi(15) = 8$ erhalten wir

$$\begin{aligned} x &\equiv 3 \cdot 8^7 \equiv 3 \cdot 8 \cdot (64)^3 \equiv 3 \cdot 8 \cdot 4^3 \equiv 3 \cdot 8 \cdot 64 \\ &\equiv 3 \cdot 8 \cdot 4 \equiv 6 \cdot 16 \equiv 6\ (15) \end{aligned}$$

und somit $x \equiv 6\ (15)$. ∎

Ü22 Zeigen Sie, dass $30 \mid n^5 - n$.

Ü23 Lösen Sie mittels Euler/Fermat

$$\begin{aligned} &4x \equiv 7\ (15) && \big(\text{L.:}\quad x \equiv 13\ (15)\big) \\ &7x \equiv 8\ (13) && \big(\text{L.:}\quad x \equiv 3\ (13)\big) \\ &5x \equiv 2\ (16) && \big(\text{L.:}\quad x \equiv 10\ (16)\big) \end{aligned}$$

3.5 Der Satz von Wilson

Mit den Sätzen von Wilson und Clement lernen wir nun Kriterien für Primzahlen bzw. Primzahlzwillinge kennen. Der Aufwand zur Überprüfung dieser Kriterien steigt mit wachsendem p sehr rasch an, so dass die praktische Bedeutung dieser Kriterien eher gering ist.

Satz 3.8 (Wilson) *p ist genau dann eine Primzahl, wenn $p \mid ((p-1)! + 1)$.*

Beweis. $\Rightarrow$: Sei p Primzahl. Für $p = 2$ ist die Aussage sicher richtig. Sei $p > 2$. In der primen Restklassengruppe G_p ist jede Gleichung $[a]_p[x]_p = [1]_p$ eindeutig lösbar. Wann ist $[x]_p = [a]_p$? Dies ist genau dann der Fall, wenn $[a]_p^2 = [1]_p$ bzw. $[a^2]_p = [1]_p$ bzw. $a^2 - 1 \equiv 0\ (p)$ bzw. $(a+1)(a-1) \equiv 0\ (p)$. Wegen der Gruppeneigenschaft muss gelten $a + 1 \equiv 0\ (p)$ oder $a - 1 \equiv 0\ (p)$, d.h. die einzigen Elemente, welche zu sich selbst invers sind, sind $[a]_p = [p-1]_p$ und $[a]_p = [1]_p$. Wir betrachten nun

$$[(p-1)!]_p = [1]_p[2]_p \ldots [p-1]_p.$$

Wie wir uns soeben überlegt haben, können wir die Restklassen $[2]_p, \ldots, [p-2]_p$ zu Paaren $([a]_p, [b]_p)$ zusammenfassen mit $[a]_p[b]_p = [1]_p$. Daher ist

$$[(p-1)!]_p = [1]_p[p-1]_p = [p-1]_p$$

bzw. $(p-1)! \equiv p - 1\ (p)$ bzw. $(p-1)! + 1 \equiv 0\ (p)$.

$\Leftarrow$: Sei $(p-1)!+1 \equiv 0\ (p)$. Angenommen, p ist keine Primzahl. Dann hat p einen Teiler d mit $1 < d < p$. Dieser teilt offenbar $(p-1)!$ und muss daher auch 1 teilen. Widerspruch. ■

Satz 3.9 (Clement 1949) *Die Zahlen n und $n+2$ bilden genau dann ein Paar von Primzahlen, wenn*

$$4[(n-1)!+1]+n \equiv 0\ \big(n(n+2)\big).$$

Beweis. $\Leftarrow$: Die Zahl n erfülle die Kongruenz. Dann ist erst recht

$$4[(n-1)!+1]+n \equiv 0\ (n), \quad \text{also} \quad 4[(n-1)!+1] \equiv 0\ (n).$$

Ist n zusammengesetzt, so ist $(n-1)!$ durch n teilbar (leicht zu sehen). Folglich ist $4 \equiv 0\ (n)$. Dies ist nur für $n = 2, 4$ möglich. Beide Zahlen erfüllen aber nicht die Ausgangskongruenz. Somit ist n eine Primzahl.
Weiter folgt aus der Ausgangskongruenz

$$4(n-1)!+4+n \equiv 4(n-1)!+2 \equiv 0\ (n+2).$$

Multiplikation $n(n+1)$ und einfache Umformungen ergeben

$$4(n+1)!+2n(n+1) \equiv 0\ (n+2),$$

$$4\big((n+1)!+1\big)+2n^2+2n-4 \equiv 0\ (n+2),$$
$$4\big((n+1)!+1\big)+(n+2)(2n-2) \equiv 0\ (n+2)$$

und schließlich

$$4\big((n+1)!+1\big) \equiv 0\ (n+2).$$

Wie oben schließen wir hieraus, dass auch $n+2$ eine Primzahl ist.

$\Rightarrow$: Seien n und $n+2$ Primzahlen. Nach dem Satz von Wilson gilt dann

$$(n-1)!+1 \equiv 0\ (n), \tag{11}$$
$$(n+1)!+1 \equiv 0\ (n+2). \tag{12}$$

Schreiben wir die Kongruenz (12) als

$$\begin{aligned} 0 \equiv (n-1)!\,n(n+1)+1 &= (n-1)![(n+2)(n-1)+2]+1 \\ &= 2(n-1)!+(n+2)(n-1)!(n-1)+1 \equiv \\ &\equiv 2(n-1)!+1\ (n+2), \end{aligned}$$

so sehen wir, dass $2(n-1)!+1$ durch $(n+2)$ teilbar ist, d.h.

$$2(n-1)!+1 = k(n+2).$$

Multiplikation mit 2 und Addition von $n+2$ liefern

$$4(n-1)!+2+(n+2) = (2k+1)(n+2). \tag{13}$$

Aus der Kongruenz (11) folgt, dass $2k+1$ durch n teilbar ist:

$$0 \equiv 2(n-1)!+2 = k(n+2)+1 \equiv 2k+1 \ (n).$$

Da $2k+1$ durch n teilbar ist, ist die rechte Seite von (13) durch $n(n+2)$ teilbar. Es ist also

$$4(n-1)!+2+(n+2) \equiv 0 \ \big(n(n+2)\big)$$

bzw. $4[(n-1)!+1]+n \equiv 0 \ \big(n(n+2)\big)$. ∎

3.6 Zyklische prime Restklassengruppen

Die einfachsten Gruppen sind die *zyklischen*; in diesen gibt es ein Element mit der Eigenschaft, dass alle anderen Elemente ein Vielfaches (bei additiver Schreibweise) oder eine Potenz (bei multiplikativer Schreibweise) dieses Elementes sind. Elemente mit dieser Eigenschaft heißen *erzeugende Elemente*. Wir haben z.B. oben gesehen, dass die Menge der Restklassen $[0]_m, \ldots, [m-1]_m$ bzgl. der Addition eine zyklische Gruppe bildet.

Ü24 Wie sehen die erzeugenden Elemente dieser Gruppe aus?

In diesem Abschnitt interessieren wir uns dafür, wann die prime Restklassengruppe G_m zyklisch ist.

Beispiele. (*a*) Für $G_5 = \{[1]_5, [2]_5, [3]_5, [4]_5\}$ ist

$$\begin{aligned} [2]_5^2 &= [4]_5, \\ [2]_5^3 &= [4]_5 \cdot [2]_5 = [8]_5 = [3]_5, \\ [2]_5^4 &= [3]_5 \cdot [2]_5 = [6]_5 = [1]_5. \end{aligned}$$

D.h. die Gruppe G_5 ist tatsächlich zyklisch, und $[2]_5$ ist ein erzeugendes Element. Man kann dies auch an Gruppentafel ablesen:

$\cdot$	$[1]_5$	$[2]_5$	$[4]_5$	$[3]_5$
$[1]_5$	$[1]_5$	$[2]_5$	$[4]_5$	$[3]_5$
$[2]_5$	$[2]_5$	$[4]_5$	$[3]_5$	$[1]_5$
$[4]_5$	$[4]_5$	$[3]_5$	$[1]_5$	$[2]_5$
$[3]_5$	$[3]_5$	$[1]_5$	$[2]_5$	$[4]_5$

(*b*) Für $G_8 = \{[1]_8, [3]_8, [5]_8, [7]_8\}$ ist

$$[1]_8^2 = [1]_8, \quad [3]_8^2 = [9]_8 = [1]_8,$$
$$[5]_8^2 = [25]_8 = [1]_8, \quad [7]_8^2 = [49]_8 = [1]_8.$$

Es gibt offenbar keine erzeugenden Elemente, d.h. G_8 ist nicht zyklisch. ■

Definition. *Eine Zahl a heißt* Primitivwurzel modulo m *wenn die Gruppe G_m zyklisch ist und $[a]_m$ ein erzeugendes Element dieser Gruppe ist.*

Diese Definition wirft einige Fragen auf:

– Für welche m ist G_m zyklisch?
– Wie viele Primitivwurzeln gibt es dann?
– Wie findet man sie?

Wir beginnen mit der zweiten 2. Frage.

Satz 3.10 *Zu einem gegebenen Modul m gibt es entweder keine oder genau $\varphi\big(\varphi(m)\big)$ modulo m inkongruente Primitivwurzeln.*

Beweis. Wir zeigen zunächst: Ist a eine Primitivwurzel modulo m und n eine Zahl mit $\mathrm{ggT}\big(n, \varphi(m)\big) = 1$, dann ist auch a^n eine Primitivwurzel modulo m.
Aus Definition des erzeugenden Elementes folgt, dass a genau dann eine Primitivwurzel modulo m ist, wenn

$$a^r \not\equiv 1 \ (m) \text{ für alle } 1 \leq r < \varphi(m)$$

(man beachte, dass $a^{\varphi(m)} \equiv 1 \ (m)$ nach Euler). Damit a^n eine Primitivwurzel modulo m wird, muss also gezeigt werden, dass $(a^n)^r \not\equiv 1 \ (m)$ für alle $1 \leq r < \varphi(m)$. Angenommen, es ist $(a^n)^r \equiv 1 \ (m)$ für ein $1 \leq r < \varphi(m)$. Da a eine Primitivwurzel ist, folgt $\varphi(m) \mid rn$, und da $\mathrm{ggT}\big(n, \varphi(m)\big) = 1$ ist, muss gelten $\varphi(m) \mid r$. Dann wäre aber $\varphi(m) \leq r$, was unmöglich ist.
Da es genau $\varphi\big(\varphi(m)\big)$ natürliche Zahlen $n < \varphi(m)$ mit der Eigenschaft

$\mathrm{ggT}\big(n, \varphi(m)\big) = 1$ gibt, gibt es auch *mindestens* $\varphi\big(\varphi(m)\big)$ Primitivwurzeln modulo m (falls es überhaupt welche gibt).
Wir zeigen noch, dass es keine weiteren Primitivwurzeln neben den bereits gefundenen gibt: Ist $\mathrm{ggT}\big(n, \varphi(m)\big) = t > 1$, so ist

$$(a^n)^{\frac{\varphi(m)}{t}} = \big(a^{\frac{n}{t}}\big)^{\varphi(m)} = 1 \ (m),$$

d.h. a^n kann keine Primitivwurzel sein. Es gibt somit *genau* $\varphi\big(\varphi(m)\big)$ Primitivwurzeln, falls es überhaupt eine gibt. ∎

Die erste Frage wird durch folgenden Satz beantwortet.

Satz 3.11 *Sei $m \in \mathbb{N}$, $m \geq 2$. Die Gruppe G_m ist genau dann zyklisch, wenn $m = 2$, $m = 4$, $m = p^n$ oder $m = 2p^n$ mit einer ungeraden Primzahl p ist.*

Einen vollständigen Beweis finden Sie z.B. in Krätzel, S. 28 – 31. Wir zeigen hier nur folgenden (für uns wichtigen) Teil dieses Satzes:

Ist p Primzahl, so ist G_p zyklisch.

Beweis. Für $p = 2$ ist die Aussage klar. Sei also $p > 2$. Für jedes ganzzahlige d mit $1 \leq d \leq p - 1 = \varphi(p)$ bezeichne $\lambda(d)$ die Anzahl der Elemente aus G_p, welche die Ordnung d haben. (Zur Erinnerung: $[a]_p \in G_p$ hat die *Ordnung* d, falls $[a]_p^d = [1]_p$ und $[a]_p^b \neq [1]_p$ für alle $1 \leq b < d$.) Zu zeigen ist dann: Es gibt Elemente der Ordnung $p - 1$, d.h. $\lambda(p - 1) > 0$.

Es sei $[a]_p \in G_p$ von der Ordnung d, und sei n eine Zahl mit $\mathrm{ggT}\,(n, d) = 1$. Dann ist auch $[a]_p^n$ von der Ordnung d. Ist andererseits $\mathrm{ggT}\,(n, d) \neq 1$, so ist $[a]_p^n$ von kleinerer Ordnung als d. (Dies kann wie in Satz 3.10 begründet werden). Somit gilt: Wenn es überhaupt Restklassen der Ordnung d gibt, dann genau $\varphi(d)$ verschiedene modulo m. Es ist also entweder $\lambda(d) = 0$ oder $\lambda(d) = \varphi(d)$.

Auf Grund der Definition von λ gilt weiter

$$\sum_{1 \leq d \leq p-1} \lambda(d) = p - 1.$$

Nun weiß man aber, dass die Ordnung eines Elementes stets Teiler von $p - 1$ sein muss. Das ist der Satz von Lagrange aus der Gruppentheorie und ergibt sich auch leicht aus folgender Überlegung: Sei $[a]_p^d = [1]_p$. Nach Fermat gilt außerdem $[a]_p^{p-1} = [1]_p$. Also gilt auch $[a]_p^{\mathrm{ggT}\,(d,p-1)} = [1]_p$ wegen der Möglichkeit der Darstellung $\mathrm{ggT}\,(d, p-1) = md + n(p-1)$. Da d die Ordnung ist, folgt $d = \mathrm{ggT}\,(d, p - 1)$, d. h. $d \mid (p - 1)$.

Also gilt sogar

$$\sum_{d|(p-1)} \lambda(d) = p - 1.$$

Andererseits wissen wir aus Satz 3.5, dass

$$\sum_{d|(p-1)} \varphi(d) = p - 1.$$

Somit muss $\lambda(d) = \varphi(d)$ für alle d gelten; insbesondere für $d = p - 1$. ∎

Zur dritten Frage: Hier bleibt uns nur Probieren. In diesem Zusammenhang gibt es eine berühmte Hypothese von Emil Artin (Brief an Helmut Hasse, 1926), die 2014 noch unbewiesen war:

Artinsche Vermutung. *Ist $a > 1$ keine Quadratzahl, so gibt es unendlich viele Primzahlen p, für die a Primitivwurzel modulo p ist.*

Ü25 Für welche Moduln $m = 2, 3, \ldots, 12$ gibt es Primitivwurzeln? Falls es Primitivwurzeln gibt, bestimme man deren Anzahl.

Ü26 Man bestimme alle Primitivwurzeln modulo 10.

3.7 Indexrechnung

Es sei m ein Modul, für den G_m zyklisch ist (beispielsweise ein Primzahl), und g sei eine Primitivwurzel modulo m. Dann gibt es zu jeder Zahl a, die teilerfremd zu m ist, eine eindeutig bestimmte Zahl r mit $0 \leq r \leq \varphi(m) - 1$ mit

$$g^r \equiv a \ (m).$$

Diese Zahl r heißt *Index von a zur Basis g modulo m*, und wir schreiben

$$r = \operatorname{ind}_g a$$

Für das Rechnen mit Indizes gelten ähnliche Regeln wie für das Rechnen mit Logarithmen (so dass man r auch den Logarithmus von a zur Basis g nennt).

Satz 3.12 *Es gilt*

(a) $\operatorname{ind}_g ab \equiv \operatorname{ind}_g a + \operatorname{ind}_g b \bmod \varphi(m)$,
(b) $\operatorname{ind}_g (a^n) \equiv n \operatorname{ind}_g a \bmod \varphi(m)$,
(c) $\operatorname{ind}_g 1 = 0$,
(d) $\operatorname{ind}_g g = 1$.

Beweis. (a) Aus $a \equiv g^{\operatorname{ind}_g a}\ (m)$ und $b \equiv g^{\operatorname{ind}_g b}\ (m)$ folgt

$$ab \equiv g^{\operatorname{ind}_g a + \operatorname{ind}_g b}\ (m).$$

Andererseits ist nach Definition $ab \equiv g^{\operatorname{ind}_g ab}\ (m)$. Ein Vergleich beider Kongruenzen liefert die Behauptung (beachte, dass genau dann $g^r \equiv e\ (m)$ ist, wenn r ein Vielfaches von $\varphi(m)$ ist).

(b) Dies folgt unmittelbar aus (a).

(c) Wegen (a) gilt

$$\operatorname{ind}_g 1 = \operatorname{ind}_g(1 \cdot 1) \equiv \operatorname{ind}_g 1 + \operatorname{ind}_g 1\ (\varphi(m)).$$

Also ist $\operatorname{ind}_g 1 \equiv 0\ (\varphi(m))$. Wegen $\operatorname{ind}_g 1 \in \{0, 1, \ldots, \varphi(m)-1\}$ muss $\operatorname{ind}_g 1 = 0$ sein.

(d) Haben $g \equiv g^1 \equiv g^{\operatorname{ind}_g g}\ (m)$. Wegen $\operatorname{ind}_g g \in \{0, 1, \ldots, \varphi(m) - 1\}$ folgt, dass $\operatorname{ind}_g g = 1$. ∎

Beispiel. Die Restklassengruppe G_{11} ist zyklisch, und es gibt genau

$$\varphi\big(\varphi(11)\big) = \varphi(10) = 4$$

Primitivwurzeln modulo 11. Eine dieser Primitivwurzeln ist 2:

$$2^1 \equiv 2,\ 2^2 \equiv 4,\ 2^3 \equiv 8,\ 2^4 \equiv 5,\ 2^5 \equiv 10,\ 2^6 \equiv 9,$$

$$2^7 \equiv 7,\ 2^8 \equiv 3,\ 2^9 \equiv 6,\ 2^{10} \equiv 1 \pmod{11}.$$

Wir fassen die gefundenen Indizes in einer Tabelle zusammen:

a	1	2	3	4	5	6	7	8	9	10
$\operatorname{ind}_2 a$	10	1	8	2	4	9	7	3	6	5

Ähnlich wie die bekannten Logarithmustabellen hat man solche Indextafeln für viele Indizes berechnet. Wir zeigen nun, wie sich die Indexrechnung zum Lösen von Kongruenzen anwenden lässt.

Lineare Kongruenzen: Zu lösen ist $7x \equiv 8\ (11)$. Übergang zu Indizes (Logarithmieren) liefert

$$\operatorname{ind}_2 7 + \operatorname{ind}_2 x \equiv \operatorname{ind}_2 8\ (10)$$

(man beachte, dass $10 = \varphi(11)$). Mit der Tabelle finden wir

$$7 + \operatorname{ind}_2 x \equiv 3\ (10) \quad \text{bzw.} \quad \operatorname{ind}_2 x \equiv 3 - 7 \equiv 6\ (10),$$

woraus mit der Tabelle folgt $x \equiv 9\ (11)$.

Exponentiale Kongruenzen: Man löse $7^x \equiv 3\ (11)$. Übergang zu Indizes liefert

$$x \operatorname{ind}_2 7 \equiv \operatorname{ind}_2 3\ (10).$$

und mit der Tabelle erhalten wir die lineare Kongruenz $7x \equiv 8\ (10)$. Diese ist eindeutig lösbar: $x \equiv 4\ (10)$. Also: Alle Zahlen, die auf 4 enden, und nur diese, lösen die Kongruenz $7^x \equiv 3\ (11)$.

Quadratische Kongruenzen: Zu lösen ist $x^2 \equiv 9\ (11)$. Nach Übergang zu Indizes erhalten wir

$$2 \operatorname{ind}_2 x \equiv \operatorname{ind}_2 9\ (10),$$

und mit der Tabelle folgt $2 \operatorname{ind}_2 x \equiv 6\ (10)$. Diese lineare Kongruenz ist wegen $\operatorname{ggT}(2, 10) = 2 \mid 6$ lösbar und hat 2 modulo 10 inkongruente Lösungen:

$$\operatorname{ind}_2 x \equiv 3\ (10) \quad \text{und} \quad \operatorname{ind}_2 x \equiv 8\ (10).$$

Wieder mit Hilfe der Tabelle finden wir die Lösungen der Ausgangsgleichung $x \equiv 8\ (11)$ und $x \equiv 3\ (11)$.

Ü27 Man bestimme eine Primitivwurzel modulo 17 und berechne die entsprechende Indextafel. Mit Hilfe dieser Tafel löse man die Kongruenzen

$$9x \equiv 7\ (17), \qquad 7^x \equiv 5\ (17), \qquad x^2 \equiv 16\ (17).$$

3.8 Das quadratische Reziprozitätsgesetz

Wir betrachten die allgemeine quadratische Kongruenz

$$a_2 y^2 + a_1 y + a_0 \equiv 0\ (m)$$

mit ganzen Zahlen a_0, a_1, a_2, m, wobei $a_2 \not\equiv 0\ (m)$ und $m > 1$ sei. Multiplikation mit $4a_2$ und einfache Umformungen ergeben

$$\begin{aligned} 4a_2^2 y^2 + 4a_1 a_2 y + 4a_0 a_2 &\equiv 0\ (m), \\ 4a_2^2 y^2 + 4a_1 a_2 y + a_1^2 &\equiv a_1^2 - 4a_0 a_2\ (m), \\ (2a_2 y + a_1)^2 &\equiv a_1^2 - 4a_0 a_2\ (m). \end{aligned}$$

Setzen wir $2a_2 y + a_1 =: x$ und $a_1^2 - 4a_0 a_2 =: a$, so bleibt

$$x^2 \equiv a\ (m). \tag{14}$$

Grundlegende Aufgabe ist Studium der Lösbarkeit dieser Kongruenz. Dazu nennen wir die Zahl a einen *quadratischen Rest modulo* m, falls die Kongruenz (14) wenigstens eine Lösung besitzt; andernfalls heißt a ein *quadratischer Nichtrest modulo* m.

Beispiele. Die Zahl 2 ist quadratischer Rest modulo 7, denn $3^2 \equiv 2\ (7)$. Die Zahl 3 ist quadratischer Nichtrest modulo 7, denn

$$1^2 \equiv 1\ (7), \quad 2^2 \equiv 4\ (7), \quad 3^2 \equiv 2\ (7),$$

$$4^2 \equiv 2\ (7), \quad 5^2 \equiv 4\ (7), \quad 6^2 \equiv 1\ (7).$$

Weiter: im Zehnersystem enden alle Quadratzahlen auf 0, 1, 4, 9, 6, 5. Es sind also 0, 1, 4, 9, 6, 5 sind quadratische Reste modulo 10 und 2, 3, 7, 8 quadratische Nichtreste modulo 10. ■

Zur Beschreibung der Eigenschaft, quadratischer Rest oder Nichtrest zu sein, dient das *Legendre-Symbol* $\left(\frac{a}{p}\right)$ (lies: a für p). Sei p eine Primzahl. Dann definiert man für $a \in \mathbb{Z}$ mit $p \not| a$

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{wenn } a \text{ quadratischer Rest für } p \\ -1 & \text{wenn } a \text{ quadratischer Nichtrest für } p. \end{cases}$$

Der folgende Satz beschreibt einfache Eigenschaften des Legendre-Symbols.

Satz 3.13 *Seien p eine ungerade Primzahl und $a, b \in \mathbb{Z}$ teilerfremd zu p. Dann gilt*
(a) $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right)\ (p)$*;*
(b) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$*;*
(c) für $a \equiv b\ (p)$ *ist* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

Aussage (a) ist auch als *Eulersches Kriterium* bekannt.

Beweis. (a) Da a und p teilerfremd sind, liefert der Satz von Fermat

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

Mit der Binomischer Formel folgt (beachte: p ist eine *ungerade* Primzahl)

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

und damit

$$a^{\frac{p-1}{2}} \equiv \pm 1 \ (p).$$

Wir zeigen, dass das Plus-Zeichen genau dann gilt, wenn a ein quadratischer Rest modulo p ist. Dazu sei g eine Primitivwurzel modulo p. (Eine solche existiert nach Satz 3.11.)

Zunächst sei a ein quadratischer Rest modulo p. Dann ist $x^2 \equiv a \ (p)$ lösbar. Nach Übergang zu Indizes ist daher auch

$$2 \operatorname{ind}_g x \equiv \operatorname{ind}_g a \ (p-1)$$

lösbar. Folglich gilt $2 \mid \operatorname{ind}_g a$, d.h. es gibt ein d mit $a \equiv g^{2d} \ (p)$. Aus dieser Kongruenz und dem kleinen Satz von Fermat folgt

$$a^{\frac{p-1}{2}} \equiv g^{2d(\frac{p-1}{2})} = g^{d(p-1)} \equiv 1 \ (p).$$

Umgekehrt, sei $a^{\frac{p-1}{2}} \equiv 1 \ (p)$ und $a \equiv g^m \ (p)$. Dann ist

$$g^{\frac{p-1}{2}m} \equiv 1 \ (p),$$

und folglich ist $\frac{(p-1)}{2}m$ ein Vielfaches von $p-1 = \varphi(p)$. Mithin ist m eine gerade Zahl, etwa $m = 2n$, und daher

$$a \equiv g^{2n} \ (p).$$

Dann ist a aber ein quadratischer Rest. Zusammengefasst: Es gilt stets $a^{\frac{p-1}{2}} \equiv \pm 1 \ (p)$, und das Plus-Zeichen gilt genau dann, wenn a ein quadratischer Rest modulo p ist, d.h. genau dann, wenn $\left(\frac{a}{p}\right) = 1$.

Aussage (b) folgt leicht aus (a): Es ist

$$(ab)^{\frac{p-1}{2}} \equiv \left(\frac{ab}{p}\right) \ (p)$$

und

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

d.h. es gilt

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

Da das Legendre-Symbol nur die Werte ± 1 annimmt, folgt die Behauptung. Schließlich folgt Aussage (c) unmittelbar aus den Definitionen. ∎

Wir formulieren nun die Hauptresultate der Theorie der quadratischen Reste.

Satz 3.14 (*a*) *(Quadratisches Reziprozitätsgesetz) Sind p und q verschiedene ungerade Primzahlen, so gilt*

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

(*b*) *(Ergänzungssätze) Ist p ungerade Primzahl, dann gilt*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \quad \textit{und} \quad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Kurz zur Geschichte: Vermutet wurde das Quadratisches Reziprozitätsgesetz bereits von Euler und Legendre. Den ersten Beweis gab Gauß (später gab Gauß noch 5 weitere Beweise). Das quadratisches Reziprozitätsgesetz bildet einen Ausgangspunkt für die höhere Zahlentheorie (Kubisches, biquadratisches Reziprozitätsgesetz; Allgemeine Reziprozitätsgesetze von Hilbert und Artin).

Beispiele. (*a*) Ist 74 quadratischer Rest modulo 131? Unter Benutzung der Eigenschaften des Legendre-Symbols und des Reziprozitätsgesetzes berechnen wir nacheinander:

$$\begin{aligned}
\left(\frac{74}{131}\right) &= \left(\frac{2}{131}\right)\left(\frac{37}{131}\right) && \text{(Eig. } (b)\text{)}\\
\left(\frac{2}{131}\right) &= (-1)^{\frac{131^2-1}{8}} = -1 && \text{(2. Erg.-satz)}\\
\left(\frac{37}{131}\right) &= \left(\frac{131}{37}\right)\cdot(-1)^{\frac{131-1}{2}\cdot\frac{37-1}{2}} = \left(\frac{131}{37}\right) && \text{(Reziproz.-gesetz)}\\
\left(\frac{131}{37}\right) &= \left(\frac{20}{37}\right) && \text{(Eig. } (c)\text{)}\\
\left(\frac{20}{37}\right) &= \left(\frac{4}{37}\right)\left(\frac{5}{37}\right) = \left(\frac{5}{37}\right) && \text{(da 4 Quadratzahl)}\\
\left(\frac{5}{37}\right) &= \left(\frac{37}{5}\right)(-1)^{\frac{5-1}{2}\cdot\frac{37-1}{2}} = \left(\frac{37}{5}\right) && \text{(Reziproz.-gesetz)}\\
\left(\frac{37}{5}\right) &= \left(\frac{2}{5}\right) && \text{(Eig. } (c)\text{)}\\
\left(\frac{2}{5}\right) &= (-1)^{\frac{5^2-1}{8}} = -1. && \text{(2. Erg.-satz)}
\end{aligned}$$

Zusammengefasst: $\left(\frac{74}{131}\right) = -1 \cdot -1 = 1$, d.h. 74 ist quadratischer Rest modulo 131 (oder anders gesagt: die Gleichung $x^2 \equiv 74\ (131)$ ist lösbar).

(*b*) Für welche Primzahlen $p > 3$ ist 3 quadratischer Rest bzw. Nichtrest? Nach dem Reziprozitätsgesetz ist

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)(-1)^{\frac{3-1}{2}\cdot\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right).$$

Wir unterscheiden 2 Fälle: $p = 6k+1$, $p = 6k-1$ (weitere Fälle kann es nicht geben).

Fall 1: $p = 6k + 1$. Dann ist

$$\left(\frac{3}{p}\right) = (-1)^{3k}\left(\frac{6k+1}{3}\right) = (-1)^k\left(\frac{1}{3}\right) = (-1)^k$$
$$= \begin{cases} 1 & \text{falls } k \text{ gerade, d.h. } k = 2r, \\ -1 & \text{falls } k \text{ ungerade, d.h. } k = 2r-1. \end{cases}$$

Somit gilt in diesem Fall: Ist $p = 12r + 1$, so ist 3 ein quadratischer Rest modulo p; ist $p = 12r - 5$, so ist 3 ein quadratischer Nichtrest modulo p.

Fall 2: $p = 6k - 1$. Dann ist

$$\left(\frac{3}{p}\right) = (-1)^{3k-1}\left(\frac{6k-1}{3}\right) = (-1)^{k-1}\left(\frac{-1}{3}\right) = (-1)^{k-1}\cdot(-1) = (-1)^k$$
$$= \begin{cases} 1 & \text{falls } k \text{ gerade, d.h. } k = 2r, \\ -1 & \text{falls } k \text{ ungerade, d.h. } k = 2r-1. \end{cases}$$

Wir erhalten damit: Ist $p = 12k - 1$, so ist 3 ein quadratischer Rest modulo p; ist $p = 12r - 7$, so ist 3 ein quadratischer Nichtrest modulo p.

Wir wollen nun Satz 3.14 beweisen und formulieren dazu zwei Lemmata.

Lemma 3.15 (Gauß) *Sei p eine ungerade Primzahl und $a \in \mathbb{Z}$ teilerfremd zu p. Weiter sei s die Anzahl der kleinsten positiven Reste der Zahlen*

$$a,\ 2a,\ \ldots,\ ((p-1)/2)a$$

modulo p, die größer als $p/2$ sind. Dann gilt

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

Beweis. Es seien $u_1, u_2, \ldots, u_s$ die kleinsten positiven Reste der Zahlen $a, 2a, \ldots, ((p-1)/2)a$ modulo p, die größer als $p/2$ sind, und $v_1, v_2, \ldots, v_t$ die entsprechenden Reste, die kleiner als $p/2$ sind. Wir zeigen, dass die Zahlen $p-u_1, p-u_2, \ldots, p-u_s, v_1, v_2, \ldots, v_t$ mit den Zahlen $1, 2, \ldots, (p-1)/2$ zusammenfallen (möglicherweise in anderer Reihenfolge). Dazu genügt es zu zeigen, dass keine zwei dieser Zahlen kongruent modulo p sind (nach Konstruktion sind ja alle Zahlen $p-u_i$ und v_j positiv und kleiner oder gleich $(p-1)/2$).

Wären zwei der $p-u_i$ kongruent modulo p, dann gäbe es Zahlen $m, n \leq (p-1)/2$ mit $ma \equiv na\ (p)$. Wegen $\mathrm{ggT}\,(a,p) = 1$ wäre dann $m \equiv n\ (p)$, was unmöglich ist. Analog können keine zwei der v_j kongruent modulo p sein. Wären schließlich ein $p-u_i$ und ein v_j kongruent modulo p, dann gäbe es Zahlen $m, n \leq (p-1)/2$ mit $ma \equiv p-na \equiv -na\ (p)$. Wie oben folgt hieraus $m \equiv -n\ (p)$, was wieder unmöglich ist.

Folglich ist

$$(p-u_1)(p-u_2)\ldots(p-u_s)\,v_1v_2\ldots v_t \equiv ((p-1)/2)!\ (p),$$

woraus folgt, dass

$$(-1)^s u_1u_2\ldots u_s\,v_1v_2\ldots v_t \equiv ((p-1)/2)!\ (p).$$

Da andererseits die $u_1, u_2, \ldots, u_s, v_1, v_2, \ldots, v_t$ die kleinsten positiven Reste der Zahlen $a, 2a, \ldots, ((p-1)/2)a$ modulo p sind, folgt

$$u_1u_2\ldots u_s\,v_1v_2\ldots v_t \equiv a\,2a\ldots\frac{p-1}{2}a \equiv a^{\frac{p-1}{2}}((p-1)/2)!\ (p).$$

Ein Vergleich der letzten beiden Identitäten liefert sofort

$$(-1)^s a^{\frac{p-1}{2}}((p-1)/2)! \equiv ((p-1)/2)!\ (p).$$

Da der größte gemeinsame Teiler von p und $((p-1)/2)!$ gleich 1 ist, folgt weiter

$$(-1)^s a^{\frac{p-1}{2}} \equiv 1\ (p) \quad \text{bzw.} \quad a^{\frac{p-1}{2}} \equiv (-1)^s\ (p).$$

Aus dem Eulerschen Kriterium wissen wir schließlich, dass

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

Wir haben somit erhalten, dass

$$\left(\frac{a}{p}\right) \equiv (-1)^s \ (p),$$

woraus das Gaußsche Lemma unmittelbar folgt. ∎

Lemma 3.16 *Sei p eine ungerade Primzahl und a eine ungerade ganze Zahl mit* $\mathrm{ggT}\,(a,p) = 1$. *Dann ist*

$$\left(\frac{a}{p}\right) = (-1)^{T(a,p)} \quad mit \quad T(a,p) := \sum_{j=1}^{(p-1)/2} [ja/p].$$

Beweis. Wir betrachten wieder die kleinsten positiven Reste der Zahlen a, $2a, \ldots,$ $((p-1)/2)a$ modulo p und bezeichnen diejenigen größer als $p/2$ mit $u_1, u_2, \ldots, u_s$ und diejenigen kleiner als $p/2$ mit $v_1, v_2, \ldots, v_t$. Division mit Rest liefert für jedes j

$$ja = p[ja/p] + Rest,$$

wobei *Rest* eine der Zahlen $u_1, u_2, \ldots, u_s, v_1, v_2, \ldots, v_t$ ist. Addieren wir alle $(p-1)/2$ Gleichungen dieser Gestalt, finden wir

$$\sum_{j=1}^{(p-1)/2} ja = \sum_{j=1}^{(p-1)/2} p[ja/p] + \sum_{j=1}^{s} u_j + \sum_{j=1}^{t} v_j. \tag{15}$$

Wie wir im Beweis des Gaußschen Lemmas gesehen haben, sind die Zahlen $p-u_1, p-u_2, \ldots, p-u_s, v_1, v_2, \ldots, v_t$ genau die Zahlen 1, 2, $\ldots$, $(p-1)/2$ (möglicherweise in anderer Reihenfolge). Daher ist

$$\sum_{j=1}^{(p-1)/2} j = \sum_{j=1}^{s}(p-u_j) + \sum_{j=1}^{t} v_j = ps - \sum_{j=1}^{s} u_j + \sum_{j=1}^{t} v_j. \tag{16}$$

Subtrahieren wir (16) von (15), folgt

$$\sum_{j=1}^{(p-1)/2} ja - \sum_{j=1}^{(p-1)/2} j = \sum_{j=1}^{(p-1)/2} p[ja/p] - ps + 2\sum_{j=1}^{s} u_j$$

bzw., mit der Notation $T(a,p)$,

$$(a-1)\sum_{j=1}^{(p-1)/2} j = p\,T(a,p) - ps + 2\sum_{j=1}^{s} u_j.$$

Wir betrachten diese Gleichheit modulo 2. Da a und p ungerade sind, folgt

$$T(a,p) \equiv s\ (2).$$

Die Behauptung folgt nun sofort aus dem Gaußschen Lemma. ∎

Beweis des Quadratisches Reziprozitätsgesetzes. (a) Wir betrachten alle Paare (x,y) ganzer Zahlen mit $1 \le x \le (p-1)/2$ und $1 \le y \le (q-1)/2$. Es gibt genau $\frac{p-1}{2}\,\frac{q-1}{2}$ solche Paare. Wir teilen diese Paare in zwei Klassen in Abhängigkeit der Größe von qx und py.

Zuerst machen wir uns klar, dass $qx \neq py$ für alle diese Paare. Wäre nämlich $qx = py$ für ein Paar, dann wäre $q \mid py$, woraus $q \mid p$ oder $q \mid y$ folgt. Ersteres ist unmöglich, da p und q verschiedene Primzahlen sind, und aus $1 \le y \le (q-1)/2$ folgt, dass q auch kein Teiler von y sein kann.

Die erste Klasse bestehe nun aus allen Paaren (x,y) ganzer Zahlen mit $1 \le x \le (p-1)/2$ und $1 \le y \le (q-1)/2$, für die $qx > py$ ist. Das sind genau die Paare mit $1 \le x \le (p-1)/2$ und $1 \le y \le qx/p$. Für jeden festen Wert von x mit $1 \le x \le (p-1)/2$ gibt es genau $[qx/p]$ ganze Zahlen y mit $1 \le y \le qx/p$. Folglich ist die Anzahl aller Paare in der ersten Klasse gleich

$$\sum_{j=1}^{(p-1)/2} [qj/p].$$

Die zweite Klasse besteht dann aus allen Paaren (x,y) ganzer Zahlen mit $1 \le x \le (p-1)/2$ und $1 \le y \le (q-1)/2$, für die $qx < py$ ist. Das sind genau die Paare mit $1 \le y \le (q-1)/2$ und $1 \le x \le py/q$. Für jeden festen Wert von y mit $1 \le y \le (q-1)/2$ gibt es genau $[py/q]$ ganze Zahlen x mit $1 \le x \le py/q$. Folglich ist die Anzahl der Paare in der zweiten Klasse gleich

$$\sum_{j=1}^{(q-1)/2} [pj/q].$$

Da jedes Paar in genau einer Klasse liegt und wir insgesamt $\frac{p-1}{2}\,\frac{q-1}{2}$ Paare haben, folgt

$$\sum_{j=1}^{(p-1)/2} [qj/p] + \sum_{j=1}^{(q-1)/2} [pj/q] = \frac{p-1}{2}\,\frac{q-1}{2}$$

(am Ende haben wir diese Identität erhalten, indem wir die betrachteten Paare auf zweierlei Art gezählt haben). In der Notation von Lemma 3.16 ist also

$$T(q,p) + T(p,q) = \frac{p-1}{2}\,\frac{q-1}{2}$$

und folglich

$$(-1)^{T(q,p)}\,(-1)^{T(p,q)} = (-1)^{\frac{p-1}{2}\,\frac{q-1}{2}}.$$

Schließlich wissen wir aus Lemma 3.16, dass

$$(-1)^{T(q,p)} = \left(\frac{q}{p}\right) \quad \text{und} \quad (-1)^{T(p,q)} = \left(\frac{p}{q}\right),$$

woraus die Behauptung des Quadratisches Reziprozitätsgesetzes folgt.

(b) Die erste Aussage von (b) ist das bereits bewiesene Eulersche Kriterium für $a = -1$; wir haben daher nur noch den zweiten der Ergänzungssätze zu beweisen. Sei s die Anzahl der kleinsten positiven Reste der Zahlen $1 \cdot 2$, $2 \cdot 2$, $(p-1)/2 \cdot 2$ modulo p, die größer als $p/2$ sind. Nach dem Gaußschen Lemma ist

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

Da die genannten Zahlen alle kleiner als p sind, müssen wir nur zählen, wieviele dieser Zahlen größer als $p/2$ sind. Nun ist eine Zahl $2j$ mit $1 \le j \le (p-1)/2$ kleiner als $p/2$ genau dann, wenn $j \le p/4$. Unter den genannten Zahlen gibt es daher $[p/4]$ Zahlen kleiner als $p/2$ und folglich $s = (p-1)/2 - [p/4]$ Zahlen größer als $p/2$. Es ist also

$$\left(\frac{2}{p}\right) = (-1)^s = (-1)^{(p-1)/2-[p/4]}.$$

Die Behauptung folgt, sobald wir gezeigt haben, dass

$$(p-1)/2 - [p/4] \equiv (p^2-1)/8 \quad (2). \tag{17}$$

Dazu betrachten wir die Restklassen von p modulo 8. Zunächst betrachten wir die Zahlen $(p^2-1)/8$. Ist $p \equiv \pm 1$ (8), dann ist $p = 8k \pm 1$ mit einem $k \in \mathbb{Z}$ und daher

$$(p^2-1)/8 = ((8k \pm 1)^2 - 1)/8 = (64k^2 \pm 16k)/8 = 8k^2 \pm 2k \equiv 0\ (2).$$

Ist dagegen $p \equiv \pm 3\ (8)$, dann ist $p = 8k \pm 3$ mit einem $k \in \mathbb{Z}$ und daher

$$(p^2-1)/8 = ((8k \pm 3)^2 - 1)/8 = (64k^2 \pm 48k + 8)/8 = 8k^2 + 6k + 1 \equiv 1\ (2).$$

Nun betrachten wir die Zahlen $(p-1)/2 - [p/4]$. Ist $p \equiv 1\ (8)$, dann ist $p = 8k+1$ mit einem $k \in \mathbb{Z}$ und daher

$$(p-1)/2 - [p/4] = 4k - [2k + 1/4] = 2k \equiv 0\ (2).$$

Ist $p \equiv 3\ (8)$, dann ist $p = 8k+3$ mit einem $k \in \mathbb{Z}$ und daher

$$(p-1)/2 - [p/4] = 4k + 1 - [2k + 3/4] = 2k + 1 \equiv 1\ (2).$$

Ist $p \equiv 5\ (8)$, dann ist $p = 8k+5$ mit einem $k \in \mathbb{Z}$ und daher

$$(p-1)/2 - [p/4] = 4k + 2 - [2k + 5/4] = 2k + 1 \equiv 1\ (2).$$

Ist schließlich $p \equiv 7\ (8)$, dann ist $p = 8k+7$ mit einem $k \in \mathbb{Z}$ und daher

$$(p-1)/2 - [p/4] = 4k + 3 - [2k + 7/4] = 2k + 2 \equiv 0\ (2).$$

Damit ist (17) gezeigt. ■

Wir haben oben das Legendre-Symbol $\left(\frac{a}{p}\right)$ für (ungerade) Primzahlen p definiert und geben nun eine Verallgemeinerung an. Sei n eine natürliche Zahl mit Primfaktorzerlegung $n = p_1^{a_1} \cdot \ldots \cdot p_k^{a_k}$ und a eine natürliche Zahl, die zu n teilerfremd ist. Dann definiert man das *Jacobi-Symbol* $\left(\frac{a}{n}\right)$ durch

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1^{a_1} \ldots p_k^{a_k}}\right) = \left(\frac{a}{p_1}\right)^{a_1} \ldots \left(\frac{a}{p_k}\right)^{a_k}.$$

Auf der rechten Seite stehen die bekannten Legendre-Symbole. Ist p eine (ungerade) Primzahl und a teilerfremd zu p, stimmen das Legendre-Symbol $\left(\frac{a}{p}\right)$ und das Jacobi-Symbol $\left(\frac{a}{p}\right)$ überein. Beispielsweise ist

$$\left(\frac{2}{45}\right) = \left(\frac{2}{3^2 \cdot 5}\right) = \left(\frac{2}{3}\right)^2 \left(\frac{2}{5}\right) = (-1)^2(-1) = -1$$

und

$$\begin{aligned}\left(\frac{109}{385}\right) &= \left(\frac{109}{5 \cdot 7 \cdot 11}\right) = \left(\frac{109}{5}\right)\left(\frac{109}{7}\right)\left(\frac{109}{11}\right) \\ &= \left(\frac{4}{5}\right)\left(\frac{4}{7}\right)\left(\frac{10}{11}\right) = \left(\frac{2}{5}\right)^2\left(\frac{2}{7}\right)^2\left(\frac{-1}{11}\right) = (-1)^2 1^2 (-1) = -1.\end{aligned}$$

Man beachte, dass uns das Jacobi-Symbol NICHTS über die Eigenschaft verrät, quadratischer Rest oder Nichtrest zu sein. So ist etwa

$$\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1;$$

da aber keine der Kongruenzen $x^2 \equiv 2\ (3)$ und $x^2 \equiv 2\ (5)$ lösbar ist, ist 2 ein quadratischer Nichtrest modulo 15. Was man sicher sagen kann, ist lediglich: *Wenn a quadratischer Rest modulo n ist, dann ist* $\left(\frac{a}{n}\right) = 1$. Ist nämlich p ein Primteiler von n und ist die Kongruenz $x^2 \equiv a\ (n)$ lösbar, so ist die Kongruenz $x^2 \equiv a\ (p)$ ebenfalls lösbar.

Das Jacobi-Symbol ist dennoch nützlich, da es viele Eigenschaften mit dem Legendre-Symbol gemeinsam hat und z.B. bei der Berechnung von Legendre-Symbolen hilfreich sein kann.

Satz 3.17 *Seien $n \in \mathbb{N}$ ungerade und $a, b \in \mathbb{Z}$ teilerfremd zu n. Dann gilt*
(a) für $a \equiv b\ (n)$, dass $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$,
(b) $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$.

Satz 3.18 *(a) (Quadratisches Reziprozitätsgesetz) Sind $n, m \in \mathbb{N}$ ungerade und teilerfremd, so gilt*

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

(b) (Ergänzungssätze) Ist $n \in \mathbb{N}$ ungerade, dann gilt

$$\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}} \quad \textit{und} \quad \left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}.$$

Die Beweise dieser Aussagen folgen meist mit wenig Aufwand aus den entsprechenden Aussagen für das Legendre-Symbol und aus der Definition des Jacobi-Symbols.

4 Zahlentheoretische Funktionen

4.1 Definition und Beispiele

Eine *zahlentheoretische Funktion* ist eine auf der Menge der natürlichen Zahlen definierte reell- oder komplexwertige Funktion (also einfach eine Folge mit Werten in $\mathbb{R}$ oder $\mathbb{C}$). Ein typisches Beispiel ist die Primzahlfunktion π, wobei $\pi(n)$ die Anzahl der Primzahlen kleiner gleich n angibt (vgl. Abschnitt 1.5.3). Es folgen einige z.T. bereits bekannte Beispiele, die sich leicht berechnen lassen, sofern die Primfaktorzerlegung

$$n = p_1^{a_1} \cdot \ldots \cdot p_k^{a_k} \tag{18}$$

von n bekannt ist.

4.1.1 Anzahl der Teiler einer Zahl

Sei $\nu(n)$ die Anzahl der positiven Teiler der natürlichen Zahl n (also z.B. $\nu(1) = 1$, $\nu(2) = 2$, $\nu(6) = 4$ und $\nu(12) = 6$). Zahlen mit $\nu(n) = 2$ sind gerade die Primzahlen.

Satz 4.1 *Für n wie in (18) ist*

$$\nu(n) = (a_1 + 1) \cdot \ldots \cdot (a_k + 1).$$

Beweis. Teiler von n ist jede Zahl der Gestalt $p_1^{b_1} \cdot \ldots \cdot p_k^{b_k}$ mit $0 \leq b_i \leq a_i$ für alle $i = 1, \ldots, k$. Wir müssen zählen, wie viele solcher Zahlen es gibt. Da es für jedes i genau $a_i + 1$ Möglichkeiten zur Wahl von b_i gibt, haben wir insgesamt $(a_1 + 1) \cdot \ldots \cdot (a_k + 1)$ Möglichkeiten. ∎

4.1.2 Summe der Teiler einer Zahl

Wir bezeichnen mit $\sigma(n)$ die Summe der positiven Teiler der Zahl n (also z.B. $\sigma(3) = 4$, $\sigma(6) = 12$ und $\sigma(12) = 28$).

Satz 4.2 *Für n wie in (18) ist*

$$\sigma(n) = \frac{p_1^{a_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{a_2+1} - 1}{p_2 - 1} \cdot \ldots \cdot \frac{p_k^{a_k+1} - 1}{p_k - 1}.$$

Beweis. Die Teiler von p^a sind 1, p, p^2, …, p^a. Mit der Summenformel für die geometrische Reihe folgt

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

Damit ist die Behauptung für $k = 1$ gezeigt. Für $k = 2$ sieht man die Bahauptung wie folgt: Alle Teiler von $p_1^{a_1} p_2^{a_2}$ haben die Gestalt $p_1^{b_1} p_2^{b_2}$ mit $0 \leq b_1 \leq a_1$ und $0 \leq b_2 \leq a_2$. Somit ist

$$\begin{aligned} \sigma(p_1^{a_1} p_2^{a_2}) &= \sum_{b_1=0}^{a_1} \sum_{b_2=0}^{a_2} p_1^{b_1} p_2^{b_2} \\ &= \left(\sum_{b_1=0}^{a_1} p_1^{b_1} \right) \left(\sum_{b_2=0}^{a_2} p_2^{b_2} \right) = \frac{p_1^{a_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{a_2+1} - 1}{p_2 - 1}. \end{aligned}$$

Der allgemeine Fall folgt ebenso leicht mit vollständiger Induktion nach der Anzahl k der verschiedenen Primteiler von n. ∎

Mit der Funktion σ ist ein berühmtes noch ungelöstes zahlentheoretisches Problem verknüpft, welches wir bereits in Abschnitt 1.5.2 kurz erwähnt haben. Eine Zahl n heißt *perfekt*, wenn $\sigma(n) = 2n$. Die einzigen perfekten Zahlen kleiner als 10^4 sind 6, 28, 496 und 8128.

Satz 4.3 *(a) (Euklid) Ist $2^{m+1} - 1$ eine Primzahl, so ist $2^m(2^{m+1} - 1)$ perfekt.*
(b) (Euler) Jede gerade perfekte Zahl ist von dieser Gestalt.

Beweis. (*a*) Sei $2^{m+1} - 1$ eine Primzahl. Mit der Formel aus dem vorangegangenen Satz erhalten wir dann

$$\begin{aligned} \sigma\big(2^m(2^{m+1} - 1)\big) &= \frac{2^{m+1} - 1}{2 - 1} \cdot \frac{(2^{m+1} - 1)^2 - 1}{2^{m+1} - 2} \\ &= (2^{m+1} - 1)2^{m+1} = 2 \cdot 2^m(2^{m+1} - 1). \end{aligned}$$

(*b*) Sei n eine gerade perfekte Zahl. Wir schreiben n als $n = 2^s t$ mit s, $t \in \mathbb{N}$ und t ungerade. Mit der Formel aus dem vorangegangenen Satz erhalten wir

$$\sigma(n) = \sigma(2^s t) = \sigma(2^s)\,\sigma(t) = (2^{s+1} - 1)\,\sigma(t).$$

Da n perfekt ist, wissen wir auch, dass $\sigma(n) = 2n = 2^{s+1} t$. Folglich ist

$$(2^{s+1} - 1)\,\sigma(t) = 2^{s+1} t. \tag{19}$$

Da der größte gemeinsame Teiler von 2^{s+1} und $2^{s+1}-1$ gleich 1 ist, folgt $2^{s+1} \mid \sigma(t)$; es gibt also ein $q \in \mathbb{N}$ mit $\sigma(t) = 2^{s+1}q$. Dies in (19) eingesetzt liefert

$$(2^{s+1}-1)\,2^{s+1}q = 2^{s+1}t$$

und folglich $(2^{s+1}-1)q = t$. Es gilt daher $q \mid t$ und $q \neq t$, und weiter ist

$$t + q = (2^{s+1}-1)q + q = 2^{s+1}q = \sigma(t). \tag{20}$$

Wir zeigen, dass $q = 1$. Wäre $q > 1$, so hätte t wenigstens drei paarweise verschiedene positive Teiler, nämlich 1, q und t. Dann wäre $\sigma(t) \geq t + q + 1$, im Widerspruch zu (20). Somit ist $q = 1$ und $t = 2^{s+1} - 1$. Wegen (20) ist weiter $\sigma(t) = t + 1$, d.h. t ist eine Primzahl. ∎

Primzahlen der Gestalt $2^m - 1$ heißen *Mersennesche Primzahlen*. Es ist unbekannt, ob es endlich oder unendlich viele Mersennesche Primzahlen gibt. Aktuell (März 2016) sind 49 Mersennesche Primzahlen bekannt; die größte aktuell bekannte (Mersennesche) Primzahl ist $2^{74.207.281} - 1$, eine Zahl mit 22.338.618 Stellen, die im Januar 2016 gefunden wurde. Entsprechend kennt man also 49 perfekte Zahlen. Alle bekannten perfekten Zahlen sind gerade. Offen: Gibt es ungerade perfekte Zahlen? Gibt es unendlich viele gerade perfekte Zahlen?

Ü29 Man zeige: Ist $2^m - 1$ Primzahl, so ist m Primzahl.

4.1.3 Die verallgemeinerte Teilersumme

Für $k = 0, 1, \ldots$ sei $\sigma_k(n)$ die Summe der k. Potenzen aller Teiler von n. Insbesondere ist also

$$\sigma_0(n) = \nu(n) \quad \text{und} \quad \sigma_1(n) = \sigma(n).$$

Wir stellen später eine Formel zur Berechnung von $\sigma_k(n)$ auf.

4.1.4 Die Eulersche Funktion

Für die Eulersche Funktion φ ist $\varphi(n)$ gleich der Anzahl der zu n teilerfremden positiven Zahlen kleiner als oder gleich n. Wir haben diese Funktion bereits in Abschnitt 3.3 eingeführt und dort gezeigt, dass für n wie in (18) gilt

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right).$$

4.1.5 Die Möbiussche Funktion

Die Möbiussche Funktion μ ist wie folgt definiert: Es sei $\mu(1) := 1$, und für $n > 1$ sei

$\mu(n) = 0$ falls n durch das Quadrat einer Primzahl teilbar ist

$\mu(n) = (-1)^l$ falls n das Produkt von l verschiedenen Primzahlen ist.

Beispielsweise ist $\mu(30) = \mu(2 \cdot 3 \cdot 5) = -1$, $\mu(210) = \mu(2 \cdot 3 \cdot 5 \cdot 7) = +1$ und $\mu(420) = \mu(2^2 \cdot 3 \cdot 5 \cdot 7) = 0$. Wir werden später sehen, wozu diese Funktion gut ist.

4.2 Das Dirichlet-Produkt

Sind f und g zahlentheoretische Funktionen, so definiert man ihr *Dirichlet-Produkt* $f * g$ durch

$$(f * g)(n) = \sum_{t|n} f(t)\, g(n/t)$$

(die Summation erstreckt sich über alle Teiler t von n).

Beispiel. Für $f(n) = n^2$ und $g(n) = n$ ist

$$\begin{aligned}(f * g)(n) &= \sum_{t|n} f(t)\, g\left(\frac{n}{t}\right) = \sum_{t|n} t^2 \cdot \frac{n}{t} \\ &= n \sum_{t|n} t = n\,\sigma(n).\end{aligned}$$

Satz 4.4 *Die Menge aller zahlentheoretischen Funktionen f mit $f(1) \neq 0$ bildet bzgl. des Dirichlet-Produkts $*$ eine kommutative Gruppe.*

Beweis. Offenbar ist das Produkt zweier zahlentheoretischer Funktionen wieder eine solche, und sind $f(1) \neq 0$ und $g(1) \neq 0$, so ist auch

$$(f * g)(1) = \sum_{t|1} f(t)\, g(1/t) = f(1)\, g(1) \neq 0.$$

Die Operation $*$ führt also nicht aus der betrachteten Menge heraus.

Um die Kommutativität von $*$ einzusehen, schreiben wir die Definition von $*$ um:

$$(f*g)(n) = \sum_{(t_1,t_2):t_1t_2=n} f(t_1)g(t_2).$$

Aus der Symmetrie dieses Ausdrucks folgt sofort die Kommutativität. Die Assoziativität folgt ganz ähnlich aus

$$\big((f*g)*h\big)(n) = \sum_{\substack{(t_1,t_2,t_3):\\ t_1t_2t_3=n}} \big(f(t_1)\ g(t_2)\big)\ h(t_3).$$

Das Einselement ist eine zahlentheoretische Funktion e so, dass

$$(f*e)(n) = \sum_{\substack{t|n\\ t<n}} f(t)\cdot e\left(\frac{n}{t}\right) + f(n)\ e(1) = f(n)$$

für alle f und alle n ist. Offenbar erfüllt die durch $e(1)=1$ und $e(n)=0$ für $n>1$ definierte Funktion diese Bedingung. Da das Einselement eindeutig bestimmt ist, ist diese Funktion das Einselement.

Schließlich müssen wir zeigen, dass jede Gleichung $f*x=e$ für alle f eine Lösung x (das inverse Element zu f) besitzt. Aus

$$\sum_{t|n} f\left(\frac{n}{t}\right)\ x(t) = \begin{cases} 1 & \text{für } n=1\\ 0 & \text{für } n>1 \end{cases}$$

folgt zunächst für $n=1$, dass $f(1)x(1)=1$, also $x(1)=1/f(1)$ ist (hier wird die Voraussetzung $f(1)\neq 0$ benötigt!). Nehmen wir nun an, wir hätten $x(1)$, $x(2)$, …, $x(n-1)$ bereits bestimmt, so kann $x(n)$ aus

$$0 = \sum_{t|n} f\left(\frac{n}{t}\right) x(t) = \sum_{\substack{t|n\\ t<n}} f\left(\frac{n}{t}\right) x(t) + f(1)\ x(n)$$

eindeutig bestimmt werden:

$$x(n) = -\frac{1}{f(1)} \sum_{\substack{t|n\\ t<n}} f\left(\frac{n}{t}\right) x(t).$$

Offenbar ist x wieder eine zahlentheoretische Funktion mit $x(1)\neq 0$. ∎

Beispiele. (*a*) Es sei I die durch $I(n) = 1$ für alle n definierte zahlentheoretische Funktion und f eine beliebige zahlentheoretische Funktion. Dann ist

$$(f * I)(n) = \sum_{t|n} f(t)\, I(n/t) = \sum_{t|n} f(t).$$

(*b*) Für $\chi_k(n) := n^k$ ist

$$(\chi_k * I)(n) = \sum_{t|n} t^k = \sigma_k(n),$$

also kurz $\chi_k * I = \sigma_k$.
(*c*) Wir zeigen, dass $\mu * I = e$. Für $n = 1$ ist offenbar $(\mu * I)(1) = \mu(1)I(1) = 1 \cdot 1 = 1 = e(1)$. Für $n > 1$ müssen wir zeigen, dass

$$(\mu * I)(n) \overset{\text{Def.}}{=} \underbrace{\sum_{t|n} \mu(t) = 0}_{\text{zu zeigen}} \overset{\text{Def.}}{=} e(n).$$

Sei $n = p_1^{a_1} \cdot \ldots \cdot p_k^{a_k}$ die Primfaktorzerlegung von n. In die Summe $\sum_{t|n} \mu(t)$ gehen nur Teiler der Gestalt $t = p_{e_1} \cdot \ldots \cdot p_{e_m}$ ein, wobei die p_{e_i} paarweise verschiedene Primzahlen aus der Primfaktorzerlegung von n sind (alle übrigen Summanden sind nach Definition der Möbius-Funktion gleich 0). Die Anzahl dieser Teiler mit m verschiedenen Primfaktoren ist gleich der Anzahl der Möglichkeiten, m aus k Elementen auszuwählen (ohne Berücksichtigung der Reihenfolge, ohne Wiederholungen), also gleich $\binom{k}{m}$.

Ist m gerade, so ist $\mu(t)$ gleich $+1$, sonst -1. Somit erhalten wir

$$\sum_{t|n} \mu(t) = 1 - \binom{k}{1} + \binom{k}{2} - \binom{k}{3} + \ldots \pm (-1)^k \binom{k}{k},$$

was nach dem binomischen Satz gleich $(1-1)^k = 0$ ist. ∎

Satz 4.5 (Möbiussche Umkehrformel) *Sei f eine zahlentheoretische Funktion und $F(n) := \sum_{t|n} f(t)$. Dann ist $f(n) = \sum_{t|n} \mu(t) F\left(\frac{n}{t}\right)$.*

Beweis. Es ist $F = f * I$, also $F * \mu = (f * I) * \mu = f * \underbrace{(I * \mu)}_{(c)} = f * e = f$. ∎

Als eine Anwendung leiten wir die Formel für die Eulersche Funktion auf anderem Wege her. Aus Satz 3.5 wissen wir, dass

$$n = \sum_{t|n} \varphi(t) \qquad \text{bzw.} \qquad \varphi * I = \chi_1$$

ist. Dirichlet-Multiplikation mit μ und Benutzung der Möbiusschen Umkehrformel liefern

$$\varphi = \chi_1 * \mu,$$

d.h.

$$\begin{aligned}\varphi(n) &= \sum_{t|n} \mu(t)\frac{n}{t} = n - \sum_i \frac{n}{p_i} + \sum_{i,j} \frac{n}{p_i p_j} - \dots \\ &= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\dots\left(1 - \frac{1}{p_k}\right).\end{aligned}$$

Ü30 Man zeige, dass für alle $n \in \mathbb{N}$

$$\sum_{t|n} \nu(t)\ \mu\left(\frac{n}{t}\right) = 1.$$

Ü31 Man zeige, dass für alle $n \in \mathbb{N}$

$$\sum_{t|n} \sigma(t)\ \mu\left(\frac{n}{t}\right) = n.$$

4.3 Multiplikative zahlentheoretische Funktionen

Eine zahlentheoretische Funktion f heißt *multiplikativ*, wenn für alle Paare $a, b \in \mathbb{N}$ mit $\mathrm{ggT}\,(a, b) = 1$ gilt $f(ab) = f(a)f(b)$. Wir haben bereits gezeigt, dass die Eulersche Funktion multiplikativ ist (Satz 3.3). Man sieht auch leicht, dass die Beispiele aus 4.1.1, 4.1.2, 4.1.3, 4.1.5 multiplikativ sind. Andererseits ist $\pi(n)$ offenbar nicht multiplikativ.

Ü32 Zeigen Sie diese Aussagen.

Satz 4.6 *Sind f und g multiplikative zahlentheoretische Funktionen, so ist auch ihr Dirichlet-Produkt $f * g$ multiplikativ.*

Beweis. Es sei $n = n_1 n_2$ mit $\mathrm{ggT}\,(n_1, n_2) = 1$. Dann ist

$$(f * g)(n) = (f * g)(n_1 n_2) = \sum_{t \mid n_1 n_2} f(t) g(n_1 n_2 / t).$$

Da $t \mid n_1 n_2$, kann t eindeutig in ein Produkt $t = t_1 \cdot t_2$ zerlegt werden, wobei $t_1 \mid n_1$ und $t_2 \mid n_2$. Hiermit erhalten wir

$$\begin{aligned}
(f * g)(n) &= \sum_{t_1 t_2 \mid n_1 n_2} f(t_1 t_2)\; g\left(\frac{n_1 n_2}{t_1 t_2}\right) \\
&= \sum_{\substack{t_1 \mid n_1 \\ t_2 \mid n_2}} f(t_1)\; f(t_2)\; g\left(\frac{n_1}{t_1}\right)\; g\left(\frac{n_2}{t_2}\right) \\
&= \left(\sum_{t_1 \mid n_1} f(t_1)\; g\left(\frac{n_1}{t_1}\right)\right) \left(\sum_{t_2 \mid n_2} f(t_2)\; g\left(\frac{n_2}{t_2}\right)\right) \\
&= (f * g)(n_1) \cdot (f * g)(n_2).
\end{aligned}$$

■

Als Anwendung wollen wir eine Formel zur Berechnung der verallgemeinerten Teilersumme σ_k aufstellen (vgl. Abschnitt 4.1.3). Die Funktionen I und χ_k sind offenbar multiplikativ. Somit ist auch die Funktion $\sigma_k = I * \chi_k$ multiplikativ. Mit der Primfaktorzerlegung $n = p_1^{a_1} \cdot \ldots \cdot p_k^{a_k}$ folgt daher

$$\sigma_k(n) = \sigma_k(p_1^{a_1}) \cdot \ldots \cdot \sigma_k(p_k^{a_k}).$$

Es verbleibt, die Werte $\sigma_k(p^a)$ für Primzahlen p zu berechnen. Dies geschieht mit der Summenformel für die geometrische Reihe:

$$\begin{aligned}
\sigma_k(p^\alpha) &= 1^k + p^k + p^{2k} + \ldots + p^{\alpha k} \\
&= \begin{cases} \frac{p^{k(\alpha+1)}-1}{p^k-1} & \text{für } k > 0, \\ \alpha + 1 & \text{für } k = 0. \end{cases}
\end{aligned}$$

Damit finden wir für $k = 0$

$$\sigma_0(n) = \nu(n) = (\alpha_1 + 1) \cdot \ldots \cdot (\alpha_e + 1)$$

sowie für $k > 0$

$$\sigma_k(n) = \left(\frac{p_1^{k(\alpha_1+1)} - 1}{p_1^k - 1}\right)\left(\frac{p_2^{k(\alpha_2+1)} - 1}{p_2^k - 1}\right)\cdots\left(\frac{p_e^{k(\alpha_e+1)} - 1}{p_e^k - 1}\right).$$

Ü33 Man zeige: Ist $\nu(n)$ ungerade, so ist n eine Quadratzahl.

Ü34 Man zeige: $\sigma_k * \mu = \chi_k$.

5 Pythagoräische Tripel

5.1 Das Problem

Die natürlichen Zahlen a, b, c, bilden ein *pythagoräisches Tripel* (a, b, c), wenn

$$a^2 + b^2 = c^2, \tag{21}$$

d.h. wenn a, b die Längen der Katheten und c die Länge der Hypotenuse eines rechtwinkligen Dreiecks bilden. Offenbar gibt es pythagoräische Tripel; so ist beispielsweise $3^2+4^2 = 5^2$ und $12^2+5^2 = 13^2$, und aus jedem Tripel mit $a^2 + b^2 = c^2$ kann man neue gewinnen: $n^2a^2 + n^2b^2 = n^2c^2$. Weniger offensichtlich ist, wie viele *teilerfremde* Tripel es gibt. Sind es ebenfalls unendlich viele?

Wir betten diese Frage in einen allgemeineren Kontext ein. Schreibt man (21) als

$$\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1,$$

so wird klar, dass obige Frage auf die Frage nach der Anzahl der Punkte mit *rationalen* Koordinaten (kurz: rationale Punkte) auf der Einheitskreislinie

$$\{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}$$

führt. Allgemeiner betrachtet man ein Polynom $P \in \mathbb{Z}[x, y]$ in zwei Veränderlichen mit ganzzahligen Koeffizienten und fragt nach rationalen Lösungen der Gleichung

$$P(x, y) = 0.$$

Man sieht sofort, dass nicht jede dieser Gleichungen rationale Lösungen hat, etwa $P(x, y) = x^2 - 2$ oder $P(x, y) = x^2 + y^2 - 3$. Für $n > 2$ findet man für die Gleichung

$$x^n + y^n = 1$$

schnell die Lösungen

$$\begin{cases} (1, 0) \text{ und } (0, 1) & \text{falls } n \text{ ungerade} \\ (\pm 1, 0) \text{ und } (0, \pm 1) & \text{falls } n \text{ gerade,} \end{cases}$$

und eines der populärsten Resultate der Mathematik sagt, dass es keine weiteren rationalen Lösungen gibt:

Satz 5.1 (Fermatsche Vermutung, Beweis von Wiles 1995) *Für $n > 2$ hat die Gleichung*

$$x^n + y^n = z^n$$

keine ganzzahligen Lösungen mit $xyz \neq 0$.

5.2 Rationale Punkte auf Geraden und Kegelschnitten

Wir betrachten zunächst rationale Punkte auf Geraden. O.E.d.A. sei

$$P(x, y) = ex + fy + h \tag{22}$$

mit $e, f, h \in \mathbb{Z}$ und $e \neq 0$. Man sieht sofort, dass die rationalen Lösungen der Gleichung $P(x, y) = 0$ wie folgt gegeben sind:

$$\{(x, y) \in \mathbb{Q} : x = -\frac{ft + h}{e},\ y = t \text{ mit } t \in \mathbb{Q}\}.$$

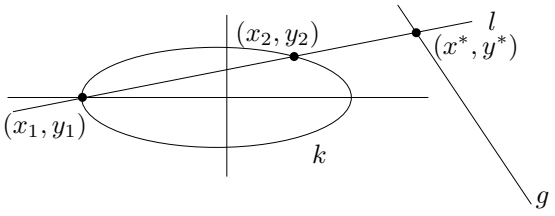
Es *gibt* also rationale Lösungen der Gleichung $P(x, y) = 0$, und es gibt *unendlich viele* davon.

Wir betrachten nun Kegelschnitte. O.E.d.A. sei

$$P(x, y) = ax^2 + bxy + cy^2 + d \tag{23}$$

mit $a, b, c, d \in \mathbb{Z}$ und $a \neq 0$. Wir haben bereits gesehen, dass auf der Kurve $P(x, y) = 0$ nicht unbedingt rationale Punkte liegen müssen und nehmen daher im Weiteren an, dass es wenigstens einen rationalen Punkt (x_1, y_1) mit $P(x_1, y_1) = 0$ gibt.

Neben der Kurve $k := \{(x, y) \in \mathbb{R} : P(x, y) = 0\}$ betrachten wir eine Gerade $g = \{(x, y) \in \mathbb{R} : ex + fy + h = 0\}$ mit e, f, h wie in (22). Wir haben gesehen, dass auf g unendlich viele rationale Punkte liegen. Sei (x^*, y^*) ein solcher Punkt. Der Schnittpunkt der Geraden l durch (x_1, y_1) und (x^*, y^*) mit k ist dann ebenfalls ein Punkt mit rationalen Koordinaten.



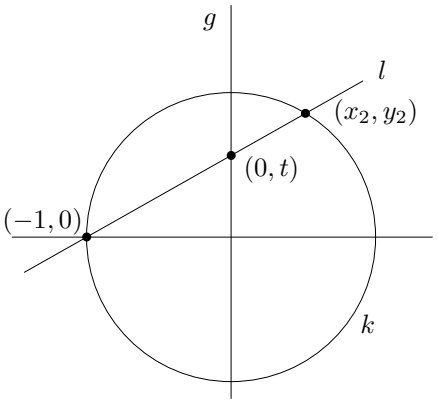
Das ist leicht einzusehen: l verläuft durch die rationalen Punkte (x_1, y_1) und (x^*, y^*) und hat daher einen rationalen Anstieg. Stellt man die Geradengleichung von l nach einer der Variablen um und setzt dies in die Gleichung für k ein, erhält man ein Polynom 2. Grades mit *rationalen* Koeffizienten, etwa ein Polynom in x. Dieses Polynom hat zwei Nullstellen x_1 (bekannt) und x_2, wobei x_1 nach Voraussetzung rational ist. Nach Vieta ist dann auch x_2 (und folglich y_2) rational.

Da auf g unendlich viele rationale Punkte liegen, findet man auf diese Weise unendlich viele rationale Punkte auf k.

Zurück zu unserem Ausgangsproblem, den pythagoräischen Tripeln. Wir führen obige Konstruktion durch mit

$$\begin{aligned} k &= \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}, & (x_1, y_1) &= (-1, 0), \\ g &= \{(x, y) \in \mathbb{R}^2 : x = 0\}, & (x^*, y^*) &= (0, t) \end{aligned}$$

mit $t \in \mathbb{Q}$.



Eine einfache Rechnung liefert für l die Geradengleichung $y = t(x + 1)$ sowie die Schnittpunkt-Koordinaten

$$(x_2, y_2) = \left(\frac{1 - t^2}{1 + t^2}, \frac{2t}{1 + t^2} \right).$$

Wählen wir speziell $t = \frac{n}{m}$ mit $m, n \in \mathbb{N}$ und $m > n$, so wird

$$(x_2, y_2) = \left(\frac{1 - \left(\frac{n}{m}\right)^2}{1 + \left(\frac{n}{m}\right)^2}, \frac{2\frac{n}{m}}{1 + \left(\frac{n}{m}\right)^2} \right) = \left(\frac{m^2 - n^2}{m^2 + n^2}, \frac{2mn}{m^2 + n^2} \right),$$

und wir erhalten eine unendliche Familie pythagoräischer Tripel

$$a = m^2 - n^2, \quad b = 2mn, \quad c = m^2 + n^2.$$