

Einführung in die Zahlentheorie

Peter Müller

12. März 2012

Inhaltsverzeichnis

1	Einführung	2
2	Teilbarkeit, Primfaktorzerlegung	2
3	Primzahlverteilung	4
4	Kongruenzen und Restklassenringe	7
5	Sätze von Fermat, Euler, Wilson	10
6	Polynome	11
7	Zyklische Gruppen und Ordnungen	13
8	Primitivwurzeln und Einheitengruppen der Restklassenringe	14
9	Quadratische Reste und Gaußsches Reziprozitätsgesetz	17
10	Primzahltests	24
11	Dirichletscher Approximationssatz	26
12	Quadratsummen	28
13	Pythagoräische Tripel und Fermat Gleichung	32
14	Pellsche Gleichungen	33
15	Quadratische Kurven	35

1 Einführung

Die elementare Zahlentheorie untersucht die multiplikativen Eigenschaften der natürlichen Zahlen $\mathbb{N} = \{1, 2, 3, \dots\}$ und verschiedene ringtheoretische Eigenschaften des Rings der ganzen Zahlen $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$. Die Beweismethoden (in dieser Vorlesung) sind meist direkt, daneben kommen als Hilfsmittel gelegentlich endliche Primkörper, Polynome und einfache gruppentheoretische Argumente hinzu.

Ein typisches Phänomen der elementaren Zahlentheorie sind die Schwierigkeiten, wenn Addition auf Multiplikation trifft. So sind etwa die Quadratzahlen ein multiplikatives Objekt. Wenn man nun fragt, wie gut man natürliche Zahlen als Summe von wenigen Quadratzahlen (inklusive 0) schreiben kann, so stößt man schnell auf schwierige Probleme. Diese Frage werden wir in der Vorlesung klären; Lagrange bewies, dass jede natürliche Zahl eine Summe von 4 Quadratzahlen ist (siehe Abschnitt 12).

Nicht viel schlimmer auf den ersten Blick sieht die Frage aus, wann eine n -te Potenz eine Summe von zwei n -ten Potenzen sein kann, d.h. wann eine Gleichung $X^n + Y^n = Z^n$ eine Lösung $X, Y, Z \in \mathbb{N}$ hat. Für $n = 2$ findet man schnell Lösungen, etwa $3^2 + 4^2 = 5^2$, und es ist auch nicht schwer, alle Lösungen anzugeben (siehe Abschnitt 15). Die Fermat-Vermutung, dass es für $n \geq 3$ keine Lösungen gibt, war viele 100 Jahre offen, und wurde erst 1995 unter Einsatz sehr tiefer und schwieriger Methoden gelöst!

Die Zahlentheorie wurde lange Zeit vor allem wegen ihrer Schönheit, der schwierigen obwohl einfach aussehenden Probleme, und ihrer zahlreichen Querverbindungen zu anderen Gebieten der Mathematik geschätzt. In neuerer Zeit erfährt die Zahlentheorie auch zahlreiche praktische Anwendungen, vor allem in der Kryptographie. Früher eher exotisch aussehende Probleme, wie die Suche nach großen Primzahlen oder Methoden, große Zahlen zu faktorisieren, haben heute eine ganz praktische Bedeutung.

2 Teilbarkeit, Primfaktorzerlegung

Definition 2.1. Es seien a, b ganze Zahlen mit $b \neq 0$. Man sagt, b teilt a , falls es eine ganze Zahl c gibt mit $a = bc$. Man schreibt dann $b \mid a$. Ist b kein Teiler von a , dann schreiben wir $b \nmid a$.

Im Zusammenhang mit Teilbarkeit ist die Division mit Rest ein wichtiges theoretisches und praktisches Hilfsmittel:

Satz 2.2. Es seien a, b ganze Zahlen mit $b \neq 0$. Dann gibt es ganze Zahlen q, r mit $a = bq + r$ und $0 \leq r < |b|$. Hierbei sind q, r eindeutig.

Beweis. Indem wir eventuell b durch $-b$ ersetzen, dürfen wir $b > 0$ annehmen. Es sei q die größte ganze Zahl mit $bq \leq a$. Setze $r = a - bq$. Dann gilt $b(q+1) > a$, also $0 \leq r = a - bq < b$, und die Existenz von q, r folgt.

Zum Beweis der Eindeutigkeit nehmen wir an, es gäbe ein weiteres solches Paar q', r' , also $a = bq' + r'$ mit $0 \leq r' < b$. Subtraktion liefert $(q - q')b = r - r'$. Ist $q = q'$, dann gilt auch $r = r'$, und wir sind fertig. Sei also $q - q' \neq 0$. Wir dürfen $q > q'$ annehmen. Aus $q - q' \geq 1$ folgt dann $r \geq r - r' = (q - q')b \geq b$, im Widerspruch zu $r < b$. \square

Definition 2.3. Es seien $a, b \in \mathbb{Z}$ nicht beide 0. Der *größte gemeinsame Teiler* ist die größte natürliche Zahl d , die a und b teilt. Wir schreiben $d = \text{ggT}(a, b)$. Ist $d = 1$, dann nennen wir a und b *teilerfremd*.

Lemma 2.4. Es seien $a, b \in \mathbb{Z}$ mit $b \neq 0$, und $a = bq + r$ eine Division mit Rest. Dann gilt $\text{ggT}(a, b) = \text{ggT}(b, r)$.

Beweis. Sei $d = \text{ggT}(a, b)$ und $d' = \text{ggT}(b, r)$. Aus $r = a - bq$ und $d \mid a, d \mid b$ folgt $d \mid r$, also d teilt b und r . Aber d' ist der größte gemeinsame Teiler von b und r , also $d \leq d'$. Andererseits ist d' ein Teiler von b und r , also auch von $a = bq + r$. Das ergibt $d' \leq d$, also $d = d'$. \square

Eine wichtige Folgerung ist das Lemma von Bézout:

Lemma 2.5. Es seien $a, b \in \mathbb{Z}$ nicht beide 0. Dann gibt es $s, t \in \mathbb{Z}$ mit $\text{ggT}(a, b) = sa + tb$.

Beweis. Wegen $\text{ggT}(a, b) = \text{ggT}(-a, b) = \text{ggT}(a, -b) = \text{ggT}(-a, -b)$ dürfen wir $a \geq b \geq 0$ annehmen. Wir beweisen die Aussage durch vollständige Induktion über b . Für $b = 0$ gilt natürlich die Aussage wegen $\text{ggT}(a, b) = \text{ggT}(a, 0) = a = 1a + 0b$.

Sei also $b > 0$. Sei wieder $a = bq + r$ eine Division mit Rest. Wegen $r < b$ gibt es nach Induktionsannahme $s', t' \in \mathbb{Z}$ mit $\text{gcd}(b, r) = s'b + t'r$. Zusammen mit dem vorigen Lemma erhalten wir

$$\text{gcd}(a, b) = \text{gcd}(b, r) = s'b + t'r = s'b + t'(a - bq) = t'a + (s' - t'q)b,$$

und die Behauptung folgt mit $s = t', t = s' - t'q$. \square

Aus dem Lemma erhalten wir eine weitere wichtige Eigenschaft des größten gemeinsamen Teilers:

Lemma 2.6. Es seien $a, b \in \mathbb{Z}$ nicht beide 0. Ist $t \in \mathbb{N}$ ein Teiler von a und b , dann gilt $t \mid \text{ggT}(a, b)$.

Beweis. Klar! \square

Bemerkung 2.7. Lemma 2.4 liefert eine schnelle Methode, den größten gemeinsamen Teiler von a und b zu berechnen, ohne einen einzigen Teiler von a und b zu bestimmen! Der Beweis des Lemmas von Bézout gibt eine konstruktive und sehr schnelle Methode, die Zahlen s und t berechnen.

Siehe auch die Übungsaufgaben zum Euklidischen Algorithmus.

Eine kleine Modifikation erlaubt es übrigens, $\text{ggT}(a, b)$ zu bestimmen, indem man lediglich Subtraktionen und Divisionen durch 2 durchführt. Es gilt nämlich $\text{ggT}(a, b) = \text{ggT}(b, a - b)$. Man setzt wieder $a > b$ voraus, und macht nun eine vollständige Induktion über $a + b$. Das Verfahren kann man beschleunigen, denn der größte gemeinsame 2-Anteil von a und b lässt sich, vor allem wenn a und b in Binärdarstellung auf dem Computer gegeben sind, schnell bestimmen. Man kann also a und b als ungerade voraussetzen, und die gerade Zahl $a - b$ durch die größte 2-Potenz dividieren, usw.

Wir kommen nun zum wichtigen Begriff der Primzahl:

Definition 2.8. Eine natürliche Zahl $p > 1$ heißt *Primzahl*, wenn 1 und p die einzigen positiven Teiler von p sind. Die Menge der Primzahlen bezeichnen wir mit \mathbb{P} .

Primzahlen treten auf natürliche Weise bei der multiplikativen Zerlegung natürlicher Zahlen auf. Ist nämlich $2 \leq a \in \mathbb{N}$, und $p > 1$ der kleinste positive Teiler von a , dann ist p eine Primzahl, denn jeder Teiler von p ist ja auch ein Teiler von a .

Man bekommt also $a = pa'$ für eine Primzahl p , und wegen $p > 1$ ist $a' < a$. Ist $a' > 1$, dann kann man wieder a' als Produkt einer Primzahl und einer Zahl $< a'$ schreiben. Dieses Verfahren setzt man fort, und erhält nach endlich vielen Schritten eine Darstellung von a als Produkt von Primzahlen.

Es ist keineswegs klar, dass eine solche Produktdarstellung (bis auf Reihenfolge der Primfaktoren) eindeutig ist, siehe die Übungsaufgaben und die Beispiele aus der Algebra-Vorlesung, wo das in zu \mathbb{Z} sehr ähnlichen Ringen schief geht. Zum Beweis der eindeutigen Primfaktorzerlegung benötigen wir die folgende wichtige Eigenschaft von Primzahlen.

Satz 2.9. Die Primzahl p teile das Produkt ab der ganzen Zahlen a und b . Dann teilt p einen der Faktoren a oder b .

Beweis. Sei $d = \text{ggT}(a, p)$. Da p eine Primzahl ist gilt $d = 1$ oder $d = p$. Falls $d = p$, dann ist p ein Teiler von a , und wir sind fertig. Sei also $d = 1$. Nach dem Lemma von Bézout gibt es $s, t \in \mathbb{Z}$ mit $1 = sa + tp$. Multiplikation mit b gibt $b = sab + tbp$. Beide Summanden der rechten Seite sind durch p teilbar, also p teilt b , was zu zeigen war. \square

Bemerkung 2.10. Der Satz gilt natürlich auch für mehr als zwei Faktoren. Ist nämlich p ein Teiler von $a_1 a_2 \dots a_k$, dann ist nach dem Satz p ein Teiler von a_1 oder von $a_2 \dots a_k$. Im ersten Fall sind wir fertig, und im zweiten Fall spalten wir a_2 ab usw.

Damit kommen wir zum Satz über die Eindeutigkeit der Primfaktorzerlegung:

Satz 2.11. Jede natürliche Zahl $n \geq 2$ hat eine (bis auf Reihenfolge der Faktoren) eindeutige Zerlegung als Produkt von Primzahlen.

Wir beweisen die Aussage durch vollständige Induktion über n . Die Aussage ist klar für die Primzahl $n = 2$. Sei nun $n > 2$, und $n = p_1 p_2 \dots p_k = q_1 q_2 \dots q_\ell$ zwei Zerlegungen in Primzahlen. Nach obigem Satz teilt p_k einen der Faktoren q_j . Nach Umbenennung sei also p_k ein Teiler von q_ℓ . Da q_ℓ eine Primzahl ist, folgt $p_k = q_\ell$. Schreibe $n = p_k n'$. Dann gilt entweder $n' = 1$ (und wir sind fertig), oder $p_1 p_2 \dots p_{k-1} = n' = q_1 q_2 \dots q_{\ell-1} < n$. Nach Induktionsannahme stimmen die Faktoren $p_1 p_2, \dots, p_{k-1}$ bis auf Reihenfolge mit den Primfaktoren $q_1, q_2, \dots, q_{\ell-1}$ überein.

3 Primzahlverteilung

Beim Umgang mit Faktorisierungen und Primzahlen taucht schnell die Frage auf, wie viele Primzahlen es eigentlich gibt. Eine Antwort darauf gibt der Satz von Euklid:

Satz 3.1 (Euklid). *Es gibt unendlich viele Primzahlen.*

Beweis (von Euklid, über 2000 Jahre alt!) Es seien p_1, p_2, \dots, p_r Primzahlen. Betrachte $P = p_1 p_2 \dots p_r + 1$. Dann ist keine der Primzahlen p_i ein Teiler von P . Denn p_i teilt $P - 1$, und wäre dann auch Teiler von $P - (P - 1) = 1$. Wegen $P > 1$ hat aber P einen Primteiler p . Dieser kommt also unter p_1, p_2, \dots, p_r nicht vor.

Jede endliche Menge von Primzahlen lässt sich also vergrößern, daher gibt es unendlich viele Primzahlen. \square

Zu diesem Beweis von Euklid gibt es zahlreiche Varianten. Man kann auch die Zahl $n! + 1$ betrachten. Offenbar hat $n! + 1$ keinen Primteiler p mit $p \leq n$. Zu jeder natürlichen Zahl n gibt es also eine Primzahl $p > n$.

Beweise dieser Art zeigen wenig über die tatsächliche Dichte von Primzahlen. Sei $\pi(n)$ die Anzahl der Primzahlen $\leq n$. Etwas näher kommt schon der folgende Satz, der zeigt, dass $\frac{n}{\log n}$ eine gute Approximation von $\pi(n)$ ist:

Satz 3.2 (Tschebyschow, 1851). *Für alle hinreichend große $n \in \mathbb{N}$ gilt*

$$0,92929 \frac{n}{\log n} \leq \pi(n) \leq 1,1056 \frac{n}{\log n}.$$

Beweise für etwas schwächere Formen dieses Satzes findet man in fast jedem Lehrbuch zur Zahlentheorie. Sie beruhen auf Primfaktorzerlegungen des Binomialkoeffizienten $\binom{2m}{m}$. Eine wenig bekannte alternative Methode stammt von Nair (1982), die wir im folgenden illustrieren.

Satz 3.3. *Für alle hinreichend große n gilt*

$$\pi(n) \geq 0,69 \frac{n}{\log n}.$$

Beweis (Nair). Für $n \in \mathbb{N}$ seien a_1, a_2, \dots, a_n ganze Zahlen mit

$$S = a_1 + \frac{a_2}{2} + \frac{a_3}{3} + \dots + \frac{a_n}{n} > 0.$$

Für alle Primzahlen $p \leq n$ sei p^{e_p} die größte Potenz, die eine der Zahlen $1, 2, \dots, n$ teilt. Setze $P = \prod_{p \leq n} p^{e_p}$. (P ist das kleinste gemeinsame Vielfache der Zahlen von 1 bis n .) Für $1 \leq k \leq n$ ist also $P \frac{1}{k}$ ganzzahlig. Insbesondere ist PS ganzzahlig und positiv, also $PS \geq 1$ und damit $P \geq \frac{1}{S}$. Andererseits gilt natürlich $p^{e_p} \leq n$. Es gibt $\pi(n)$ Primzahlen $p \leq n$. Damit erhalten wir

$$P = \prod_{p \leq n} p^{e_p} \leq n^{\pi(n)},$$

also

$$\pi(n) \geq \frac{\log P}{\log n} \geq \frac{\log \frac{1}{S}}{\log n}.$$

Um eine gute untere Abschätzung für $\pi(n)$ zu finden, braucht man also eine Wahl der a_k , so dass $S > 0$ möglichst klein wird.

Für $n = 2m + 1$ setze

$$a_k = \begin{cases} 0 & \text{falls } 1 \leq k \leq m \\ (-1)^{m+1+k} \binom{m}{k-m-1} & \text{falls } m+1 \leq k \leq 2m+1 \end{cases}$$

Wir berechnen

$$\begin{aligned} S &= \sum_{k=0}^{2m+1} \frac{a_k}{k} \\ &= \sum_{k=m+1}^{2m+1} (-1)^{m+1+k} \binom{m}{k-m-1} \frac{1}{k} \\ &= \sum_{k=0}^m (-1)^k \binom{m}{k} \frac{1}{k+m+1} \\ &= \sum_{k=0}^m \left((-1)^k \binom{m}{k} \int_0^1 x^{k+m} dx \right) \\ &= \int_0^1 \left(x^m \sum_{k=0}^m \binom{m}{k} (-x)^k \right) dx \\ &= \int_0^1 x^m (1-x)^m dx. \end{aligned}$$

Für $0 < x < 1$ gilt $0 < x(1-x) \leq \frac{1}{4}$, also

$$0 < \int_0^1 x^m (1-x)^m dx \leq \frac{1}{4^m},$$

und damit $0 < S \leq \frac{1}{4^m}$. Wir für ungerade n folgt

$$\pi(n) \geq \frac{\log 4^m}{\log 2m+1} = \log 2 \frac{2m}{\log(2m+1)} = \log 2 \frac{n-1}{\log n}.$$

Ist $n > 2$ gerade, dann ist $n-1$ ungerade, und wegen $\pi(n) = \pi(n-1)$ liefert obige Ungleichung

$$\pi(n) \geq \pi(n-1) \geq \log 2 \frac{n-2}{\log(n-1)}.$$

Aus

$$\lim_{n \rightarrow \infty} \frac{(n-1)/\log n}{n/\log n} = 1 = \lim_{n \rightarrow \infty} \frac{(n-2)/\log(n-1)}{n/\log n}$$

und $\log 2 > 0$, 69 folgt die gewünschte Aussage. \square

Wesentlich tiefer liegt der so genannte Primzahlsatz, der gegen Ende des 19. Jahrhunderts mit funktionentheoretischen Mitteln und erst Mitte des 20. Jahrhunderts mit elementaren (aber extrem komplizierten) Methoden bewiesen wurde.

Satz 3.4 (Primzahlsatz). *Es gilt*

$$\lim_{n \rightarrow \infty} \frac{\pi(n)}{n / \log n} = 1.$$

Obwohl Gauß den Primzahlsatz noch nicht beweisen konnte, so bemerkte er doch aufgrund empirischer Daten (und heuristischer Überlegungen?), dass $\pi(n)$ noch besser durch den Integrallogarithmus $Li(n) = \int_2^n \frac{dx}{\log x}$ als durch $\frac{n}{\log n}$ approximiert wird.

Eine der wichtigsten Vermutungen der Mathematik (für die es übrigens ein Preisgeld von 1.000.000 Dollar gibt) ist die sogenannte Riemannsche Vermutung über die Nullstellen der Riemannschen Zetafunktion. Diese Vermutung ist äquivalent zu folgender Verschärfung des Primzahlsatzes: Es gibt eine Konstante C mit $|\pi(n) - Li(n)| \leq C \sqrt{n} \log n$ für alle $n \geq 2$.

4 Kongruenzen und Restklassenringe

Wir beginnen mit einem einführenden Beispiel: Hat das Polynom $f(X) = 11X^{21} - 117X^8 + 32X - 3^{100}$ eine ganzzahlige Nullstelle? Offensichtlich will man diese Frage nicht dadurch lösen, indem man hinreichend gute Approximationen der 21 komplexen Nullstellen berechnet. Ist $f(a) = 0$ für $a \in \mathbb{Z}$, dann ist offenbar $a|3^{100}$. Es gibt also 202 potenzielle Möglichkeiten für a , die man nicht alle ausprobieren möchte. (In besseren Fällen, wenn der Absolutterm des Polynoms nicht zu viele Teiler hat, ist das allerdings meist das Mittel der Wahl.)

Wenn man allerdings genau hinsieht, erkennt man das folgende: Ist a gerade, dann ist jeder Summand von $f(a)$ außer dem letzten gerade, also $f(a)$ ungerade und daher insbesondere $f(a) \neq 0$. Ist hingegen a ungerade, dann hat $f(a)$ genau 3 ungerade Summanden, d.h. $f(a)$ ist wieder ungerade und somit ungleich 0.

Wir sehen also, dass wir durch eine starke Vergrößerung der ganzen Zahlen, wo es nur wichtig war, ob sie gerade oder ungerade sind, eine kompliziert aussehende Frage beantworten konnten.

Uns interessierte also nur der Rest, den eine Zahl bei Division durch 2 lässt. Das kann man natürlich auch für andere Zahlen als 2 machen, und führt direkt zu Kongruenzen.

Definition 4.1. Es seien a, b, n ganze Zahlen mit $n \neq 0$. Man sagt, dass a kongruent zu b modulo n ist, wenn $n|a - b$. Statt $n|a - b$ benutzen wir die flexiblere Schreibweise $a \equiv b \pmod{n}$.

Die Kongruenz modulo n ist eine Äquivalenzrelation. Für die Transitivität etwa beachte man $(a - b) + (b - c) = a - c$. Die Äquivalenzklasse von a besteht aus allen $u \in \mathbb{Z}$ mit $n|a - u$, also aus den Zahlen $a + kn$ mit $k \in \mathbb{Z}$. Diese Menge schreiben wir auch als \bar{a} oder $a + n\mathbb{Z}$. Man nennt \bar{a} auch die *Kongruenzklasse (oder auch Restklasse) von a modulo n* .

Für $n = 2$ ist $\bar{0}$ die Menge der geraden Zahlen, und $\bar{1}$ die Menge der ungeraden Zahlen.

Die folgenden Eigenschaften sind wichtig für das Rechnen mit Kongruenzen.

Lemma 4.2. *Es sei $n, k \in \mathbb{N}$, und $a, a', b, b' \in \mathbb{Z}$ mit $a \equiv a' \pmod{n}$ und $b \equiv b' \pmod{n}$. Dann gilt*

$$(a) \quad a \pm b \equiv a' \pm b' \pmod{n}.$$

$$(b) \quad ab \equiv a'b' \pmod{n}.$$

$$(c) \quad a^k \equiv a'^k \pmod{n}.$$

Beweis. Nach Voraussetzung gilt $a = a' + un$ und $b = b' + vn$ mit $u, v \in \mathbb{Z}$. Aus $a + b = a' + b' + (u + v)n$ folgt (a), und (b) folgt aus $ab = (a' + un)(b' + vn) = a'b' + (a'v + ub' + uvn)n$. Mehrfache Anwendung von (b) mit $b = a$, $b' = a'$ ergibt (c). \square

Für $a \in \mathbb{Z}$ sei $a = qn + r$ eine Division durch n mit Rest r . Dann gilt $a \equiv r \pmod{n}$. Ferner ist $r \not\equiv r' \pmod{n}$, falls $0 \leq r, r' \leq n - 1$ und $r \neq r'$. Daher ist z.B. $\{0, 1, 2, \dots, n - 1\}$ ein Vertretersystem der Restklassen von \mathbb{Z} modulo n . Die Menge der Restklassen modulo n bezeichnet man mit $\mathbb{Z}/n\mathbb{Z}$. Wir transportieren die Ringstruktur von \mathbb{Z} nach $\mathbb{Z}/n\mathbb{Z}$.

Satz 4.3. Sei $2 \leq n \in \mathbb{N}$. Dann wird durch $\bar{a} + \bar{b} := \overline{a + b}$, $\bar{a}\bar{b} := \overline{ab}$ eine wohldefinierte Addition und Multiplikation auf $\mathbb{Z}/n\mathbb{Z}$ eingeführt, welche $\mathbb{Z}/n\mathbb{Z}$ zu einem Ring macht.

Beweis. Die Wohldefiniertheit der Addition und Multiplikation folgt aus Lemma 4.2. Die Ringaxiome von \mathbb{Z} übertragen sich direkt auf $\mathbb{Z}/n\mathbb{Z}$, da die Abbildung $\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$, $a \mapsto \bar{a}$ per definitionem additiv und multiplikativ ist. Wir haben $n \geq 2$ vorausgesetzt, da für $n = 1$ der degenerierte Fall $\bar{0} = \bar{1}$ auftritt. Üblicherweise fordert man in einem Ring, dass das Nullelement verschieden vom Einselement ist. \square

Die Menge der multiplikativ invertierbaren Elemente $\mathbb{Z}/n\mathbb{Z}$ bildet eine Gruppe (warum?). Wir bezeichnen diese Gruppe mit $(\mathbb{Z}/n\mathbb{Z})^*$, und nennen sie die *Einheitengruppe* von $\mathbb{Z}/n\mathbb{Z}$. Beachte, dass $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^*$ gleichbedeutend mit der Lösbarkeit der Kongruenz $ax \equiv 1 \pmod{n}$ ist. Eine Antwort darauf, wann das geht, liefert der folgende Satz.

Satz 4.4. Sei $n \in \mathbb{N}$ und $a \in \mathbb{Z}$. Dann hat $ax \equiv 1 \pmod{n}$ genau dann eine Lösung $x \in \mathbb{Z}$, wenn a und n teilerfremd sind.

Beweis. Es sei $ax \equiv 1 \pmod{n}$, also $ax = 1 + un$ mit $u \in \mathbb{Z}$. Wir sehen $\text{ggT}(a, n) | 1$, also $\text{ggT}(a, n) = 1$.

Sei nun $\text{ggT}(a, n) = 1$. Nach dem Lemma von Bézout gibt es $x, t \in \mathbb{Z}$ mit $ax + nt = 1$, also $ax \equiv 1 \pmod{n}$. \square

Die Größe der Einheitengruppe $(\mathbb{Z}/n\mathbb{Z})^*$ ist eine wichtige zahlentheoretische Funktion von n .

Definition 4.5. Die *Eulersche φ -Funktion* ist folgendermaßen definiert: Für $n \in \mathbb{N}$ ist $\varphi(n)$ die Anzahl der natürlichen Zahlen von 1 bis n , die teilerfremd zu n sind. Nach dem vorherigen Satz ist also $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$.

Für $n \geq 2$ ist offenbar $\varphi(n) \leq n - 1$, mit Gleichheit genau dann, wenn alle Zahlen $1, 2, \dots, n - 1$ zu n teilerfremd sind. Das ist sowohl äquivalent dazu, dass jedes Element $\bar{0} \neq \bar{a} \in \mathbb{Z}/n\mathbb{Z}$ multiplikativ invertierbar ist, als auch äquivalent dazu, dass n eine Primzahl ist. Damit erhalten wir den wichtigen Satz.

Satz 4.6. Sei $2 \leq n \in \mathbb{N}$. Dann ist $\mathbb{Z}/n\mathbb{Z}$ genau dann ein Körper, wenn n eine Primzahl ist.

Eine gelegentlich auftretende Situation ist die, dass man ein System von Kongruenzen $x \equiv a_i \pmod{n_i}$, $i = 1, 2, \dots, r$, lösen möchte. Das geht natürlich nicht ohne einschränkende Voraussetzungen an die a_i und n_i . Ist etwa d ein gemeinsamer Teiler von n_i und n_j , und x eine Lösung, dann sind $x - a_i$ und $x - a_j$ durch d teilbar, eine notwendige Bedingung für Lösbarkeit ist also $a_i \equiv a_j \pmod{\text{ggT}(n_i, n_j)}$. Ein wichtiger Fall ist der, in dem die n_i paarweise teilerfremd sind. Der folgende Satz zeigt dann, dass das System der Kongruenzen lösbar ist.

Satz 4.7 (Chinesischer Restsatz). *Es seien $n_1, n_2, \dots, n_r \in \mathbb{N}$ paarweise teilerfremd, und $a_1, a_2, \dots, a_r \in \mathbb{Z}$. Dann gibt es genau eine ganze Zahl $0 \leq x < n_1 n_2 \dots n_r$ mit $x \equiv a_i \pmod{n_i}$ für alle $i = 1, 2, \dots, r$.*

Beweis. Wir zeigen zunächst die Existenz von x . Sei $N = n_1 n_2 \dots n_r$. Da die n_i paarweise teilerfremd sind, gilt das folgende: n_i ist teilerfremd zu N/n_i , und n_i teilt N/n_j für $j \neq i$. Für jedes i gibt es nach Bézout eine ganzzahlige Relation $r_i n_i + s_i \frac{N}{n_i} = 1$. Setze $x = \sum_j a_j s_j \frac{N}{n_j}$. Wir betrachten x modulo n_i . Beachte, dass die Summanden in x für $j \neq i$ durch n_i teilbar sind, also $x \equiv a_i s_i \frac{N}{n_i} \pmod{n_i}$. Aber $s_i \frac{N}{n_i} = 1 - r_i n_i \equiv 1 \pmod{n_i}$, also $x \equiv a_i \pmod{n_i}$.

Mit x ist auch jedes Element in $x + N\mathbb{Z}$ eine Lösung des Kongruenzsystems, insbesondere gibt es auch eine Lösung x mit $0 \leq x < N$.

Wir müssen noch die Eindeutigkeit zeigen: Seien $0 \leq x, x' < N$ zwei Lösungen. Dann ist $n_i | x - x'$ für alle i . Da die n_i paarweise teilerfremd sind, ist $x - x'$ auch durch das Produkt N dieser n_i teilbar. Aber dann gilt $x = x'$ oder $|x - x'| \geq N$, im Widerspruch zu $0 \leq x, x' < N$. \square

Der angegebene Beweis liefert, mittels des Euklidischen Algorithmus, auch eine praktische Methode zur Bestimmung von x . Man kann die Existenz von x auch eleganter zeigen. Der Beweis ist zwar nicht konstruktiv, zeigt aber ein ringtheoretisch wichtiges Konzept. Vorher benötigen wir ein Lemma. Eine additive und multiplikative Abbildung $\phi : R \rightarrow S$ zwischen Ringen mit $\phi(1_R) = 1_S$ heißt *Ringhomomorphismus*.

Zum Beispiel ist die schon früher betrachtete Abbildung $\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$, $a \mapsto \bar{a} = a + n\mathbb{Z}$ ein Ringhomomorphismus.

Lemma 4.8. *Sei $m > 1$ ein Teiler von n . Dann gibt es genau einen Ringhomomorphismus $\mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$. Dieser Ringhomomorphismus ist surjektiv.*

Beweis. Für $a \in \mathbb{Z}$ setze $\phi(a + n\mathbb{Z}) := a + m\mathbb{Z}$. Dabei ist ϕ wohldefiniert, denn falls $a \equiv a' \pmod{n}$, dann gilt erst recht $a \equiv a' \pmod{m}$. Die Additivität und Multiplikativität folgt aus der Ringstruktur der Restklassenringe, und die 1 aus $\mathbb{Z}/n\mathbb{Z}$ wird auf die 1 von $\mathbb{Z}/m\mathbb{Z}$ abgebildet. Die Surjektivität ist klar, da $1 + m\mathbb{Z}$ die additive Gruppe von $\mathbb{Z}/m\mathbb{Z}$ erzeugt. \square

Zum alternativen Beweis des Chinesischen Restsatz betrachte man die Ringhomomorphismen $\mathbb{Z}/N\mathbb{Z} \rightarrow \mathbb{Z}/n_i\mathbb{Z}$ aus dem Lemma, und definiert eine Abbildung

$$\phi : \mathbb{Z}/N\mathbb{Z} \rightarrow \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \dots \times \mathbb{Z}/n_r\mathbb{Z}$$

durch

$$x + N\mathbb{Z} \mapsto (x + n_1\mathbb{Z}, x + n_2\mathbb{Z}, \dots, x + n_r\mathbb{Z}).$$

Diese Abbildung ist injektiv: Sei etwa $\phi(x + N\mathbb{Z}) = 0$. Dann ist $x \equiv 0 \pmod{n_i}$ für alle i , also $x \equiv 0 \pmod{N}$, d.h. $\bar{x} = 0$.

ϕ ist eine injektive Abbildung zwischen zwei Mengen gleicher Mächtigkeit, daher ist ϕ auch surjektiv. Die Surjektivität ist aber gerade die Existenzaussage im Chinesischen Restsatz, nur etwas anders formuliert.

Man verifiziert sofort, dass ϕ sogar ein Homomorphismus von Ringen ist. Genauer gilt:

Satz 4.9. *Es seien n_1, n_2, \dots, n_r paarweise teilerfremde natürliche Zahlen > 1 . Sei n das Produkt dieser Zahlen. Dann sind die Ringe $\mathbb{Z}/n\mathbb{Z}$ und $\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \dots \times \mathbb{Z}/n_r\mathbb{Z}$ isomorph.*

Natürlich wird die Eigenschaft, eine Einheit zu sein, unter Ringhomomorphismen erhalten. Ferner ist ein Tupel aus $\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \dots \times \mathbb{Z}/n_r\mathbb{Z}$ genau dann eine Einheit, wenn jede Komponente im zugehörigen Ring eine Einheit ist. Wir erhalten also

Korollar 4.10. *Es seien n_1, n_2, \dots, n_r paarweise teilerfremde natürliche Zahlen > 1 , und n das Produkt dieser Zahlen. Dann ist die Einheitengruppe von $\mathbb{Z}/n\mathbb{Z}$ isomorph zum direkten Produkt der Einheitengruppen der Ringe $\mathbb{Z}/n_1\mathbb{Z}, \mathbb{Z}/n_2\mathbb{Z}, \dots, \mathbb{Z}/n_r\mathbb{Z}$.*

Dieses Korollar wird meist in der Form verwendet, dass die n_i die Primpotenzen in der Primfaktorzerlegung einer natürlichen Zahl n sind.

Eine wichtige Konsequenz des Korollars ist

Satz 4.11. *Sei φ die Eulersche φ -Funktion, und $u, v \in \mathbb{N}$ teilerfremd. Dann gilt $\varphi(uv) = \varphi(u)\varphi(v)$.*

Beweis. Nach dem Korollar sind

$$(\mathbb{Z}/uv\mathbb{Z})^* \text{ und } (\mathbb{Z}/u\mathbb{Z})^* \times (\mathbb{Z}/v\mathbb{Z})^*$$

isomorph. Vergleich der Gruppenordnungen liefert die Behauptung. □

Ist also $n = \prod_p p^{e_p}$ die Primfaktorzerlegung von n , dann liefert mehrfache Anwendung des Lemmas $\varphi(n) = \prod_p \varphi(p^{e_p})$. Die Zahlen von 1 bis p^e , die nicht zu p^e teilerfremd sind, sind genau die p^{e-1} Zahlen $p, 2p, 3p, \dots, p^{e-1}p$, daher gilt $\varphi(p^e) = p^e - p^{e-1} = (p-1)p^{e-1}$. Wir erhalten also

Satz 4.12. *Sei $n = \prod_p p^{e_p}$ die Primfaktorzerlegung von n mit $e_p \geq 1$. Dann gilt*

$$\varphi(n) = \prod_p (p-1)p^{e_p-1} = n \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

5 Sätze von Fermat, Euler, Wilson

Einigen Sätzen der elementaren Zahlentheorie liegt ein einfacher Satz der Gruppentheorie zugrunde. Das folgende ist ein Spezialfall des Satzes von Lagrange aus der Algebra.

Lemma 5.1. *Sei G eine endliche abelsche Gruppe der Ordnung n mit neutralem Element e . Dann gilt $g^n = e$ für alle $g \in G$.*

Beweis. Sei $g \in G$ gegeben. Durchläuft h die Gruppe G , dann durchläuft auch gh die Gruppe G . Insbesondere gilt

$$\prod_{h \in G} h = \prod_{h \in G} gh = g^n \prod_{h \in G} h,$$

also $g^n = e$. □

Bemerkung 5.2. Das Lemma gilt auch dann, wenn G nicht abelsch ist. Dazu wendet man den aus der Algebra bekannten Satz von Lagrange auf die von g erzeugte Untergruppe von G an.

Aus dem Lemma erhalten wir

Satz 5.3 (Euler). Sei $a \in \mathbb{Z}$ teilerfremd zu $n \in \mathbb{N}$, und φ die Eulersche φ -Funktion. Dann gilt $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Beweis. Da a zu n teilerfremd ist, liegt $\bar{a} = a + n\mathbb{Z}$ in der Einheitengruppe $(\mathbb{Z}/n\mathbb{Z})^*$. Die Ordnung dieser Einheitengruppe ist $\varphi(n)$, aus dem Lemma folgt also $\bar{a}^{\varphi(n)} = \bar{1}$, was gleichbedeutend mit $a^{\varphi(n)} \equiv 1 \pmod{n}$ ist. □

Für Primzahlen p gilt $\varphi(p) = p - 1$, also

Satz 5.4 (Fermat). Sei $a \in \mathbb{Z}$ nicht durch die Primzahl p teilbar. Dann gilt $a^{p-1} \equiv 1 \pmod{p}$.

Ein weiterer interessanter Satz wird gelegentlich Wilson zugeschrieben, obwohl er ihn lediglich in einer alten Schrift gefunden hatte.

Satz 5.5 (Wilson). Für jede Primzahl p gilt $(p - 1)! \equiv -1 \pmod{p}$.

Beweis. Die Aussage gilt offenbar für $p = 2$. Sei ab jetzt p ungerade. Wir betrachten die Einheitengruppe $G = (\mathbb{Z}/p\mathbb{Z})^* = \{1, 2, \dots, p - 1\}$ des endlichen Körpers $\mathbb{Z}/p\mathbb{Z}$. Zu jedem Element $a \in G$ gibt es ein Inverses b , d.h. $ab = 1$ in G . Wann gilt $a = b$? Das passiert offenbar für $a = 1$ und $a = -1$. Andere Fälle gibt es nicht. Denn $\mathbb{Z}/p\mathbb{Z}$ ist ein Körper, und aus $a^2 = 1$ folgt $(a - 1)(a + 1) = 0$, also $a = \pm 1$. Die Elemente aus $G \setminus \{1, -1\}$ können wir also in Paare zueinander inverser Elemente anordnen. In $\mathbb{Z}/p\mathbb{Z}$ gilt also $1 \cdot 2 \cdot 3 \cdots (p - 1) = -1$, und die Behauptung folgt. □

Bemerkung 5.6. Es gilt auch die Umkehrung: Ist $(n - 1)! \equiv -1 \pmod{n}$ für eine natürliche Zahl $n \geq 2$, dann ist n eine Primzahl, denn jeder Teiler $d < n$ von n teilt $(n - 1)!$ und damit auch 1.

6 Polynome

Ein wichtiges Hilfsmittel in der elementaren Zahlentheorie sind Polynome. In diesem Abschnitt sei K stets ein Körper und X ein formales Symbol.

Ein *Polynom* in der Variablen X ist eine formale Summe $a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$ für ein $n \in \mathbb{N}_0$ und Koeffizienten $a_i \in K$. Hierbei trifft man die Festsetzung $X^0 = 1$. Die Menge der Polynome bildet einen Ring unter koeffizientenweiser Addition, und den Festsetzungen $aX = Xa$ und $X^mX^n = X^{m+n}$. Man schreibt $K[X]$ für diesen Ring. Man fasst den Koeffizientenkörper

K als Teilring von $K[X]$ auf, indem man $a \in K$ mit dem Polynom $a = aX^0$ identifiziert. Sei $0 \neq f \in K[X]$, und $n \in \mathbb{N}_0$ maximal mit $a_n \neq 0$. Dann heißt n der *Grad* von f , und a_n der *Leitkoeffizient*. Man schreibt $n = \text{grad } f$. Man nennt f *normiert*, wenn $a_n = 1$ gilt. Der Koeffizient a_0 wird *konstanter Term* oder *Absolutglied* genannt. Für $f = 0$ setzt man $\text{grad } f = -\infty$.

Bemerkung. Der Begriff des Polynoms ist sorgfältig von dem einer polynomialen Abbildung zu unterscheiden. Ist etwa $K = \mathbb{Z}/2\mathbb{Z}$ der Körper mit zwei Elementen und $f(X) = X^2 - X$, dann gilt $f(0) = f(1) = 0$, d.h. f ist die 0-Abbildung auf K , aber $f \neq 0$.

Aus den Definitionen folgt unmittelbar

Lemma 6.1. *Seien $f, g \in K[X]$ Polynome. Dann gilt $\text{grad}(f + g) \leq \max(\text{grad } f, \text{grad } g)$ und $\text{grad}(f \cdot g) = \text{grad } f + \text{grad } g$.*

Wie bei ganzen Zahlen hat man auch für Polynome über Körpern eine Division mit Rest. Genauer gilt:

Satz 6.2. *Seien $f, g \in K[X]$ Polynome mit $g \neq 0$. Dann gibt es eindeutige Polynome $q, r \in K[X]$ mit $f = q \cdot g + r$ und $\text{grad } r < \text{grad } g$.*

Beweis. Wir wollen zunächst die Eindeutigkeit beweisen. Dazu sei $f = q' \cdot g + r'$ eine weitere Darstellung der gegebenen Form. Dann folgt $(q - q')g = r' - r$, also $\text{grad}(r' - r) = \text{grad}(q - q') + \text{grad } g$. Wegen $\text{grad}(r' - r) < \text{grad } g$ folgt $q = q'$ und $r' = r$.

Es bleibt die Existenz zu zeigen. Wir dürfen g als normiert voraussetzen.

Ist $\text{grad } f < \text{grad } g$, dann gibt es nichts zu zeigen, da wir $q = 0$ und $r = f$ setzen können. Wir verwenden nun vollständige Induktion über $\text{grad } f$. Sei $n = \text{grad } f \geq \text{grad } g$, und a der Leitkoeffizient von f . Setze $f' = f - aX^{\text{grad } f - \text{grad } g}g$. Dann gilt $\text{grad } f' < \text{grad } f$. Nach Induktionsvoraussetzung gibt es also eine Darstellung $f' = q'g + r$ mit $\text{grad } r < \text{grad } g$. Die Behauptung folgt nun aus $f = f' + aX^{\text{grad } f - \text{grad } g}g = q'g + r' + aX^{\text{grad } f - \text{grad } g}g = (q' + aX^{\text{grad } f - \text{grad } g})g + r$. \square

Ist $f = \sum a_i X^i \in K[X]$ ein Polynom, und $u \in K$, dann setzen wir $f(u) = \sum a_i u^i$, mit der Konvention $u^0 = 1$ auch dann, wenn $u = 0$ gilt. Falls $f(u) = 0$, dann nennt man u eine *Nullstelle* von f .

Satz 6.3. *Ist $f(u) = 0$ für $f \in K[X]$ und $u \in K$, dann gibt es ein eindeutiges Polynom $g \in K[X]$ mit $f = (X - u)g$.*

Beweis. Schreibe $f = (X - u)g + r$ mit $\text{grad } r < \text{grad}(X - u) = 1$. Dann gilt $r \in K$. Einsetzen von u für X liefert $0 = f(u) = (u - u)g(u) + r = r$, und die Existenz von g folgt. Die Eindeutigkeit von g ist klar. \square

Eine wichtige Folgerung ist

Satz 6.4. *Sei $0 \neq f \in K[X]$. Dann hat f höchstens $\text{grad } f$ verschiedene Nullstellen.*

Beweis. Für $\text{grad } f = 0$ ist die Aussage klar. Wir beweisen sie allgemein durch vollständige Induktion über $\text{grad } f$. Seien u_1, \dots, u_r verschiedene Nullstellen von f . Wir schreiben $f = (X - u_1)g$. Wegen $0 = f(u_i) = (u_i - u_1)g(u_i)$ und der Nullteilerfreiheit von K ist u_i eine Nullstelle von g für alle $i \geq 2$. Daher gilt $r - 1 \leq \text{grad } g = \text{grad } f - 1$, und die Behauptung folgt. \square

7 Zyklische Gruppen und Ordnungen

Sei G eine beliebige Gruppe. Man sagt, dass $g \in G$ eine endliche Ordnung hat, falls es ein $n \in \mathbb{N}$ gibt mit $g^n = e$. Das kleinste solche n nennt man die *Ordnung* von G , man schreibt $\text{ord}(g) = n$.

Lemma 7.1. *Das Element g einer Gruppe habe die endliche Ordnung $n \in \mathbb{N}$. Für $i, j \in \mathbb{Z}$ gilt $g^i = g^j$ genau dann, wenn $i \equiv j \pmod{n}$.*

Beweis. $g^i = g^j$ ist äquivalent zu $g^{i-j} = e$. Wir müssen also zeigen: Für $m \in \mathbb{Z}$ gilt $g^m = e$ genau dann, wenn $m \equiv 0 \pmod{n}$.

Sei $m \equiv 0 \pmod{n}$, also $m = kn$ für ein $k \in \mathbb{Z}$. Dann folgt $g^m = g^{kn} = (g^n)^k = e^k = e$.

Sei nun umgekehrt $g^m = e$, und $m = qn + r$ eine Division mit Rest, also $q \in \mathbb{Z}$ und $0 \leq r < n$. Wir erhalten

$$e = g^m = g^{qn+r} = (g^n)^q g^r = e^q g^r = g^r.$$

Aber n ist die kleinste natürliche Zahl mit $g^n = e$, also $r = 0$ da $r < n$. Es gilt also $n|m$. \square

Zur Illustration des Lemma geben wir eine Anwendung, aus der wiederum die Unendlichkeit der Primzahlmenge folgt.

Beispiel 7.2. Für jede Primzahl p ist jeder Primteiler von $2^p - 1$ größer als p .

Das sieht man folgendermaßen: Sei q ein Primteiler von $2^p - 1$, also $2^p \equiv 1 \pmod{q}$. Offenbar ist q ungerade. Nach dem Satz von Fermat gilt $2^{q-1} \equiv 1 \pmod{q}$. Sei r die Ordnung von 2 in der multiplikativen Gruppe $(\mathbb{Z}/q\mathbb{Z})^*$. Nach dem vorigen Lemma ist r ein Teiler von $q - 1$ und von p . Da p eine Primzahl ist, gilt $r = p$ oder $r = 1$. Aber $r = 1$ gilt offenbar nicht, da $2 \not\equiv 1 \pmod{q}$. Es folgt $r = p$ und $p|q - 1$, also $q \geq p + 1$.

Mit dem Lemma sieht man auch das folgende: Hat das Gruppenelement g die endliche Ordnung n , dann besteht die von g erzeugte Gruppe genau aus den verschiedenen Elementen $g^1, g^2, \dots, g^{n-1}, g^n = e$. Insbesondere hat diese Gruppe die Ordnung n .

Lemma 7.3. *Das Gruppenelement g habe die Ordnung $n \in \mathbb{N}$. Sei $m \in \mathbb{Z}$. Dann hat g^m die Ordnung $\frac{n}{\text{ggT}(n,m)}$.*

Beweis. Sei $d = \text{ggT}(n, m)$. Da d ein Teiler von m und n ist, gilt

$$(g^m)^{\frac{n}{d}} = (g^n)^{\frac{m}{d}} = e^{\frac{m}{d}} = e,$$

d.h. die Ordnung von g^m ist höchstens $\frac{n}{d}$.

Sei nun r die Ordnung von g^m . Dann gilt $e = (g^m)^r = g^{mr}$, also $mr \equiv 0 \pmod{n}$. Nach Bézout finden wir $u, v \in \mathbb{Z}$ mit $um + vn = d$, also $dr = umr + vnr$. Es folgt $n|dr$, also $n \leq dr$ und damit $\frac{n}{d} \leq r$. Die umgekehrte Ungleichung sahen wir oben, die Behauptung folgt. \square

Eine direkte Folge des Lemmas ist

Korollar 7.4. *Das Gruppenelement g habe die Ordnung $n \in \mathbb{N}$. Dann gilt:*

(a) Für $d|n$ ist $\text{ord } g^d = \frac{n}{d}$.

(b) Für $m \in \mathbb{Z}$ gilt $\text{ord } g^m = n$ genau dann, wenn m und n teilerfremd sind.

Eine *zyklische Gruppe* ist eine von einem einzigen Element g erzeugte Gruppe G , es gilt also $G = \{g^m | m \in \mathbb{Z}\}$. Hat dabei G die endliche Ordnung n , dann folgt aus dem bisherigen, dass g die Ordnung n hat, und $G = \{g^1, g^2, \dots, g^n = e\}$. Ein Element g^m ist dann ein Erzeuger von G genau dann, wenn m und n teilerfremd sind. Wir erhalten

Satz 7.5. Die Anzahl der Erzeuger einer endlichen zyklischen Gruppe der Ordnung n ist $\varphi(n)$.

Wir benötigen eine wichtige Eigenschaft der φ -Funktion:

Lemma 7.6. Für $n \in \mathbb{N}$ gilt $\sum_{d|n} \varphi(d) = n$.

Beweis. Betrachte die n Brüche $\frac{m}{n}$ für $m = 1, 2, \dots, n$. Kürzt man diese Brüche, dann tauchen als Nenner nur Teiler d von n auf, und zu einem Nenner d gibt es genau $\varphi(d)$ mögliche Zähler. \square

Der folgende Satz gilt auch für nicht abelsche Gruppen. Allerdings benötigen wir für den Beweis ein Lemma, das wir nur für abelsche Gruppen bewiesen hatten.

Satz 7.7. Sei G eine endliche abelsche Gruppe der Ordnung n . Für jeden Teiler d von n gebe es höchstens d Elemente $g \in G$ mit $g^d = e$. Dann ist G zyklisch.

Beweis. Nach Lemma 5.1 ist die Ordnung jedes Elements von G ein Teiler von n . Für jeden Teiler d von n sei $\psi(d)$ die Anzahl der Elemente von G der Ordnung d . Dann gilt

$$\sum_{d|n} \psi(d) = n.$$

Nach Voraussetzung hat G für jedes d höchstens eine Untergruppe der Ordnung d , und daher höchstens $\varphi(d)$ Elemente der Ordnung d . Es gilt also

$$\psi(d) \leq \varphi(d) \text{ für alle } d.$$

Summation und das vorherige Lemma liefern

$$n = \sum_{d|n} \psi(d) \leq \sum_{d|n} \varphi(d) = n,$$

also $\psi(d) = \varphi(d)$ für alle Teiler d von n . Insbesondere gilt $\psi(n) = \varphi(n) \geq 1$, und die Behauptung folgt. \square

8 Primitivwurzeln und Einheitengruppen der Restklassenringe

Die vorangegangenen zwei Abschnitte dienten als Vorbereitung der Beweis des folgenden Satzes, den unter anderem Euler schon vermutet hatte, der aber erstmals von Gauß bewiesen wurde.

Satz 8.1 (Gauß). Sei p eine Primzahl. Dann ist die multiplikative Gruppe von $\mathbb{Z}/p\mathbb{Z}$ zyklisch.

Da $\mathbb{Z}/p\mathbb{Z}$ ein Körper ist, ist der Satz ein Spezialfall des folgenden Satzes.

Satz 8.2. Sei G eine endliche Untergruppe der multiplikativen Gruppe eines Körpers. Dann ist G zyklisch.

Beweis. Sei n die Ordnung einer endlichen Untergruppe der multiplikativen Gruppe eines Körpers K . Nach Satz 6.4 hat für jeden Teiler d von n das Polynom $X^d - 1$ höchstens d Nullstellen in K . Es gibt also höchstens d Elemente $g \in G$ mit $g^d = 1$. Wegen Satz 7.7 ist G dann zyklisch. \square

Bemerkung 8.3. Der Satz gilt nicht für unendliche Gruppen, so ist z.B. die multiplikative Gruppe von \mathbb{Q} nicht zyklisch (warum?).

Der Satz stimmt auch nicht für Schiefkörper. Im reellen Quaternionenschiefkörper mit der Standardbasis $\{1, i, j, k\}$ bilden die 8 Elemente $\{\pm 1, \pm i, \pm j, \pm k\}$ eine nicht abelsche Untergruppe. Diese 8 Elemente sind übrigens (ein Teil der unendlich vielen) Nullstellen des Polynoms $X^2 + 1$.

Eine ganze Zahl g nennt man eine *Primitivwurzel* modulo n , wenn $\bar{g} = g + n\mathbb{Z}$ ein Erzeuger der Einheitengruppe von $\mathbb{Z}/n\mathbb{Z}$ ist. Der Satz von Gauß zeigt also, dass es modulo Primzahlen immer Primitivwurzeln gibt. Im folgenden wollen wir unter anderem klären, modulo welchen natürlichen Zahlen n es eine Primitivwurzel gibt.

Lemma 8.4. Sei $g \in \mathbb{Z}$ eine Primitivwurzel modulo der ungeraden Primzahl p . Dann ist g oder $g + p$ eine Primitivwurzel modulo p^m für alle $m \in \mathbb{N}$.

Beweis. Es gilt $g^{p-1} \equiv 1 \pmod{p}$, also $g^{p-1} = 1 + ap$ für ein $a \in \mathbb{Z}$. Mit g ist natürlich auch $g + p$ eine Primitivwurzel modulo p . Schreibe $(g + p)^{p-1} = 1 + a'p$. Dann können nicht a und a' beide durch p teilbar sein: Es ist nämlich

$$1 + a'p = (g + p)^{p-1} = g^{p-1} + (p-1)g^{p-2}p + (\dots)p^2 = 1 + ap + (p-1)g^{p-2}p + (\dots)p^2.$$

Wären nun a und a' durch p teilbar, dann wäre auch $(p-1)g^{p-2}$ durch p teilbar, was natürlich nicht der Fall ist.

Indem wir gegebenenfalls g durch $g + p$ ersetzen dürfen wir annehmen, dass a nicht durch p teilbar ist. Unter dieser Voraussetzung zeigen wir, dass g modulo p^m die Ordnung $\varphi(p^m) = p^m - p^{m-1} = p^{m-1}(p-1)$ hat.

Hat g modulo p^m eine kleinere Ordnung als $p^{m-1}(p-1)$, dann hat $p^{m-1}(p-1)$ einen Primteiler q mit $g^{\frac{p^{m-1}(p-1)}{q}} \equiv 1 \pmod{p^m}$. Insbesondere gilt auch $g^{\frac{p^{m-1}(p-1)}{q}} \equiv 1 \pmod{p}$. Aber die Ordnung von g modulo p ist $p-1$, und damit ist $p-1$ ein Teiler von $\frac{p^{m-1}(p-1)}{q}$. Da $p-1$ und p teilerfremd sind geht das nur für $q = p$. Wir erhalten also

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

und daher

$$(1 + ap)^{p^{m-2}} \equiv 1 \pmod{p^m}.$$

Das aber widerspricht dem folgenden Lemma. \square

Lemma 8.5. *Es sei $p \geq 3$ eine Primzahl, $m \geq 2$ und $a \in \mathbb{Z}$ nicht durch p teilbar. Dann gilt $(1 + ap)^{p^{m-2}} = 1 + a'p^{m-1}$ mit $p \nmid a'$.*

Beweis. Wir beweisen die Aussage durch vollständige Induktion über m . Für $m = 2$ gibt es nichts zu zeigen. Wir wollen nun sehen, dass aus der Gültigkeit der Aussage für $m \geq 2$ auch die für $m + 1$ folgt: Dazu berechnen wir

$$(1 + ap)^{p^{m-1}} = ((1 + ap)^{p^{m-2}})^p = (1 + a'p^{m-1})^p = 1 + a'p^m + \binom{p}{2}a'^2p^{2(m-1)} + \dots$$

Wegen $m \geq 2$ gilt $2(m - 1) \geq m$, und aus $p \geq 3$ folgt $p \mid \binom{p}{2}$. Der dritte Summand der rechten Seite ist also durch p^{m+1} teilbar. Auch die nachfolgenden Summanden sind durch p^{m+1} teilbar, da $k(m - 1) \geq m + 1$ für $k \geq 3$. Die Behauptung folgt. \square

Lemma 8.6. *Für $n > 2$ ist $\varphi(n)$ gerade.*

Beweis. $\text{ggT}(k, n) = 1$ ist äquivalent zu $\text{ggT}(n - k, k)$. Ferner kann für $\text{ggT}(k, n) = 1$ nicht $k = n - k$ gelten, denn $2k = n$ impliziert $k = 1, n = 2$. Daher lassen sich die Zahlen von 1 bis n , die zu n teilerfremd sind, als Vereinigung disjunkter Paare schreiben. \square

Wir kommen nun zum ersten Hauptergebnis

Satz 8.7. *Die Einheitengruppe von $\mathbb{Z}/n\mathbb{Z}$ ($n \geq 2$) ist genau dann zyklisch, wenn $n = 2, 4, p^m$ oder $2p^m$ für eine ungerade Primzahl p und $m \geq 1$.*

Beweis. Wir zeigen zunächst die Notwendigkeit dieser Bedingung. Zunächst wollen wir sehen, dass nicht $n = uv$ mit $u, v > 2$ und $\text{ggT}(u, v) = 1$ gelten kann: Nach Satz 4.11 gilt dann $\varphi(n) = \varphi(u)\varphi(v)$. Wegen $u, v > 2$ und dem vorigen Lemma sind $\varphi(u)$ und $\varphi(v)$ gerade. Nach Eulers Satz 5.3 gilt $a^{\varphi(v)} \equiv 1 \pmod{v}$ für alle a mit $\text{ggT}(a, v) = 1$. Wegen $\frac{\varphi(u)}{2} \in \mathbb{N}$ erhalten wir

$$a^{\frac{\varphi(n)}{2}} = (a^{\varphi(v)})^{\frac{\varphi(u)}{2}} \equiv 1 \pmod{v},$$

und analog folgt

$$a^{\frac{\varphi(n)}{2}} \equiv 1 \pmod{u}.$$

Beides zusammen gibt

$$a^{\frac{\varphi(n)}{2}} \equiv 1 \pmod{n}.$$

Insbesondere gibt es keine ganze Zahl, die modulo n die Ordnung $\varphi(n)$ hat.

Daher ist n entweder von der angegebenen Form, oder $n = 2^m \geq 8$. Ist $(\mathbb{Z}/n\mathbb{Z})^*$ zyklisch, dann zeigt der Ringhomomorphismus $\mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/8\mathbb{Z}$, dass auch $(\mathbb{Z}/8\mathbb{Z})^*$ zyklisch ist. Aber man rechnet sofort nach, dass in $(\mathbb{Z}/8\mathbb{Z})^*$ jedes Element die Ordnung 1 oder 2 hat, im Widerspruch zu $\varphi(8) = 4$.

Nun wollen wir sehen, dass die angegebenen Bedingungen hinreichend sind. Sei p^m eine ungerade Primpotenz. Wir bewiesen bereits, dass $(\mathbb{Z}/p^m\mathbb{Z})^*$ zyklisch ist. Auch $(\mathbb{Z}/2p^m\mathbb{Z})^*$ ist zyklisch, denn $(\mathbb{Z}/2p^m\mathbb{Z})^*$ ist isomorph zu $(\mathbb{Z}/2\mathbb{Z})^* \times (\mathbb{Z}/p^m\mathbb{Z})^* = (\mathbb{Z}/p^m\mathbb{Z})^*$.

Schließlich rechnet man direkt nach, dass 3 eine Primitivwurzel modulo 2 und auch modulo 4 ist. \square

Bemerkung 8.8. Im Zusammenhang mit Primitivwurzeln modulo Primzahlen gibt es eine interessante noch heute offene Vermutung. Wir sahen ja, dass es zu jeder Primzahl p eine Primitivwurzel $a \in \mathbb{Z}$ gibt. Umgekehrt kann man fragen, ob jede ganze Zahl $a \neq 0$ modulo unendlich vielen Primzahlen eine Primitivwurzel ist. Natürlich geht das nicht für $a = -1$. Auch eine Quadratzahl $a = b^2$ kann keine Primitivwurzel modulo $p > 2$ sein. Artins Vermutung besagt nun, dass das die einzigen Ausnahmen sind: Sei $-1 \neq a \in \mathbb{Z}$ keine Quadratzahl, dann ist a eine Primitivwurzel modulo unendlich vielen Primzahlen.

Interessanterweise konnte das bis heute nicht einmal für eine einzige Zahl a bewiesen werden! Das bislang beste Resultat stammt von Heath–Brown: Die Artin–Vermutung ist richtig für alle Primzahlen a , bis auf höchstens zwei Ausnahmen. Allerdings liefert der Beweis keine Anhaltspunkte, wie die zwei eventuellen Ausnahmen aussehen können.

9 Quadratische Reste und Gaußsches Reziprozitätsgesetz

Die Lösbarkeit linearer Kongruenzen stellt keine besondere Schwierigkeit dar. So ist $aX + b \equiv 0 \pmod{n}$ genau dann lösbar, wenn $\text{ggT}(a, n) | b$ (warum?).

Schwieriger und interessanter wird es für quadratische Gleichungen. Wir betrachten die Kongruenz $aX^2 + bX + c \equiv 0 \pmod{n}$. Diese ist äquivalent zu $(2aX + b)^2 \equiv b^2 - 4ac \pmod{4an}$, was also zur Frage nach Quadraten in Restklassenringen führt.

Ist $n = \prod p^{e_p}$ die Primfaktorzerlegung von n , dann sieht man mit dem Chinesischen Restsatz sofort, dass die Kongruenz $X^2 \equiv a \pmod{n}$ genau dann lösbar ist, wenn jede der Kongruenzen $X^2 \equiv a \pmod{p^{e_p}}$ lösbar ist.

Ist $p \in \mathbb{P}$ kein Teiler von a und $p \neq 2$, $e \in \mathbb{N}$, dann sieht man auch schnell, dass $X^2 \equiv a \pmod{p^e}$ genau dann lösbar ist, wenn schon $X^2 \equiv a \pmod{p}$ lösbar ist. Auch die Fälle $p = 2$ oder $p | a$ lassen sich leicht behandeln.

Man kann also die Frage nach der Lösbarkeit quadratischer Gleichungen in Restklassenringen im wesentlichen darauf reduzieren, wann eine ganze Zahl ein Quadrat modulo einer Primzahl ist. Das motiviert die folgende Definition.

Definition. Sei $p \neq 2$ eine Primzahl, und $a \in \mathbb{Z}$ nicht durch p teilbar. Man sagt, dass a ein *quadratischer Rest* modulo p ist, wenn die Kongruenz $X^2 \equiv a \pmod{p}$ lösbar ist. Im anderen Fall ist a ein *quadratischer Nichtrest* modulo p .

Eine kompakte Notation für diesen Begriff bildet das *Legendre-Symbol*. Für $2 \neq p \in \mathbb{P}$ und $a \in \mathbb{Z}$ setzt man

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & a \text{ ist quadratischer Rest modulo } p \\ -1, & a \text{ ist quadratischer Nichtrest modulo } p \\ 0, & p \text{ teilt } a \end{cases}$$

Im folgenden werden wir mehrfach im Restklassenring $\mathbb{Z}/p\mathbb{Z}$ arbeiten. Wegen $p \in \mathbb{P}$ ist dieser Ring ein Körper, wir verwenden hierfür die übliche Bezeichnung \mathbb{F}_p .

Natürlich hängt $\left(\frac{a}{p}\right)$ nur von der Restklasse von a modulo p ab. Ist $\bar{a} \in \mathbb{F}_p$ die Restklasse von a modulo p .

Satz 9.1. Sei $3 \leq p \in \mathbb{P}$, dann gibt es unter den Zahlen $1, 2, \dots, p-1$ genau $\frac{p-1}{2}$ quadratische Reste und genauso viele quadratische Nichtreste modulo p .

Beweis. Die Anzahl der quadratischen Reste modulo p unter den Zahlen $1, 2, \dots, p-1$ ist gleich der Anzahl der verschiedenen Quadrate u^2 in \mathbb{F}_p für $0 \neq u \in \mathbb{F}_p$. Wegen $u^2 - v^2 = (u-v)(u+v)$ gilt $u^2 = v^2$ genau dann, wenn $u = v$ oder $u = -v$. Wegen $p > 2$ und $u \neq 0$ kann nicht $u = -u$ gelten. Es gibt also genau $\frac{p-1}{2}$ Quadrate $\neq 0$ in \mathbb{F}_p , und dann natürlich auch genau $p-1 - \frac{p-1}{2} = \frac{p-1}{2}$ Nichtquadrate. \square

Satz 9.2 (Euler-Kriterium). Sei $2 \neq p \in \mathbb{P}$ und $a \in \mathbb{Z}$. Dann gilt

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

Beweis. Die Aussage ist klar für $p|a$. Sei also p kein Teiler von a . Sei $\left(\frac{a}{p}\right) = 1$, und \bar{a} das Bild von a in \mathbb{F}_p . Daher ist \bar{a} ein Quadrat \bar{b}^2 in \mathbb{F}_p . Es folgt

$$\bar{a}^{\frac{p-1}{2}} = \bar{b}^{p-1} = 1.$$

Daher sind genau die $\frac{p-1}{2}$ Quadrate in \mathbb{F}_p^\times die Nullstellen von $X^{\frac{p-1}{2}} - 1$. Die Nichtquadrate sind also keine Nullstellen dieses Polynoms. Sei $\bar{a} \in \mathbb{F}_p^\times$ ein Nichtquadrat. Wegen $1 = \bar{a}^{p-1} = (\bar{a}^{\frac{p-1}{2}})^2$ ist daher $\bar{a}^{\frac{p-1}{2}} = \pm 1$, also $\bar{a}^{\frac{p-1}{2}} = -1$, und die Behauptung folgt. \square

Ein einfaches Korollar ist die Multiplikativität des Legendre-Symbols.

Lemma 9.3. Sei $2 \neq p \in \mathbb{P}$, $a, b \in \mathbb{Z}$. Dann gilt

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

Daher sind vor allem die Werte $\left(\frac{p}{q}\right)$ für Primzahlen p (oder $p = -1$) und q interessant. Diese wurden schon zu Eulers Zeiten für große Werte für p und q berechnet. Dabei stellte Euler schon 1740 eine merkwürdige Beziehung zwischen $\left(\frac{p}{q}\right)$ und $\left(\frac{q}{p}\right)$ fest. Ist mindestens eine der Primzahlen p und q kongruent 1 modulo 4, dann fand er in allen berechneten Beispielen $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$. Ist hingegen weder p noch q kongruent 1 modulo 4, dann scheint $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$ gelten. Eigentlich sollte man denken, dass die Frage, ob p ein Quadrat modulo q ist, nichts damit zu tun hat, ob q ein Quadrat modulo p ist. Auch der chinesische Restsatz legt ja nahe, dass Kongruenzen modulo p nicht mit Kongruenzen modulo einer anderen Primzahl q zu tun haben sollten. Umso überraschender waren also diese empirischen Beobachtungen die Euler allerdings noch nicht beweisen konnte. Auch Legendre bemerkte 1785 diese merkwürdigen Beziehungen, er lieferte einen Beweisansatz, der allerdings auf dem damals noch unbewiesenen Dirichletschen Satz über Primzahlen in arithmetischen Folgen beruhte. Erst Gauß gab ab 1801 acht verschiedene Beweise. Bis heute sind weit über 100 Beweise bekannt. Die Vielzahl der Beweise rührt vielleicht auch daher, dass man (im wesentlichen vergeblich) nach einem natürlichen Beweis suchte. Die von Euler, Legendre und Gauß gefundene Beobachtung lässt sich so zusammenfassen.

Satz 9.4 (Quadratisches Reziprozitätsgesetz). *Seien p, q ungerade und verschiedene Primzahlen. Dann gilt*

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

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

$$(c) \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

Wir werden das Reziprozitätsgesetz nach einer Methode von Eisenstein beweisen, welche eine vereinfachte Variante des dritten von Gauß gegebenen Beweis ist.

Für eine reelle Zahl x bezeichne $[x]$ die größte ganze Zahl, welche $\leq x$ ist. Es gilt also $[x] \in \mathbb{Z}$ und $x - 1 < [x] \leq x$. Ist z.B. $p \in \mathbb{N}$ und $n = mp + r$ eine Division von n durch p mit Rest r , dann gilt $r = n - p[\frac{n}{p}]$.

Lemma 9.5 (Eisenstein). *Es sei $p \neq 2$ eine Primzahl, und $q \in \mathbb{Z}$ nicht durch p teilbar. Dann gilt*

$$\left(\frac{q}{p}\right) = (-1)^\mu \text{ mit } \mu = \sum_{k=1}^{(p-1)/2} \left[\frac{2kq}{p}\right].$$

Beweis. Für $k = 1, 2, \dots, \frac{p-1}{2}$ sei r_k der Rest bei Division von $2kq$ durch p , also $r_k = 2kq - p\left[\frac{2kq}{p}\right]$. Sei s_k der Rest bei Division von $(-1)^{r_k}r_k$ durch p . Die $\frac{p-1}{2}$ Zahlen s_k sind alle gerade: Ist r_k gerade, dann gilt $s_k = r_k$, und ist r_k ungerade, dann gilt $s_k = p - r_k$. Für $k \neq l$ gilt $s_k \neq s_l$. Denn aus $s_k = s_l$ folgt $r_k \equiv \pm r_l \pmod{p}$, also $2kq \equiv \pm 2lq \pmod{p}$. Aber p teilt nicht $2q$, es folgt $k \equiv \pm l \pmod{p}$. Wegen $0 < k, l < \frac{p}{2}$ ist das aber nicht möglich.

Die $\frac{p-1}{2}$ geraden Zahlen s_k erfüllen $2 \leq s_k \leq p-1$ und sind paarweise verschieden. Sie sind deshalb eine Permutation der Zahlen $2, 4, 6, \dots, p-1$. Wir erhalten also modulo p

$$\begin{aligned} 2 \cdot 4 \cdot 6 \cdots (p-1) &= \prod_{k=1}^{(p-1)/2} s_k \\ &\equiv \prod_{k=1}^{(p-1)/2} (-1)^{r_k} r_k \\ &\equiv \prod_{k=1}^{(p-1)/2} ((-1)^{r_k} 2kq) \\ &= 2 \cdot 4 \cdot 6 \cdots (p-1) \cdot q^{\frac{p-1}{2}} \prod_{k=1}^{(p-1)/2} (-1)^{r_k} \end{aligned}$$

Da p kein Teiler von $2 \cdot 4 \cdot 6 \cdots (p-1)$ ist, können wir diesen Faktor kürzen. Nach dem Euler-Kriterium gilt $q^{\frac{p-1}{2}} \equiv \left(\frac{q}{p}\right) \pmod{p}$. Wegen $\left(\frac{q}{p}\right) = \pm 1$ gilt $\left(\frac{q}{p}\right) = \left(\frac{q}{p}\right)^{-1}$. Wir erhalten also

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

Aber $r_k \equiv \left[\frac{2kq}{p} \right] \pmod{2}$, also $(-1)^{r_k} = (-1)^{\left[\frac{2kq}{p} \right]}$, und hieraus folgt schließlich die Behauptung. \square

Die folgende Aussage ähnelt dem Lemma von Eisenstein und folgt auch aus diesem.

Lemma 9.6 (Gauß). *Es sei $p \neq 2$ eine Primzahl, und $q \in \mathbb{N}$ ungerade und nicht durch p teilbar. Dann gilt*

$$\left(\frac{q}{p} \right) = (-1)^\nu \text{ mit } \nu = \sum_{k=1}^{(p-1)/2} \left[\frac{kq}{p} \right].$$

Beweis (Eisenstein). Wir folgen hier Eisensteins geometrischer Interpretation. Sei wieder

$$\mu = \sum_{k=1}^{(p-1)/2} \left[\frac{2kq}{p} \right].$$

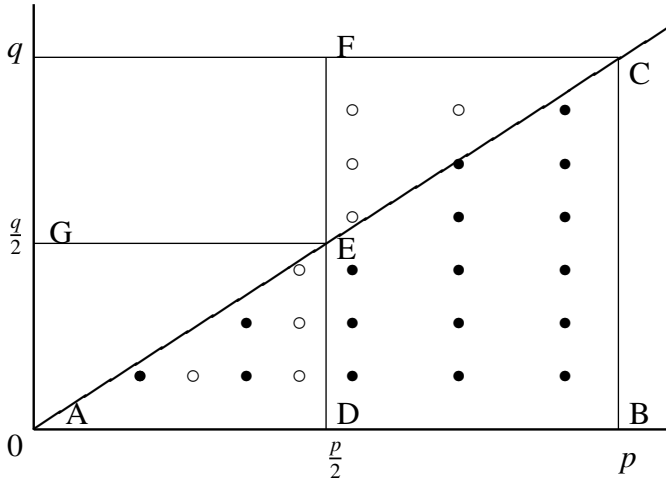
In der kartesischen Zahlenebene betrachten wir den Graphen der Funktion $y = \frac{q}{p}x$ und die Punkte $A = (0, 0)$, $B = (p, 0)$, $C = (p, q)$, $D = (\frac{p}{2}, 0)$, $E = (\frac{p}{2}, \frac{q}{2})$, $F = (\frac{p}{2}, q)$ und $G = (0, \frac{q}{2})$, siehe die Skizze.

Da p und q teilerfremd sind, liegen keine Gitterpunkte im Inneren der Strecke AC .

$\left[\frac{2kq}{p} \right]$ ist gleich der Anzahl der natürlichen Zahlen $\leq 2k\frac{q}{p}$, und diese Anzahl ist gleich der Anzahl der Gitterpunkte $(2k, \ell)$ mit $\ell \geq 1$, die unterhalb des Graphen von $y = \frac{q}{p}x$ liegen. Daher ist μ die Anzahl der Gitterpunkte im Inneren des Dreiecks ABC mit geraden Abszissen, im Bild dargestellt durch \bullet .

Wir betrachten die inneren Gitterpunkte im Viereck $BCFD$ mit gerader Abszisse. Auf jeder Spalte liegt die gerade Anzahl $q - 1$ von Gitterpunkten. Die Anzahl dieser Gitterpunkte unterhalb der Strecke EC unterscheidet sich also um eine gerade Anzahl von der Anzahl dieser Punkte oberhalb der Strecke EC . Um also $(-1)^\mu$ zu berechnen, können wir also den Anteil der Punkte mit gerader Abszisse im Viereck $BCED$ ersetzen durch die Anzahl der Punkte mit gerader Abszisse im Dreieck CFE , hier durch \circ dargestellt.

Eine Drehung des Dreiecks CFE um E um 180° ergibt das Dreieck ADE , wobei die Gitterpunkte in CFE mit gerader Abszisse übergehen in die Gitterpunkte in ADE mit ungerader Abszisse. Modulo 2 ist also μ gleich der Anzahl aller Gitterpunkte im Inneren des Dreiecks ADE . Diese Anzahl wird aber gerade durch ν gegeben, und die Behauptung folgt.



□

Nach diesen Vorbereitungen können wir nun das quadratische Reziprozitätsgesetz 9.4 rasch beweisen: Seien also p und q ungerade Primzahlen. Nach dem vorigen Lemma gilt $\left(\frac{q}{p}\right) = (-1)^\nu$, wobei wir ν interpretieren können als die Anzahl der Gitterpunkte im Inneren des Dreiecks ADE . Durch Vertauschen der Rollen von p und q folgt $\left(\frac{p}{q}\right) = (-1)^\lambda$, wobei λ die Anzahl der Gitterpunkte im Dreieck AEG ist. Daher gilt

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right)(-1)^{\nu+\lambda}.$$

Aber $\nu + \lambda$ ist die Anzahl der Gitterpunkte im Rechteck $ADEG$, und diese Anzahl ist offensichtlich gleich $\frac{p-1}{2} \frac{q-1}{2}$. Hieraus folgt die Teilaussage (a).

Die Aussage (b) ist einfach das Euler-Kriterium für $a = -1$.

Die Aussage (c) kann man z.B. mit dem Lemma 9.5 von Eisenstein beweisen: Sei $q = 2$, also $\mu = \sum_{k=1}^{(p-1)/2} \left[\frac{4k}{p}\right]$. Offenbar gilt $0 \leq \frac{4k}{p} < 2$, also $\left[\frac{4k}{p}\right] = 0$ oder 1 . Daher ist μ gleich der Anzahl der natürlichen Zahlen k mit

$$\frac{p}{4} < k \leq \frac{p-1}{2},$$

also

$$\mu = \mu_p = \frac{p-1}{2} - \left[\frac{p}{4}\right].$$

Die folgenden Überlegungen gelten für alle ungeraden $p \geq 3$. Wegen

$$\mu_{p+8} = 2 + \mu_p$$

hängt $(-1)^\mu$ nur von der Restklasse von p modulo 8 ab. Für $p = 9, 3, 5, 7$ erhalten wir nacheinander $\mu = 2, 1, 1, 2$. Daher ist $(-1)^\mu = 2$ genau dann, wenn $p \equiv \pm 1 \pmod{8}$. Dies wiederum ist äquivalent dazu, dass $\frac{p^2-1}{8} \equiv 0 \pmod{2}$. Hieraus folgt die Behauptung.

Ein Beispiel Wenn man wissen will, ob etwa 13 ein Quadrat modulo 3001 ist, dann muss man nicht die 1500 quadratischen Reste in \mathbb{F}_{3001} bestimmen und überprüfen, ob 13 dabei ist. Das Reziprozitätsgesetz und $3001 = 230 \cdot 13 + 11$ liefern sofort

$$\left(\frac{13}{3001}\right) = \left(\frac{3001}{13}\right) = \left(\frac{11}{13}\right) = \left(\frac{13}{11}\right) = \left(\frac{2}{11}\right) = -1.$$

Die Verwendung des Reziprozitätsgesetzes wie angedeutet zur Berechnung des Legendresymbols $\left(\frac{p}{q}\right)$ für Primzahlen p und q erfordert im Allgemeinen, dass man in Zwischenschritten die obere Zahl faktorisieren muss. So gilt etwa

$$\left(\frac{53}{3001}\right) = \left(\frac{3001}{53}\right) = \left(\frac{33}{53}\right) = \left(\frac{3}{53}\right)\left(\frac{11}{53}\right) = \dots,$$

d.h. man musste in einem Zwischenschritt 33 faktorisieren. Bei sehr großen Zahlen kann aber die Primfaktorzerlegung sehr teuer oder sogar unmöglich sein. Daher ist es eine gewisse Überraschung, dass es Jacobi durch eine einfache Verallgemeinerung des Legendresymbols gelungen war, die Notwendigkeit der Faktorisierung zu umgehen und einen dem Euklidischen ähnlichen Algorithmus anzugeben.

Definition 9.7. Sei $n = \prod_p p^{e_p}$ die Primfaktorzerlegung der ungeraden natürlichen Zahl $n \geq 3$, und $a \in \mathbb{Z}$. Setze

$$\left(\frac{a}{n}\right) := \prod_p \left(\frac{a}{p}\right)^{e_p},$$

wobei im Produkt auf der rechten Seite das Legendresymbol gemeint ist. Ferner setze $\left(\frac{a}{1}\right) = 1$ für alle $a \in \mathbb{Z}$. Das Symbol auf der linken Seite verallgemeinert also das Legendresymbol, man nennt es das *Jacobisymbol*.

Es besteht keine Notwendigkeit, für das Jacobisymbol eine andere Schreibweise zu verwenden, da es für Primzahlen n mit dem Legendresymbol zusammenfällt.

Bemerkung 9.8. Aus $\left(\frac{a}{n}\right) = 1$ folgt im allgemeinen nicht, dass a ein Quadrat modulo n ist. Ist hingegen $\left(\frac{a}{n}\right) = -1$, dann weiß man, dass a kein Quadrat modulo n ist.

Übung: Begründe diese zwei Aussagen.

Direkt aus der Definition des Jacobisymbols und der Verwendung der bekannten Eigenschaften des Legendresymbols erhalten wir

Lemma 9.9. *Es seien $a, b \in \mathbb{Z}$ und $m, n \in \mathbb{N}$ ungerade. Dann gilt:*

(a) Aus $a \equiv b \pmod{n}$ folgt $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$.

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

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

(d) $\left(\frac{a}{n}\right) = \pm 1$, falls $\text{ggT}(a, n) = 1$, und $\left(\frac{a}{n}\right) = 0$, falls $\text{ggT}(a, n) > 1$.

Es ist auf den ersten Blick sicher überraschend, dass sich das quadratische Reziprozitätsgesetz fast wörtlich auch für das Jacobisymbol gilt:

Satz 9.10 (Jacobi). *Es seien $m, n \in \mathbb{N}$ ungerade und teilerfremd. Dann gilt*

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

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

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

Dem Beweis schicken wir einige Hilfsaussagen voraus.

Lemma 9.11. *Es seien $m, n \in \mathbb{Z}$ ungerade. Dann gilt*

$$(a) \frac{mn-1}{2} \equiv \frac{m-1}{2} + \frac{n-1}{2} \pmod{2}$$

$$(b) \frac{(mn)^2-1}{8} \equiv \frac{m^2-1}{8} + \frac{n^2-1}{8} \pmod{2}$$

Beweis. Offenbar gilt $(m-1)(n-1) \equiv 0 \pmod{4}$, und daraus folgt $mn-1 \equiv (m-1) + (n-1) \pmod{4}$, also (a).

m^2-1 und n^2-1 sind durch 8 teilbar, daher ist das Produkt durch 64 und damit insbesondere durch 16 teilbar. Aus $(m^2-1)(n^2-1) \equiv 0 \pmod{16}$ folgt aber $(mn)^2-1 \equiv (m^2-1) + (n^2-1) \pmod{16}$, und daraus (b). \square

Durch Induktion folgt aus diesem Lemma

Lemma 9.12. *Es seien $r_1, r_2, \dots, r_k \in \mathbb{Z}$ ungerade. Dann gilt*

$$(a) \sum_{i=1}^k \frac{r_i-1}{2} \equiv \frac{r_1 r_2 \dots r_k - 1}{2} \pmod{2}$$

$$(b) \sum_{i=1}^k \frac{r_i^2-1}{8} \equiv \frac{(r_1 r_2 \dots r_k)^2-1}{8} \pmod{2}$$

Beweis von Satz 9.10. Sei $m = p_1 p_2 \dots p_k$ und $n = q_1 q_2 \dots q_l$ mit nicht notwendig verschiedenen Primzahlen p_i und q_j . Wegen der Teilerfremdheit von m und n gilt allerdings $p_i \neq q_j$. Aus dem Quadratischen Reziprozitätsgesetz und den Eigenschaften des Jacobisymbols folgt

$$\begin{aligned} \left(\frac{m}{n}\right)\left(\frac{n}{m}\right) &= \prod_{i,j} \left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right) \\ &= \prod_{i,j} (-1)^{\frac{p_i-1}{2} \frac{q_j-1}{2}}. \end{aligned}$$

Nach dem vorigen Lemma gilt modulo 2:

$$\begin{aligned} \sum_{i,j} \frac{p_i - 1}{2} \frac{q_j - 1}{2} &= \left(\sum_i \frac{p_i - 1}{2} \right) \left(\sum_j \frac{q_j - 1}{2} \right) \\ &\equiv \frac{p_1 p_2 \dots p_k - 1}{2} \frac{q_1 q_2 \dots q_l - 1}{2} \\ &= \frac{m - 1}{2} \frac{n - 1}{2}, \end{aligned}$$

also

$$\prod_{i,j} (-1)^{\frac{p_i - 1}{2} \frac{q_j - 1}{2}} = (-1)^{\sum_{i,j} \frac{p_i - 1}{2} \frac{q_j - 1}{2}} = (-1)^{\frac{m-1}{2} \frac{n-1}{2}}.$$

Hieraus folgt (a). Die Aussagen (b) und (c) folgen mit entsprechenden Argumenten. \square

Bemerkung 9.13. Das Eulersche Kriterium überträgt sich nicht auf das Jacobisymbol. Für ungerade natürliche Zahlen n und sogar dazu teilerfremde ganze Zahlen a gilt im allgemeinen nicht $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}$. In der Tat kann man das Versagen dieser Kongruenz als Primzahltest benutzen, siehe den nächsten Abschnitt.

Das Jacobische Reziprozitätsgesetz können wir nun effizient zur Berechnung des Legendresymbols verwenden, wobei wir bis auf das billige Abspalten des Faktors 2 keine Zahlen faktorisieren müssen.

Beispiel 9.14. Im Beispiel von vorhin bei der Berechnung von $\left(\frac{53}{3001}\right)$ ist es also nicht nötig, im entsprechenden Zwischenschritt 33 zu faktorisieren, sondern wir können direkt rechnen:

$$\begin{aligned} \left(\frac{53}{3001}\right) &= \left(\frac{3001}{53}\right) = \left(\frac{33}{53}\right) = \left(\frac{53}{33}\right) = \left(\frac{20}{33}\right) \\ &= \left(\frac{2}{33}\right)^2 \left(\frac{5}{33}\right) = \left(\frac{5}{33}\right) = \left(\frac{33}{5}\right) = \left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1. \end{aligned}$$

10 Primzahltests

Der kleine Satz von Fermat legt einen möglichen Primzahltest nahe: Wir wollen die natürliche Zahl n auf die Primzahleigenschaft testen. Wie wählen eine ganze Zahl $a \neq 0$. Mit dem Euklidischen Algorithmus sieht man schnell, ob a und n teilerfremd sind. Ist $\text{ggT}(a, n) > 1$, aber a kein Vielfaches von n , dann ist n keine Primzahl und wir sind fertig.

Sei also $\text{ggT}(a, n) = 1$. Ist n eine Primzahl, dann ist $a^{n-1} \equiv 1 \pmod{n}$. Für diesen Test muss man im Übrigen nicht $n - 2$ Multiplikationen durchführen (dann wäre sogar das naive Probieren potentieller Teiler von 1 bis $\lfloor \sqrt{n} \rfloor$ noch billiger!), sondern man kann durch eine Binärentwicklung von n das Berechnen der Kongruenz auf die Größenordnung von $\log_2(n)$ Multiplikationen und Reduktionen modulo n reduzieren. (Man überlege sich die Details!) Ist $a^{n-1} \not\equiv 1 \pmod{n}$, dann wissen wir wenigstens, dass n keine Primzahl ist.

Allerdings hat dieser Test ein Problem: Leider gibt es natürliche Zahlen $n \geq 3$, die nicht prim sind, aber für die $a^{n-1} \equiv 1 \pmod{n}$ sogar für alle ganzen a mit $\text{ggT}(a, n) = 1$ gilt! Um das zu testen, muss man für a natürlich nur die Zahlen von 1 bis $n - 1$ überprüfen.

Definition 10.1. Die ungerade Zahl $n \geq 3$ heißt *Carmichael-Zahl*, falls sie keine Primzahl ist, aber dennoch $a^{n-1} \equiv 1 \pmod{n}$ für alle $1 \leq a \leq n-1$ mit $\text{ggT}(a, n) = 1$ gilt.

Man kann der Primfaktorzerlegung von n ansehen, ob n eine Carmichael-Zahl ist:

Satz 10.2. Die ungerade zusammengesetzte¹ Zahl $n \geq 3$ ist genau dann eine Carmichael-Zahl, wenn für jeden Primteiler p von n das folgende gilt: p^2 teilt nicht n , aber $p-1$ teilt $n-1$.

Beweis. Es sei n eine Carmichael-Zahl, und $p^k | n$ für eine Primzahl p und $k \geq 1$. Insbesondere gilt

$$a^{n-1} \equiv 1 \pmod{p^k}$$

für alle a mit $\text{ggT}(a, n) = 1$. Da p ungerade ist, gibt es eine Primitivwurzel a modulo p^k . Dabei können wir a so wählen, dass a teilerfremd ist zu n . (Z.B. mit dem Chinesischen Restsatz, oder in dieser Situation auch elementarer.) Wegen $\varphi(p^k) = (p-1)p^{k-1}$ ist also $(p-1)p^{k-1}$ die multiplikative Ordnung von a modulo p^k , d.h. $(p-1)p^{k-1}$ teilt $n-1$. Da p ein Teiler von n ist, kann p nicht auch $n-1$ teilen. Daher gilt $k=1$ und $p-1 | n-1$, und die eine Beweisrichtung folgt.

Sei nun n das Produkt verschiedener Primzahlen p , und $p-1 | n-1$ für jede dieser Primzahlen. Sei a teilerfremd zu n . Dann gilt $a^{p-1} \equiv 1 \pmod{p}$. Da aber $n-1$ ein Vielfaches von $p-1$ ist, gilt auch $a^{n-1} \equiv 1 \pmod{p}$, d.h. $a^{n-1} - 1$ ist durch alle Primteiler p von n teilbar, und damit auch durch das Produkt n dieser Primteiler teilbar. \square

Beispiel 10.3. Die kleinste Carmichael-Zahl ist $n = 561 = 3 \cdot 11 \cdot 17$. Beachte dass $n-1 = 560 = 2^4 \cdot 5 \cdot 7$ durch 2, 10 und 16 teilbar ist. Man weiß seit 1994, dass es unendlich viele Carmichael-Zahlen gibt.

Die Kongruenz $a^{n-1} \equiv 1 \pmod{n}$ ist das Quadrat der Kongruenz $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}$. Gilt also $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}$ für alle ganzen Zahlen a , die zur ungeraden Zahl n teilerfremd sind, dann ist insbesondere n eine Carmichael-Zahl. Man kann hoffen, dass die stärkere Kongruenz $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}$ auch für viele Carmichael-Zahlen nicht mehr gilt. Es ist sogar noch besser:

Satz 10.4. Die ungerade Zahl $n \geq 3$ ist genau dann eine Primzahl, wenn

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

für alle zu n teilerfremde Zahlen a mit $1 \leq a \leq n-1$ gilt.

Beweis. Ist n eine Primzahl, dann ist das einfach das Eulerkriterium.

Sei nun n keine Primzahl, und $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}$ für alle zu n teilerfremde Zahlen a . Wie oben schon bemerkt, gilt dann $a^{n-1} \equiv 1 \pmod{n}$ für all diese Zahlen a , d.h. n ist eine Carmichael-Zahl. Dann gilt $n = p_1 p_2 \dots p_r$ mit verschiedenen Primzahlen p_i . Sei a ein

¹zusammengesetzt = nicht prim

quadratischer Nichtrest modulo p_1 . Nach dem Chinesischen Restsatz können wir dabei a so wählen, dass $a \equiv 1 \pmod{p_i}$ für alle $i \geq 2$. Insbesondere gilt dann

$$\left(\frac{a}{p_1}\right) = -1 \text{ und } \left(\frac{a}{p_i}\right) = 1 \text{ für alle } i \geq 2.$$

Hieraus folgt $\left(\frac{a}{n}\right) = -1$, also $a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$ nach Voraussetzung und daher insbesondere $a^{\frac{n-1}{2}} \equiv -1 \pmod{p_2}$. Aber $a^{\frac{p_2-1}{2}} \equiv \left(\frac{a}{p_2}\right) = 1 \pmod{p_2}$, also $a^{\frac{n-1}{2}} \equiv 1 \pmod{p_2}$ da $p_2 - 1 | n - 1$, ein Widerspruch. \square

Für große Zahlen n ist das vorstehende Kriterium natürlich nicht effizient als Primzahltest benutzbar, da man ja möglicherweise alle Zahlen von 1 bis $n - 1$ durchtesten muss, was teurer ist, als die Zahlen von 1 bis $\lfloor \sqrt{n} \rfloor$ als Teiler von n zu testen. Die Bedeutung dieses Kriteriums wird durch den folgenden Satz geliefert.

Satz 10.5. *Die ungerade Zahl n sei keine Primzahl. Dann gilt die Kongruenz*

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

für höchstens die Hälfte der zu n teilerfremden Zahlen a zwischen 1 und $n - 1$.

Beweis. Nach dem vorigen Satz gibt es ein a mit $\text{ggT}(a, n) = 1$ und $a^{\frac{n-1}{2}} \not\equiv \left(\frac{a}{n}\right) \pmod{n}$. Es sei B die Menge der Zahlen b von 1 bis $n - 1$ mit $\text{ggT}(b, n) = 1$ und $b^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right) \pmod{n}$. Für alle $b \in B$ gilt dann

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

Betrachten wir a, B usw. modulo n , dann bildet die Bijektion $\bar{x} \mapsto \bar{a}\bar{x}$ von $(\mathbb{Z}/n\mathbb{Z})^*$ die Menge \bar{B} in das Komplement von \bar{B} in $(\mathbb{Z}/n\mathbb{Z})^*$ ab. Daher gilt $|B| \leq \varphi(n) - |B|$, und die Behauptung folgt. \square

Der obenstehende Satz ist ein probabilistischer Primzahltest im folgenden Sinn: Man prüft die Kongruenz $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}$ nacheinander für k zufällige zu n teilerfremde Zahlen a zwischen 1 und $n - 1$. Ist die Kongruenz einmal nicht erfüllt, dann ist n keine Primzahl. Gilt sie hingegen für alle k Zahlen a , dann ist n eine mögliche Primzahl, mit einer Irrtumswahrscheinlichkeit (im heuristischen Sinn) von höchstens $1/2^k$. Für vergleichsweise kleine k (etwa $k = 30$) kann man also die Wahrscheinlichkeit schon sehr klein halten.

Solche Tests helfen vor allem bei der Suche nach sehr großen Primzahlen, da man die meisten Nichtprimzahlen sehr schnell erkennt, und für die wenigen möglichen Primzahlen dann teurere Tests verwenden kann.

11 Dirichletscher Approximationssatz

Im folgenden wollen wir untersuchen, wie gut sich reelle Zahlen durch rationale Zahlen approximieren lassen. Im nächsten Abschnitt werden wir mit Dirichlets Satz sofort sehen, dass jede Primzahl p mit $p \equiv 1 \pmod{4}$ eine Summe von zwei Quadratzahlen ist.

Ist ζ reell und $q \in \mathbb{N}$, dann gibt es natürlich ein $p \in \mathbb{Z}$ mit $|\zeta - \frac{p}{q}| < \frac{1}{q}$, man nehme etwa $p = [\zeta q]$. Etwas tiefer und wesentlich anwendungsreicher ist folgender Satz:

Satz 11.1 (Dirichlet). *Es sei $\zeta \in \mathbb{R}$ und $n \in \mathbb{N}$. Dann gibt es ganze Zahlen p, q mit $1 \leq q \leq n$ mit*

$$|\zeta - \frac{p}{q}| \leq \frac{1}{q(n+1)}.$$

Beweis. Dem Beweis liegt folgende anschauliche Idee zugrunde: Auf einem Kreis vom Umfang 1 tragen wir, startend mit einem 0-Punkt, die Punkte $0\zeta, 1\zeta, 2\zeta, \dots, n\zeta$ ab. Da sich die Segmente zwischen zwei aufeinander folgenden Punkten zum Kreisumfang 1 aufaddieren und wir $n+1$ Punkte haben, muss es zwei Punkte $k\zeta$ und $l\zeta$ mit $k \neq l$ geben, die auf der Kreislinie einen Abstand $\leq \frac{1}{n+1}$ haben. Es gibt also eine ganze Zahl p mit $|k\zeta - l\zeta - p| \leq \frac{1}{n+1}$ und daraus folgt dann die Behauptung. Das folgende ist die gleiche Idee, nur etwas formaler aufgeschrieben:

Für reelles x gilt $0 \leq x - [x] < 1$. Wir ordnen die $n+1$ Zahlen $k\zeta - [k\zeta]$, $k = 0, 1, \dots, n$, nach aufsteigender Größe und bezeichnen sie mit $0 = a_0 \leq a_1 \leq a_2 \leq \dots \leq a_n < 1$. Wir unterscheiden zwei Fälle:

(a) Es gilt $a_n \leq 1 - \frac{1}{n+1}$. In der Teleskopsumme

$$\sum_{i=1}^n (a_i - a_{i-1}) = a_n - a_0 = a_n \leq 1 - \frac{1}{n+1}$$

sind alle n Summanden ≥ 0 . Daher gibt es ein i mit

$$0 \leq a_i - a_{i-1} \leq \frac{1}{n} \left(1 - \frac{1}{n+1}\right) = \frac{1}{n+1}.$$

Seien $k \neq l$ mit $a_i = k\zeta - [k\zeta]$ und $a_{i-1} = l\zeta - [l\zeta]$. Es gilt also

$$0 \leq (k-l)\zeta - p \leq \frac{1}{n+1}$$

mit $p = [k\zeta] - [l\zeta] \in \mathbb{Z}$. Aus

$$|\zeta - \frac{p}{k-l}| \leq \frac{1}{|k-l|(n+1)}$$

und $1 \leq |k-l| \leq n$ folgt in diesem Fall die Behauptung.

(b) Es gilt $a_n > 1 - \frac{1}{n+1}$, also $0 < 1 - a_n < \frac{1}{n+1}$. Sei k gewählt mit $a_n = k\zeta - [k\zeta]$. Dann gilt

$$0 < 1 - k\zeta + [k\zeta] < \frac{1}{n+1},$$

mit $p = -1 - [k\zeta]$ folgt also

$$|\zeta - \frac{p}{k}| < \frac{1}{k(n+1)},$$

was zu zeigen war.

□

Eine typische Anwendung ist

Satz 11.2. Die reelle Zahl ζ sei irrational. Dann gilt

$$\left| \zeta - \frac{p}{q} \right| < \frac{1}{q^2}$$

für unendlich viele $p, q \in \mathbb{Z}$.

Beweis. Es gibt mindestens eine Lösung dieser Ungleichung, z.B. $p = [\zeta]$, $q = 1$. Wir zeigen nun, dass es für jede endliche Menge (p_i, q_i) , $i = 1, \dots, m$, von Lösungen eine weitere Lösung (p, q) gibt, woraus dann die Behauptung folgt.

Sei also $\left| \zeta - \frac{p_i}{q_i} \right| < \frac{1}{q_i^2}$ für $i = 1, 2, \dots, m$. Da ζ irrational ist, gilt $\left| \zeta - \frac{p_i}{q_i} \right| \neq 0$. Sei $n \in \mathbb{N}$ mit $n > \frac{1}{\left| \zeta - \frac{p_i}{q_i} \right|}$ für alle i . Nach dem vorigen Satz gibt es $p, q \in \mathbb{Z}$ mit $1 \leq q \leq n$ und

$$\left| \zeta - \frac{p}{q} \right| \leq \frac{1}{q(n+1)} < \frac{1}{q^2}.$$

Wegen $\left| \zeta - \frac{p}{q} \right| \leq \frac{1}{n+1} < \left| \zeta - \frac{p_i}{q_i} \right|$ gilt $(p, q) \neq (p_i, q_i)$ für alle i . □

12 Quadratsummen

In diesem Abschnitt wollen wir sehen, welche natürlichen Zahlen Summen von 2 bzw. 4 Quadratzahlen sind. Wir beginnen mit

Satz 12.1. Jede Primzahl p mit $p \equiv 1 \pmod{4}$ hat eine Darstellung $p = a^2 + b^2$ mit $a, b \in \mathbb{N}$.

Beweis. Wir suchen $a, b \in \mathbb{N}$ mit $a^2 + b^2 = p$. Falls $a^2 + b^2 = p$, dann gilt $a^2 \equiv -b^2 \pmod{p}$ und $b \not\equiv 0 \pmod{p}$. Sei $b' \in \mathbb{Z}$ multiplikativ invers zu b modulo p . Dann gilt $(ab')^2 \equiv -1 \pmod{p}$, also $\left(\frac{-1}{p}\right) = 1$.

Das gibt einen Hinweis, wie man a und b bestimmen kann. Wegen $p \equiv 1 \pmod{4}$ gilt tatsächlich $\left(\frac{-1}{p}\right) = 1$, und wir finden ein $c \in \mathbb{N}$ mit $c^2 \equiv -1 \pmod{p}$. Nach den obigen Betrachtungen muss also $a \equiv bc \pmod{p}$, d.h. $a = bc - dp$ für ein $d \in \mathbb{N}$ gelten. Wir suchen also $a, d \in \mathbb{N}$ mit $p = a^2 + b^2 = (bc - dp)^2 + b^2$.

Setze $u := \lfloor \sqrt{p} \rfloor$. Für das gesuchte b muss $b \leq u$ gelten, und ferner $|bc - dp|^2 \leq p$, d.h. $\left| \frac{c}{p} - \frac{d}{b} \right| \leq \frac{1}{\sqrt{pb}}$. Aber im vorigen Abschnitt haben wir genau solche Ungleichungen studiert:

Sei also $c \in \mathbb{N}$ wie oben. Nach Satz 11.1, mit $\zeta = \frac{c}{p}$ und $n = u$, gibt es $b, d \in \mathbb{Z}$ mit

$$\left| \frac{c}{p} - \frac{d}{b} \right| \leq \frac{1}{(u+1)b} \text{ und } 1 \leq b \leq u.$$

Beachte dass $u+1 > \sqrt{p}$. Setze $a = |bc - dp|$. Es folgt

$$0 \leq a = bp \left| \frac{c}{p} - \frac{d}{b} \right| \leq \frac{p}{u+1} < \sqrt{p}$$

und

$$1 \leq b \leq u \leq \sqrt{p}.$$

Es gilt also

$$1 \leq a^2 + b^2 < 2p.$$

Wegen

$$a^2 + b^2 = (bc - dp)^2 + b^2 \equiv b^2(c^2 + 1) \equiv 0 \pmod{p}$$

ist aber $a^2 + b^2$ auch durch p teilbar, also $a^2 + b^2 = p$. \square

Im folgenden wollen wir klären, welche natürlichen Zahlen Summen von zwei Quadratzahlen sind. Zur Vorbereitung benötigen wir einige einfache Hilfsaussagen.

Lemma 12.2. Sind $n_1, n_2 \in \mathbb{N}$ Summe von zwei Quadratzahlen aus \mathbb{N}_0 , dann gilt das auch für $n_1 n_2$.

Beweis. Sei $n_i = a_i^2 + b_i^2$. Die Behauptung folgt dann aus

$$\begin{aligned} n_1 n_2 &= (a_1^2 + b_1^2)(a_2^2 + b_2^2) \\ &= (a_1 a_2 - b_1 b_2)^2 + (a_1 b_2 + a_2 b_1)^2. \end{aligned}$$

\square

Bemerkung 12.3. Der Beweis beruht auf einer algebraischen Identität, die eine einfache Interpretation hat: Seien a_1, a_2, b_1 und b_2 reell, und $i \in \mathbb{C}$ eine imaginäre Einheit, d.h. $i^2 = -1$. Dann gilt nach Pythagoras

$$|a_1 + ib_1|^2 = a_1^2 + b_1^2,$$

Der komplexe Betrag ist aber multiplikativ, d.h.

$$\begin{aligned} (a_1^2 + b_1^2)(a_2^2 + b_2^2) &= (|a_1 + ib_1||a_2 + ib_2|)^2 \\ &= |(a_1 + ib_1)(a_2 + ib_2)|^2 \\ &= |(a_1 a_2 - b_1 b_2) + i(a_1 b_2 + a_2 b_1)|^2 \\ &= (a_1 a_2 - b_1 b_2)^2 + (a_1 b_2 + a_2 b_1)^2. \end{aligned}$$

Lemma 12.4. Sei $n = a^2 + b^2$ mit $a, b \in \mathbb{N}_0$ und $\text{ggT}(a, b) = 1$. Dann hat n keinen Primteiler p mit $p \equiv 3 \pmod{4}$.

Beweis. Sei p ein Primteiler von n . Natürlich ist weder a noch b durch p teilbar. Es gilt $a^2 + b^2 \equiv 0 \pmod{p}$. Sei $c \in \mathbb{Z}$ mit $bc \equiv 1 \pmod{p}$. Es folgt $(ac)^2 \equiv -(bc)^2 \equiv -1 \pmod{p}$, also $p = 2$ oder $p > 2$ und $\left(\frac{-1}{p}\right) = -1$. Aber für $p > 2$ gilt $\left(\frac{-1}{p}\right) = -1 = (-1)^{\frac{p-1}{2}}$, also $p \equiv 1 \pmod{4}$. \square

Satz 12.5. Sei $n \in \mathbb{N}$. Die folgenden Aussagen sind äquivalent:

(i) Es gibt $a, b \in \mathbb{N}_0$ mit $n = a^2 + b^2$.

(ii) Jeder Primteiler p von n mit $p \equiv 3 \pmod{4}$ kommt mit einer geraden Vielfachheit in n vor.

Beweis. Es gelte (i). Setze $d = \text{ggT}(a, b)$. Dann gilt $d^2 | n$, und $\frac{n}{d^2} = (\frac{a}{d})^2 + (\frac{b}{d})^2$. Aber $\text{ggT}(\frac{a}{d}, \frac{b}{d}) = 1$, nach dem vorigen Lemma hat also $\frac{n}{d^2}$ keine Primfaktoren $\equiv 3 \pmod{4}$. Aus $n = d^2 \frac{n}{d^2}$ folgt (ii).

Nun gelte (ii). Dann gibt es eine Darstellung $n = p_1 p_2 \dots p_k d^2$, so dass die Primzahlen p_1, p_2, \dots, p_k entweder 2 oder $\equiv 1 \pmod{4}$ sind. Wir sahen aber schon, dass diese Primzahlen Summen von Quadraten sind. Aus Lemma 12.2 folgt (i). \square

Man sieht leicht, dass z.B. jede natürliche Zahl n mit $n \equiv 7 \pmod{8}$ keine Summe von 3 Quadratzahlen ist. Wir bereiten nun den Beweis des Satzes von Lagrange vor, dass jede natürliche Zahl allerdings die Summe von 4 Quadratzahlen ist.

Die Multiplikativität der Norm auf den Hamiltonschen Quaternionen liefert eine Identität, die zu obiger analog ist.

Lemma 12.6. *Es seien $a_i, b_i \in \mathbb{R}$ für $i = 1, 2, 3, 4$. Dann gilt*

$$(a_1^2 + a_2^2 + a_3^2 + a_4^2)(b_1^2 + b_2^2 + b_3^2 + b_4^2) = c_1^2 + c_2^2 + c_3^2 + c_4^2$$

mit

$$\begin{aligned} c_1 &= a_1 b_1 + a_2 b_2 + a_3 b_3 + a_4 b_4 \\ c_2 &= a_1 b_2 - a_2 b_1 + a_3 b_4 - a_4 b_3 \\ c_3 &= a_1 b_3 - a_3 b_1 + a_4 b_2 - a_2 b_4 \\ c_4 &= a_1 b_4 - a_4 b_1 + a_2 b_3 - a_3 b_2 \end{aligned}$$

Beweis. Nachrechnen. \square

Wegen $2 = 1^2 + 1^2 + 0^2 + 0^2$ müssen wir also nur zeigen, dass ungerade Primzahlen Summen von 4 Quadratzahlen sind.

Lemma 12.7. *Sei p eine ungerade Primzahl. Dann gibt $a, b \in \mathbb{Z}$ mit $0 \leq a, b \leq \frac{p-1}{2}$ und $a^2 + b^2 + 1 \equiv 0 \pmod{p}$.*

Beweis. Für $a = 0, 1, 2, \dots, \frac{p-1}{2}$ sind die Quadrate a^2 paarweise inkongruent modulo p . Denn aus $a^2 \equiv b^2 \pmod{p}$ folgt $p | (a-b)(a+b)$, also $a = b$ oder $|a-b| \geq p$ oder $a+b \geq p$, was aber wegen der Einschränkungen an a und b nicht möglich ist.

Sei \bar{x} die Restklasse von x modulo p .

Setze $A = \{\bar{a}^2 | 0 \leq a \leq \frac{p-1}{2}\}$, und $B = \{-1 - \bar{b}^2 | 0 \leq b \leq \frac{p-1}{2}\}$. Wir sahen, dass $|A| = \frac{p+1}{2}$, und natürlich gilt dann auch $|B| = \frac{p+1}{2}$. Wegen $|A| + |B| = p + 1 > p$ haben A und B einen nicht leeren Schnitt, es gibt also a, b mit $a^2 \equiv -1 - b^2 \pmod{p}$. Die Behauptung folgt. \square

Satz 12.8 (Lagrange 1770). *Jede natürliche Zahl ist eine Summe von vier Quadratzahlen.*

Beweis. Wegen Lemma 12.6 reicht es, die Aussage für Primzahlen p zu beweisen. Wegen $2 = 1^2 + 1^2 + 0^2 + 0^2$ dürfen wir auch $p \neq 2$ annehmen.

Nach Lemma 12.7 gibt es $a, b \in \mathbb{N}_0$ und $k \in \mathbb{Z}$ mit $a, b \leq \frac{p-1}{2}$, so dass $a^2 + b^2 + 1^2 + 0^2 = kp$. Offenbar gilt dabei $k \geq 1$, und

$$pk = a^2 + b^2 + 1 \leq 2\left(\frac{p-1}{2}\right)^2 + 1 < p^2,$$

also $k < p$.

Sei nun $k \in \mathbb{N}$ minimal, so dass es eine Darstellung $pk = a^2 + b^2 + c^2 + d^2$ mit $a, b, c, d \in \mathbb{Z}$ gibt. Wir müssen $k = 1$ zeigen. Gerade sahen wir, dass wenigstens $k < p$ gilt.

Wir machen eine Fallunterscheidung. Zunächst sei k gerade. Dann ist pk gerade, d.h. unter den Zahlen a, b, c, d sind genau 0, 2 oder 4 ungerade. Insbesondere können wir annehmen, dass $a \pm b$ und $c \pm d$ beide gerade sind. Wegen

$$\left(\frac{a+b}{2}\right)^2 + \left(\frac{a-b}{2}\right)^2 + \left(\frac{c+d}{2}\right)^2 + \left(\frac{c-d}{2}\right)^2 = \frac{1}{2}(a^2 + b^2 + c^2 + d^2) = \frac{k}{2}p$$

ist auch $\frac{k}{2}p$ eine Summe von 4 Quadratzahlen, im Widerspruch zur Minimalität von k .

Ab nun sei k ungerade, und $k > 1$, denn andernfalls sind wir fertig. Wähle $a' \in \mathbb{Z}$ mit

$$-\frac{k}{2} < a' < \frac{k}{2} \text{ und } a \equiv a' \pmod{k}.$$

Analog wähle b', c' und d' . Modulo k gilt

$$pk = a^2 + b^2 + c^2 + d^2 \equiv a'^2 + b'^2 + c'^2 + d'^2 \pmod{k},$$

also $a'^2 + b'^2 + c'^2 + d'^2 \equiv 0 \pmod{k}$. Die Zahlen a', b', c' und d' können nicht alle 0 sein, denn dann wären a, b, c und d durch k teilbar, also $pk = a^2 + b^2 + c^2 + d^2$ durch k^2 teilbar, und damit p durch k teilbar. Da p prim ist und $k > 1$ gilt, wäre $k = p$, im Widerspruch zu $k < p$.

Es gilt also

$$1 \leq a'^2 + b'^2 + c'^2 + d'^2 < 4\left(\frac{k}{2}\right)^2 = k^2.$$

Wir haben also

$$a'^2 + b'^2 + c'^2 + d'^2 = kk' \text{ mit } 1 \leq k' < k.$$

Wir benutzen die Identität aus Lemma 12.6, und erhalten

$$k^2 pk' = (pk)(kk') = (a^2 + b^2 + c^2 + d^2)(a'^2 + b'^2 + c'^2 + d'^2) = \tilde{a}^2 + \tilde{b}^2 + \tilde{c}^2 + \tilde{d}^2$$

mit z.B.

$$\tilde{b} = ab' - ba' + cd' - dc'.$$

Aus $a \equiv a' \pmod{k}$ und $b' \equiv b \pmod{k}$ folgt $ab' - ba' \equiv 0 \pmod{k}$, und analog $cd' - dc' \equiv 0 \pmod{k}$. Das ergibt $\tilde{b} \equiv 0 \pmod{k}$. Genauso folgt, dass auch \tilde{c} und \tilde{d} durch k teilbar sind. Da $\tilde{b}^2, \tilde{c}^2, \tilde{d}^2$ und $\tilde{a}^2 + \tilde{b}^2 + \tilde{c}^2 + \tilde{d}^2 = k^2 pk'$ alle durch k^2 teilbar sind, ist auch \tilde{a} durch k teilbar. Wir erhalten also

$$pk' = \left(\frac{\tilde{a}}{k}\right)^2 + \left(\frac{\tilde{b}}{k}\right)^2 + \left(\frac{\tilde{c}}{k}\right)^2 + \left(\frac{\tilde{d}}{k}\right)^2,$$

was wegen $k' < k$ wieder ein Widerspruch zur Minimalität von k ist.

Daher muss $k = 1$ gelten, und die Behauptung folgt. \square

13 Pythagoräische Tripel und Fermat Gleichung

Seien a, b, c ganzzahlige Seitenlängen eines rechtwinkligen Dreiecks. Dann gilt $a^2 + b^2 = c^2$. Ein Beispiel ist $3^2 + 4^2 = 5^2$. In diesem Abschnitt wollen wir alle Lösungen dieser Gleichung bestimmen.

Schon Fermat studierte diese Gleichung für höhere Exponenten, d.h. $a^n + b^n = c^n$ mit $a, b, c \in \mathbb{N}$ und $n \geq 3$. Er vermutete, dass es keine Lösungen gibt, konnte das aber nur für $n = 4$ beweisen. Nachdem der allgemeine Fall $n \geq 3$ für etwa 200 Jahre ungelöst blieb, wurde 1906 der Wolfskehl-Preis (100.000 Goldmark) für eine Lösung ausgesetzt. Erst 1995 konnte Andrew Wiles, mit Unterstützung seines Schülers Richard Taylor, dieses klassische Problem der Zahlentheorie lösen. Der Beweis benutzt viele moderne und tiefliegende Techniken der Zahlentheorie und Analysis, es gibt nur wenige Mathematiker, die ihn komplett verstehen.

Lemma 13.1. Sei $a^n + b^n = c^n$ mit $a, b, c, n \in \mathbb{N}$. Dann gilt $\text{ggT}(a, b) = \text{ggT}(a, c) = \text{ggT}(b, c) = \text{ggT}(a, b, c)$.

Beweis. Es ist klar, dass $\text{ggT}(a, b, c)$ jede der Zahlen $\text{ggT}(a, b)$, $\text{ggT}(a, c)$ und $\text{ggT}(b, c)$ teilt. Sei nun $d = \text{ggT}(a, b)$. Dann gilt $d^n | a^n$, $d^n | b^n$, also auch $d^n | a^n + b^n = c^n$, und daher $d | c$, d.h. $d | \text{ggT}(a, b, c)$. Analog folgt $\text{ggT}(a, c) | \text{ggT}(a, b, c)$, und $\text{ggT}(b, c) | \text{ggT}(a, b, c)$. \square

Definition. Ein Tripel (a, b, c) mit $a^n + b^n = c^n$ ($a, b, c, n \in \mathbb{N}$) heißt *primitiv*, falls $\text{ggT}(a, b, c) = 1$.

Ist $a^n + b^n = c^n$, und $d = \text{ggT}(a, b, c)$, dann ist $(\frac{a}{d}, \frac{b}{d}, \frac{c}{d})$ eine primitive Lösung der Fermat-Gleichung.

Im folgenden bestimmen wir die primitiven und damit auch alle ganzzahligen Lösungen der Gleichung $X^2 + Y^2 = Z^2$.

Satz 13.2. Sei $a^2 + b^2 = c^2$ mit $a, b, c \in \mathbb{N}$ und $\text{ggT}(a, b, c) = 1$. Dann ist a oder b gerade. Sei etwa a gerade. Dann gilt $a = 2uv$, $b = u^2 - v^2$, $c = u^2 + v^2$ für $u, v \in \mathbb{N}$ mit $u > v$ und $\text{ggT}(u, v) = 1$.

Beweis. Nach Lemma 13.1 sind a, b, c paarweise teilerfremd. Insbesondere sind a, b, c nicht alle gerade. Wegen $a^2 + b^2 \equiv c^2 \pmod{4}$ und $k^2 \equiv 0$ oder $1 \pmod{4}$ ist c ungerade und a oder b gerade. Sei also o.E. a gerade, und damit b ungerade. Wir erhalten

$$\left(\frac{a}{2}\right)^2 = \frac{c^2 - b^2}{4} = \frac{c+b}{2} \frac{c-b}{2}.$$

Sei $d = \text{ggT}(\frac{c+b}{2}, \frac{c-b}{2})$. Dann gilt $d | \frac{c+b}{2} + \frac{c-b}{2} = c$ und $d | \frac{c+b}{2} - \frac{c-b}{2} = b$, also $d | \text{ggT}(b, c) = 1$. Daher sind $\text{ggT}(\frac{c+b}{2}, \frac{c-b}{2})$ teilerfremd. Da das Produkt dieser teilerfremden Zahlen eine Quadratzahl ist, muss jeder der Faktoren eine Quadratzahl sein, also $\frac{c+b}{2} = u^2$ und $\frac{c-b}{2} = v^2$ mit $u, v \in \mathbb{N}$ und $u > v$.

Hieraus folgt $c = \frac{c+b}{2} + \frac{c-b}{2} = u^2 + v^2$, $b = \frac{c+b}{2} - \frac{c-b}{2} = u^2 - v^2$, und $a^2 = c^2 - b^2 = (c+b)(c-b) = 4u^2v^2$, also $a = 2uv$. Aus dieser Darstellung sieht man auch, dass $\text{ggT}(u, v) | \text{ggT}(a, b, c) = 1$, also $\text{ggT}(u, v) = 1$. \square

Der Fall $n = 3$ der Fermat–Gleichung ließe sich mit einigem Aufwand noch im Rahmen einer Vorlesung in elementarer Zahlentheorie machen. Wesentlich einfacher ist allerdings der Fall $n = 4$. Wir beweisen sogar eine stärkere Aussage:

Satz 13.3. *Die Gleichung $X^4 + Y^4 = Z^2$ hat keine Lösung in \mathbb{N} .*

Beweis. Sei (x, y, z) eine Lösung mit z minimal. Aus dieser Lösung werden wir eine (bezüglich z) kleinere Lösung konstruieren, im Widerspruch zur Wahl einer minimalen Lösung.

Es gilt $\text{ggT}(x, y, z) = 1$: Sei $p \mid \text{ggT}(x, y, z)$ für eine Primzahl p . Dann ist p^4 ein Teiler von x^4 und y^4 , also auch von z^2 . Somit gilt $p^2 \mid z$, und $(\frac{x}{p}, \frac{y}{p}, \frac{z}{p^2})$ ist eine kleinere Lösung, ein Widerspruch.

Wegen $(x^2)^2 + (y^2)^2 = z^2$ ist daher (x^2, y^2, z) eine primitive Lösung der pythagoräischen Gleichung. Nach Satz 13.2 gibt es also teilerfremde $u, v \in \mathbb{N}$ mit $x^2 = 2uv$, $y^2 = u^2 - v^2$, $z = u^2 + v^2$. (Falls x ungerade ist, dann vertauschen wir x mit y .)

Wegen $y^2 \equiv 1 \pmod{4}$ ist u ungerade und v gerade.

Aus $(\frac{x}{2})^2 = u\frac{v}{2}$ und $\text{ggT}(u, \frac{v}{2}) = 1$ folgt $u = d^2$, $v = 2e^2$ mit $d, e \in \mathbb{N}$ und $\text{ggT}(d, e) = 1$.

Wir haben also $y^2 = u^2 - v^2 = d^4 - (2e^2)^2$, und somit $(2e^2)^2 + y^2 = (d^2)^2$.

Daher ist $(2e^2, y, d^2)$ eine primitive Lösung der Pythagoras–Gleichung.

Wiederum mit Satz 13.2 folgt

$$2e^2 = 2lm, \quad d^2 = l^2 + m^2$$

mit $l, m \in \mathbb{N}$ und $\text{ggT}(l, m) = 1$. Wegen $e^2 = lm$ und der Teilerfremdheit von l und m gilt $l = r^2$, $m = s^2$ für $r, s \in \mathbb{N}$, also

$$r^4 + s^4 = d^2.$$

Aber

$$d \leq d^2 = u < u^2 < u^2 + v^2 = z,$$

im Widerspruch zur Wahl von z . □

14 Pellische Gleichungen

Eine Pellische Gleichung hat die Form $X^2 - dY^2 = 1$ für eine ganze Zahl d , wobei man sich für ganzzahlige Lösungen dieser Gleichung interessiert.

Pellische Gleichungen haben viele Beziehungen zu anderen Gebieten der Zahlentheorie und Algebra, wie etwa Kettenbrüchen und Einheitengruppen quadratischer Zahlkörper. So tauchten sie schon vor über 2000 Jahren in der indischen und griechischen Mathematik im Zusammenhang mit der rationalen Approximation von Quadratwurzeln auf. Ist nämlich $a^2 - db^2 = 1$ für große a und b , dann ist $\frac{a}{b}$ eine gute Approximation von \sqrt{d} . Ein schon in der Antike vorkommendes Beispiel ist $577^2 - 2 \cdot 408^2 = 1$, man vergleiche $\frac{577}{408} = 1,414215\dots$ mit $\sqrt{2} = 1,414213\dots$

Ist d negativ, dann hat die Pellische Gleichung nur langweilige Lösungen. Auch wenn $d = e^2$ eine Quadratzahl ist, dann gilt $1 = X^2 - dY^2 = (X - eY)(X + eY)$. In einer ganzzahligen Lösung sind also beide Faktoren gleich 1 oder -1 , es gibt also nur die triviale Lösung $(\pm 1, 0)$.

Daher setzt man beim Studium Pellischer Gleichungen meist voraus, dass $d \in \mathbb{N}$ keine Quadratzahl ist.

Unter dieser Voraussetzung wollen wir den Satz von Lagrange beweisen, dass die Pellische Gleichung unendlich viele ganzzahlige Lösungen besitzt. In einem gewissen Sinne werden wir die Lösungsmenge, in Abhängigkeit von einer minimalen und nicht immer einfach bestimm- baren Lösung, auch explizit beschreiben.

Vorher benötigen wir eine schwächere Version, den wir mit Dirichlets Approximationsatz beweisen.

Lemma 14.1. *Sei $d \in \mathbb{N}$ keine Quadratzahl. Dann gibt es ein $0 \neq m \in \mathbb{Z}$, so dass die Gleichung $X^2 - dY^2 = m$ unendlich viele Lösungen $x, y \in \mathbb{Z}$ hat.*

Beweis. Da \sqrt{d} irrational ist, gibt es nach Satz 11.2 unendlich viele Paare (x, y) mit $x \in \mathbb{Z}$, $y \in \mathbb{N}$ und $|x - \sqrt{d}y| < \frac{1}{y}$. Zusammen mit $|x + \sqrt{d}y| = |x - \sqrt{d}y + 2\sqrt{d}y| \leq \frac{1}{y} + 2\sqrt{d}y$ folgt

$$|x^2 - dy^2| < \frac{1}{y} \left(\frac{1}{y} + 2\sqrt{d}y \right) = \frac{1}{y^2} + 2\sqrt{d} \leq 1 + 2\sqrt{d}.$$

Für die unendlich vielen betrachteten Paare (x, y) ist also $x^2 - dy^2$ nach unten und oben be- schränkt, d.h. mindestens ein Wert $m \in \mathbb{Z}$ tritt unendlich oft auf. Dabei ist $m \neq 0$, da d keine Quadratzahl ist. \square

Definition 14.2. Sei $d \in \mathbb{N}$ keine Quadratzahl. Die Menge $\mathbb{Z}[\sqrt{d}]$ der Zahlen von der Form $r + s\sqrt{d}$ mit $r, s \in \mathbb{Z}$ bildet offenbar einen Teilring von \mathbb{R} . Man rechnet sofort nach, dass die Abbildung $\prime : \mathbb{Z}[\sqrt{d}] \rightarrow \mathbb{Z}[\sqrt{d}]$, $(r + s\sqrt{d})' := (r - s\sqrt{d})$ ein Ringautomorphismus von $\mathbb{Z}[\sqrt{d}]$ ist. Wir setzen $N(x) := xx'$. Dann gilt $N(r + s\sqrt{d}) = (r + s\sqrt{d})(r - s\sqrt{d}) = r^2 - ds^2 \in \mathbb{Z}$. Da \prime multiplikativ ist, ist auch N multiplikativ.

Da 1 und \sqrt{d} über \mathbb{Q} linear unabhängig sind, hat jedes Element aus $\mathbb{Z}[\sqrt{d}]$ eine eindeutige Darstellung $r + s\sqrt{d}$ mit $r, s \in \mathbb{Z}$.

Satz 14.3. *Sei $d \in \mathbb{N}$ keine Quadratzahl. Dann hat $X^2 - dY^2 = 1$ unendlich viele ganzzahlige Lösungen. Ferner gibt es eine Lösung (x_1, y_1) , so dass jede Lösung die Form $(\pm x_n, \pm y_n)$ mit $x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n$ für ein $n \in \mathbb{N}_0$ hat.*

Beweis. Gemäß dem vorigen Satz wählen wir $0 \neq m \in \mathbb{Z}$ so, dass $X^2 - dY^2 = m$ unendlich viele ganzzahlige Lösungen hat. Nach dem Schubfachprinzip gibt es zwei verschiedene Lösungen (x_1, y_1) und (x_2, y_2) mit $x_i, y_i \in \mathbb{N}$ mit $x_1 \equiv x_2 \pmod{m}$ und $y_1 \equiv y_2 \pmod{m}$. Wir setzen $\alpha = x_1 - y_1\sqrt{d}$ und $\beta = x_2 - y_2\sqrt{d}$. Wir berechnen

$$\begin{aligned} \alpha\beta' &= (x_1 - y_1\sqrt{d})(x_2 + y_2\sqrt{d}) \\ &= (x_1x_2 - y_1y_2d) + (x_1y_2 - y_1x_2)\sqrt{d} \\ &=: A + B\sqrt{d} \end{aligned}$$

Aber

$$A \equiv x_1^2 - dy_1^2 = m \equiv 0 \pmod{m},$$

und $B \equiv 0 \pmod{m}$. Daher teilt m sowohl A als auch B , d.h. $\alpha\beta' = m(x + y\sqrt{d})$ mit $x, y \in \mathbb{Z}$. Wegen $N(\alpha) = N(\beta') = m$ gilt

$$m^2 = N(\alpha)N(\beta') = N(\alpha\beta') = m^2(x^2 - dy^2),$$

also $x^2 - dy^2 = 1$. Dabei gilt $y \neq 0$, denn andernfalls wäre $x = \pm 1$, also $\pm m = \alpha\beta'$. Multiplikation mit β liefert $\pm m\beta = \alpha\beta\beta' = \alpha N(\beta) = \alpha m$, also $\alpha = \pm\beta$. Dann aber gilt $x_1 = x_2$, und dann auch $y_1 = y_2$, ein Widerspruch.

Wir haben also eine Lösung (x, y) mit $x, y \in \mathbb{N}$ der Pellischen Gleichung gefunden. Wir müssen nun zeigen, dass alle Lösungen von der angegebenen Form sind. Für jede Zahl $M \in \mathbb{R}$ gibt es nur endlich viele Paare (x, y) natürlicher Zahlen mit $x + y\sqrt{d} < M$. Insgesamt gibt es also unter den Lösungen (x, y) der Pellischen Gleichung (mit $x, y \in \mathbb{N}$) eine, in der $x + y\sqrt{d}$ minimal ist. Da \sqrt{d} irrational ist, ist diese minimale Lösung eindeutig. Im folgenden sei (x, y) diese minimale Lösung, und $u, v \in \mathbb{N}$ eine weitere Lösung, d.h. $u^2 - dv^2 = 1$. Wir setzen $\alpha = x + y\sqrt{d}$ und $\beta = u + v\sqrt{d}$, und müssen also zeigen, dass es ein $n \in \mathbb{N}$ gibt mit $\beta = \alpha^n$.

Wir nehmen an, dass es eine solche Zahl n nicht gibt. Wegen $\alpha < \beta$ und $\alpha = x + y\sqrt{d} > 1$ gibt es ein $n \in \mathbb{N}$ mit

$$\alpha^n < \beta < \alpha^{n+1}.$$

Wegen $\alpha\alpha' = N(\alpha) = 1$ und $\alpha' = \frac{1}{\alpha} > 0$ folgt nach Multiplikation mit α'

$$1 = \alpha^n \alpha'^n < \beta \alpha'^n < \alpha(\alpha\alpha')^n = \alpha.$$

Es gilt $\beta\alpha'^n = A + B\sqrt{d}$ mit $A, B \in \mathbb{Z}$. Wegen $N(A + B\sqrt{d}) = N(\beta)N(\alpha')^n = 1$ gilt $A^2 - dB^2 = 1$, und obige Ungleichung zeigt $1 < A + B\sqrt{d} < \alpha$. Insbesondere gilt $A + B\sqrt{d} > 0$, und damit auch $A - B\sqrt{d} = \frac{1}{A + B\sqrt{d}} > 0$. Addition dieser zwei Ungleichungen zeigt $A > 0$, also $A \geq 1$. Wegen $A + B\sqrt{d} > 1$ und $1 = (A + B\sqrt{d})(A - B\sqrt{d})$ gilt $A - B\sqrt{d} < 1$, also $B\sqrt{d} > A - 1 \geq 0$ und daher $B \geq 1$. Zusammen haben wir also $1 < A + B\sqrt{d} < \alpha$ mit $A, B \in \mathbb{N}$ und $A^2 - dB^2 = 1$, im Widerspruch zur Minimalität von α . \square

Bemerkung. Die Lösung (x_1, y_1) aus dem Satz nennt man *Fundamentallösung*. Auch schon für relativ kleine Werte von d kann es schwierig sein, sie zu bestimmen. So ist z.B. $(x_1, y_1) = (32188120829134849, 1819380158564160)$ die Fundamentallösung zu $X^2 - 313Y^2 = 1$.

15 Quadratische Kurven

Eine quadratische Kurve über \mathbb{Q} ist die Nullstellenmenge in \mathbb{R}^2 eines Polynoms der Form

$$Q(X, Y) = AX^2 + BXY + CY^2 + DX + EY + F$$

mit $A, B, C, D, E, F \in \mathbb{Q}$, wobei eine der Zahlen A, B, C nicht verschwindet.

Wir interessieren uns für rationale Punkte $(x, y) \in \mathbb{Q}^2$ auf dieser Kurve. Ein alter Trick von Diophant erlaubt es, aus der Kenntnis eines einzigen solchen Punktes alle rationalen Punkte zu gewinnen:

Sei (x_0, y_0) ein rationaler Punkt auf der Kurve. Für jeden anderen rationalen Punkt (x_1, y_1) hat die Gerade durch (x_0, y_0) und (x_1, y_1) entweder rationale Steigung, oder ist senkrecht falls

$x_0 = x_1$. Man erhält also rationale Punkte auf folgende Weise: Sei $Y = y_0 + t(X - x_0)$ die Gerade durch (x_0, y_0) mit rationaler Steigung t . Einsetzen von $Y = y_0 + t(X - x_0)$ in die Gleichung $AX^2 + BXY + CY^2 + DX + EY + F = 0$ liefert ein Polynom vom Grad ≤ 2 in X mit rationalen Koeffizienten. Ist der Grad 2, so ist eine Nullstelle x_0 , und es gibt eine weitere Nullstelle x_t (eventuell $x_t = x_0$ im Fall einer doppelten Nullstelle). Nach Vieta ist $x_0 + x_t$ rational, also $x_t \in \mathbb{Q}$. Einsetzen in die Geradengleichung liefert schließlich den rationalen Punkt (x_t, y_t) auf der Kurve.

Ein Sonderfall ist die senkrechte Gerade $X = x_0$. Einsetzen in die Kurvengleichung liefert ein (höchstens) quadratisches Polynom in Y . Eine Nullstelle ist y_0 , wie oben gewinnen wir also den anderen Punkt auf dieser Geraden (sofern es ihn gibt).

Beispiel. Die Frage nach den ganzzahligen Lösungen der Pythagorasgleichung $X^2 + Y^2 = Z^2$ ist äquivalent zur Frage nach den rationalen Lösungen der Gleichung $X^2 + Y^2 = 1$. Ein Punkt dieser Gleichung $(x_0, y_0) = (0, -1)$. Die Gerade mit Steigung t durch diesen Punkt hat die Form $Y = -1 + tX$. Einsetzen liefert

$$X^2 + (-1 + tX)^2 = 1,$$

also

$$X((t^2 + 1)X - 2t) = 0.$$

Die Lösung $x = 0$ liefert nur die Punkte $(0, \pm 1)$. Für $X \neq 0$ erhalten wir

$$x_t = \frac{2t}{t^2 + 1} \text{ und } y_t = -1 + tx_t = \frac{t^2 - 1}{t^2 + 1},$$

d.h. neben $(0, \pm 1)$ ist die Menge der rationalen Punkte durch $(x_t, y_t) = (\frac{2t}{t^2+1}, \frac{t^2-1}{t^2+1})$ ($0 \neq t \in \mathbb{Q}$) parametrisiert.

Wir haben gesehen, dass wir alle rationalen Punkte der Kurve $Q(X, Y) = 0$ bestimmen können, sobald wir einen kennen. Schwieriger ist die Frage zu entscheiden, ob die Kurve $Q(X, Y) = 0$ rationale Punkte hat. Die Existenz hängt stark von Q ab, so ist etwa $X^2 + Y^2 + 1$ für rationale Argumente stets positiv, verschwindet also nie. Aber auch $X^2 - 2Y^2 = 0$ hat keine rationale Punkte, da $\sqrt{2}$ irrational ist.

Durch eine Folge von Substitutionen können wir die Gleichung $Q(X, Y) = 0$ vereinfachen. Ist $A = C = 0$, dann kommen X und Y nur linear vor, und die Gleichung ist natürlich lösbar. Sei also o.E. $A \neq 0$. Nach Division mit A dürfen wir $A = 1$ annehmen. Die Substitution $X = X' - \frac{B}{2}Y$ führt auf die Kurve $0 = Q'(X', Y) = X'^2 + C'Y^2 + D'X' + E'Y + F'$, die natürlich genau dann einen rationalen Punkt hat, wenn die ursprüngliche Kurve einen hat.

Ist $C' = 0$, dann kommt wieder Y nur linear vor, und die Kurve hat einen rationalen Punkt. Sei also $C' \neq 0$. Die Substitution $X' = X'' - \frac{D'}{2}$, $Y = Y - \frac{E'}{2C'}$ führt auf die Gleichung $X''^2 + C''Y^2 + F'' = 0$.

Die Fälle $C'' = 0$ oder $F'' = 0$ sind wieder langweilig, wir nehmen also $C'', F'' \neq 0$ an. Wir schreiben die gesuchten rationalen Punkte in der Form $(\frac{x}{z}, \frac{y}{z})$ mit $x, y \in \mathbb{Z}$, $z \in \mathbb{Z} \setminus \{0\}$. Nach Multiplikation mit dem Hauptnenner von C'' und F'' führt das auf die Gleichung der Form

$$aX^2 + bY^2 + cZ^2 = 0,$$

mit $a, b, c \in \mathbb{Z} \setminus \{0\}$, für die wir ganzzahlige Lösungen (x, y, z) mit $(x, y, z) \neq (0, 0, 0)$ suchen. Solche ganzzahligen Lösungen existieren natürlich genau dann, wenn es rationale Lösungen $(x, y, z) \neq (0, 0, 0)$ dieser Gleichung gibt.

Wir dürfen a, b und c als paarweise teilerfremd annehmen: Sei etwa $d = \text{ggT}(a, b) > 1$. Die Substitution $X = \frac{X'}{d}, Y = \frac{Y'}{d}$ führt auf $a'X'^2 + b'Y'^2 + c'Z^2 = 0$ mit $a' = \frac{a}{d}, b' = \frac{b}{d}, c' = cd$. Wegen $a'b'c' = \frac{abc}{d} < abc$ erreicht man nach endlich vielen Schritten dieser Art paarweise Teilerfremdheit der Koeffizienten.

Desweiteren dürfen wir die Koeffizienten als quadratfrei voraussetzen, denn ist etwa $a = a'u^2$ mit quadratfreiem a' , dann kann man die Substitution $X = \frac{X'}{u}$ machen.

Zur Beantwortung der Ausgangsfrage müssen wir also untersuchen, wann die Gleichung $aX^2 + bY^2 + cZ^2 = 0$ eine nicht triviale ganze Lösung hat, wobei $a, b, c \in \mathbb{Z}$ quadratfrei und paarweise teilerfremd sind. Haben a, b und c alle das gleiche Vorzeichen, dann hat die Gleichung natürlich keine nicht triviale Lösung. Wir dürfen also $a, b > 0$ und $c < 0$ annehmen.

Die Lösbarkeit solcher Gleichungen beantwortet der folgende

Satz 15.1 (Legendre). *Seien $a, b, c \in \mathbb{N}$ quadratfrei und paarweise teilerfremd. Dann sind die folgenden beiden Aussagen äquivalent:*

- (i) *Die Gleichung $aX^2 + bY^2 - cZ^2 = 0$ hat eine nicht triviale ganzzahlige Lösung.*
- (ii) *Es existieren $u, v, w \in \mathbb{Z}$ mit*

$$\begin{aligned} u^2 &\equiv bc \pmod{a} \\ v^2 &\equiv ca \pmod{b} \\ w^2 &\equiv -ab \pmod{c}. \end{aligned}$$

Beweis. Wir zeigen zunächst die einfache Richtung (i) \implies (ii):

Sei $ax^2 + by^2 - cz^2 = 1$ mit $x, y, z \in \mathbb{Z}$ und $(x, y, z) \neq (0, 0, 0)$. Wir dürfen $\text{ggT}(x, y, z) = 1$ annehmen. Es gilt $\text{ggT}(a, y) = 1$: Falls das nicht der Fall wäre, dann gäbe es eine Primzahl p mit $p | \text{ggT}(a, y)$. Dann gilt $p | cz^2$, also $p | z^2$ wegen $\text{ggT}(a, c) = 1$. Hieraus folgt $p | z$, also $p | x$ und somit $p^2 | z^2$. Zusammen mit $p^2 | y^2$ folgt $p^2 | ax^2$, also $p | x^2$, da a quadratfrei ist. Es folgt $p | x$, also schließlich der Widerspruch $p | \text{ggT}(x, y, z) = 1$.

Es gilt also $\text{ggT}(a, y) = 1$. Daher ist y modulo a invertierbar, d.h. es gibt ein $y' \in \mathbb{Z}$ mit $yy' \equiv 1 \pmod{a}$. Modulo a gilt

$$0 = cy'^2(ax^2 + by^2 - cz^2) \equiv bcy^2y'^2 - c^2z^2y'^2 \equiv bc - (czy')^2 \pmod{a},$$

d.h. bc ist ein Quadrat modulo a . Analog folgen die anderen zwei Kongruenzen.

Zum Beweis von (ii) \implies (i) seien nun u, v und w wie in (ii). Sind $f(X, Y, Z)$ und $g(X, Y, Z)$ Polynome über \mathbb{Z} und $n \in \mathbb{N}$, dann bedeutet $f(X, Y, Z) \equiv g(X, Y, Z) \pmod{n}$, dass die entsprechenden Koeffizienten von f und g modulo n übereinstimmen.

Polynome der Form $l(X, Y, Z) = rX + sY + tZ$ mit r, s, t nennen wir linear und homogen über \mathbb{Z} .

Wir zeigen nun, dass es für jeden Primteiler p von abc lineare homogene Polynome l_p und m_p über \mathbb{Z} gibt mit

$$aX^2 + bY^2 - cZ^2 \equiv l_p(X, Y, Z)m_p(X, Y, Z) \pmod{p}.$$

Dazu sei zum Beispiel $p|c$. Wegen $w^2 \equiv -ab \pmod{c}$ gilt insbesondere $w^2 \equiv -ab \pmod{p}$. Sei $a' \in \mathbb{Z}$ mit $aa' \equiv 1 \pmod{p}$, also $b \equiv -a'w^2 \pmod{p}$. Modulo p folgt

$$\begin{aligned} aX^2 + bY^2 - cZ^2 &\equiv aX^2 + bY^2 \\ &\equiv aX^2 - a'w^2Y^2 \\ &\equiv aX^2 - aa'^2w^2Y^2 \\ &\equiv a(X^2 - (a'wY)^2) \\ &\equiv a(X - a'wY)(X + a'wY) \pmod{p}, \end{aligned}$$

in diesem Fall können wir also $l_p = a(X - a'wY)$ und $m_p = X + a'wY$ wählen. Die Fälle $p|b$ und $p|a$ behandelt man analog.

Anwenden des Chinesischen Restsatzes auf die Koeffizienten von l_p und m_p für die Primteiler p von abc liefert lineare homogene Polynome $l(X, Y, Z)$ und $m(X, Y, Z)$ über \mathbb{Z} mit

$$l(X, Y, Z) \equiv l_p(X, Y, Y) \pmod{p} \text{ und } m(X, Y, Z) \equiv m_p(X, Y, Y) \pmod{p}$$

für alle Primteiler p von abc . Für diese Primteiler gilt also

$$aX^2 + bY^2 - cZ^2 \equiv l(X, Y, Z)m(X, Y, Z) \pmod{p}.$$

Da abc quadratfrei ist, ist die Zahl abc das Produkt ihrer Primteiler. Hieraus folgt

$$aX^2 + bY^2 - cZ^2 \equiv l(X, Y, Z)m(X, Y, Z) \pmod{abc}.$$

Wir betrachten die Menge

$$S = \{(x, y, z) \in \mathbb{N}_0^3 \mid x < \sqrt{bc}, y < \sqrt{ca}, z < \sqrt{ab}\}.$$

Da für $(a, b, c) = 1$ nichts zu beweisen ist, sei dieser Fall im folgenden ausgeschlossen. Für positive reelle α ist die Anzahl der ganzzahligen x mit $0 \leq x < \alpha$ stets $\geq \alpha$, und sogar $> \alpha$, falls α irrational ist. Wegen unserer Annahme über a, b und c ist mindestens eine der Zahlen \sqrt{bc} , \sqrt{ca} oder \sqrt{ab} irrational, also

$$|S| > \sqrt{bc} \sqrt{ca} \sqrt{ab} = abc.$$

Nach dem Schubfachprinzip gibt es also zwei verschiedene Tripel (x_1, y_1, z_1) und (x_2, y_2, z_2) in S mit

$$l(x_1, y_1, z_1) \equiv l(x_2, y_2, z_2) \pmod{abc}.$$

Für $x = x_1 - x_2, y = y_1 - y_2, z = z_1 - z_2$ gilt also $(x, y, z) \neq (0, 0, 0)$ und

$$l(x, y, z) \equiv 0 \pmod{abc},$$

also

$$ax^2 + by^2 - cz^2 \equiv l(x, y, z)m(x, y, z) \equiv 0 \pmod{abc}.$$

Aus den Ungleichungen für x_1, x_2, y_1 usw. folgt

$$|x| < \sqrt{bc}, |y| < \sqrt{ca}, |z| < \sqrt{ab}.$$

also

$$-abc < ax^2 + by^2 - cz^2 < 2abc.$$

Wir sahen aber auch, dass $ax^2 + by^2 - cz^2$ durch abc teilbar ist. Daher gilt entweder $ax^2 + by^2 - cz^2 = 0$, oder $ax^2 + by^2 - cz^2 = abc$.

Im ersten Fall sind wir fertig, und im zweiten Fall folgt die Aussage aus der Identität

$$a(xz + by)^2 + b(yz - ax)^2 - c(z^2 + ab)^2 = (z^2 + ab)(ax^2 + by^2 - cz^2 - abc) = 0.$$

□

Index

Absolutglied, 12

Carmichael-Zahl, 25

Einheitengruppe, 8

Eulersche φ -Funktion, 8

Fundamentallösung, 35

größte gemeinsame Teiler, 3

Grad, 12

Jacobisymbol, 22

Koeffizient, 11

konstanter Term, 12

Legendre-Symbol, 17

Leitkoeffizient, 12

normiert, 12

Nullstelle, 12

Ordnung, 13

Polynom, 11

Primitivwurzel, 15

Primzahl, 4

quadratischer Nichtrest, 17

quadratischer Rest, 17

Ringhomomorphismus, 9

teilerfremd, 3

teilt, 2

Variablen, 11

zyklische Gruppe, 14