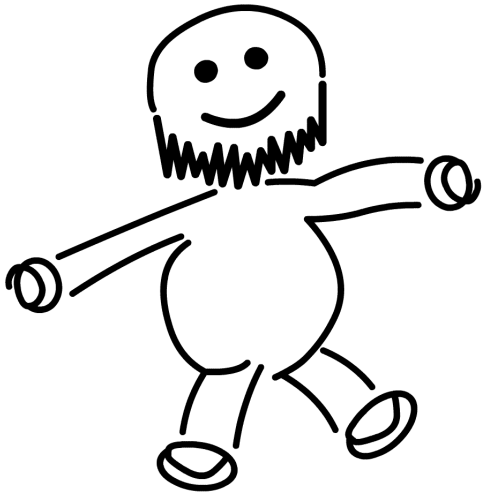
Zahlentheorie



Daniel Scholz im Winter 2006 / 2007

Überarbeitete Version vom 7. September 2007.

Inhaltsverzeichnis

1 Einleitung und Grundlagen

1.1 Einleitung

In der Zahlentheorie beschäftigen wir uns hauptsächlich mit Fragen über die natürlichen Zahlen $\mathbb{N}$. Eine Gruppe von klassischen Fragen sind die ***diophantischen Gleichungen*** wie zum Beispiel

$$y^2 - x^3 \;=\; 1.$$

Hierbei sind x und y natürliche Zahlen und es wird nach den Paaren (x, y) gefragt, die diese Gleichunge lösen. Mit $x = 2$ und $y = 3$ erhalten wir zum Beispiel

$$3^2 - 2^3 \;=\; 9 - 8 \;=\; 1.$$

Hilberts zehntes Problem besagt: *Gebe einen Algorithmus an, womit alle diophantischen Gleichungen gelöst werden können.* In kürzerer Vergangenheit haben aber Robinson, Davis und Matiasevich zeigen können, dass dies gar nicht möglich ist.

Bevor wir nun mit derartigen schwierigen Fragen umgehen können, müssen wir zunächst ganz formal Zahlensysteme und vor allem die natürlichen Zahlen $\mathbb{N}$ einführen und untersuchen.

1.2 Zahlensysteme

Setzen wir nur die Menge der natürlichen Zahlen

$$\mathbb{N} \;=\; \{0, 1, 2, 3, 4, 5, \ldots\}$$

voraus, so können wir alle weiteren wichtigen Zahlensysteme aus $\mathbb{N}$ herleiten. Unter Verwendung von Äquivalenzklassen bieten sich zum Beispiel die folgenden Konstruktionen an:

(1) Wir erhalten die ganzen Zahlen $\mathbb{Z}$ aus $\mathbb{N}$, wenn wir Subtraktion zulassen.

(2) Wir erhalten die rationalen Zahlen $\mathbb{Q}$ aus $\mathbb{Z}$, wenn wir Division zulassen.

(3) Wir erhalten die reellen Zahlen $\mathbb{R}$ aus $\mathbb{Q}$, wenn wir Grenzwerte bilden.

(4) Wir erhalten die komplexen Zahlen $\mathbb{C}$ aus $\mathbb{R}$, wenn wir die Lösbarkeit algebraischer Gleichungen zulassen.

Wir sehen also noch einmal, wie wichtig die natürlichen Zahlen sind. Dazu wollen wir diese nun ganz formal mit ihren Operationen und Ordnungen einführen.

1.3 Peano Axiome und Operationen auf $\mathbb{N}$

Um die natürlichen Zahlen $\mathbb{N}$ so sicher wie möglich begründen zu können, dient die folgende Definition:

Definition 1.3.1 (Peano Axiome)

Sei $\mathbb{N}$ eine ausgezeichnete Menge und $0 \in \mathbb{N}$ ein Element aus $\mathbb{N}$.

Weiter Sei $S : \mathbb{N} \to \mathbb{N}$ eine Abbildung, für die gilt:

(1) $0 \notin S(\mathbb{N})$.

(2) S ist injektiv.

(3) Sei $A \subset \mathbb{N}$ mit $0 \in A$ und für jedes $a \in A$ gelte $S(a) \in A$.

Dann ist $A = \mathbb{N}$

Wir sagen, dass $(\mathbb{N}, 0, S)$ die natürlichen Zahlen sind.

Die Abbildung S ist damit die ***Nachfolgerabbildung***.

Das wichtige Axion **(3)** heißt ***Induktionsprinzip***. Viele Beweise zu den folgenden Rechenregeln müssen mit dem Induktionsprinzip begründet werden.

Das Ziel wird es nun sein aus den Peano Axiomen die Grundsätze der Arithmetik herzuleiten. Dazu konstruieren wir die Operationen der Addition und Multiplikation sowie Vergleiche, also Ordnungen.

Satz 1.3.2 (Addition)

Für jedes $a \in \mathbb{N}$ gibt es eine eindeutig bestimmte Funktion F_a mit

$$F_a(0) \;=\; a \qquad \text{und} \qquad F_a(S(x)) \;=\; S(F_a(x)).$$

Für jedes $a \in \mathbb{N}$ wird die Funktion F_a gegeben durch

$$F_a(x) \;=\; a + x.$$

Daher schreiben wir nun auch stets $a + x$ für $F_a(x)$.

Satz 1.3.3 (Multiplikation)

Für jedes $a \in \mathbb{N}$ gibt es eine eindeutig bestimmte Funktion G_a mit

$$G_a(0) \;=\; 0 \qquad \text{und} \qquad G_a(S(x)) \;=\; G_a(x) + a.$$

Für jedes $a \in \mathbb{N}$ wird die Funktion G_a gegeben durch

$$G_a(x) \;=\; a \cdot x.$$

Daher schreiben wir nun auch stets $a \cdot x$ für $G_a(x)$. Zur Verdeutlichung der Operation schreiben wir in diesem einleitenden Kapitel auch stets das Zeichen „$\cdot$“, wenn wir eine Multiplikation durchführen. Später kürzen wir dann wie üblich zu $a \cdot x = ax$ ab.

Satz 1.3.4 (Rechenregeln)

Seien $x, y, z \in \mathbb{N}$. Dann gilt:

(1) $x + y = y + x$.

(2) $x + (y + z) = (x + y) + z$.

(3) $x \cdot y = y \cdot x$.

(4) $x \cdot (y \cdot z) = (x \cdot y) \cdot z$.

(5) $x \cdot (y + z) = x \cdot y + x \cdot z$.

Beweis

Alle diese Aussagen lassen sich mit Hilfe des Induktionsprinzips beweisen. Wir zeigen hier exemplarisch nur die Aussage **(1)**.

Wir betrachten für jedes $y \in \mathbb{N}$ die Menge

$$T_y \;=\; \{x \in \mathbb{N} \mid x + y = y + x\}.$$

Es gilt $F_x(0) = x + 0 = x$ und da wir $F_0(x)$ explizit als x konstruiert hatten, gilt auch $F_0(x) = 0 + x = x$. Somit folgt $0 + x = x + 0$ und für jedes $y \in \mathbb{N}$ ergibt sich $0 \in T_y$.

wir wollen nun zeigen, dass aus $x \in T_y$ auch $S(x) \in T_y$ folgt, dass also auch jeder Nachfolger in der Menge T_y enthalten ist. Dazu haben wir

$$S(x) + y \;=\; x + S(y)$$

zu zeigen. Die linke Seite ist $F_{S(x)}(y)$. Nach Konstruktion gilt $F_{S(x)}(y) = F_x(S(y))$ und da $x \in T_y$ ist, folgt

$$\begin{aligned} S(x) + y \;&=\; S(F_x(y)) \;=\; S(x + y) \;=\; S(y + x) \\ &=\; S(F_y(x)) \;=\; F_y(S(x)) \;=\; y + S(x). \end{aligned}$$

Nach dem ***Induktionsprinzip*** ergibt sich somit $T_y = \mathbb{N}$, was die Behauptung zeigt. □

1.4 Ordnungen auf $\mathbb{N}$

Die Idee zur Einführung von Ordnungen auf $\mathbb{N}$ ist die folgende: Zu zwei beliebigen natürlichen Zahlen x und y sollte es ein $z \in \mathbb{N}$ geben, so dass $x + z = y$ oder $y + z = x$ lösbar ist. Dies liefert der folgende Satz:

Satz 1.4.1 (Kalmár)

Seien $x, y \in \mathbb{N}$. Dann gilt genau eine der folgenden Aussagen:

(1) $x = y$.

(2) $x = y + z$ mit $z \neq 0$.

(3) $y = x + z$ mit $z \neq 0$.

Nach dem Satz von Kalmár haben wir nicht nur eine totale Ordnung auf $\mathbb{N}$ erhalten, wir können sogar subtrahieren: Ist $x < y$, so gibt es ein $z \in \mathbb{N}$ mit $x + z = y$.

Die üblichen Eigenschaften Reflexivität, Antisymmetrie und Transitivität der Ordnung $<$ können leicht nachgerechnet werden.

Satz 1.4.2

Sei $A \subset \mathbb{N}$ eine nicht leere Teilmenge der natürlichen Zahlen und es existiere ein $n \in \mathbb{N}$ mit $A \subset \{x \in \mathbb{N} \mid x < n\}$.

Dann gibt es genau ein $a_0 \in A$, so dass für alle $a \in A$ mit $a_0 \neq a$ gerade $a < a_0$ gilt.

Wir schreiben $\max(A) := a_0$ und nennen $\max(A)$ das ***Maximum*** von A.

Satz 1.4.3

Sei $B \subset \mathbb{N}$ eine nicht leere Teilmenge der natürlichen Zahlen.

Dann gibt es genau ein $b_0 \in B$, so dass für alle $b \in B$ mit $b_0 \neq b$ gerade $b_0 < b$ gilt.

Wir schreiben $\min(B) := b_0$ und nennen $\min(B)$ das ***Minimum*** von B.

Bemerkung

Beim Satz über das Maximum mussten wir eine endliche Menge A fordern, beim Satz über das Minimum kann B auch unendlich viele Elemente haben.

1.5 Zahlen und Mengen

Aus den Peano Axiomen haben wir die Konstruktionen $+$, $\cdot$, $<$ und $-$ hergeleitet und haben damit die Grundlagen der Arithmetik sichergestellt. Wir stellen uns nun die Frage, ob die Peano Axiome auch überzeugend sind. Dazu untersuchen wir die Mengentheorie und vergleichen deren grundlegende Axiome mit den natürlichen Zahlen, die aus den Peano Axiomen entstehen.

Es wäre wünschenswert, wenn wir den Begriff einer endlichen Menge und ihre Kardinalität einführen könnten. Dazu verwendet man in der *Standard*-Mengenlehre die Zermelo-Fraenkel Axiome:

Zermelo-Fraenkel Axiome

Neben Buchstaben benötigen wir die folgenden Grundsymbole:

$$\in, \quad \Rightarrow, \quad \Leftrightarrow, \quad \forall, \quad \exists, \quad \exists!, \quad \vee, \quad \wedge, \quad \neg.$$

Damit können wir die Zermelo-Fraenkel Axiome angeben (welche wir hier teilweise sinngemäß wiedergeben):

(1) Zwei Mengen A und B sind genau dann gleich, wenn sie dieselben Elemente enthalten.

(2) Es gibt eine Menge ohne Elemente.

(3) Wenn A und B Mengen sind, dann gibt es eine Menge C, die genau A und B als Elemente hat.

(4) Für jede Menge A gibt es eine Menge B, deren Elemente genau die Elemente der Elemente von A sind.

(5) Es gibt eine Menge A, die die leere Menge und mit jedem Element x auch die Menge $x \cup \{x\}$ enthält.

(6) Für jede Menge A gibt es eine Menge P, deren Elemente genau die Teilmengen von A sind.

(7) Jede nichtleere Menge A enthält ein Element B, so dass A und B disjunkt sind.

(8) Zu jeder Menge A existiert eine Teilmenge von A die genau die Elemente C von A enthält, für die $P(C)$ wahr ist.

(9) Für jede Menge A gibt es eine Menge B, deren Elemente genau die Bilder der Menge A unter der Abbildung F sind.

(10) Ist A eine Menge von paarweise disjunkten nichtleeren Mengen, dann gibt es eine Menge, die genau ein Element aus jedem Element von A enthält.

Aber auch bei diesen grundlegenden Axiomen haben wir zwei Probleme: Erstens ist es zweifelhaft, ob diese Axiome intuitiv sind. Wenn wir versuchen die Zahlen auf so einer Mengentheorie aufzubauen, dann haben wir vielleicht keine weitere Sicherheit mehr. Zweitens setzen die Axiome nicht nur die Logik voraus, sondern auch die Prädikatenlogik, welche sehr reichhaltig ist.

Wir erhalten damit das Fazit, dass sich die drei Bereiche Mengentheorie, Logik und Arithmetik gegenseitig bedingen.

Kardinalität

Wir sagen, dass zwei Mengen A und B ***gleichmächtig*** sind, wenn es eine Bijektion $f : A \to B$ gibt.

Falls es eine Injektion $F : A \to B$ gibt, so sagen wir, dass A eine kleinere ***Kardinalität*** als B hat und schreiben $\text{card}(A) \leq \text{card}(B)$. Gilt zusätztlich auch $\text{card}(B) \leq \text{card}(A)$, so folt aus dem Satz von Schröder-Bernstein, dass $\text{card}(A) = \text{card}(B)$, die Mengen A und B haben also gleiche Kardinalität.

Damit erhalten wir mehrere Möglichkeiten eine endliche Kardinalität zu definieren.

(1) Die Kardinalität $\text{card}(A)$ ist endlich, wenn jede Injektion $F : A \to A$ eine Bijektion ist.

(2) Die Kardinalität $\text{card}(A)$ ist endlich, wenn jede Surjektion $F : A \to A$ eine Bijektion ist.

(3) Die Kardinalität $\text{card}(A)$ ist endlich, wenn für alle $x \in A$ gerade $\text{card}(A - \{x\}) \neq \text{card}(A)$ gilt.

Um nun zu untersuchen, ob die Kardinalitäten in dem System der Peano Axiome gleich sind, nutzen wir die Variante von v. Neumann. Wir sagen

$$0 = \emptyset \qquad \text{und} \qquad S(n) = n \cup \{n\}$$

und erhalten damit

$$\begin{aligned} 1 &= S(0) = \emptyset \cup \{\emptyset\} = \{\emptyset\}, \\ 2 &= S(1) = \{\emptyset\} \cup \{\{\emptyset\}\} = \{\emptyset, \{\emptyset\}\}, \\ &\vdots \end{aligned}$$

Wir sehen die Zahl n hier also als eine Menge mit n Elementen an und nutzen nur das eine Element $\emptyset$ der leeren Menge.

Auch weitere Versuche die natürlichen Zahlen $\mathbb{N}$ grundlegend axiomatisch zu definieren führten zum gleichen Ergebnis:

Fazit

Für die Grundlagen der Mathematik sind Logik, Mengentheorie und Arithmetik nötig. Alle Versuche die Mathematik nur auf eine dieser Gedanken zu reduzieren sind gescheitert.

1.6 Aufgaben

Aufgabe 1.6.1

Sei $2 = S(S(0))$ und $4 = S(S(S(S(0))))$. Zeige, dass dann gilt:

(1) $2 + 2 \;=\; 4$,

(2) $2 \times 2 \;=\; 4$.

Lösung

(1) Nach der Definition der Addition gilt

$$F_a(0) \;=\; a \qquad \text{und} \qquad F_a(S(x)) \;=\; S(F_a(x))\,.$$

Damit folgt

$$\begin{aligned} 2+2 \;&=\; F_{S(S(0))}(S(S(0))) \;=\; S(F_{S(S(0))}S(0)) \\ &=\; S(S(F_{S(S(0))}(0))) \;=\; S(S(S(S(0)))) \;=\; 4. \end{aligned}$$

(2) Nach der Definition der Multiplikation gilt

$$G_a(0) \;=\; 0 \qquad \text{und} \qquad G_a(S(x)) \;=\; G_a(x) + a\,.$$

Damit folgt

$$\begin{aligned} 2 \times 2 \;&=\; G_{S(S(0))}(S(S(0))) \;=\; G_{S(S(0))}S(0) + S(S(0)) \\ &=\; G_{S(S(0))} + S(S(0)) + S(S(0)) \;=\; 0 + 2 + 2 \;=\; 4. \end{aligned}$$

Wobei die letzte Gleichheit aus **(1)** folgt.

Aufgabe 1.6.2

Zeige, dass

$$(1 + 2x + 3x^2 + \ldots + nx^{n-1})(1-x)^2 \;=\; 1 - (n+1)x^n + nx^{n+1}$$

für alle $n \in \mathbb{N}$ gilt.

Lösung

Um eine vollständige Induktion zu umgehen, nutzen wir die Differenzierbarkeit von Reihen:

$$\begin{aligned} 1 + 2x + 3x^2 + \ldots + nx^{n-1} &= \frac{\mathrm{d}}{\mathrm{d}x}(1 + x + x^2 + \ldots + x^n) \\ &= \frac{\mathrm{d}}{\mathrm{d}x}\left(\frac{x^{n+1} - 1}{x - 1}\right) \\ &= \frac{(n+1)x^n(x-1) - x^{n+1} + 1}{(x-1)^2} \\ &= \frac{1 - (n+1)x^n + nx^{n+1}}{(x-1)^2}. \end{aligned}$$

Aufgabe 1.6.3

Zeige die Irrationalität von $\sqrt{2}$.

Lösung

Angenommen $\sqrt{2}$ ist nicht irrational, dann gilt

$$\sqrt{2} \;=\; \frac{a}{b} \qquad \text{mit} \qquad a, b \in \mathbb{N}.$$

Demnach gibt es ein kleinstes $n \in \mathbb{N}$ mit $n \cdot \sqrt{2} \in \mathbb{N}$.

Sei nun $m := n \cdot (\sqrt{2} - 1)$. Da

$$0 \;<\; (\sqrt{2} - 1) \;<\; 1$$

ist, folgt $m < n$. Nun haben wir

$$m \cdot \sqrt{2} \;=\; n \cdot \sqrt{2} \cdot (\sqrt{2} - 1) \;=\; 2 \cdot n - n \cdot \sqrt{2}.$$

Nun ist aber nicht nur $2 \cdot n$, sondern nach der Annahme auch $n \cdot \sqrt{2}$ eine natürliche Zahl, und damit ist auch die Differenz aus $\mathbb{N}$. Da aber $m < n$ ist und wir n als minimal vorausgesetzt haben, folgt ein Widerspruch zur Annahme.

Aufgabe 1.6.4

Sei $c \in \mathbb{Z}$ und seien $a_1, \ldots, a_m \in \{0, \ldots, 9\}$.

Periodische Dezimalentwicklungen schreiben wir damit als

$$c, \overline{a_1 \ldots a_m} \;:=\; c, a_1 \ldots a_m a_1 \ldots a_m a_1 \ldots .$$

Zeige für ein beliebiges $n \in \mathbb{N}$

$$\frac{10^{n-1}}{10^n - 1} \;=\; 0,\underbrace{\overline{10\ldots0}}_{n \text{ Ziffern}}.$$

Benutze diese Formel, um

$$0,\overline{a_1 \ldots a_m} \;=\; \frac{a_1 a_2 \ldots a_m}{99\ldots9}$$

zu zeigen.

Lösung

Es gilt

$$\begin{aligned}
0,\underbrace{\overline{10\ldots0}}_{n \text{ Ziffern}} \cdot (10^n - 1) &= 0,\underbrace{\overline{10\ldots0}}_{n \text{ Ziffern}} \cdot \underbrace{99\ldots9}_{n \text{ Ziffern}} \\
&= \sum_{k=0}^{\infty} (\underbrace{99\ldots9}_{n \text{ Ziffern}} \cdot 10^{-kn-1}) \\
&= \underbrace{9\ldots9}_{n-1 \text{ Ziffern}}\,,\overline{9} \;=\; 10^{n-1},
\end{aligned}$$

was die erste Behauptung zeigt. Die zweite Aussage folgt damit aus folgenden Gleichungskette:

$$\begin{aligned}
0,\overline{a_1 \ldots a_m} &= \frac{a_1}{10^0} \cdot 0,\overbrace{\overline{10\ldots0}}^{m \text{ Ziffern}} + \ldots + \frac{a_m}{10^{m-1}} \cdot 0,\overbrace{\overline{10\ldots0}}^{m \text{ Ziffern}} \\
&= \frac{1}{10^m - 1} \cdot \left(a_1 \cdot \frac{10^{m-1}}{10^0} + \ldots + a_m \cdot \frac{10^{m-1}}{10^{m-1}} \right) \\
&= \frac{1}{99\ldots9} \cdot \left(a_1 \cdot 10^{m-1} + \ldots + a_m \cdot 10^0 \right) \;=\; \frac{a_1 a_2 \ldots a_m}{99\ldots9}.
\end{aligned}$$

Damit ergibt sich auch die Formel

$$0,\overline{1234567890} \;=\; \frac{1\,234\,567\,890}{9\,999\,999\,999} \;=\; \frac{137\,174\,210}{1\,111\,111\,111}.$$

Aufgabe 1.6.5

Berechne $1,\overline{2} \cdot 0,\overline{81}$.

Lösung

Es gilt

$$\begin{aligned} 1,\overline{2} &= 1 + 0,\overline{2} = 1 + \frac{2}{9} = \frac{11}{9}, \\ 0,\overline{81} &= \frac{81}{99} = \frac{9}{11}. \end{aligned}$$

Damit ergibt sich sofort

$$1,\overline{2} \cdot 0,\overline{81} = \frac{11}{9} \cdot \frac{9}{11} = 1.$$

Aufgabe 1.6.6

Eine reelle (oder komplexe) Zahl z heißt ***quadratisch***, falls sie einer quadratischen Gleichung $pz^2 + qz + r = 0$ mit ganzzahligen Koeffizienten p, q und r genügt.

Seien α und β irrational, aber nicht quadratisch. Zeige, dass dann auch mindestens eine der beiden Zahlen $\alpha + \beta$ oder $\alpha \cdot \beta$ irrational ist.

Lösung

Angenommen $\alpha + \beta$ und $\alpha \cdot \beta$ sind rational, dann gibt es $a, b, c, d \in \mathbb{Z}$ mit

$$\alpha + \beta = \frac{a}{b} \qquad \text{und} \qquad \alpha \cdot \beta = \frac{c}{d}.$$

Durch einfache Umformungen erhalten wir die Gleichung

$$\frac{c}{\beta \cdot d} + \beta = \frac{a}{b}$$

und daraus ergibt sich

$$db \cdot \beta^2 - da \cdot \beta + bc = 0$$

Die Koeffizienten dieser quadratischen Gleichung sind aber alle ganzzahlig und β löst die Gleichung. Somit erhalten wir einen Widerspruch dazu, dass β als nicht quadratisch vorausgesetzt wurde.

Da e und π beide irrational und nicht quadratisch sind, muss mindestens eine der beiden Zahlen $\mathrm{e} + \pi$ oder $\mathrm{e} \cdot \pi$ irrational sein. Die Antwort auf diese Frage ist bis heute nicht geklärt.

Aufgabe 1.6.7

Mit der Ordnung von $\mathbb{R}$ betrachten wir den Ring

$$R \;=\; \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}.$$

Zeige, dass das Induktionsaxiom hier nicht gilt.

Lösung

Seien α und β zwei beliebige Zahlen aus R mit $\alpha < \beta$. Wir suchen zunächst ein γ aus R mit

$$\alpha \;<\; \gamma \;<\; \beta.$$

Sei $\varepsilon = \beta - \alpha > 0$. Wir betrachten die Folge $(a_n)_{n\in\mathbb{N}}$, wobei a_n die Zahl $\sqrt{2}$ auf n Nachkommastellen genau angibt. Damit ist $(a_n)_{n\in\mathbb{N}}$ eine Folge in $\mathbb{Q}$, die gegen $\sqrt{2}$ konvergiert, und wir können jedes a_n als Quotient von zwei natürlichen Zahlen schreiben.

Wir finden also $p, q \in \mathbb{N}$, so dass

$$0 \;<\; \sqrt{2} - \frac{p}{q} \;<\; \frac{\varepsilon}{q}$$

gilt. Daraus folgt aber auch

$$0 \;<\; q\sqrt{2} + p \;<\; \varepsilon$$

Mit $\gamma := \alpha + (p + q\sqrt{2}) \in R$ haben wir ein γ zwischen α und β gefunden. Damit ist R dicht in $\mathbb{R}$ und das Induktionsaxiom kann nicht gelten.

2 Zahlentheorie

Um es noch einmal zu verdeutlichen: Mit $\mathbb{N}$ bezeichnen wir die natürlichen Zahlen mit der Null. Für ein Element $a \in \mathbb{N}$, dass nicht die Null sein soll, schreiben wir explizit $a \in \mathbb{N} - \{0\}$.

2.1 Der Restsatz

Satz 2.1.1

(1) Für alle $a, b, x \in \mathbb{N}$ gilt: Aus

$$a + x \;=\; b + x \qquad \text{folgt} \qquad a \;=\; b.$$

(2) Für alle $a, b \in \mathbb{N}$ und $c \in \mathbb{N} - \{0\}$ gilt: Aus

$$a \;<\; b \qquad \text{folgt} \qquad a \cdot c \;<\; b \cdot c.$$

(3) Für alle $a, b \in \mathbb{N}$ und $x \in \mathbb{N} - \{0\}$ gilt: Aus

$$a \cdot x \;=\; b \cdot x \qquad \text{folgt} \qquad a \;=\; b.$$

(4) Für alle $a, b, x \in \mathbb{N}$ gilt: Aus

$$a + x \;<\; b + x \qquad \text{folgt} \qquad a \;<\; b.$$

Beweis

Wir wollen exemplarisch nur Punkt **(4)** beweisen.

Wir nehmen an aus $a + x < b + x$ folgt $a = b$. Dann folgt direkt aus **(1)** aber $a + x = b + x$, was ein Widerspruch ist.

Sei nun $b < a$. Dann gibt es ein $y \neq 0$ mit $b + y = a$. Damit folgt aus der Voraussetztung $a + x < b + x$

$$b + y + x \;<\; b + x$$

was zum Widerspruch führt. Es bleibt also nur die Möglichkeit $a < b$. □

Satz 2.1.2 (Restsatz)

Sei $a \in \mathbb{N}$ und $b \in \mathbb{N} - \{0\}$.

Dann gibt es $q, r \in \mathbb{N}$ mit $r < b$ und

$$a \;=\; q \cdot b + r.$$

Wir nennen q den ***Quotienten*** und r den ***Rest***.

Notation

Wir schreiben (wie auch in einigen Programmiersprachen üblich)

$$a \text{ div } b \quad \text{für} \quad q \qquad \text{und} \qquad a \text{ MOD } b \quad \text{für} \quad r.$$

Definition 2.1.3

Seien $a, b \in \mathbb{N} - \{0\}$. Falls es ein $q \in \mathbb{N}$ gibt, für dass

$$a \;=\; b \cdot q$$

gilt, so sagen wir a ist ***teilbar*** durch b.

Wir schreiben dafür $b \mid a$, b ist Teiler von a. Für den Fall, dass ein kein solches q gibt, schreiben wir $b \nmid a$, b ist kein Teiler von a.

Definition 2.1.4

Für $a, b \in \mathbb{N} - \{0\}$ betrachten wir

$$S \;:=\; \{x \mid x \mid b,\; x \mid a\}.$$

Die Menge S ist nicht leer, da auf jeden Fall $1 \in S$ gilt. Mit

$$\text{ggT}(a, b) \;:=\; \max(S)$$

bezeichnen wir den ***größten gemeinsamen Teiler*** von a und b.

Gilt $\text{ggT}(a, b) = 1$, so sagen wir a und b sind ***teilerfremd***.

Definition 2.1.5

Für $a, b \in \mathbb{N} - \{0\}$ betrachten wir

$$T \;:=\; \{x \mid a \mid x,\; b \mid x\}.$$

Die Menge T ist nicht leer, da auf jeden Fall $a \cdot b \in T$ gilt. Mit

$$\text{kgV}(a, b) \;:=\; \min(T)$$

bezeichnen wir das ***kleinste gemeinsame Vielfache*** von a und b.

Satz 2.1.6

Seien $a, b, c, d \in \mathbb{N} - \{0\}$. Dann gilt:

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

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

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

(4) Aus $a \mid c$ und $b \mid c$ folgt $\mathrm{kgV}(a, b) \mid c$.

(5) Aus $d \mid a$ und $d \mid b$ folgt $d \mid \mathrm{ggT}(a, b)$.

2.2 Euklidischer Algorithmus

Bevor wir den Euklidischen Algorithmus angeben können, brauchen wir noch einen wichtigen Satz:

Satz 2.2.1

Seien $a, b \in \mathbb{N} - \{0\}$. Nach dem Restsatz gibt es dann $q, r \in \mathbb{N}$ mit $0 \leq r < b$, so dass

$$a \;=\; q \cdot b + r$$

gilt. Damit gilt für $r > 0$

$$\mathrm{ggT}(a, b) \;=\; \mathrm{ggT}(b, r).$$

Euklidischer Algorithmus

Der Euklidische Algorithmus dient zur Berechnung des größten gemeinsamen Teilers zweier Zahlen. Dabei wird der Algorithmus durch den vorherigen Satz gerechtfertigt.

Seien $a, b \in \mathbb{N} - \{0\}$ mit $a > b$. Setze $a_0 := a$ und $a_1 := b$. Dann teile mit Rest:

$$\begin{aligned}
a_0 &= q_1 a_1 + r_1 && \text{mit} \quad 0 \leq r_1 < a_1, \;\; a_2 := r_1 \;\; \text{wenn} \;\; r_1 \neq 0 \\
a_1 &= q_2 a_2 + r_2 && \text{mit} \quad 0 \leq r_2 < a_2, \;\; a_3 := r_2 \;\; \text{wenn} \;\; r_2 \neq 0 \\
a_2 &= q_3 a_3 + r_3 && \text{mit} \quad 0 \leq r_3 < a_3, \;\; a_4 := r_3 \;\; \text{wenn} \;\; r_3 \neq 0 \\
&\vdots \\
a_{n-1} &= q_n a_n + r_n && \text{mit} \quad r_n = 0 \quad \text{und} \quad a_n := r_{n-1} \neq 0.
\end{aligned}$$

Offenbar gilt

$$a_0 > a_1 > a_2 > \ldots > a_{n-1} > a_n \geq 1.$$

Da $a_n \mid a_{n-1}$, gilt nach Satz 2.2.1 gerade

$$\text{ggT}(a,b) = \text{ggT}(a_0,a_1) = \text{ggT}(a_1,a_2) = \ldots = \text{ggT}(a_{n-1},a_n) = a_n.$$

Beispiel 2.2.2

Wir wollen $\text{ggT}(163,97)$ berechnen. Der Euklidische Algorithmus liefert die folgenden Gleichungen:

$$\begin{aligned} 163 &= 1 \cdot 97 + 66 \\ 97 &= 1 \cdot 66 + 31 \\ 66 &= 2 \cdot 31 + 4 \\ 31 &= 7 \cdot 4 + 3 \\ 4 &= 1 \cdot 3 + 1 \\ 3 &= 3 \cdot \mathbf{1}. \end{aligned}$$

Damit gilt $\text{ggT}(163,97) = 1$.

Beispiel 2.2.3

Wir wollen $\text{ggT}(162,21)$ berechnen. Der Euklidische Algorithmus liefert die folgenden Gleichungen:

$$\begin{aligned} 162 &= 7 \cdot 21 + 15 \\ 21 &= 1 \cdot 15 + 6 \\ 15 &= 2 \cdot 6 + 3 \\ 6 &= 2 \cdot \mathbf{3}. \end{aligned}$$

Damit gilt $\text{ggT}(162,21) = 3$.

Hat man die Folge $q_1, \ldots, q_n$ aus dem Euklidischen Algorithmus einmal berechnet, so liefert dieser noch ein wichtiges Ergebnis:

Satz 2.2.4

Seien $a, b, c \in \mathbb{N} - \{0\}$. Dann gibt es genau dann $x, y \in \mathbb{N}$ mit

$$x \cdot a - y \cdot b = c,$$

wenn $\text{ggT}(a,b)$ ein Teiler von c ist.

Eulersche Rekursionsformeln

Wir setzen

$$P_0 := 1, \quad P_{-1} := 0, \quad Q_0 := 0, \quad Q_{-1} := 1.$$

Damit sind die ***Eulerschen Rekursionsformeln***

$$P_r = q_r \cdot P_{r-1} + P_{r-2} \qquad \text{und} \qquad Q_r = q_r \cdot Q_{r-1} + Q_{r-2},$$

wobei die Folge der ***partiellen Quotienten*** $q_1, \ldots, q_n$ aus dem Euklidischen Algorithmus zu den Zahlen $a, b \in \mathbb{N} - \{0\}$ berechnet wurde.

Es gilt dann

$$a = P_n \cdot \mathrm{ggT}(a,b) \qquad \text{und} \qquad b = Q_n \cdot \mathrm{ggT}(a,b).$$

Es gilt nun

$$(-1)^n \cdot \mathrm{ggT}(a,b) = Q_{n-1} \cdot a - P_{n-1} \cdot b.$$

Beispiel 2.2.5

Wir wollen die Gleichung

$$\mathrm{ggT}(163, 97) = 1 = x \cdot 163 - y \cdot 97$$

lösen. Dazu nutzen wir die Folge der partiellen Quotienten aus Beispiel 2.2.2 und die Eulerschen Rekursionsformeln liefern das Schema aus Tabelle 2.1.

r	-1	0	1	2	3	4	5	6
q_r	$-$	$-$	1	1	2	7	1	3
P_r	0	1	1	2	5	37	$\mathbf{42}$	163
Q_r	1	0	1	1	3	22	$\mathbf{25}$	97

Tabelle 2.1: Schema zu den Eulerschen Rekursionsformeln.

Wir erhalten damit die Lösungen $x = 25$ und $y = 42$:

$$x \cdot 163 - y \cdot 97 = 25 \cdot 163 - 42 \cdot 97 = 4075 - 4074 = 1.$$

Beispiel 2.2.6

Wir wollen die Gleichung

$$\mathrm{ggT}(162, 21) = 3 = x \cdot 162 - y \cdot 21$$

lösen. Dazu nutzen wir die Folge der partiellen Quotienten aus Beispiel 2.2.3 und die Eulerschen Rekursionsformeln liefern das Schema aus Tabelle 2.2.

Wir erhalten damit die Lösungen $x = 3$ und $y = 23$:

$$x \cdot 162 - y \cdot 21 = 3 \cdot 162 - 23 \cdot 21 = 486 - 483 = 3.$$

r	-1	0	1	2	3	4
q_r	$-$	$-$	7	1	2	2
P_r	0	1	7	8	**23**	54
Q_r	1	0	1	1	**3**	7

Tabelle 2.2: Schema zu den Eulerschen Rekursionsformeln.

2.3 Kongruenzarithmetik

Wir wollen nun die Kongruenzarithmetik einführen. Dazu benötigen wir zunächst die folgende grundlegende Definition:

Definition 2.3.1

Sei $n \in \mathbb{N} - \{0\}$ und seien $a, b \in \mathbb{N}$.

Wir sagen *a ist kongruent zu b modulo n* und schreiben

$$a \equiv b \,(\mathrm{mod}\ n),$$

wenn es $r, s \in \mathbb{N}$ gibt mit

$$a + r \cdot n \;=\; b + s \cdot n.$$

Mit dieser Definition können wir zunächst einige Aussagen treffen.

Satz 2.3.2

Die Relation $\equiv$ ist eine Äquivalenzrelation.

Falls $a \equiv a' \,(\mathrm{mod}\ n)$ und $b \equiv b' \,(\mathrm{mod}\ n)$ gilt, dann folgt auch

$$a + b \equiv a' + b' \,(\mathrm{mod}\ n) \qquad \text{und} \qquad a \cdot b \equiv a' \cdot b' \,(\mathrm{mod}\ n).$$

Satz 2.3.3

Für jedes $a \in \mathbb{N}$ existiert ein eindeutig bestimmtes $r \in \mathbb{N}$ mit $r < n$, so dass

$$a \equiv r \,(\mathrm{mod}\ n)$$

gilt. Dies folgt aus dem Restsatz.

Satz 2.3.4

Die Aussagen $a \equiv 0 \,(\mathrm{mod}\ n)$ und $n \mid a$ sind äquivalent.

Satz 2.3.5

Sei $a \in \mathbb{N}$ und $n \in \mathbb{N} - \{0\}$. Dann gibt es ein $b \in \mathbb{N}$ mit

$$a + b \equiv 0 \,(\mathrm{mod}\ n).$$

Von jetzt an werden wir für die Äquivalenzklassen von $\mathbb{N}\,(\mathrm{mod}\, n)$ immer $R(n)$ schreiben. Die übliche Notation ist $\mathbb{Z}/n\mathbb{Z}$, aber da wir hier nur natürliche Zahlen betrachten, bietet sich diese Schreibweise für uns nicht an.

Nach Satz 2.3.2, da $0\,(\mathrm{mod}\, n)$ sowie $1\,(\mathrm{mod}\, n)$ aus $R(n)$ sind und nach Satz 2.3.5 bildet $R(n)$ einen kommutativen Ring. Dies ist die wichtigste Aussage über $R(n)$, da wir darin nun gut *rechnen* können.

Beispiel 2.3.6

Für $n = 4$ haben wir in $R(n)$ die folgende Addition- bzw. Multiplikationtabelle:

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Satz 2.3.7

(1) Seien $a, n \in \mathbb{N} - \{0\}$, so dass $\mathrm{ggT}(a, n) \neq 1$ gilt. Dann gibt es ein $d \in \mathbb{N}$ mit $d \not\equiv 0 \,(\mathrm{mod}\ n)$, so dass

$$a \cdot d \equiv 0 \,(\mathrm{mod}\ n)$$

gilt.

(2) Seien $a, n \in \mathbb{N} - \{0\}$, so dass $\mathrm{ggT}(a, n) = 1$ gilt. Dann gibt es ein $d \in \mathbb{N}$, so dass

$$a \cdot d \equiv 1 \,(\mathrm{mod}\ n)$$

gilt.

Es gibt offenbar eine Abbildung $R(nm) \to R(n)$, die surjektiv ist. Setze dazu einfach

$$0\,(\bmod mn) \mapsto 0\,(\bmod n), \qquad 1\,(\bmod mn) \mapsto 1\,(\bmod n), \qquad \ldots .$$

Diese Abbildung erhält Addition und Multiplikation, sie ist also ein Homomorphismus von Ringen.

Weiter werden wir die folgende Notation verwenden:

$$R^\times(n) \;:=\; \{a\,(\bmod n) \in R(n) \mid \mathrm{ggT}(a,n) = 1\} \;\subset\; R(n).$$

Damit gilt sogar der folgende Satz:

Satz 2.3.8

Seien $m, n \in \mathbb{N} - \{0\}$ mit $\mathrm{ggT}(m,n) = 1$. Dann gibt es eine Abbildung

$$R(mn) \;\to\; R(m) \times R(n),$$

die bijektiv ist. Weiter ist das Bild von $R^\times(mn)$ gerade $R^\times(m) \times R^\times(n)$.

2.4 Chinesischer Restsatz

Wir sind nun in der Lage den chinesischen Restsatz in einer zunächst sehr einfachen Weise zu beweisen:

Satz 2.4.1 (Chinesischer Restsatz in einfacher Form)

Seien $m, n \in \mathbb{N} - \{0\}$ mit $\mathrm{ggT}(m,n) = 1$ und seien weiter $a, b \in \mathbb{N}$.

Dann gibt es ein $x \in \mathbb{N}$ mit

$$x \;\equiv\; a\,(\bmod\; m\,) \qquad \text{und} \qquad x \;\equiv\; b\,(\bmod\; n\,).$$

Beweis

Ohne Beschränkung der Allgemeinheit nehmen wir an, dass $a < m$ und $b < n$ gilt.

Der Beweis nutzt im Wesentlichen die Eulerschen Rekursionsformeln. Danach gibt es $M, N \in \mathbb{N}$, so dass

$$Mm \;=\; 1 + Nn$$

gilt, da ja gerade $\mathrm{ggT}(m,n) = 1$. Somit genügt $u = Mm$ den Kongruenzen

$$u \equiv 0 \,(\mathrm{mod}\ m) \qquad \text{und} \qquad u \equiv 1 \,(\mathrm{mod}\ n).$$

Weiter genügt aber auch $v = Nn$ den Kongruenzen

$$v \equiv m-1 \,(\mathrm{mod}\ m) \qquad \text{und} \qquad v \equiv 0 \,(\mathrm{mod}\ n).$$

Mit $x = (m-a)v + bu$ folgt

$$x \equiv a \cdot 1 + b \cdot 0 \,(\mathrm{mod}\ m) \qquad \text{und} \qquad x \equiv a \cdot 0 + b \cdot 1 \,(\mathrm{mod}\ n),$$

was die Behauptung zeigt. □

Der Beweis zum chinesischen Restsatz liefert damit auch einen Algorithmus, mit dem die natürliche Zahl x gefunden werden kann:

Beispiel 2.4.2

Seien $m = 7$ und $n = 4$. Die Gleichung

$$Mm \;=\; 1 + Nn$$

wird gelöst durch $M = 7$ und $N = 12$. Dies ergibt der Euklidische Algorithmus und die Eulerschen Rekursionsformel oder wie in diesem Fall einfaches Raten. Wir erhalten

$$u \;=\; Mm \;=\; 49 \qquad \text{und} \qquad v \;=\; Nn \;=\; Mn - 1 \;=\; 48.$$

Zu den beliebigen natürlichen Zahlen $a = 3$ und $b = 2$ erhalten wir also

$$x \;=\; (m-a)v + bu \;=\; 4 \cdot 48 + 2 \cdot 49 \;=\; 290.$$

Für dieses x gilt wie behauptet

$$290 \equiv 3 \,(\mathrm{mod}\ 7) \qquad \text{und} \qquad 290 \equiv 2 \,(\mathrm{mod}\ 4).$$

Es ist zu beachten, dass die nach diesem Algorithmus gefundene Lösung x nicht das kleinste x ist, das den Anforderungen genügt. In diesem Beispiel hätte auch $x = 10$ das geforderte erbracht.

Beispiel 2.4.3

Seien $m = 163$ und $n = 97$. Nach Beispiel 2.2.5 gilt $\mathrm{ggT}(163, 97) = 1$ und aus den Eulerschen Rekursionsformeln erhalten wir

$$25 \cdot 163 - 42 \cdot 97 \;=\; 1.$$

Seien also $M = 25$ und $N = 42$. Damit seien

$$u \;=\; Mm \;=\; 4075 \qquad \text{und} \qquad v \;=\; Nn \;=\; 4074.$$

Zu den beliebigen natürlichen Zahlen $a = 17$ und $b = 21$ erhalten wir also

$$x \;=\; (m-a)v + bu \;=\; 594804 + 85575 \;=\; 680379.$$

Für dieses x gilt wie behauptet

$$680379 \equiv 17\,(\bmod\ 163) \qquad \text{und} \qquad 680379 \equiv 21\,(\bmod\ 97).$$

Satz 2.4.4 (Chinesischer Restsatz)

Seien $m_1, \ldots, m_k \in \mathbb{N} - \{0\}$ mit $\mathrm{ggT}(m_i, m_j) = 1$ für $i \neq j$.

Dann sind die Abbildungen

$$\begin{array}{rcl} R(m_1 \cdot \ldots \cdot m_k) & \to & R(m_1) \times \ldots \times R(m_k) \\ x \text{ MOD } m_1 \cdot \ldots \cdot m_k & \mapsto & (x \text{ MOD } m_1, \ldots, x \text{ MOD } m_k) \end{array}$$

sowie

$$\begin{array}{rcl} R^\times(m_1 \cdot \ldots \cdot m_k) & \to & R^\times(m_1) \times \ldots \times R^\times(m_k) \\ x \text{ MOD } m_1 \cdot \ldots \cdot m_k & \mapsto & (x \text{ MOD } m_1, \ldots, x \text{ MOD } m_k) \end{array}$$

Bijektionen.

2.5 Primzahlen

Definition 2.5.1

Eine ***Primzahl*** p ist ein Element $p \in \mathbb{N} - \{0\}$ mit $p > 1$, für dass die einzigen Teiler 1 und p sind.

Für eine Primzahl p schreiben wir auch p ist ***prim***.

Satz 2.5.2

Sei p eine Primzahl und $1 < n < p$. Dann gilt

$$\mathrm{ggT}(p, n) \;=\; 1.$$

Satz 2.5.3

Eine natürliche Zahl $p > 1$ ist genau dann eine Primzahl, wenn aus $p \mid ab$ gerade $p \mid a$ oder $p \mid b$ folgt.

Hauptsatz der Arithmetik

Sei $n > 1$ eine natürliche Zahl. Dann gibt es Primzahlen $p_1, \ldots, p_s$ und natürliche Zahlen $e_1, \ldots, e_s \geq 1$, so dass

$$n \;=\; p_1^{e_1} \cdot \ldots \cdot p_s^{e_s}$$

gilt. Mit $p_1 < \ldots < p_s$ ist diese Darstellung eindeutig.

Dieser Satz gilt verallgemeinert auch für Primideale in Ringen.

Beweis

Wir zeigen nur die Darstellung der Primfaktorenzerlegung.

Ist n eine Primzahl, so muss nichts gezeigt werden. Ist n keine Primzahl, so gibt es $a, b \in \mathbb{N}$ mit $n = a \cdot b$.

Nun wenden wir die gleichen Überlegungen induktiv auf a und b an, bis wir eine Darstellung von n als endliches Produkt von Primzahlen erhalten. □

Um sich eine Tabelle von Primzahlen zu konstruieren, kann das Sieb des Eratosthenes genutzt werden:

Das Sieb des Eratosthenes

Man schreibe sich alle natürlichen Zahlen $n \geq 2$ bis zu einer maximalen Schranke M in einer Tabelle auf. Dabei sind zunächst alle Zahlen unmakiert. Die kleinste unmarkierte Zahl ist immer eine Primzahl, wir beginnen also mit der 2. Danach streichen wir alle Zahlen aus der Liste, die ein Vielfaches von dieser unmarkierten Zahl sind. Haben wir dies getan, ist auch die nächst größere unmakierte Zahl eine Primzahl und wir streichen deren Vielfaches aus der Liste.

Sobald das Quadrat der nächsten Primzahl größer als die Schranke M ist, sind alle Primzahlen kleiner oder gleich M bestimmt (es sind die unmarkierten Zahlen der Liste). Dies folgt aus dem Hauptsatz der Arithmetik.

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

Tabelle 2.3: Sieb des Eratosthenes zu $M = 100$.

Notationen 2.5.4

Sei p eine Primzahl.

(1) Wir schreiben $p^k \parallel n$ falls $p^k \mid n$ aber $p^{k+1} \nmid n$. Wir sagen p^k *teilt* n *genau*.

(2) Wir schreiben $\mathrm{ord}_p(n) = k$, wenn $p^k \parallel n$. Wir sagen n hat bezüglich p die Ordnung k.

Beispiel 2.5.5

Für $60 = 2^2 \cdot 3 \cdot 5$ gilt zum Beispiel

$$\mathrm{ord}_2(60) = 2, \quad \mathrm{ord}_3(60) = 1, \quad \mathrm{ord}_5(60) = 1, \quad \mathrm{ord}_7(60) = 0.$$

Satz 2.5.6

Seien $n = p_1^{e_1} \cdot \ldots \cdot p_s^{e_s}$ und $m = p_1^{f_1} \cdot \ldots \cdot p_s^{f_s}$ mit Primzahlen p_k und $e_k, f_k \geq 0$ zwei natürliche Zahlen.

Dann gilt

$$\mathrm{ggT}(m,n) = \prod_{i=1}^{s} p_i^{\min\{e_i,f_i\}} \qquad \text{und} \qquad \mathrm{kgV}(m,n) = \prod_{i=1}^{s} p_i^{\max\{e_i,f_i\}}.$$

Satz 2.5.7

Sei $T \subset \mathbb{N} - \{0\}$ eine endliche Menge und sei p eine Primzahl. Sei weiter $e(k)$ die Anzahl der $t \in T$, für die $p^k \mid t$ gilt.

Dann gilt

$$\operatorname{ord}_p\left(\prod_{t\in T} t\right) \;=\; \sum_{k>0} e(k).$$

Dabei ist zu bemerken, dass die Summe immer endlich ist. Da T endlich ist, wird die Bedingung $p^k \mid t$ für große k für kein $t \in T$ erfüllt.

Mit diesem Satz sind wir zum Beispiel in der Lage die Ordnungen von Fakultäten zu bestimmen:

Beispiel 2.5.8

Wir wollen $\operatorname{ord}_3(100!)$ berechnen. Sei also $T = \{1, 2, 3, \ldots, 100\}$. Damit erhalten wir

$$\begin{aligned}
e(1) &= \operatorname{card}\{n \le 100 \mid 3 \mid n\} = \operatorname{card}\{3 \cdot m \mid 1 \le m \le 33\} = 33,\\
e(2) &= \operatorname{card}\{n \le 100 \mid 9 \mid n\} = \operatorname{card}\{9 \cdot m \mid 1 \le m \le 11\} = 11,\\
e(3) &= \operatorname{card}\{n \le 100 \mid 27 \mid n\} = \operatorname{card}\{27 \cdot m \mid 1 \le m \le 3\} = 3,\\
e(4) &= \operatorname{card}\{n \le 100 \mid 81 \mid n\} = \operatorname{card}\{81 \cdot m \mid 1 \le m \le 1\} = 1.
\end{aligned}$$

Für $k > 4$ gilt $3^k \ge 243 > 100$ und somit $e(k) = 0$ für $k > 4$. Es folgt also

$$\operatorname{ord}_3(100!) \;=\; \operatorname{ord}_3\left(\prod_{t\in T} t\right) \;=\; \sum_{k=1}^{4} e(k) \;=\; 48.$$

Definition 2.5.9

Wir definieren die ***Gauß-Funktion***

$$\begin{aligned}
[\,\cdot\,] : \mathbb{R} &\to \mathbb{Z}\\
x &\mapsto [x]
\end{aligned}$$

mit $[x] \le x < [x] + 1$.

Satz 2.5.10

Für eine Primzahl p und ein $n \in \mathbb{N} - \{0\}$ gilt

$$\operatorname{ord}_p(n!) \;=\; \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \ldots + \left[\frac{n}{p^k}\right],$$

wobei k so zu wählen ist, dass $p^{k+1} \geq n$ gilt. Weiterhin erhalten wir auch

$$n! \;=\; \prod_{\substack{p \leq n \\ p \text{ prim}}} p^{\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\ldots+\left[\frac{n}{p^k}\right]}.$$

Satz 2.5.11 (Euklid)

Es gibt unendlich viele Primzahlen.

Beweis

Angenommen es gibt endlich viele Primzahlen und diese seien $p_1, \ldots, p_m$. Nun betrachten wir

$$N \;:=\; p_1 \cdot \ldots \cdot p_m + 1 \;\in\; \mathbb{N} - \{0\}.$$

Dann gilt aber $p_k \nmid N$ für alle $k = 1, \ldots, m$. Somit können wir keine Primfaktorenzerlegung von N finden und dies ist ein Widerspruch zum Hauptsatz der Arithmetik. □

Satz 2.5.12 (Euler)

Die unendliche Reihe

$$\sum_{p \text{ prim}} \frac{1}{p}$$

divergiert.

Beweis

Angenommen die Reihe konvergiert, dann gibt es ein $s \in \mathbb{N}$ mit

$$\sum_{\substack{p \text{ prim} \\ p > s}} \frac{1}{p} \;<\; \frac{1}{2}.$$

Zudem nutzen wir die Bernoulli-Ungleichung, welche sich leicht durch vollständige Induktion zeigen lässt: Sind $0 \leq a_k \leq 1$ für $k = 1, \ldots, n$ mit $n \geq 2$, so gilt

$$\prod_{k=1}^{n} (1 - a_k) \;\geq\; 1 - \sum_{k=1}^{n} a_k.$$

Damit folgt für alle $r > s$

$$\begin{aligned}\prod_{\substack{p \text{ prim}\\ p\le r}}\left(1-\frac{1}{p}\right) &= \prod_{\substack{p \text{ prim}\\ p\le s}}\left(1-\frac{1}{p}\right)\cdot\prod_{\substack{p \text{ prim}\\ s<p\le r}}\left(1-\frac{1}{p}\right)\\ &\ge \prod_{\substack{p \text{ prim}\\ p\le s}}\left(1-\frac{1}{p}\right)\cdot\left(1-\sum_{\substack{p \text{ prim}\\ s<p\le r}}\frac{1}{p}\right)\\ &\ge \prod_{\substack{p \text{ prim}\\ p\le s}}\left(1-\frac{1}{p}\right)\cdot\left(1-\sum_{\substack{p \text{ prim}\\ p> s}}\frac{1}{p}\right) \;>\; \frac{1}{2}\cdot\prod_{\substack{p \text{ prim}\\ p\le s}}\left(1-\frac{1}{p}\right).\end{aligned}$$

Da aber $1 - p^{-1} < 1$ für alle Primzahlen p, kann die Ungleichung

$$\prod_{\substack{p \text{ prim}\\ p\le r}}\left(1-\frac{1}{p}\right) \;>\; \frac{1}{2}\cdot\prod_{\substack{p \text{ prim}\\ p\le s}}\left(1-\frac{1}{p}\right)$$

für kein $r > s$ erfüllt sein. Damit folgt die Behauptung. □

Es sei bekannt, dass auch die harmonische Reihe

$$\sum_{n=1}^{\infty}\frac{1}{n}$$

divergiert. Die endliche harmonische Reihe

$$\sum_{n=1}^{N}\frac{1}{n}$$

wächst mit der Größenordnung $\log(N)$. Dies zeigt, dass die unendliche Reihe aus dem Satz von Euler noch langsamer divergiert als die harmonische Reihe.

Weiter sei bekannt, dass die Reihe

$$\zeta(s) \;:=\; \sum_{n=1}^{\infty}\frac{1}{n^s}$$

für alle $s > 1$ konvergiert. Weiter ergibt sich das in der Zahlentheorie wichtige ***Euler-Produkt***

$$\zeta(s) \;=\; \prod_{p \text{ prim}}\left(1-p^{-s}\right)^{-1}.$$

Dies folgt aus dem Hauptsatz der Arithmetik, da für jede Primzahl p und $s > 1$ nach der geometrischen Reihe gerade

$$\left(1 - p^{-s}\right)^{-1} \;=\; \frac{1}{1 - \frac{1}{p^s}} \;=\; \sum_{k=0}^{\infty} \left(\frac{1}{p^s}\right)^k$$

gilt.

Satz 2.5.13 (Tschebycheff)

Zu einem $X \in \mathbb{N} - \{0\}$ gibt es Konstanten c und C, so dass

$$c \cdot \log(X) \;<\; \sum_{\substack{p \leq X \\ p \text{ prim}}} \frac{1}{p} \log(p) \;<\; C \cdot \log(X)$$

gilt.

Der Satz von Tschebycheff verdeutlicht damit, dass die *Dichte* der Primzahlen bis X etwa $1/\log(X)$ ist. Es lässt sich sogar zeigen, dass die Anzahl der Primzahlen bis X asymptotisch zu $X/\log(X)$ ist.

Satz 2.5.14 (Dirichlet)

Seien $a, b \in \mathbb{N} - \{0\}$ mit $\mathrm{ggT}(a, b) = 1$.

Dann gibt es in der Menge

$$\{a + nb \mid n \in \mathbb{N}\}$$

unendlich viele Primzahlen.

Trotz langjährigen und aktuellen Bemühungen gibt es immer noch viele Fagen über Primzahlen, die ungeklärt sind. Dies sind zum Beispiel:

(1) Gibt es unendlich viele Primzahlen der Form $n^2 + 1$? Dazu zählen zum Beispiel 5, 17 und 101.

(2) ***Goldbach Problem***: Ist jede gerade Zahl ≥ 6 die Summe von zwei ungeraden Primzahlen?

(3) ***Primzahl Zwillinge***: Gibt es unendlich viele Primzahlen p, so dass auch $p+2$ eine Primzahl ist? Hierzu zählen zum Beispiel 3 und 5 sowie 29 und 31.

2.6 Aufgaben

Aufgabe 2.6.1

Finde alle Lösungen der Gleichung

$$\frac{1}{p} + \frac{1}{q} + \frac{1}{r} \;=\; 1$$

für natürliche Zahlen p, q und r.

Lösung

Keine der Zahlen p, q und r kann den Wert 0 annehmen, da wir nicht durch 0 teilen dürfen.

Keine der Zahlen p, q und r kann den Wert 1 annehmen, denn damit würden wir auf der linken Seite der Gleichung eine Zahl erhalten, die immer größer als 1 ist.

Keine der Zahlen p, q und r kann einen Wert annehmen, der größer oder gleich 7 ist. Die maximale Summe der übrigen beiden Summanden ist $1/2 + 1/3 = 5/6$, jeder Summand muss also mindestens $1/6$ zur Lösung beitragen.

Es muss somit $p, q, r \in \{2, 3, 4, 5, 6\}$ gelten und wir haben eine endliche Menge von Möglichkeiten mit 3^5 Elementen. Diese Möglichkeiten können leicht mit einem PC überprüft werden, wir erhalten die folgenden Lösungstripel:

$$\begin{array}{lllll} (2,3,6), & (2,4,4), & (2,6,3), & (3,2,6), & (3,3,3), \\ (3,6,2), & (4,2,4), & (4,4,2), & (6,2,3), & (6,3,2). \end{array}$$

Aufgabe 2.6.2

Berechne $\mathrm{ggT}(571, 418)$ mit dem Euklidische Algorithmus und finde mit den Eulerschen Rekursionsformeln natürliche Zahlen x und y, so dass

$$\mathrm{ggT}(571, 418) \;=\; x \cdot 571 - y \cdot 418$$

gilt.

Lösung

Der Euklidische Algorithmus liefert:

$$571 \;=\; 1 \cdot 418 + 153$$

$$\begin{aligned} 418 &= 2 \cdot 153 + 112 \\ 153 &= 1 \cdot 112 + 41 \\ 112 &= 2 \cdot 41 + 30 \\ 41 &= 1 \cdot 30 + 11 \\ 30 &= 2 \cdot 11 + 8 \\ 11 &= 1 \cdot 8 + 3 \\ 8 &= 2 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot \mathbf{1}. \end{aligned}$$

Es folgt also $\mathrm{ggT}(571, 418) = 1$. Die Eulerschen Rekursionsformeln liefern nach dem Schema aus Tabelle 2.4

$$x \cdot 571 - y \cdot 418 \;=\; 153 \cdot 571 - 209 \cdot 418 \;=\; 87363 - 87362 \;=\; 1.$$

r	-1	0	1	2	3	4	5	6	7	8	9	10
q_r	$-$	$-$	1	2	1	2	1	2	1	2	1	2
P_r	0	1	1	3	4	11	15	41	56	153	**209**	571
Q_r	1	0	1	2	3	8	11	30	41	112	**153**	418

Tabelle 2.4: Schema zu den Eulerschen Rekursionsformeln.

Aufgabe 2.6.3

Berechne $\mathrm{ggT}(1219, 901)$ mit dem Euklidische Algorithmus und finde mit den Eulerschen Rekursionsformeln natürliche Zahlen x und y, so dass

$$\mathrm{ggT}(1219, 901) \;=\; x \cdot 1219 - y \cdot 901$$

gilt.

Lösung

Der Euklidische Algorithmus liefert:

$$\begin{aligned} 1219 &= 1 \cdot 901 + 318 \\ 901 &= 2 \cdot 318 + 265 \\ 318 &= 1 \cdot 265 + 53 \\ 265 &= 5 \cdot \mathbf{53}. \end{aligned}$$

Es folgt also $\mathrm{ggT}(1219, 901) = 53$. Die Eulerschen Rekursionsformeln liefern nach dem Schema aus Tabelle 2.5

$$x \cdot 1219 - y \cdot 901 \;=\; 3 \cdot 1219 - 4 \cdot 901 \;=\; 3657 - 3604 \;=\; 53.$$

Dieses Ergebnis erhalten wir auch durch direktes Einsetzen in den Gleichungen des Euklidischen Algorithmus:

$$\begin{aligned} 53 &= 318 - 1 \cdot 265 = 318 - 1 \cdot (901 - 2 \cdot 318) \\ &= 3 \cdot 318 - 1 \cdot 901 = 3 \cdot (1219 - 1 \cdot 901) = 3 \cdot 1219 - 4 \cdot 901. \end{aligned}$$

r	-1	0	1	2	3	4
q_r	$-$	$-$	1	2	1	5
P_r	0	1	1	3	**4**	23
Q_r	1	0	1	2	**3**	17

Tabelle 2.5: Schema zu den Eulerschen Rekursionsformeln.

Aufgabe 2.6.4

Seien $a, b, c \in \mathbb{N} - \{0\}$. Zeige, dass gilt:

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

Lösung

Nach der Definition des kleinsten gemeinsamen Vielfachen gilt

$$\begin{aligned} \mathrm{kgV}(\mathrm{kgV}(a,b),c) &= \min\left\{x \in \mathbb{N} \;\middle|\; \mathrm{kgV}(a,b) \mid x \text{ und } c \mid x\right\} \\ &= \min\left(\left\{x \in \mathbb{N} \;\middle|\; c \mid x\right\} \cap \left\{x \in \mathbb{N} \;\middle|\; \mathrm{kgV}(a,b) \mid x\right\}\right) \\ &= \min\left(\left\{x \in \mathbb{N} \;\middle|\; c \mid x\right\} \cap \{\mathrm{kgV}(a,b)\}\right) \\ &= \min\left(\left\{x \in \mathbb{N} \;\middle|\; c \mid x\right\} \cap \left\{x \in \mathbb{N} \;\middle|\; a \mid x \text{ und } b \mid x\right\}\right) \\ &= \min\left\{x \in \mathbb{N} \;\middle|\; a \mid x \text{ und } b \mid x \text{ und } c \mid x\right\} \\ &= \mathrm{kgV}(a,b,c). \end{aligned}$$

Aufgabe 2.6.5

Sei $F_1 = F_2 = 1$ und für $n \geq 3$

$$F_n = F_{n-1} + F_{n-2}$$

die Folge der ***Fibonacci-Zahlen***.

Zeige, dass für $n \geq 2$

$$\mathrm{ggT}(F_n, F_{n+1}) = 1$$

gilt. Bestimme weiter F_n MOD 2.

Lösung

Wenden wir der Euklidische Algorithmus auf zwei aufeinanderfolgende Fibonacci-Zahlen F_n und F_{n+1} an, so erhalten wir:

$$\begin{aligned} F_{n+1} &= 1 \cdot F_n + F_{n-1} \\ F_n &= 1 \cdot F_{n-1} + F_{n-2} \\ F_{n-1} &= 1 \cdot F_{n-2} + F_{n-3} \\ &\vdots \\ 5 &= 1 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 1 \cdot 1 + 1 \\ 1 &= 1 \cdot 1. \end{aligned}$$

Der Euklidische Algorithmus endet also immer mit der Gleichung $1 = 1 \cdot 1$, somit gilt $\mathrm{ggT}(F_n, F_{n+1}) = 1$. Wir erhalten übrigens partielle Quotienten q_k, die alle gleich 1 sind. Daher verläuft der Euklidische Algorithmus bei der Fibonacci-Folge besonders langsam.

Die Addition von zwei ungeraden Zahlen ergibt eine gerade Zahl. Die Addition von einer geraden und einer ungeraden Zahl ergibt eine ungerade Zahl. Die Fibonacci-Folge beginnt mit zwei ungeraden Zahlen, gefolgt von einer geraden, dann wieder zwei ungerade Zahlen, eine gerade und so weiter. Wir erhalten also

$$F_n \text{ MOD } 2 \;=\; \begin{cases} 0 & \text{wenn} \quad 3 \mid n \\ 1 & \text{wenn} \quad 3 \nmid n \end{cases} .$$

Speziell ist F_{1000} ungerade, also F_{1000} MOD $2 = 1$.

Aufgabe 2.6.6

Zeige, dass $2^n + 1$ keine fünfte Potenz einer natürlichen Zahl ist.

Lösung

Wir haben also zu zeigen, dass für kein $n \in \mathbb{N} - \{0\}$ und kein $q \in \mathbb{N} - \{0\}$

$$2^n + 1 \;=\; q^5$$

gilt. Diese Gleichung ist aber äquivalent zu

$$2^n \;=\; (q-1) \cdot (q^4 + q^3 + q^2 + q + 1).$$

Da Potenzen von geraden Zahlen immer gerade und von ungeraden Zahlen immer ungerade sind, ist der Faktor $(q^4+q^3+q^2+q+1)$ für alle $q \in \mathbb{N} - \{0\}$

ungerade. Nun gilt aber für alle $k \in \mathbb{N}$ gerade $(2k+1) \nmid 2^n$, somit gibt es keine ungerade Zahl, die 2^n teilt. Demnach kann es auch keine Lösung der Gleichung

$$2^n \;=\; (q-1)\cdot(q^3+q^3+q^2+q+1).$$

geben.

Aufgabe 2.6.7

Bestimme alle Lösungen des folgenden Systems von Kongruenzen:

$$5x \equiv 2\,(\bmod\ 3\,), \quad 4x \equiv 7\,(\bmod\ 9\,) \quad \text{und} \quad 2x \equiv 4\,(\bmod\ 10\,).$$

Lösung

Zunächst formen wir alle Kongruenzen in äquivalente Aussagen um. Es gilt:

$$5x \equiv 2\,(\bmod\ 3\,) \;\Leftrightarrow\; 10x \equiv 4\,(\bmod\ 3\,) \;\Leftrightarrow\; x \equiv 1\,(\bmod\ 3\,)$$

$$\begin{aligned} 4x \equiv 7\,(\bmod\ 9\,) &\;\Leftrightarrow\; 8x \equiv 14\,(\bmod\ 9\,) \;\Leftrightarrow\; -x \equiv 5\,(\bmod\ 9\,), \\ &\;\Leftrightarrow\; x \equiv -5\,(\bmod\ 9\,) \;\Leftrightarrow\; x \equiv 4\,(\bmod\ 9\,), \end{aligned}$$

$$2x \equiv 4\,(\bmod\ 10\,) \;\Leftrightarrow\; x \equiv 2\,(\bmod\ 5\,).$$

Dabei haben wir die folgenden drei Rechenregeln verwendet:

(1) Für alle $k \in \mathbb{N} - \{0\}$ gilt

$$a \equiv b\,(\bmod\ c\,) \;\Leftrightarrow\; k\cdot a \equiv k\cdot b\,(\bmod\ c\,).$$

(2) Für alle $k \in \mathbb{Z}$ gilt

$$ax \equiv b\,(\bmod\ c\,) \;\Leftrightarrow\; (a-kc)x \equiv b\,(\bmod\ c\,).$$

(3) Für $d = \mathrm{ggT}(a,b,c)$ gilt

$$a \equiv b\,(\bmod\ c\,) \;\Leftrightarrow\; a/d \equiv b/d\,(\bmod\ c/d\,).$$

In der oben erhaltenden Form ist leicht zu erkennen, dass die Lösungen der zweiten Kongruenz eine Teilmenge der Lösungen der ersten Kongruenz ist. Somit haben wir nur das System aus den beiden Kongruenzen

$$x \equiv 4\,(\bmod\ 9\,) \qquad \text{und} \qquad x \equiv 2\,(\bmod\ 5\,)$$

zu untersuchen. Da 5 und 9 teilerfremd sind, können wir den chinesischen Restsatz anwenden: Wir haben also nur eine Lösung x zu finden, die kleiner als $5\cdot 9 = 45$ ist. Es ist leicht zu sehen, dass $x = 22$ diese beiden Kongruenzen löst. Somit ist die gesamt Lösungsmenge M des Systems gerade

$$M \;=\; \{22 + 45k \mid k \in \mathbb{N}\}.$$

Aufgabe 2.6.8

Löse die Kongruenz

$$323x \equiv 120 \,(\bmod\ 1001)\,.$$

Lösung

Um die Lösbarkeit der Kongruenz zu überprüfen, berechnen wir zunächst ggT$(323, 1001)$ mit dem Euklidischen Algorithmus:

$$\begin{aligned} 1001 &= 3 \cdot 323 + 32 \\ 323 &= 10 \cdot 32 + 3 \\ 32 &= 10 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot \mathbf{1} + 0\,. \end{aligned}$$

Die Kongruenz ist lösbar, da $d := \text{ggT}(323, 1001) = 1$ gilt und die Anzahl der Lösungen entspricht gerade d. Wir suchen nun ein x, für das gilt

$$323 \cdot x - 120 \;=\; 1001 \cdot y \quad \Leftrightarrow \quad 120 \;=\; 323 \cdot x - 1001 \cdot y.$$

Nun finden wir mit dem Eulerschen Rekursionsschema in Tabelle 2.6, dass

$$1 \;=\; 323 \cdot 344 - 1001 \cdot 111 \;\Rightarrow\; 120 \;=\; 323 \cdot 344 \cdot 120 - 1001 \cdot 111 \cdot 120\,.$$

Wir haben also mit $x = 344 \cdot 120 = 41280$ eine Lösung gefunden. Nun ist

$$41280 \text{ MOD } 1001 = 239\,,$$

und somit sind alle Lösungen gegeben durch

$$x \;=\; 239 + k \cdot 1001, \quad k \in \mathbb{Z}\,.$$

r	-1	0	1	2	3	4	5
q_r	$-$	$-$	3	10	10	1	2
Q_r	1	0	1	10	101	$\mathbf{111}$	323
P_r	0	1	3	31	313	$\mathbf{344}$	1001

Tabelle 2.6: Eulersches Rekursionsschema zu 323 und 1001.

Aufgabe 2.6.9

Zeige, dass

$$p(n) \;=\; n^4 + 2n^3 + 2n^2 + 2n + 5$$

nur für $n = 2$ eine Quadratzahl ist.

Lösung

Für $n = 0$ erhalten wir 5, für $n = 1$ erhalten wir 12 und für $n = 2$ erhalten wir 49, somit ist der Term

$$n^4 + 2n^3 + 2n^2 + 2n + 5$$

für $n = 2$ eine Quadratzahl, für $n < 2$ hingegen nicht. Nun untersuchen wir den Term für alle $n > 2$. Dazu betrachten wir die beiden Quadratzahlen

$$(n^2+n)^2 \;=\; n^4+2n^3+n^2 \quad \text{und} \quad (n^2+n+1)^2 \;=\; n^4+2n^3+3n^2+2n+1.$$

Damit gilt für $n > 2$ mit Hilfe von $3n^2 + 1 > 2n^2 + 5$

$$\begin{aligned}(n^2+n)^2 &= n^4+2n^3+n^2 \;<\; n^4+2n^3+2n^2+2n+5 \;=\; p(n)\\ &< n^4+2n^3+3n^2+2n+1 \;=\; (n^2+n+1)^2,\end{aligned}$$

somit liegt der gegebene Term für $n > 2$ immer zwischen zwei aufeinander folgenden Quadratzahlen und kann damit selber keine Quadratzahl sein.

Aufgabe 2.6.10

Bestimme die Primfaktorenzerlegung von $n! + 1$ für $n = 1, \ldots, 9$.

Lösung

Es gilt

$$\begin{aligned}1!+1 &= 2,\\ 2!+1 &= 3,\\ 3!+1 &= 7,\\ 4!+1 &= 25 \;=\; 5^2,\\ 5!+1 &= 121 \;=\; 11^2,\\ 6!+1 &= 721 \;=\; 7\cdot 103,\\ 7!+1 &= 5041 \;=\; 71^2,\\ 8!+1 &= 40321 \;=\; 61\cdot 661,\\ 9!+1 &= 362881 \;=\; 19\cdot 71\cdot 269.\end{aligned}$$

Aufgabe 2.6.11

Es seien $F_n := 2^{2^n} - 1$. Zeige, das N eine Potenz von 2 ist, wenn $2^N + 1$ eine Primzahl ist. Zeige umgekehrt

$$2^{32} \;\equiv\; -1 \,(\bmod\; 641)$$

und schließe daraus, dass F_5 keine Primzahl ist.

Lösung

Sei $2^N + 1$ eine Primzahl und wir nehmen an, dass N keine Potenz von 2 ist. Dann gibt es eine ungerade $u \geq 3$, die N teilt. Wir finden damit ein $t \geq 1$, so dass $N = u \cdot t$ gilt. Somit folgt

$$\begin{aligned} 2^N + 1 &= 2^{u \cdot t} + 1 = \left(2^t\right)^u + 1 \\ &= (2^t + 1) \cdot \left(\left(2^t\right)^{u-1} - \left(2^t\right)^{u-2} + \left(2^t\right)^{u-3} - \ldots - 2^t + 1\right). \end{aligned}$$

Somit wäre aber auch $2^N - 1$ keine Primzahl, was ein Widerspruch zur Annahme ist.

Für die Umkehrrichtung gilt zunächst

$$\begin{aligned} 641 &= 640 + 1 = 5 \cdot 2^7 + 1, \\ 641 &= 625 + 16 = 5^4 + 2^4. \end{aligned}$$

Damit ergibt sich

$$5 \cdot 2^7 \equiv -1 \,(\bmod\ 641)$$

und betrachten wir hiervon die vierte Potenz, so erhalten wir

$$5^4 \cdot 2^{28} \equiv 1 \,(\bmod\ 641).$$

Nun ist

$$5^4 \equiv -2^4 \,(\bmod\ 641)$$

und damit

$$5^4 \cdot 2^{28} \equiv -2^4 \cdot 2^{28} \,(\bmod\ 641) \equiv -2^{32} \,(\bmod\ 641) \equiv 1 \,(\bmod\ 641),$$

es folgt

$$2^{2^5} \equiv -1 \,(\bmod\ 641).$$

Schließlich ist $F_5 = 2^{2^5} + 1$ durch 641 teilbar und kann damit keine Primzahl sein.

Aufgabe 2.6.12

Es seien $M_n := 2^n - 1$. Zeige, dass n eine Primzahl ist, wenn M_n eine Primzahl ist. Finde umgekehrt Primzahlen p, für die M_p keine Primzahl ist.

Lösung

Sei M_n eine Primzahl und wir nehmen an, dass n keine Primzahl ist. Dann gibt es $a, b \in \mathbb{N} - \{0\}$ mit $n = a \cdot b$. Damit folgt

$$\begin{aligned} 2^n - 1 &= 2^{a \cdot b} - 1 = (2^a)^b - 1 \\ &= (2^a - 1) \cdot \left((2^a)^{b-1} + (2^a)^{b-2} + \ldots + 2^a + 1 \right). \end{aligned}$$

Somit wäre aber auch $2^n - 1$ kein Primzahl, was ein Widerspruch zur Annahme ist.

Die kleinsten Primzahlen p, für die M_p keine Primzahl ist, sind $\{11, 23, 29\}$. Hier gilt

$$\begin{aligned} M_{11} &= 2047 = 23 \cdot 89, \\ M_{23} &= 8388607 = 47 \cdot 178481, \\ M_{29} &= 536870911 = 233 \cdot 1103 \cdot 2089. \end{aligned}$$

Dass M_{23} keine Primzahl ist, erhalten wir auch durch die folgende Rechnung: Es gilt

$$2^{23} = 2^{20} \cdot 2^3 = 2^{5 \cdot 4} \cdot 2^3 = \left(2^5\right)^4 \cdot 2^3 = \left(32^2\right)^2 \cdot 2^3.$$

Damit ergibt sich

$$\begin{aligned} 2^{23} &\equiv \left(32^2\right)^2 \cdot 2^3 \,(\bmod\ 47) \\ &\equiv (1024)^2 \cdot 2^3 \,(\bmod\ 47) \\ &\equiv (-10)^2 \cdot 2^3 \,(\bmod\ 47) \\ &\equiv 100 \cdot 2^3 \,(\bmod\ 47) \\ &\equiv 6 \cdot 8 \,(\bmod\ 47) \\ &\equiv 48 \,(\bmod\ 47) \\ &\equiv 1 \,(\bmod\ 47). \end{aligned}$$

Dies zeigt, dass 47 die Zahl $M_{23} = 2^{23} + 1$ teilt.

Aufgabe 2.6.13

Zeige, dass für alle $a, b \in \mathbb{N} - \{0\}$

$$\mathrm{ggT}(a^2, b^2) = \mathrm{ggT}(a, b)^2$$

gilt.

Lösung

Es seien

$$a \;=\; p_1^{e_1} \cdot \ldots \cdot p_s^{e_s} \qquad \text{und} \qquad b \;=\; p_1^{f_1} \cdot \ldots \cdot p_s^{f_s}$$

die Primfaktorenzerlegungen von a und b mit $e_k, f_k \geq 0$.

Dann gilt

$$a^2 \;=\; p_1^{2e_1} \cdot \ldots \cdot p_s^{2e_s} \qquad \text{und} \qquad b^2 \;=\; p_1^{2f_1} \cdot \ldots \cdot p_s^{2f_s}$$

und wir erhalten sofort

$$\mathrm{ggT}(a^2, b^2) \;=\; \prod_{i=1}^{s} p_i^{\min\{2e_i, 2f_i\}} \;=\; \left(\prod_{i=1}^{s} p_i^{\min\{e_i, f_i\}} \right)^2 \;=\; \mathrm{ggT}(a, b)^2.$$

Aufgabe 2.6.14

Finde alle Primzahlen p, für die auch $p-2$ sowie $p+2$ eine Primzahl ist.

Lösung

Die Primzahl $p = 2$ kann die Bedingung offenbar nicht erfüllen und auch für $p = 3$ mit $p - 2 = 1$ macht die Aussage keinen Sinn. Somit haben wir nur Primzahlen $p > 3$ zu untersuchen.

Damit erhalten wir aber mit $\{p-2,\, p,\, p+2\}$ ein Tripel von drei ungeraden Zahlen. Von diesen drei Zahlen ist immer genau eine Zahl durch 3 teilbar. Dies zeigt, dass nur für $p = 5$ die drei Zahlen $p-2$, p und $p+2$ Primzahlen sind.

Aufgabe 2.6.15

Vier aufeinanderfolgende Jahre im 21. Jahrhundert haben $4 \cdot 365 + 1$ Tage. Der 1. Januar 2007 ist ein Montag. Berechne den Wochentag vom 1. Januar 2099.

Lösung

Vom 1. Januar 2007 bis zum 1. Januar 2099 vergehen

$$92 \cdot 365 + 23$$

Tage. Nun berechnen wir

$$92 \cdot 365 \;\equiv\; 92 \cdot 1 \,(\bmod\ 7) \;\equiv\; 1 \,(\bmod\ 7)$$

und damit

$$92 \cdot 365 + 23 \equiv 1 + 23 \cdot 1 \,(\bmod\ 7) \equiv 3 \,(\bmod\ 7).$$

Somit ist der 1. Januar 2099 ein *Montag plus* 3 *Tage*, also ein Donnerstag.

Aufgabe 2.6.16

Bestimme die Anzahl der Lösungen $x, y \geq 0$ mit

$$3x + 7y \;=\; 10\,000.$$

Lösung

Zunächst finden wir sofort die Lösung $x = y = 1000$. Eine weitere Lösung wäre

$$x \;=\; 1000 - 7 \qquad \text{und} \qquad y \;=\; 1000 + 3$$

und so weiter. Da $\mathrm{kgV}(3, 7) = 21$, erhalten wir insgesamt

$$\left[\frac{10\,000}{21}\right] \;\approx\; [476, 19] \;=\; 476$$

Lösungen für die gegebene Gleichung.

Aufgabe 2.6.17

Finde das kleinste N, so dass für alle $n \geq N$ die Gleichung

$$3x + 5y \;=\; n$$

mit $x, y \geq 0$ lösbar ist.

Lösung

Die Gleichung

$$3x + 5y \;=\; 7$$

besitzt keine Lösung, die folgenden jedoch schon:

$$\begin{aligned}
3x + 5y &= 8 && \text{mit} \quad x = 1, \;\; y = 1,\\
3x + 5y &= 9 && \text{mit} \quad x = 3, \;\; y = 0,\\
3x + 5y &= 10 && \text{mit} \quad x = 0, \;\; y = 2,\\
3x + 5y &= 11 && \text{mit} \quad x = 2, \;\; y = 1,\\
3x + 5y &= 12 && \text{mit} \quad x = 4, \;\; y = 0.
\end{aligned}$$

Für jedes $n \geq 13$ gilt nun einer der folgenden Fälle:

(1) n ist durch 3 teilbar, dann löst

$$x = \frac{n}{3} \qquad \text{und} \qquad y = 0$$

die Gleichung $3x + 5y = n$.

(2) $n - 5$ ist durch 3 teilbar, dann löst

$$x = \frac{n-5}{3} \qquad \text{und} \qquad y = 1$$

die Gleichung $3x + 5y = n$.

(3) $n - 10$ ist durch 3 teilbar, dann löst

$$x = \frac{n-10}{3} \qquad \text{und} \qquad y = 2$$

die Gleichung $3x + 5y = n$.

Somit ist $N = 8$ die gesuchte kleinste Zahl.

3 Zahlentheoretische Funktionen

Im weiteren Verlauf beschäftigen wir uns mit Funktionen, die auf $\mathbb{N}-\{0\}$ definiert sind. Mit derartigen Funktionen können wir weiter zahlentheoretsiche Aussagen treffen.

3.1 Multiplikative Funktionen

Definition 3.1.1

Eine auf $\mathbb{N}$ definierte Funktion $f : \mathbb{N} \to \mathbb{C}$ nennen wir ***arithmetisch***.

Wir sind dabei vor allem an den folgenden speziellen arithmetischen Funktionen interessiert:

Definition 3.1.2

Eine Funktion $f : \mathbb{N} - \{0\} \to \mathbb{C}$ heißt ***multiplikativ***, wenn für alle teilerfremde m und n

$$f(m \cdot n) \;=\; f(m) \cdot f(n)$$

gilt. f heißt ***streng multiplikativ***, wenn für alle m und n

$$f(m \cdot n) \;=\; f(m) \cdot f(n)$$

gilt.

Satz 3.1.3

Seien $p_1 < \ldots < p_k$ Primzahlen, sei f eine multiplikative Funktion und seien $e_1, \ldots, e_k \in \mathbb{N}$.

Dann gilt

$$f(p_1^{e_1} \cdot \ldots \cdot p_k^{e_k}) \;=\; f(p_1^{e_1}) \cdot \ldots \cdot f(p_k^{e_k}).$$

Dies folgt aus dem Hauptsatz der Arithmetik, da die $p_i^{e_i}$ paarweise teilerfremd sind.

Wichtige multiplikative Funktionen

Wir wollen nun drei wichtige multiplikative Funktionen einführen:

(1) Sei $d : \mathbb{N} - \{0\} \to \mathbb{N}$ mit

$$d(n) \;=\; \sum_{r|n} 1 \;=\; \text{Anzahl der Teiler von } n.$$

(2) Sei $\sigma : \mathbb{N} - \{0\} \to \mathbb{N}$ mit

$$\sigma(n) \;=\; \sum_{d|n} d \;=\; \text{Summe der Teiler von } n.$$

(3) Sei $\varphi : \mathbb{N} - \{0\} \to \mathbb{N}$ mit

$$\varphi(n) \;=\; \mathrm{card}(R^{\times}(n)) \;=\; \text{Anzahl der } x \leq n \text{ mit } (\mathrm{ggT}(n, x) = 1).$$

Bemerkung

Dass die Funktion d multiplikativ ist, folgt direkt mithilfe des Hauptsatzes der Arithmetik. Damit ist auch σ multiplikativ.

Aus dem chinesischen Restsatz folgt schließlich, dass auch φ multiplikativ ist.

Keine der drei Funktionen ist jedoch streng multiplikativ ist, es lassen sich einfach Gegenbeispiele konstruieren.

Beispiel 3.1.4

Die Teiler von 24 sind

$$1,\ 2,\ 3,\ 4,\ 6,\ 8,\ 12 \text{ und } 24.$$

Somit gilt

$$d(24) \;=\; 8 \qquad \text{und} \qquad \sigma(24) \;=\; 60.$$

Die folgenden Zahlen x sind kleiner gleich 24 mit $\mathrm{ggT}(24, x) = 1$:

$$1,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19 \text{ und } 23.$$

Demnach folgt

$$\varphi(24) \;=\; 8.$$

Satz 3.1.5

Für jede Primzahl p und $k \geq 1$ gilt

$$d(p^k) \;=\; k+1, \qquad \sigma(p^k) \;=\; \frac{p^{k+1}-1}{p-1} \qquad \text{und} \qquad \varphi(p^k) \;=\; p^k - p^{k-1}.$$

Ist uns die Primfaktorenzerlegung einer natürlichen Zahl n bekannt, können wir nach diesem Satz sehr einfach die Funktionswerte der multiplikativen Funktionen d, σ und φ berechnen.

Beweis

Die einzigen Teiler von p^k sind

$$T \;=\; \{1,\; p,\; p^2,\; \ldots,\; p^k\},$$

damit folgt direkt $d(p^k) = k+1$ und die Formel für $\sigma(p^k)$ ergibt sich aus der endlichen geometrischen Reihe.

Da wir mit T aber gerade alle Teiler von p^k gefunden haben, sind in der Menge

$$S \;=\; \{1,\; 2,\; 3,\; 4,\; \ldots,\; p^k\}$$

genau die Elemente aus

$$U \;=\; \{p,\; 2p,\; 3p,\; \ldots,\; p^{k-1}p\}$$

nicht teilerfremd zu p^k und damit ergibt sich $\varphi(p^k) = p^k - p^{k-1}$. □

Beispiel 3.1.6

Es gilt

$$24 \;=\; 2^3 \cdot 3.$$

Damit erhalten wir

$$\begin{aligned}
d(24) &= d(2^3)\cdot d(3^1) \;=\; 4\cdot 2 \;=\; 8,\\
\sigma(24) &= \sigma(2^3)\cdot \sigma(3^1) \;=\; \frac{2^4-1}{1}\cdot\frac{3^2-1}{2} \;=\; 15\cdot 4 \;=\; 60,\\
\varphi(24) &= \varphi(2^3)\cdot \varphi(3^1) \;=\; (2^3-2^2)\cdot(3^1-3^0) \;=\; 4\cdot 2 \;=\; 8.
\end{aligned}$$

3.2 Arithmetische Faltungen

Definition 3.2.1

Seien $f, g : \mathbb{N} - \{0\} \to \mathbb{C}$ zwei arithmetische Funktionen.

Dann definieren wir die ***arithmetische Faltung*** durch

$$(f * g)(n) \ := \ \sum_{d|n} f(d) \cdot g(n/d).$$

Lemma 3.2.2

Für die arithmetische Faltung gilt:

(1) $f * g \ = \ g * f$.

(2) $(f * g) * h \ = \ f * (g * h)$.

(3) Sind f und g multiplikativ, dann auch $f * g$.

Beispiel 3.2.3

Wir definieren $\mathbf{1} : \mathbb{N} - \{0\} \to \mathbb{N}$ mit

$$\mathbf{1}(n) \ = \ 1 \qquad \text{für alle} \qquad n \in \mathbb{N} - \{0\}.$$

Diese Funktion ist offenbar multiplikativ und wir erhalten

$$(\mathbf{1} * \mathbf{1})(n) \ = \ \sum_{d|n} \mathbf{1}(d) \cdot \mathbf{1}(n/d) \ = \ \sum_{d|n} 1 \ = \ d(n).$$

Damit haben wir auch die Multiplikativität von d gezeigt.

Beispiel 3.2.4

Wir definieren $E : \mathbb{N} - \{0\} \to \mathbb{N}$ mit

$$E(n) \ = \ \begin{cases} 1 & \text{für} \quad n = 1 \\ 0 & \text{für} \quad n \neq 1 \end{cases}.$$

Damit gilt für eine multiplikative Funktion f

$$(f * E)(n) \ = \ \sum_{d|n} f(d) \cdot E(n/d) \ = \ f(n).$$

Wir nennen die Funktion E daher ***Einheit***.

3.3 Die Möbius-Funktion

Definition 3.3.1

Die ***Möbius-Funktion*** $\mu : \mathbb{N} - \{0\} \to \{-1, 0, 1\}$ sei multiplikativ und es gelte:

(1) $\mu(1) = 1$.

(2) $\mu(p) = -1$ für jede Primzahl p.

(3) $\mu(p^k) = 0$ für jede Primzahl p mit $k \geq 2$.

Damit ist μ wohldefiniert.

n	1	2	3	4	5	6	7	8	9	10
$\mu(n)$	1	-1	-1	0	-1	1	-1	0	0	1
n	11	12	13	14	15	16	17	18	19	20
$\mu(n)$	-1	0	-1	1	1	0	-1	0	-1	0
n	21	22	23	24	25	26	27	28	29	30
$\mu(n)$	1	1	-1	0	0	1	0	0	-1	-1

Tabelle 3.1: Die ersten Funktionswerte der Möbius-Funktion.

Satz 3.3.2

Es gilt

$$m(n) \;:=\; \sum_{d|n} \mu(d) \;=\; \begin{cases} 1 & \text{für} \quad n = 1 \\ 0 & \text{für} \quad n \neq 1 \end{cases} .$$

Beweis

Für $n = 1$ ist die Behauptung klar. Es gilt $m = \mathbf{1} * \mu$, somit ist auch m multiplikativ. Für $n > 1$ gilt für jede Primzahl p für $k \geq 1$ gerade

$$\begin{aligned} m(p^k) &= \sum_{j \leq k} \mu(p^j) \;=\; \mu(1) + \mu(p) + \mu(p^2) + \ldots + \mu(p^k) \\ &= 1 + (-1) + 0 + \ldots + 0 \;=\; 0. \end{aligned}$$

Aus der Multiplikativität und dem Hauptsatz der Arithmetik folgt nun die Behauptung. □

Satz 3.3.3 (Möbius-Inversion)

Sei f eine arithmetische Funktion und sei

$$F(n) \;:=\; (f * \mathbf{1})(n) \;=\; \sum_{d|n} f(d).$$

Dann gilt

$$(\mu * F)(n) \;=\; \sum_{d|n} \mu(n/d) \cdot F(d) \;=\; \sum_{d|n} \mu(d) \cdot F(n/d) \;=\; f(n).$$

Der Name Inversion stammt daher, dass wir hier die eigentliche Funktion f aus ihrer *Summation* F zurückgewinnen können.

Wir erhalten damit nun einige Aussagen:

Beispiel 3.3.4

(1) Es gilt mit $f(n) = \mathbf{1}(n) = 1$ für alle $n \in \mathbb{N}$

$$F(n) \;=\; \sum_{d|n} f(d) \;=\; \sum_{d|n} 1 \;=\; d(n).$$

Wir erhalten damit

$$\sum_{r|n} \mu(n/r) \cdot d(r) \;=\; 1.$$

(2) Ähnlich erhalten wir

$$\sum_{d|n} \mu(n/d) \cdot \sigma(d) \;=\; n.$$

(3) Es gilt außerdem

$$\sum_{d|n} \varphi(d) \;=\; n \qquad \text{und} \qquad \varphi(n) \;=\; \sum_{d|n} \mu(d) \cdot (n/d).$$

3.4 Dirichlet-Reihen

Sei a eine arithmetische Funktion. Dann definieren wir

$$f(s, a) \;=\; \sum_{n=1}^{\infty} \frac{a(n)}{n^s}$$

als die ***Dirichlet-Reihe*** zu $a(n)$. Es gilt also zum Beispiel

$$f(s,\mathbf{1}) \;=\; \sum_{n=1}^{\infty} \frac{1}{n^s} \;=\; \zeta(s) \qquad \text{und} \qquad f(s,E) \;=\; \frac{1}{1^s} \;=\; 1.$$

Für zwei Funktionen a und b erhalten wir

$$f(s,a) \cdot f(s,b) \;=\; f(s, a * b).$$

Die arithmetische Faltung entspricht also der Multiplikation der entsprechenden Dirichlet-Reihen.

Beispiel 3.4.1

Mit Hilfe von Dirichlet-Reihen erhalten wir die folgenden Ergebnisse:

(1) Mit $d = \mathbf{1} * \mathbf{1}$ erhalten wir

$$\sum_{n=1}^{\infty} \frac{d(n)}{n^s} \;=\; \zeta^2(s).$$

Diese Reihe ist für alle $s > 1$ konvergent.

(2) Sei $a(n) = n$. Mit $\sigma = \mathbf{1} * a$ erhalten wir

$$\sum_{n=1}^{\infty} \frac{\sigma(n)}{n^s} \;=\; \zeta(s) \cdot \zeta(s-1).$$

Diese Reihe ist für alle $s > 2$ konvergent.

(3) Ähnlich erhalten wir

$$\sum_{n=1}^{\infty} \frac{\varphi(n)}{n^s} \;=\; \frac{\zeta(s-1)}{\zeta(s)}.$$

Diese Reihe ist für alle $s > 2$ konvergent.

3.5 Kongruenzarithmetik

Wir hatten bereits $R(n)$ definiert als die Äquivalenzklassen von $\mathbb{N}\,(\bmod n)$ sowie

$$R^{\times}(n) \;:=\; \{a\,(\bmod n) \in R(n) \mid \mathrm{ggT}(a,n) = 1\} \;\subset\; R(n).$$

Wir wissen auch, das $R^{\times}(n)$ unter der Multiplikation eine Gruppe bildet. Daran wollen wir nun anknüpfen.

Bemerkung 3.5.1

In der Algebra ist ein Element a aus einem Ring $\mathcal{R}$ mit Einselement e eine ***Einheit***, wenn es ein b in $\mathcal{R}$ mit $a \cdot b = e$ gibt. Die Menge der Einheiten wird in der Regel mit $\mathcal{R}^\times$ bezeichnet.

In unseren Ringen $R(n)$ ist die Menge der Einheiten gerade die Menge der Zahlen a aus $R(n)$, die zu n teilerfremd sind. Somit entspricht $R^\times(n)$ hier auch gerade der Menge der Einheiten.

Definition 3.5.2

Für ein $a \in R^\times(n)$ definieren wir die ***Ordnung*** von a in $R^\times(n)$ als die kleinste Zahl $k > 0$ mit

$$a^k \equiv 1 \,(\bmod\ n\,).$$

Wir schreiben dann $\mathrm{ord}^n(a) = k$.

Weiterhin definieren wir die Ordnung von n als die Kardinalität von $R^\times(n)$.

Wir schreiben $\mathrm{ord}(n) = \mathrm{card}(R^\times(n))$.

Achtung!

Wir haben damit drei ähnliche Bezeichnungen für unterschiedliche Ordnungen verwendet:

(1) Wir schreiben $\mathrm{ord}_p(n) = k$, wenn n bezüglich p die Ordnung k hat, siehe Notation 2.5.4.

(2) Wir schreiben $\mathrm{ord}^n(a) = k$, wenn

$$a^k \equiv 1 \,(\bmod\ n\,)$$

gilt und $k > 0$ mit dieser Eigenschaft minimal ist.

(3) Wir schreiben $\mathrm{ord}(n)$ für die Kardinalität von $R^\times(n)$.

Satz 3.5.3 (Euler-Fermat)

Für alle $x \in R^\times(n)$ gilt

$$x^{\varphi(n)} \equiv 1 \,(\bmod\ n\,).$$

Beweisskizze

Die Ordnung $\mathrm{ord}^n(x) = \mathrm{card}(G)$ ist nach dem Satz von Lagrange eine Teiler von $\varphi(n) = \mathrm{ord}(n)$, da

$$G \;=\; \{1,\; x,\; x^2,\; \ldots,\; x^{\mathrm{ord}^n(x)-1}\}$$

eine Untergruppe von $R^\times(n)$ ist.

Zudem gilt nach Definition

$$x^{\mathrm{ord}^n(x)} \;\equiv\; 1\,(\bmod\; n\,)$$

und damit auch

$$x^{\varphi(n)} \;\equiv\; 1\,(\bmod\; n\,).$$

Speziell gilt der folgende Satz:

Satz 3.5.4 (Fermat)

Sei p eine Primzahl.

Für ein a mit $a \not\equiv 0\,(\bmod\; p\,)$, also $a \in R^\times(p)$, gilt

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

Für alle a mit $a \equiv 0\,(\bmod\; p\,)$, also $a \notin R^\times(p)$, gilt

$$a^{p} \;\equiv\; a\,(\bmod\; p\,).$$

Satz 3.5.5 (Wilson)

Sei p eine Primzahl. Dann gilt

$$(p-1)! \;\equiv\; -1\,(\bmod\; p\,).$$

Beweisskizze

Die Fälle $p = 2$ und $p = 3$ sind schnell nachgerechnet, daher sei $p \geq 5$.

Wir betrachten die Mengen

$$\{1, -1\} \qquad \text{und} \qquad \{a, a^{-1}\} \quad \text{für} \quad a \;\in\; R^\times(p) - \{1\},$$

dabei gelte $a \cdot a^{-1} \;\equiv\; 1\,(\bmod\; p\,)$.

Damit erhalten wir $(p-1)/2$ Mengen, die eine disjunkte Zerlegung von $R^\times(n)$ darstellen und in der jede Menge wirklich aus zwei Elementen besteht.

Nun gilt

$$1 \cdot (-1) \equiv -1 \,(\bmod\ p)$$

sowie für alle $a \in R^\times(p)$ gerade

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

Somit ist das Produkt aller Zahlen aus $R^\times(n)$ gerade -1, was die Behauptung zeigt.

Im folgenden Abschnitt werden wir Anwendungen der wichtigen Sätze von Fermat und Wilson diskutieren. Zunächst geben wir jedoch zwei weitere Ergebnisse an.

Satz 3.5.6

Sei

$$\varepsilon(n) \equiv \left(\prod_{x \in R^\times(n)} x \right) \,(\bmod\ n).$$

Dann gilt

$$\varepsilon(n) \equiv -1 \,(\bmod\ n)$$

falls $n \in \{1, 2, 4, p^k, 2p^k\}$ für alle Primzahlen p und

$$\varepsilon(n) \equiv 1 \,(\bmod\ n)$$

für alle anderen n.

Satz 3.5.7

Sei $p > 2$ eine Primzahl und $k > 0$. Dann hat

$$x^2 \equiv 1 \,(\bmod\ p^k)$$

genau zwei Lösungen in $R(n)$, nähmlich

$$x \equiv 1 \,(\bmod\ p^k) \qquad \text{und} \qquad x \equiv -1 \,(\bmod\ p^k).$$

Wir wissen nun, dass $\varphi(n)$ für alle $n > 2$ gerade ist. Ungeklärt bleibt die Frage, ob es zu jedem m mit $\varphi(m) = N$ eine weiter Zahl $m' \neq m$ gibt, so dass auch $\varphi(m') = N$ gilt.

n	1	2	3	4	5	6	7	8	9	10
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4
n	11	12	13	14	15	16	17	18	19	20
$\varphi(n)$	10	4	16	6	8	8	16	6	18	8

Tabelle 3.2: Die ersten Funktionswerte von $\varphi(n)$.

3.6 Anwendungen der Sätze von Fermat und Wilson

In diesem Abschnitt wollen wir auf einige Beispiele und Anwendungsmöglichkeiten der vorherigen Sätze von Euler-Fermat, Fermat und Wilson eingehen.

Beispiel 3.6.1

In diesem Beispiel wollen wir einmal die Aussagekraft der vorherigen Sätze untersuchen.

Wir betrachten die Zahl

$$n \;=\; 1729 \;=\; 10^3 + 9^3 \;=\; 12^3 + 1^1 \;=\; 7 \cdot 13 \cdot 19.$$

Für alle x, die zu 7, 13 bzw. 19 teilerfremd sind, gilt nach dem Satz von Fermat

$$\begin{aligned} x^6 &\equiv 1 \,(\bmod\ 7\,), \\ x^{12} &\equiv 1 \,(\bmod\ 13\,), \\ x^{18} &\equiv 1 \,(\bmod\ 19\,). \end{aligned}$$

Das kleinste gemeinsame Vielfache von $\{6, 12, 18\}$ ist 36, somit folgt für alle x, die zu 7, 13 und 19 teilerfremd sind,

$$x^{36} \equiv 1 \,(\bmod\ 1729\,).$$

Mit $\varphi(1729) = 6 \cdot 12 \cdot 18 = 1296$ liefert der Satz von Euler-Fermat nur

$$x^{1296} \equiv 1 \,(\bmod\ 1729\,).$$

Pseudoprimzahlen

Sei n eine ungerade Zahl. Dazu berechnen wir $k = 2^{n-1}$ MOD n.

Ist n eine Primzahl, so gilt nach dem Satz von Fermat $k = 1$. Ist n keine Primzahl, dann gilt *meistens* $k \neq 1$. Gilt umgekehrt $k = 1$, dann ist n also *meistens* eine Primzahl, wir sprechen dann von einer ***Pseudoprimzahl***.

Mit $1728 = 12^3 = 36 \cdot 48$ folgt

$$2^{1728} \equiv 1 \,(\mathrm{mod}\ 1729),$$

somit ist 1729 eine Pseudoprimzahl, aber keine Primzahl.

Periodenlänge

Sei $q \in \mathbb{N} - \{0\}$. Dazu betrachten wir die rationale Zahl

$$\frac{1}{q} \;=\; 0, b_0 \ldots b_k \overline{c_1 \ldots c_s} \;=\; 0, b_0 \ldots b_k + \frac{1}{10^{k+1}} \cdot \frac{c_1 \ldots c_s}{9 \ldots 9}.$$

Sei zunächst $\mathrm{ggT}(q, 10) = 1$. Aus den vorherigen Sätzen folgt dann, dass die Periodenlänge s von $1/q$ gerade die kleinste Zahl s mit

$$10^s \equiv 1 \,(\mathrm{mod}\ q)$$

ist. Gilt $\mathrm{ggT}(q, 10) \neq 1$, so hat $1/q$ eine Periodenlänge von 0.

Beispiele 3.6.2

Für $q = 7$ mit $\varphi(7) = 6$ sowie $\mathrm{ggT}(7, 10) = 1$ erhalten wir nach dem Satz von Euler-Fermat

$$10^6 \equiv 1 \,(\mathrm{mod}\ 7).$$

Die Zahl 6 ist auch die kleinste Zahl, die diese Bedingung erfüllt. Somit ist die Periodenlänge von $1/6$ gerade $s = 6$. In der Tat gilt

$$\frac{1}{7} \;=\; 0,142857142857142857142857142857142857\ldots \;=\; 0, \overline{142857}.$$

Für $q = 81$ erhalten wir mit

$$10^9 \equiv 1 \,(\mathrm{mod}\ 81)$$

eine Periodenlänge von 9:

$$\frac{1}{81} \;=\; 0, \overline{012345679}.$$

Für $q = 25$ gilt $\mathrm{ggT}(10, 25) = 5 \neq 1$. Somit hat $1/25$ eine Periodenlänge von 0, es gilt

$$\frac{1}{25} \;=\; 0,04.$$

Satz 3.6.3 (Lagrange)

Sei p eine Primzahl, seien $a_0, \ldots, a_{n-1} \in \mathbb{Z}$ und sei

$$f(x) \;=\; x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0.$$

Dann gibt es höchstens n Restklassen $u \,(\bmod\ p)$, so dass

$$f(u) \;\equiv\; 0 \,(\bmod\ p)$$

gilt.

Beispiel 3.6.4

Der Satz von Fermat behauptet

$$x^{p-1} - 1 \;\equiv\; 0 \,(\bmod\ p)$$

für alle $x \not\equiv 0 \,(\bmod\ p)$ zu einer Primzahl p. Nun gilt aber auch

$$(x-1)\cdot(x-2)\cdot\ldots\cdot(x-p+1) \;\equiv\; 0 \,(\bmod\ p)$$

für alle $x \not\equiv 0 \,(\bmod\ p)$. Wir betrachten

$$f(x) \;=\; (x-1)\cdot(x-2)\cdot\ldots\cdot(x-p+1)$$

als Polynom vom Grad $p-1$, das mit x^{p-1} beginnt. Die $p-1$ Nullstellen sind die Restklassen

$$1 \,(\bmod\ p), \qquad 2 \,(\bmod\ p), \qquad \ldots, \qquad p-1 \,(\bmod\ p).$$

Nach dem Satz von Lagrange muss damit auch

$$\left(x^{p-1} - 1\right) - (x-1)(x-2)\ldots(x-p+1) \;\equiv\; 0 \,(\bmod\ p)$$

gelten, also

$$x^{p-1} - 1 \;\equiv\; (x-1)(x-2)\ldots(x-p+1) \,(\bmod\ p).$$

Setzen wir nun $x = 0$, so erhalten wir

$$-1 \;\equiv\; (-1)^{p-1} 1\cdot 2\cdot\ldots\cdot(p-1) \,(\bmod\ p).$$

Dies ist aber gerade äquivalent zu

$$(p-1)! \;\equiv\; -1 \,(\bmod\ p),$$

was der Satz von Wilson besagt.

3.7 Primitivwurzeln

Definition 3.7.1

Sei n eine positive natürliche Zahl.

Die Restklasse $g \,(\mathrm{mod}\ n)$ heißt ***Primitivwurzel modulo*** n, falls

$$g \in R^\times(n) \qquad \text{und} \qquad \mathrm{ord}^n(g) = \varphi(n)$$

gilt. Die zweite Bedingung bedeutet also, dass die Zahlen

$$1, g, g^2, \ldots, g^{\varphi(n)-1} \,(\mathrm{mod}\ n)$$

alle unterschiedlich sind, dass also g ein erzeugendes Element von $R^\times(n)$ ist.

Wenn es eine Primituvwurzel g modulo n gibt, dann können wir die Elemente von $R^\times(n)$ durch

$$g^k \cdot g^l \equiv g^{(k+l) \bmod \varphi(n)} \,(\mathrm{mod}\ n)$$

multiplizieren. Die Multiplikation kann also durch eine Addition ersetzt werden.

Die Aussage, dass es eine Primituvwurzel modulo n gibt, ist äquivalent zur Aussage, dass die Gruppe $R^\times(n)$ zyklisch ist.

Satz 3.7.2

Es gibt genau dann eine Primituvwurzel modulo n, wenn

$$n \in \{1, 2, 4, p^k, 2p^k \mid p > 2 \text{ ist eine Primzahl}, \ k \geq 1\}$$

gilt.

Satz 3.7.3

Sei g eine Primituvwurzel modulo n.

Dann ist auch g^r genau dann eine Primituvwurzel modulo n, wenn

$$\mathrm{ggT}(r, \varphi(n)) = 1$$

gilt.

Insbesondere gibt es $\varphi(\varphi(n))$ Primituvwurzeln modulo n, sofern es überhaupt eine gibt.

Beispiel 3.7.4

Wir wollen alle Primitivwurzel modulo $n = 18$ bestimmen.

Es gilt $18 = 2 \cdot 3^2$, somit wissen wir, dass es überhaupt Primitivwurzeln gibt. Weiter gilt

$$\varphi(18) \;=\; \varphi(2) \cdot \varphi(3^2) \;=\; 6 \qquad \text{sowie} \qquad \varphi(6) \;=\; \varphi(2) \cdot \varphi(3) \;=\; 2,$$

somit hat die Gruppe $R^\times(18)$ genau sechs Elemente und es gibt zwei Primituvwurzeln modulo 18. Nach Definition haben wir nur die Elemente aus

$$R^\times(18) \;=\; \{1, 5, 7, 11, 13, 17\}$$

darauf hin zu überprüfen, ob sie die ganze Menge $R^\times(18)$ erzeugen, ob sie also die Ordnung 6 haben. Die 1 kann niemals eine Primitivwurzel sein, somit beginnen wir mit der 5:

$$\begin{aligned}
5 &\equiv 5 \,(\bmod\ 18) \\
5 \cdot 5 &\equiv 25 \,(\bmod\ 18) \equiv 7 \,(\bmod\ 18) \\
5 \cdot 7 &\equiv 35 \,(\bmod\ 18) \equiv -1 \,(\bmod\ 18) \\
5 \cdot (-1) &\equiv -5 \,(\bmod\ 18) \\
5 \cdot (-5) &\equiv -25 \,(\bmod\ 18) \equiv -7 \,(\bmod\ 18) \\
5 \cdot (-7) &\equiv -35 \,(\bmod\ 18) \equiv 1 \,(\bmod\ 18).
\end{aligned}$$

Damit gilt $\mathrm{ord}^{18}(5) = 6 = \varphi(18)$ und somit ist 5 eine Primitivwurzel modulo 18. Nun untersuchen wir die 7:

$$\begin{aligned}
7 &\equiv 7 \,(\bmod\ 18) \\
7 \cdot 7 &\equiv 49 \,(\bmod\ 18) \equiv -5 \,(\bmod\ 18) \\
7 \cdot (-5) &\equiv -35 \,(\bmod\ 18) \equiv 1 \,(\bmod\ 18),
\end{aligned}$$

es gilt also $\mathrm{ord}^{18}(7) = 3 < \varphi(18)$ und damit ist 7 keine Primitivwurzel. Kommen wir zur 11:

$$\begin{aligned}
11 &\equiv 11 \,(\bmod\ 18) \\
11 \cdot 11 &\equiv 121 \,(\bmod\ 18) \equiv -5 \,(\bmod\ 18) \\
11 \cdot (-5) &\equiv -55 \,(\bmod\ 18) \equiv -1 \,(\bmod\ 18) \\
11 \cdot (-1) &\equiv -11 \,(\bmod\ 18) \\
11 \cdot (-11) &\equiv -121 \,(\bmod\ 18) \equiv 5 \,(\bmod\ 18) \\
11 \cdot 5 &\equiv 55 \,(\bmod\ 18) \equiv 1 \,(\bmod\ 18),
\end{aligned}$$

damit ist auch 11 eine Primitivwurzel modulo 18. Wir wissen, dass es nur $\varphi(\varphi(18)) = 2$ Primitivwurzeln geben kann und diese haben wir nun mit 5 und 11 gefunden.

Definition 3.7.5

Sei $n \in \mathbb{N}$ so gewählt, dass es eine Primitivwurzel modulo n gibt.

Sei g eine Primitivwurzel modulo n. Dann schreiben wir für jedes $a \in R^{\times}(n)$

$$\mathrm{ind}_g(a) \;=\; \min\{k \geq 1 \mid g^k \equiv a \,(\mathrm{mod}\; n)\}.$$

Für $a, b \in R^{\times}(n)$ gilt dann

$$\mathrm{ind}_g(a \cdot b) \equiv \mathrm{ind}_g(a) + \mathrm{ind}_g(b) \,(\mathrm{mod}\; \varphi(n)),$$

dies zeigt noch einmal, dass Multiplikation durch Addition ersetzt werden kann.

Beispiel 3.7.6

In diesem abschließenden Beispiel wollen wir zeigen, dass 2 eine Primitivwurzel modulo $n = 163$ ist.

Da 163 eine Primzahl ist, folgt für die Kardinalität von $R^{\times}(163)$

$$\mathrm{card}(R^{\times}(163)) \;=\; 162 \;=\; 2 \cdot 81 \;=\; 2 \cdot 3^4.$$

Die möglichen Ordnungen von 2 sind daher die Teiler von 162:

$$1,\;\; 2,\;\; 3,\;\; 6,\;\; 9,\;\; 18,\;\; 27,\;\; 54,\;\; 81,\;\; 162.$$

Wenn wir zeigen können, dass

$$2^{54} \not\equiv 1 \,(\mathrm{mod}\; 163) \qquad \text{und} \qquad 2^{81} \not\equiv 1 \,(\mathrm{mod}\; 163)$$

gilt, dann muss 2 die Ordnung 162 besitzen und wäre damit eine Primitivwurzel modulo 163. Nun gilt

$$54 \;=\; 32 + 16 + 4 + 2 \qquad \text{und} \qquad 81 \;=\; 64 + 16 + 1$$

und damit folgt

$$\begin{aligned}
2^1 &\equiv 2 \,(\mathrm{mod}\; 163) \\
2^2 &\equiv 4 \,(\mathrm{mod}\; 163) \\
2^4 &\equiv 16 \,(\mathrm{mod}\; 163) \\
2^8 &\equiv -70 \,(\mathrm{mod}\; 163) \\
2^{16} &\equiv 10 \,(\mathrm{mod}\; 163) \\
2^{32} &\equiv 100 \,(\mathrm{mod}\; 163)
\end{aligned}$$

$$\begin{aligned}
2^{64} &\equiv 57 \,(\bmod\ 163) \\
2^{54} &\equiv 2^{32} \cdot 2^{16} \cdot 2^4 \cdot 2^2 \\
&\equiv 100 \cdot 10 \cdot 16 \cdot 4 \,(\bmod\ 163) \equiv 104 \,(\bmod\ 163) \\
2^{81} &\equiv 2^{64} \cdot 2^{16} \cdot 2^1 \,(\bmod\ 163) \\
&\equiv 57 \cdot 10 \cdot 2 \,(\bmod\ 163) \equiv -1 \,(\bmod\ 163).
\end{aligned}$$

Dies zeigt, dass $\mathrm{ord}^{163}(2) = 162$ gilt und somit ist 2 tatsächlich eine Primitivwurzel modulo 163. Wir können also alle Restklassen $(\bmod\ 163)$ mit Ausnahme der 0 also Potenzen der 2 darstellen.

Es stellt sich heraus, dass auch 3 eine Primitivwurzel modulo $n = 163$ ist, die 5 hingegen nicht.

3.8 Aufgaben

Aufgabe 3.8.1

Berechne $d(10!)$, $\sigma(10!)$ sowie $\varphi(10!)$.

Lösung

Es gilt

$$\begin{aligned}
10! &= 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \\
&= 2 \cdot 3 \cdot 2 \cdot 2 \cdot 5 \cdot 2 \cdot 3 \cdot 7 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 2 \cdot 5 \;=\; 2^8 \cdot 3^4 \cdot 5^2 \cdot 7,
\end{aligned}$$

dies ist also die Primfaktorenzerlegung von 10!. Nach Lemma 3.1.5 erhalten wir damit

$$\begin{aligned}
d(10!) &= 9 \cdot 5 \cdot 3 \cdot 2 \;=\; 270, \\
\sigma(10!) &= \frac{2^9 - 1}{1} \cdot \frac{3^5 - 1}{2} \cdot \frac{5^3 - 1}{4} \cdot \frac{7^2 - 1}{6} \;=\; 15334088, \\
\varphi(10!) &= (2^8 - 2^7) \cdot (3^4 - 3^3) \cdot (5^2 - 5) \cdot (7 - 1) \;=\; 829440.
\end{aligned}$$

Aufgabe 3.8.2

Bestimme die Periodenlänge von $\frac{17}{101}$.

Lösung

Die Periodenlänge muss ein Teiler von $101 - 1 = 100$ sein. Wenn 10 eine Primitivwurzel modulo 100 wäre, dann würden wir die maximale Periodenlänge von 100 erhalten.

In unserem Beispiel gilt aber

$$\frac{17}{101} \;=\; \frac{17}{101} \cdot \frac{99}{99} \;=\; \frac{1683}{9999} \;=\; 0,\overline{1683}.$$

Die Periodenlänge von $\frac{17}{101}$ ist also 4 und es gibt keine Vorperiode.

Aufgabe 3.8.3

Finde jeweils das kleinste $n \in \mathbb{N} - \{0\}$, so dass

$$2^n \equiv 1 \,(\bmod\ 17) \qquad \text{bzw.} \qquad 3^n \equiv 1 \,(\bmod\ 17)$$

gilt.

Lösung

Da 17 eine Primzahl ist und da $2 \not\equiv 0 \,(\bmod\ 17)$ bzw. $3 \not\equiv 0 \,(\bmod\ 17)$ gilt, folgt nach dem Satz von Fermat

$$2^{16} \equiv 1 \,(\bmod\ 17) \qquad \text{bzw.} \qquad 3^{16} \equiv 1 \,(\bmod\ 17).$$

Nun müssen wir noch prüfen, ob $n = 16$ wirklich die kleinste Zahl mit der gegebenen Bedingung ist. Es gilt

$$\begin{aligned}
2 &\equiv 2 \,(\bmod\ 17) \\
2 \cdot 2 &\equiv 4 \,(\bmod\ 17) \\
2 \cdot 4 &\equiv 8 \,(\bmod\ 17) \\
2 \cdot 8 &\equiv 16 \,(\bmod\ 17) \equiv -1 \,(\bmod\ 17) \\
2 \cdot (-1) &\equiv -2 \,(\bmod\ 17) \\
2 \cdot (-2) &\equiv -4 \,(\bmod\ 17) \\
2 \cdot (-4) &\equiv -8 \,(\bmod\ 17) \\
2 \cdot (-8) &\equiv -16 \,(\bmod\ 17) \equiv 1 \,(\bmod\ 17),
\end{aligned}$$

somit ist im ersten Fall sogar $n = 8$ die kleinste Zahl mit

$$2^n \equiv 1 \,(\bmod\ 17).$$

Im zweiten Falle ist tatsächlich $n = 16$ die kleinste Zahl mit

$$3^n \equiv 1 \,(\mathrm{mod}\ 17),$$

dies zeigen die folgenden Kongruenzen:

$$\begin{aligned}
3 &\equiv 3 \,(\mathrm{mod}\ 17) \\
3 \cdot 3 &\equiv 9 \,(\mathrm{mod}\ 17) \\
3 \cdot 9 &\equiv 27 \,(\mathrm{mod}\ 17) \equiv 10 \,(\mathrm{mod}\ 17) \\
3 \cdot 10 &\equiv 30 \,(\mathrm{mod}\ 17) \equiv -4 \,(\mathrm{mod}\ 17) \\
3 \cdot (-4) &\equiv -12 \,(\mathrm{mod}\ 17) \\
3 \cdot (-12) &\equiv -36 \,(\mathrm{mod}\ 17) \equiv -2 \,(\mathrm{mod}\ 17) \\
3 \cdot (-2) &\equiv -6 \,(\mathrm{mod}\ 17) \\
3 \cdot (-6) &\equiv -18 \,(\mathrm{mod}\ 17) \equiv -1 \,(\mathrm{mod}\ 17) \\
3 \cdot (-1) &\equiv -3 \,(\mathrm{mod}\ 17) \\
3 \cdot (-3) &\equiv -9 \,(\mathrm{mod}\ 17) \\
3 \cdot (-9) &\equiv -27 \,(\mathrm{mod}\ 17) \equiv -10 \,(\mathrm{mod}\ 17) \\
3 \cdot (-10) &\equiv -30 \,(\mathrm{mod}\ 17) \equiv 4 \,(\mathrm{mod}\ 17) \\
3 \cdot 4 &\equiv 12 \,(\mathrm{mod}\ 17) \\
3 \cdot 12 &\equiv 36 \,(\mathrm{mod}\ 17) \equiv 2 \,(\mathrm{mod}\ 17) \\
3 \cdot 2 &\equiv 6 \,(\mathrm{mod}\ 17) \\
3 \cdot 6 &\equiv 18 \,(\mathrm{mod}\ 17) \equiv 1 \,(\mathrm{mod}\ 17).
\end{aligned}$$

Aufgabe 3.8.4

Für alle $n \in \mathbb{N} - \{0\}$ definieren wir

$$\Lambda(n) \ := \ \begin{cases} \log p & \text{falls } n \text{ Potenz der Primzahl } p \\ 0 & \text{sonst} \end{cases} .$$

Zeige, dass Λ keine multiplikative Funktion ist. Zeige weiter

$$\sum_{d|n} \Lambda(d) \ = \ \log n$$

und folgere daraus, dass

$$\sum_{d|n} \mu(d) \log(n/d) \ = \ \Lambda(n) \qquad \text{sowie} \qquad \sum_{d|n} \mu(d) \log(d) \ = \ -\Lambda(n)$$

gilt.

Lösung

Seien p und q zwei unterschiedliche Primzahlen. Dann gilt

$$\Lambda(p \cdot q) \;=\; 0 \;\neq\; \log p \cdot \log q \;=\; \Lambda(p) \cdot \Lambda(q).$$

Dies zeigt, dass Λ keine multiplikative Funktion ist.

Sei nun $n = p_1^{e_1} \cdot \ldots \cdot p_s^{e_s}$ die Primfaktorenzerlegung einer beliebigen natürlichen Zahl n. Betrachten wir nur die Teiler d von n, für die $\Lambda(d) \neq 0$ gilt, dann erhalten wir direkt

$$\begin{aligned}
\sum_{d|n} \Lambda(d) &= \Lambda(p_1) + \ldots + \Lambda(p_1^{e_1}) + \ldots + \Lambda(p_s) + \ldots + \Lambda(p_s^{e_s}) \\
&= \underbrace{\log(p_1) + \ldots + \log(p_1)}_{e_1 \text{ Summanden}} + \ldots + \underbrace{\log(p_s) + \ldots + \log(p_s)}_{e_s \text{ Summanden}} \\
&= \log\left(p_1^{e_1} \cdot \ldots \cdot p_s^{e_s}\right) \;=\; \log n.
\end{aligned}$$

Für die nächte Behauptung nutzen wir die Möbius-Inversion:

Sei $f(n) = \Lambda(n)$. Mit dem vorherigen Ergebnis erhalten wir

$$F(k) \;:=\; \sum_{r|k} \Lambda(r) \;=\; \log(k).$$

Mit der Möbius-Inversion aus Satz 3.3.3 folgt sofort

$$\sum_{d|n} \mu(d) \cdot \log(n/d) \;=\; \sum_{d|n} \mu(d) \cdot F(n/d) \;=\; f(n) \;=\; \Lambda(n).$$

Nach Satz 3.3.2 ist bekannt, dass $\sum_{d|n} \mu(d) = 0$ gilt für alle $n > 1$. Somit folgt mit dem zweiten Ergebnis und der Gleichungskette

$$\begin{aligned}
\sum_{d|n} \mu(d)\log(d) + \Lambda(n) &= \sum_{d|n} \mu(d)\log(d) + \sum_{d|n} \mu(d)\log(n/d) \\
&= \sum_{d|n} \mu(d)\left(\log(d) + \log(n/d)\right) \\
&= \sum_{d|n} \mu(d)\log(n) \;=\; \log(n) \cdot \sum_{d|n} \mu(d) \;=\; 0
\end{aligned}$$

die letzte Behauptung.

Aufgabe 3.8.5

Finde das kleinste $m \in \mathbb{N} - \{0\}$, so dass für jedes zu 65 teilerfremde $x \in \mathbb{N} - \{0\}$

$$x^m \;\equiv\; 1 \,(\bmod\; 65)$$

gilt.

Lösung

Zunächst können wir die gegebene Kongruenz nach dem chinesischen Restsatz in

$$x^m \equiv 1 \,(\mathrm{mod}\ 5) \qquad \text{und} \qquad x^m \equiv 1 \,(\mathrm{mod}\ 13)$$

zerlegen. Wir wissen nach dem Satz von Fermat, dass

$$x^4 \equiv 1 \,(\mathrm{mod}\ 5) \qquad \text{und} \qquad x^{12} \equiv 1 \,(\mathrm{mod}\ 13)$$

gilt. Es bleibt also zu prüfen, ob $m = 12$ wirklich die kleinste Zahl ist, die die gegebene Bedingung für alle zu 65 teilerfremde x erfüllt. Dazu wählen wir $x = 2$:

$$\begin{aligned}
2 &\equiv 2 \,(\mathrm{mod}\ 13) \\
2 \cdot 2 &\equiv 4 \,(\mathrm{mod}\ 13) \\
2 \cdot 4 &\equiv 8 \,(\mathrm{mod}\ 13) \\
2 \cdot 8 &\equiv 16 \,(\mathrm{mod}\ 13) \equiv 3 \,(\mathrm{mod}\ 13) \\
2 \cdot 3 &\equiv 6 \,(\mathrm{mod}\ 13) \\
2 \cdot 6 &\equiv 12 \,(\mathrm{mod}\ 13) \equiv -1 \,(\mathrm{mod}\ 13) \\
2 \cdot (-1) &\equiv -2 \,(\mathrm{mod}\ 13) \\
2 \cdot (-2) &\equiv -4 \,(\mathrm{mod}\ 13) \\
2 \cdot (-4) &\equiv -8 \,(\mathrm{mod}\ 13) \\
2 \cdot (-8) &\equiv -16 \,(\mathrm{mod}\ 13) \equiv -3 \,(\mathrm{mod}\ 13) \\
2 \cdot (-3) &\equiv -6 \,(\mathrm{mod}\ 13) \\
2 \cdot (-6) &\equiv -12 \,(\mathrm{mod}\ 13) \equiv 1 \,(\mathrm{mod}\ 13).
\end{aligned}$$

Dieses Beispiel zeigt, dass tatsächlich $m = 12$ die kleinste Zahl ist, für die

$$x^m \equiv 1 \,(\mathrm{mod}\ 65)$$

für jedes zu 65 teilerfremde x gilt.

Aufgabe 3.8.6

Finde alle Primitivwurzeln modulo 8.

Lösung

Zunächst halten wir fest, dass es nach Satz 3.7.2 überhaupt keine Primitivwurzeln modulo 8 geben kann, dies wollen wir aber auch noch zeigen:

Es gilt

$$\varphi(8) \;=\; \varphi(2^3) \;=\; 4 \qquad \text{und} \qquad \varphi(4) \;=\; \varphi(2^2) \;=\; 2.$$

Wir erhalten

$$R^{\times}(8) \;=\; \{1, 3, 5, 7\}.$$

Die 1 kann wie üblich keine Primitivwurzel sein und für 3, 5 und 7 erhalten wir eine Ordnung von $2 < \varphi(8)$:

$$\begin{aligned} 3^2 &\equiv 9 \,(\bmod\ 8) \equiv 1 \,(\bmod\ 8), \\ 5^2 &\equiv 25 \,(\bmod\ 8) \equiv 1 \,(\bmod\ 8), \\ 7^2 &\equiv 49 \,(\bmod\ 8) \equiv 1 \,(\bmod\ 8). \end{aligned}$$

Wir haben also noch einmal gezeigt, dass es keine Primitivwurzeln modulo 8 gibt.

Aufgabe 3.8.7

Bestimme die Anzahl der Primitivwurzeln modulo 73.

Lösung

Die Zahl $73 > 2$ ist eine Primzahl, somit gibt es mindestens eine Primitivwurzel modulo 73. Für die Anzahl haben wir lediglich $\varphi(\varphi(73))$ zu bestimmen:

$$\varphi(\varphi(73)) \;=\; \varphi(72) \;=\; \varphi(2^3 \cdot 3^2) \;=\; \varphi(2^3) \cdot \varphi(3^2) \;=\; 4 \cdot 6 \;=\; 24.$$

Aufgabe 3.8.8

Finde das kleinste $s > 0$ mit

$$10^s \;\equiv\; 1 \,(\bmod\ 17).$$

Lösung

17 ist eine Primzahl, es gilt $\varphi(17) = 16$ und weiter $10 \in R^{\times}(17)$. Somit gilt nach Euler-Fermat

$$10^{16} \;\equiv\; 1 \,(\bmod\ 17).$$

Ob 16 wirklich die kleinste Zahl mit dieser Bedingung ist, bleib zu prüfen:

$$\begin{aligned}
10 &\equiv 10 \,(\mathrm{mod}\ 17) \\
10 \cdot 10 &\equiv 100 \,(\mathrm{mod}\ 17) \equiv -2 \,(\mathrm{mod}\ 31) \\
10 \cdot (-2) &\equiv -20 \,(\mathrm{mod}\ 17) \equiv -3 \,(\mathrm{mod}\ 31) \\
10 \cdot (-3) &\equiv -30 \,(\mathrm{mod}\ 17) \equiv 4 \,(\mathrm{mod}\ 31) \\
10 \cdot 4 &\equiv 40 \,(\mathrm{mod}\ 17) \equiv 6 \,(\mathrm{mod}\ 31) \\
10 \cdot 6 &\equiv 60 \,(\mathrm{mod}\ 17) \equiv -8 \,(\mathrm{mod}\ 31) \\
10 \cdot (-8) &\equiv -80 \,(\mathrm{mod}\ 17) \equiv 5 \,(\mathrm{mod}\ 31) \\
10 \cdot 5 &\equiv 50 \,(\mathrm{mod}\ 17) \equiv -1 \,(\mathrm{mod}\ 31)
\end{aligned}$$

Nun wiederholt sich auf Grund der -1 bei 10^8 alle mit umgekehrten Vorzeichen und wir erkennen daher, dass $s = 16$ wirklich die kleinste Zahl mit der gegebenen Bedingung ist.

Zudem gilt $\mathrm{ggT}(17, 10) = 1$, somit hat $1/17$ eine Periodenlänge von $s = 16$.

Aufgabe 3.8.9

Bestimme alle Primitivwurzeln modulo 31.

Lösung

Zunächst gilt $\varphi(31) = 30$ und

$$\varphi(30) \;=\; \varphi(2 \cdot 3 \cdot 5) \;=\; \varphi(2) \cdot \varphi(3) \cdot \varphi(5) \;=\; 2 \cdot 4 \;=\; 8,$$

es gibt also 8 Primitivwurzeln modulo 31. Weiter haben wir

$$R^{\times}(31) \;=\; \{1, 2, 3, 4, 5, \ldots, 30\}$$

und die Teiler von 30 sind

$$1, \quad 2, \quad 3, \quad 5, \quad 6, \quad 10, \quad 15 \quad \text{und} \quad 30.$$

Die Ordnungen von den Restklassen aus $R^{\times}(31)$ können also nur diese 8 Werte annehmen.

Zunächst wollen wir überprüfen, ob 3 eine Primitivwurzel modulo 31 ist. Es gilt

$$\begin{aligned}
3 &\equiv 3 \,(\mathrm{mod}\ 31) \\
3 \cdot 3 &\equiv 9 \,(\mathrm{mod}\ 31) \\
3 \cdot 9 &\equiv 27 \,(\mathrm{mod}\ 31) \equiv -4 \,(\mathrm{mod}\ 31) \\
3 \cdot (-4) &\equiv -12 \,(\mathrm{mod}\ 31) \\
3 \cdot (-12) &\equiv -36 \,(\mathrm{mod}\ 31) \equiv -5 \,(\mathrm{mod}\ 31) \\
3 \cdot (-5) &\equiv -15 \,(\mathrm{mod}\ 31).
\end{aligned}$$

Nun folgt damit

$$\begin{aligned} 3^{10} &\equiv 3^5 \cdot 3^5 \,(\mathrm{mod}\ 31) \equiv (-5)^2 \,(\mathrm{mod}\ 31) \equiv -6 \,(\mathrm{mod}\ 31) \\ 3^{15} &\equiv 3^{10} \cdot 3^5 \,(\mathrm{mod}\ 31) \equiv (-6) \cdot (-5) \,(\mathrm{mod}\ 31) \equiv -1 \,(\mathrm{mod}\ 31) \\ 3^{30} &\equiv 3^{15} \cdot 3^{15} \,(\mathrm{mod}\ 31) \equiv (-1) \cdot (-1) \,(\mathrm{mod}\ 31) \equiv 1 \,(\mathrm{mod}\ 31), \end{aligned}$$

somit ist die Ordnung von 3 gerade 30 und daher ist $3 \in R^\times(31)$ eine Primitivwurzel modulo 31.

Haben wir eine Primitivwurzel erst einmal gefunden, dann können wir nach Satz 3.7.3 auch auf weitere Primitivwurzel schließen: Ist g eine Primitivwurzel modulo n, dann ist auch g^r genau dann eine Primitivwurzel modulo n, wenn

$$\mathrm{ggT}(r, \varphi(n)) \;=\; 1$$

gilt. In unserem Falle gilt nur für die acht Zahlen

$$r \;\in\; \{1, 7, 11, 13, 17, 19, 23, 29\} \;=:\; R$$

$\mathrm{ggT}(r, 30) = 1$. Da wir nun wissen, dass 3 eine Primitivwurzel modulo 31 und da wir zudem auch wissen, dass es genau 8 Primitivwurzel geben muss, müssen gerade die acht Zahlen 3^r mit $r \in R$ die gesuchten Primitvwurzeln sein. Nun müssen wir diese noch berechnen:

$$\begin{aligned} 3 \cdot (-15) &\equiv -45 \,(\mathrm{mod}\ 31) \equiv 17 \,(\mathrm{mod}\ 31) \equiv 3^7 \,(\mathrm{mod}\ 31) \\ 3 \cdot (-6) &\equiv -18 \,(\mathrm{mod}\ 31) \equiv 13 \,(\mathrm{mod}\ 31) \equiv 3^{11} \,(\mathrm{mod}\ 31) \\ 3^2 \cdot 13 &\equiv 117 \,(\mathrm{mod}\ 31) \equiv 24 \,(\mathrm{mod}\ 31) \equiv 3^{13} \,(\mathrm{mod}\ 31) \\ 3^2 \cdot (-1) &\equiv -9 \,(\mathrm{mod}\ 31) \equiv 22 \,(\mathrm{mod}\ 31) \equiv 3^{17} \,(\mathrm{mod}\ 31) \\ 3^2 \cdot (-9) &\equiv -81 \,(\mathrm{mod}\ 31) \equiv 12 \,(\mathrm{mod}\ 31) \equiv 3^{19} \,(\mathrm{mod}\ 31) \\ 12 \cdot (-12) &\equiv -144 \,(\mathrm{mod}\ 31) \equiv 11 \,(\mathrm{mod}\ 31) \equiv 3^{23} \,(\mathrm{mod}\ 31) \\ 11 \cdot (-15) &\equiv -165 \,(\mathrm{mod}\ 31) \equiv 21 \,(\mathrm{mod}\ 31) \equiv 3^{29} \,(\mathrm{mod}\ 31). \end{aligned}$$

Die gesuchten Primitivwurzeln modulo 31 sind damit

$$3, \quad 17, \quad 13, \quad 24, \quad 22, \quad 12, \quad 11 \quad \text{und} \quad 21.$$

Aufgabe 3.8.10

Zeige, dass es genau sechs Zahlen n gibt, so dass es genau 8 Primitivwurzeln modulo n gibt.

Lösung

Wir wissen, dass die Anzahl der Primitivwurzeln modulo n gerade $\varphi(\varphi(n))$ ist. Weiter wissen wir, dass es nur dann eine Primitivwurzel modulo n geben

kann, wenn

$$n \in \{1, 2, 4, p^k, 2p^k \mid p > 2 \text{ ist eine Primzahl}, \ k \geq 1\}$$

gilt. Nun ist leicht einzusehen, dass $\varphi(x) = 8$ nur für

$$x \in \{15, 16, 20, 24, 30\} =: X$$

erfüllt wird. Wir erhalten also zu p^k genau dann 8 Primitivwurzeln modulo p^k, wenn

$$\varphi(p^k) = p^k - p^{k-1} \in X = \{15, 16, 20, 24, 30\}$$

gilt. Auch hier ist leicht einzusehen, dass dies nur für

$$p^k = 17^1, \qquad p^k = 31^1 \qquad \text{und} \qquad p^k = 5^2$$

erfüllt ist. Mit diesen Werte von p^k folgt auch

$$\varphi(2p^k) = p^k - p^{k-1} \in X = \{15, 16, 20, 24, 30\},$$

damit gibt es nur sechs Zahlen n, so dass es genau 8 Primitivwurzeln modulo n gibt und diese sechs Zahlen sind

$$17, \quad 34, \quad 31, \quad 62, \quad 25 \quad \text{und} \quad 50.$$

Aufgabe 3.8.11

Bestimme die letzten vier Stellen in der Dezimaldarstellung von 2^{504}.

Lösung

Wir versuchen auf das Problem den Satz von Euler-Fermat anzuwenden. Es gilt

$$\varphi(5^4) = 5^4 - 5^3 = 500,$$

also folgt direkt nach Euler-Fermat

$$2^{500} \equiv 1 \,(\bmod\ 5^4)$$

und damit auch

$$2^{504} \equiv 16 \,(\bmod\ 5^4).$$

Nun gilt $2^4 \mid 2^{504}$ und $2^4 \mid 16$ und somit auch

$$2^{504} \equiv 16 \,(\bmod\ 5^4 \cdot 2^4) \equiv 16 \,(\bmod\ 10^4),$$

Die letzten vier Stellen in der Dezimaldarstellung von 2^{504} sind damit

$$0016.$$

Aufgabe 3.8.12

Zeige $3^{400} \equiv 1 \,(\mathrm{mod}\ 1000)$.

Lösung

Mit $1000 = 2^3 \cdot 5^3$ und damit $\varphi(1000) = 4 \cdot 100 = 400$ folgt aus dem Satz von Euler-Fermat direkt

$$3^{400} = 3^{\varphi(1000)} \equiv 1 \,(\mathrm{mod}\ 1000),$$

da $\mathrm{ggT}(3, 1000) = 1$.

4 Quadratische Kongruenzen

In der Zahlenthoerie ist man häufig daran interessiert Kongruenzen der Form

$$a_m x^m + \ldots + a_1 x + a_0 \equiv 0 \,(\bmod\ n)$$

zu lösen. Dazu betrachten wir das Polynom

$$f(x) \;=\; a_m x^m + \ldots + a_1 x + a_0$$

mit $a_0, \ldots, a_m \in \mathbb{N}$. Es reicht dabei n von der Form p^k für $k \geq 1$ zu betrachten. Soll ein Problem mit

$$n \;=\; p_1^{k_1} \cdot \ldots \cdot p_s^{k_s}$$

gelöst werden, so bestimmen wir die Lösungen von

$$\begin{aligned} f(x_1) &\equiv 0 \,(\bmod\ p_1^{k_1}), \\ f(x_2) &\equiv 0 \,(\bmod\ p_2^{k_2}), \\ &\vdots \\ f(x_s) &\equiv 0 \,(\bmod\ p_s^{k_s}). \end{aligned}$$

Nach dem chinesischen Restsatz finden wir dann auch ein ξ, so dass

$$f(\xi) \equiv 0 \,(\bmod\ n)$$

gilt.

Für ein allgemeines $f(x)$ sind diese Probleme unglaublich schwer zu lösen. Wir beschränken uns daher an dieser Stelle nur auf die Fälle $m = 1$ (lineare Kongruenzen) und $m = 2$ (quadratische Kongruenzen).

4.1 Lineare Kongruenzen

Wir betrachten nur ***lineare Kongruenzen*** zu einem

$$f(x) \;=\; a_1 x + a_0.$$

Wie zuvor beschrieben, betrachten wir nur die Fälle $n = p^k$ für eine Primzahl p und $k \geq 1$.

Wir bezeichnen mit l die größte natürliche Zahl, so dass p^l die Zahl a_1 teilt. Damit führen wir einige Fallunterscheidungen durch:

(1) Falls $l \geq k$ gilt, erhalten wir

$$0 \cdot x + a_0 \;=\; a_0 \;\equiv\; 0 \,(\bmod\; p^k\,).$$

Somit gibt es entweder gar keine Lösung x oder alle x lösen die gegebene lineare Kongruenz.

(2) Für $l < k$ und $p^l \nmid a_0$ gibt es keine Lösung.

(3) Wir untersuchen nun den Fall $l < k$ und $p^l \mid a_0$. Dazu suchen wir natürliche Zahlen $\overline{a_0}$ und $\overline{a_1}$, so dass

$$a_0 \;=\; p^l \cdot \overline{a_0} \qquad \text{und} \qquad a_1 \;=\; p^l \cdot \overline{a_1}$$

gilt. Damit erhalten wir das äquivalente Problem

$$\overline{a_1} \cdot x \;\equiv\; -\overline{a_0} \,(\bmod\; p^{k-l}\,).$$

Alle b, die die Kongruenz

$$b \cdot \overline{a_1} \;\equiv\; 1 \,(\bmod\; p^{k-l}\,)$$

lösen, sind damit auch Ergebnisse der gesuchen linearen Kongruenz, denn es gilt

$$x \;\equiv\; -b \cdot \overline{a_0} \,(\bmod\; p^{k-l}\,).$$

4.2 Quadratische Kongruenzen

Nun beschäftigen wir uns mit ***quadratischen Kongruenzen*** zu einem

$$f(x) \;=\; a_2x^2 + a_1x + a_0.$$

Wir untersuchen also die Lösbarkeit von

$$f(x) \;\equiv\; 0 \,(\bmod\; p^k\,)$$

für eine Primzahl p und $k \geq 1$.

Eine allgemeine Lösung dieses Problems ist schon so kompliziert, dass wir hier nur einen wichtigen Spezialfall betrachten:

Satz 4.2.1

Seien a_0, a_1, a_2 und die Primzahl $p > 2$ so gewählt, dass

$$a_2 \in R^\times(p) \qquad \text{und} \qquad d := a_1^2 - 4a_0a_2 \in R^\times(p)$$

gilt, dass also $\mathrm{ggT}(a_2, p) = \mathrm{ggT}(d, p) = 1$ gilt.

Dann hat die quadratische Kongruenz

$$a_2x^2 + a_1x + a_0 \equiv 0 \,(\mathrm{mod}\ p^k)$$

keine Lösung, wenn

$$y^2 \equiv d \,(\mathrm{mod}\ p)$$

keine Lösung besitzt. Anderenfalls hat

$$a_2x^2 + a_1x + a_0 \equiv 0 \,(\mathrm{mod}\ p^k)$$

zwei Lösungen, wenn

$$y^2 \equiv d \,(\mathrm{mod}\ p)$$

lösbar ist.

Beweisidee

Der Beweis nutzt im Wesentlichen die quadratische Ergänzung.

Für alle $x \in \mathbb{N}$ gilt

$$\begin{aligned} & a_2x^2 + a_1x + a_0 \equiv 0 \,(\mathrm{mod}\ p^k) \\ \Leftrightarrow \quad & 4a_2^2x^2 + 4a_2a_1x + 4a_2a_0 \equiv 0 \,(\mathrm{mod}\ p^k) \\ \Leftrightarrow \quad & (2a_2x + a_1)^2 \equiv a_1^2 - 4a_2a_0 \,(\mathrm{mod}\ p^k). \end{aligned}$$

Ist nun z eine Lösung der Kongruenz

$$z^2 \equiv a_1^2 - 4a_2a_0 \,(\mathrm{mod}\ p^k),$$

dann ist die Lösung y von

$$2a_2y + a_1 \equiv z \,(\mathrm{mod}\ p^k)$$

auch eine Lösung von $y^2 \equiv d \,(\mathrm{mod}\ p)$.

Ist umgekehrt $z^2 \equiv a_1^2 - 4a_2a_0 \,(\mathrm{mod}\ p^k)$ nicht lösbar, dann auch $y^2 \equiv d \,(\mathrm{mod}\ p)$ nicht.

Dieser Satz rechtfertigt damit auch, dass wir im Folgenden nur Kongruenzen der Form

$$y^2 \equiv d \,(\mathrm{mod}\ p)$$

lösen werden.

4.3 Quadratische Reste

Definition 4.3.1

Sei $p > 2$ eine Primzahl.

Wir sagen, dass $d \in R^\times(p)$ ein ***quadratischer Rest modulo*** p ist, falls

$$y^2 \equiv d \,(\mathrm{mod}\ p)$$

lösbar ist. Umgekehrt heißt $d \in R^\times(p)$ ein ***quadratischer Nichtrest modulo*** p, falls

$$y^2 \equiv d \,(\mathrm{mod}\ p)$$

nicht lösbar ist.

Beispiel 4.3.2

Sei $p > 2$ eine beliebige Primzahl. Dann hat

$$-1 \in R^\times(p)$$

die Ordnung 2 und es gibt eine Primitivwurzel g modulo p. Die beiden Elemente der Ordnung 2 sind von der Gestalt

$$1 \,(\mathrm{mod}\ p) \qquad \text{und} \qquad g^{\frac{p-1}{2}} \,(\mathrm{mod}\ p),$$

es gilt also

$$-1 \equiv g^{\frac{p-1}{2}} \,(\mathrm{mod}\ p).$$

Somit ist -1 genau dann ein Quadrat, wenn $(p-1)/2$ gerade ist, wenn also

$$p - 1 \equiv 0 \,(\mathrm{mod}\ 4) \qquad \text{bzw.} \qquad p \equiv 1 \,(\mathrm{mod}\ 4)$$

gilt. Es folgt damit sofort, dass

$$y^2 \equiv -1 \,(\mathrm{mod}\ p) \qquad \text{bzw.} \qquad y^2 \equiv p - 1 \,(\mathrm{mod}\ p)$$

genau dann lösbar ist, wenn

$$p \equiv 1 \,(\mathrm{mod}\ 4)$$

gilt. Somit ist $p-1$ genau dann ein quadratischer Rest modulo p, wenn $p-1$ ein Vielfaches von 4 ist.

Satz 4.3.3 (Euler-Kriterium)

Sei $p > 2$ eine Primzahl und $d \in R^{\times}(p)$, also $\mathrm{ggT}(d, p) = 1$.

Dann ist d genau dann ein quadratischer Rest modulo p, wenn

$$d^{\frac{p-1}{2}} \equiv 1 \,(\mathrm{mod}\ p)$$

gilt.

Da stets

$$d^{\frac{p-1}{2}} \equiv 1 \,(\mathrm{mod}\ p) \qquad \text{oder} \qquad d^{\frac{p-1}{2}} \equiv -1 \,(\mathrm{mod}\ p)$$

gilt, folgt umgekehrt, dass d genau dann ein quadratischer Nichtrest modulo p ist, wenn

$$d^{\frac{p-1}{2}} \equiv -1 \,(\mathrm{mod}\ p)$$

gilt.

Beispiel 4.3.4

Wir betrachten das Beispiel $p = 7$ und wollen alle quadratischen Reste d modulo 7 für $d < 7$ bestimmt.

Diese sind nach Tabelle 4.1 gerade 1, 2 und 4.

d	1	2	3	4	5	6
$d^{\frac{p-1}{2}}$	1	8	27	64	125	216
$d^{\frac{p-1}{2}}$ MOD 7	1	1	-1	1	-1	-1

Tabelle 4.1: Zur Berechnung der quadratischen Reste modulo 7.

4.4 Quadratisches Reziprozitätsgesetz

Das Ziel in diesem Abschnitt ist es zu verstehen, dass die Lösbarkeit von

$$y^2 \equiv d \,(\mathrm{mod}\ p)$$

für ein festes $d \in \mathbb{Z}$ nur von

$$p \,(\mathrm{mod}\ 4|d|)$$

abhängt. Dazu untersuchen wir die entsprechenden quadratischen Reste.

Zunächst bedarf es jedoch einiger Vorbereitungen.

Definition 4.4.1

Sei $p > 2$ eine Primzahl.

Dann definieren wir das ***Legendre-Symbol*** als

$$\left(\frac{d}{p}\right) \;:=\; \begin{cases} 1 & \text{falls} \quad d \text{ ein quadratischer Rest modulo } p \text{ ist} \\ -1 & \text{falls} \quad d \text{ ein quadratischer Nichtrest modulo } p \text{ ist} \end{cases}.$$

Nach dieser Definition besitzt die Kongruenz

$$y^2 \equiv d \,(\bmod\ p\,)$$

genau dann eine Lösung, wenn mit $d \in R^{\times}(p)$ gerade

$$\left(\frac{d}{p}\right) \;=\; 1$$

gilt. Das Ziel ist es nun das Legendre-Symbol noch weiter zu verallgemeinern, um damit weitere Aussagen zur Lösbarbeit derartiger quadratischer Kongruenzen treffen zu können.

Mit Hilfe des vorherigen Abschnitts lassen sich nun leicht einige Eigenschaften des Legendre-Symbols zeigen:

Eigenschaften des Legendre-Symbols

Sei $p > 2$ eine Primzahl und seien $d, d_1, d_2 \in R^{\times}(p)$. Dann gilt:

(1) Es folgt sofort

$$\left(\frac{1}{p}\right) \;=\; 1,$$

da $y^2 \equiv 1 \,(\bmod\ p\,)$ mit $y = 1$ immer lösbar ist.

(2) Es folgt weiter

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

(3) Es gilt für d_1, d_2 mit $\mathrm{ggT}(d_1, p) = \mathrm{ggT}(d_2, p) = 1$

$$\left(\frac{d_1 \cdot d_2}{p}\right) \;=\; \left(\frac{d_1}{p}\right) \cdot \left(\frac{d_2}{p}\right).$$

(4) Die Funktion $\left(\frac{d}{p}\right)$ hängt nur von $d \,(\bmod\ p)$ ab.

(5) Es gibt $(p-1)/2$ quadratische Rest sowie $(p-1)/2$ quadratische Nichtreste modulo p.

Damit folgen auch sofort einige Eigenschaften für quadratische Reste modulo einer Primzahl $p > 2$:

Eigenschaften von quadratischen Resten

Sei $p > 2$ eine Primzahl. Dann gilt:

(1) Das Produkt aus einem quadratischen Nichtrest mit einem quadratischen Nichtrest modulo p ist ein quadratischer Rest modulo p.

(2) Das Produkt aus einem quadratischen Rest mit einem quadratischen Nichtrest modulo p ist ein quadratischer Nichtrest modulo p.

(3) Das Produkt aus einem quadratischen Rest mit einem quadratischen Rest modulo p ist ein quadratischer Rest modulo p.

Lemma 4.4.2 (Gauß)

Sei $p > 2$ eine Primzahl und sei $S \subset \{1, 2, \ldots, p-1\}$ so gewählt, dass für jedes $x \in R^\times(p)$ entweder $x \in S$ oder $-x \in S$ gilt, aber nicht beides gleichzeitig. Weiter sei $a \in R^\times(p)$ und $s = \mathrm{card}((-S) \cap (aS))$.

Dann gilt

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

Hierbei gelte

$$(-S) \;=\; \{-s \in R^\times(p) \mid s \in S\} \quad \text{und} \quad (aS) \;=\; \{as \in R^\times(p) \mid s \in S\}.$$

Mögliche Beispiele für S sind

$$S \;=\; \{1, 2, 3, \ldots, (p-1)/2\} \qquad \text{oder} \qquad S \;=\; \{1, 3, 5, 7, \ldots, p-2\}.$$

Beispiel 4.4.3

Sei $p = 7$ und $S = \{1, 2, 3\}$. Somit haben wir

$$(-S) \;=\; \{-1, -2, -3\} \;=\; \{4, 5, 6\}.$$

Sei zunächst $a = 2$, damit gilt

$$(aS) \;=\; \{2 \cdot 1, 2 \cdot 2, 2 \cdot 3\} \;=\; \{2, 4, 6\}.$$

Wir erhalten

$$s \;=\; \mathrm{card}((-S) \cap (aS)) \;=\; \mathrm{card}(\{4, 6\}) \;=\; 2$$

und damit folgt nach dem Lemma von Gauß

$$\left(\frac{a}{p}\right) \;=\; \left(\frac{2}{7}\right) \;=\; 1.$$

Mit anderen Worten: $a = 2$ ist ein quadratischer Rest modulo $p = 7$, somit besitzt

$$y^2 \;\equiv\; 2 \,(\mathrm{mod}\; 7)$$

eine Lösung. Sei nun $b = 3$ mit

$$(bS) \;=\; \{3 \cdot 1, 3 \cdot 2, 3 \cdot 3\} \;=\; \{2, 3, 6\}.$$

Nun gilt

$$t \;=\; \mathrm{card}((-S) \cap (bS)) \;=\; \mathrm{card}(\{6\}) \;=\; 1$$

und es ergibt sich

$$\left(\frac{b}{p}\right) \;=\; \left(\frac{3}{7}\right) \;=\; -1.$$

Demnach ist $b = 3$ ein quadratischer Nichtrest modulo $p = 7$ und

$$y^2 \;\equiv\; 3 \,(\mathrm{mod}\; 7)$$

besitzt keine Lösung.

Wir kommen nun zum Hauptergebnis dieses Abschnitts:

Satz 4.4.4 (Quadratisches Reziprozitätsgesetz)

Seien $p, q > 2$ zwei unterschiedliche Primzahlen. Dann gilt

$$\begin{aligned}\left(\frac{p}{q}\right) \;&=\; (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \cdot \left(\frac{q}{p}\right) \\ &=\; \begin{cases} \left(\frac{q}{p}\right) & \text{falls} \quad p \equiv 1 \,(\mathrm{mod}\; 4) \text{ oder } q \equiv 1 \,(\mathrm{mod}\; 4) \\ -\left(\frac{q}{p}\right) & \text{falls} \quad p \equiv 3 \,(\mathrm{mod}\; 4) \text{ und } q \equiv 3 \,(\mathrm{mod}\; 4) \end{cases}.\end{aligned}$$

Ein Beispiel hierzu ist unter Beispiel 4.5.4 zu finden.

Sehr viel einfacher lassen sich die folgenden Ergänzungssätze zum quadratischen Reziprozitätsgesetz mit dem Lemma von Gauß unter Verwendung von $S = \{1, 2, \ldots, (p-1)/2\}$ sowie $a = -1$ bzw. $a = 2$ beweisen:

Satz 4.4.5 (Ergänzungssätze)

Für eine Primzahl $p > 2$ gilt:

(1) Erster Ergänzungssatz:

$$\left(\frac{-1}{p}\right) \;=\; (-1)^{\frac{p-1}{2}} \;=\; \begin{cases} 1 & \text{falls} \quad p \equiv 1 \,(\bmod\ 4) \\ -1 & \text{falls} \quad p \equiv 3 \,(\bmod\ 4) \end{cases} .$$

(2) Zweiter Ergänzungssatz:

$$\begin{aligned} \left(\frac{2}{p}\right) \;&=\; (-1)^{\frac{p^2-1}{8}} \\ &=\; \begin{cases} 1 & \text{falls} \quad p \equiv 1 \,(\bmod\ 8) \text{ oder } p \equiv 7 \,(\bmod\ 8) \\ -1 & \text{falls} \quad p \equiv 3 \,(\bmod\ 8) \text{ oder } p \equiv 5 \,(\bmod\ 8) \end{cases} . \end{aligned}$$

4.5 Folgerungen aus dem Reziprozitätsgesetz

Bislang haben wir mehrere Definitionen eingeführt und konnten das wichtige quadratische Reziprozitätsgesetz formulieren.

Ziel dieses Abschnitts ist nun das Finden von Rechenregeln zur Berechnung des Legendre-Symbol. Dazu verallgemeinern wir dieses zunächst:

Definition 4.5.1

Seien $a, b \in \mathbb{N} - \{0\}$ so gewählt, dass a und b teilerfremd sind und dass b ungerade ist. Weiter sei

$$b \;=\; p_1^{e_1} \cdot \ldots \cdot p_s^{e_s}$$

die Primfaktorenzerlegung von b.

Dann definieren wir das ***Jacobi-Symbol*** als

$$\left(\frac{a}{b}\right)_J \;:=\; \prod_{k=1}^{s} \left(\frac{a}{p_k}\right)^{e_k} .$$

Ist das b eine Primzahl, so erhalten wir direkt das Legendre-Symbol, anderenfalls ein Produkt aus Legendre-Symbolen. Damit ist die Darstellung des Jacobi-Symbols eindeutig über die Legendre-Symbole festgelegt, wir werden daher auf den Index J im Folgenden verzichten.

Achtung!

Es gilt zum Beispiel

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

obwohl

$$y^2 \equiv 2 \,(\bmod\ 9\,)$$

keine Lösung besitzt. Ist das Jacobi-Symbol zu a und b gleich 1, können wir also nicht auf die Lösbarkeit der quadratischen Kongruenz

$$y^2 \equiv a \,(\bmod\ b\,)$$

schließen. Die Umkehrung ist jedoch richtig: Ist das Jacobi-Symbol zu a und b gleich -1, so ist

$$y^2 \equiv a \,(\bmod\ b\,)$$

nicht lösbar.

Aus den Ergänzungssätzen zum quadratischen Reziprozitätsgesetz erhalten wir einige Eigenschaften:

Eigenschaften des Jacobi-Symbols

Sei $b > 2$ ungerade. Dann gilt

$$\left(\frac{-1}{b}\right) \;=\; (-1)^{\frac{b-1}{2}} \qquad \text{und} \qquad \left(\frac{2}{b}\right) \;=\; (-1)^{\frac{b^2-1}{8}}.$$

Satz 4.5.2

Seien a und b größer als 2 und ungerade. Dann gilt

$$\left(\frac{a}{b}\right) \;=\; (-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}}\left(\frac{b}{a}\right).$$

Satz 4.5.3

Sei $a \in \mathbb{Z}$ und $b \in \mathbb{N}$ ungerade. Weiter gelte

$$a \equiv a' \,(\mathrm{mod}\ b) \qquad \text{und} \qquad b \equiv b' \,(\mathrm{mod}\ 4|a|\,).$$

Dann folgt

$$\left(\frac{a}{b}\right) = \left(\frac{a'}{b}\right) \qquad \text{und} \qquad \left(\frac{a}{b}\right) = \left(\frac{a}{b'}\right).$$

Beispiel 4.5.4

Mit diesen Eigenschaften und den Ergebnissen aus dem vorherigen Abschnitt können wir nun das Jacobi-Symbol recht einfach berechnen. Dies führen wir auf zwei Wegen durch, der erste nutzt im Wesentlichen das quadratische Reziprozitätsgesetz:

$$\begin{aligned}
\left(\frac{111}{163}\right) &= \left(\frac{3}{163}\right)\cdot\left(\frac{37}{163}\right) = (-1)\left(\frac{163}{3}\right)\cdot(+1)\left(\frac{163}{37}\right)\\
&= (-1)\left(\frac{1}{3}\right)\cdot(+1)\left(\frac{15}{37}\right) = (-1)(+1)\cdot(+1)\left(\frac{3}{37}\right)\cdot\left(\frac{5}{37}\right)\\
&= (-1)(+1)\cdot(+1)(+1)\left(\frac{37}{3}\right)\cdot(+1)\left(\frac{37}{5}\right)\\
&= (-1)(+1)\cdot(+1)(+1)\left(\frac{1}{3}\right)\cdot(+1)\left(\frac{2}{5}\right)\\
&= (-1)(+1)\cdot(+1)(+1)(+1)\cdot(+1)(-1) = (+1).
\end{aligned}$$

Dies zeigt also, dass die Kongruenz

$$y^2 \equiv 111 \,(\mathrm{mod}\ 163\,)$$

eine Lösung besitzen könnte.

Noch etwas einfacher wäre jedoch der folgende Lösungsweg:

$$\begin{aligned}
\left(\frac{111}{163}\right) &= (-1)\left(\frac{163}{111}\right) = (-1)\left(\frac{52}{111}\right) = (-1)\left(\frac{4\cdot 13}{111}\right)\\
&= (-1)\left(\frac{13}{111}\right) = (-1)\left(\frac{111}{13}\right) = (-1)\left(\frac{7}{13}\right)\\
&= (-1)\left(\frac{13}{7}\right) = (-1)\left(\frac{-1}{7}\right) = (-1)(-1) = (+1),
\end{aligned}$$

da ja gilt

$$\left(\frac{2\cdot 2\cdot 13}{111}\right) = \left(\frac{2}{111}\right)\cdot\left(\frac{2}{111}\right)\cdot\left(\frac{13}{111}\right) = \left(\frac{13}{111}\right).$$

An dieser Stelle wollen wir noch einmal die wichtigsten Rechenregeln zusammenfassen, die zur Berechnung des Legendre- bzw. des Jacobi-Symbols ausgenutzt werden können:

Zusammenfassung

Seien $a, b > 2$ ungerade. Dann gelten die folgenden Rechenregeln zur Bestimmung des Legendre- bzw. des Jacobi-Symbols:

$$\left(\frac{0}{b}\right) = \left(\frac{1}{b}\right) = 1, \quad \left(\frac{-1}{b}\right) = (-1)^{\frac{b-1}{2}} \quad \text{und} \quad \left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{8}}.$$

Weiter gilt für zwei Primzahlen p und q

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) & \text{falls} \quad p \equiv 1 \,(\bmod\ 4) \text{ oder } q \equiv 1 \,(\bmod\ 4) \\ -\left(\frac{q}{p}\right) & \text{falls} \quad p \equiv 3 \,(\bmod\ 4) \text{ und } q \equiv 3 \,(\bmod\ 4) \end{cases}$$

und für eine Quadratzahl a^2 folgt stets

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

Für alle $a_1, a_2 \in \mathbb{N}$ mit $\mathrm{ggT}(a_1, b) = \mathrm{ggT}(a_2, b) = 1$ gilt

$$\left(\frac{a_1 \cdot a_2}{b}\right) = \left(\frac{a_1}{b}\right) \cdot \left(\frac{a_2}{b}\right).$$

Für ungerade $b \in \mathbb{N}$ und $a \in \mathbb{Z}$ sind auch die Regeln

$$\left(\frac{a}{b}\right) = \left(\frac{a - k \cdot b}{b}\right) \qquad \text{und} \qquad \left(\frac{a}{b}\right) = \left(\frac{a}{b - l \cdot 4|a|}\right)$$

für beliebige $k, l \in \mathbb{Z}$ sehr wichtig.

Mit diesen Regeln lässt sich jedes Jacobi-Symbol berechnen.

Um das Jacobi-Symbol auch für gerade b zu definieren und um dessen Berechnung algorithmisch darstellen zu können, nutzen wir das Hilbert-Symbol:

Definition 4.5.5

Seien $a_0, b_0 \in \mathbb{N} - \{0\}$ ungerade und für $\alpha, \beta \in \mathbb{N}$

$$a = 2^\alpha a_0 \qquad \text{und} \qquad b = 2^\beta b_0$$

so gewählt, dass a und b teilerfremd sind. Dann definieren wir das ***Hilbert-Symbol*** als

$$(a, b)_2 = (-1)^{\frac{a_0-1}{2} \cdot \frac{b_0-1}{2} + \alpha \frac{b_0^2-1}{8} + \beta \frac{a_0^2-1}{8}}.$$

Eigenschaften des Hilbert-Symbols

Seien a, b und c so gewählt, dass jeweils das Hilbert-Symbol definiert ist.

Dann gilt

$$(a,b) \;=\; (b,a) \qquad \text{und} \qquad (a\cdot b,c)_2 \;=\; (a,c)_2\cdot(b,c)_2.$$

Satz 4.5.6

Seien a und b so gewählt, dass das Hilbert-Symbol definiert ist (also so wie in der vorherigen Definition gefordert).

Dann gilt

$$\left(\frac{a}{b}\right) \;=\; (a,b)_2\cdot\left(\frac{b}{a}\right).$$

Definition 4.5.7

Für ein $b<0$ definieren wir

$$\left(\frac{a}{b}\right) \;:=\; \left(\frac{a}{|b|}\right).$$

Weiter gelte

$$(a,b)_\infty \;:=\; \begin{cases} 1 & \text{falls} \quad a>0 \text{ oder } b>0 \\ -1 & \text{falls} \quad a<0 \text{ und } b<0 \end{cases}.$$

Satz 4.5.8 (Hilbert)

Seien $a_0, b_0 \in \mathbb{Z}$ ungerade und für $\alpha,\beta\in\mathbb{N}$

$$a \;=\; 2^\alpha a_0 \qquad \text{und} \qquad b \;=\; 2^\beta b_0$$

so gewählt, dass a und b teilerfremd sind. Dann gilt

$$\left(\frac{a}{b}\right) \;=\; (a,b)_2\cdot(a,b)_\infty\cdot\left(\frac{b}{a}\right).$$

Damit erhalten wir eine Verallgemeinerung von Satz 4.5.6.

Algorithmische Anwendung

Ähnlich zu Beispiel 4.5.4 können wir nun das Jacobi-Symbol

$$\left(\frac{a}{b}\right)$$

algorithmisch ganz allgemein berechnen, also auch für $a, b \in \mathbb{Z}$. Die Koeffizienten

$$(a,b)_2 \qquad \text{und} \qquad (a,b)_\infty$$

lassen sich in jedem Schritt einfach bestimmen. Wir nutzen dann den Satz von Hilbert, berechnen zu

$$\left(\frac{a_k}{b_k}\right)$$

die nächste Zahl $a_{k+1} = a_k \text{ MOD } b_k$, wenden wieder dan Satz von Hilbert an und so weiter.

4.6 Aufgaben

Aufgabe 4.6.1

Prüfe, ob die quadratische Kongruenz

$$y^2 \equiv 6 \,(\bmod\ 15)$$

eine Lösung besitzt.

Lösung

Wir berechnen dazu das Jacobi-Symbol und nutzen die Rechenregeln aus der Zusammenfassung von Seite 81:

$$\left(\frac{6}{15}\right) \;=\; \left(\frac{6}{3}\right)\cdot\left(\frac{6}{5}\right) \;=\; \left(\frac{0}{3}\right)\cdot\left(\frac{1}{5}\right) \;=\; 1\cdot 1 \;=\; 1,$$

somit besteht die Möglichkeit, dass die gegebene quadratische Kongruenz lösbar. Tatsächlich gilt mit $y = 6$ gerade

$$6^2 \equiv 6 \,(\bmod\ 15).$$

Aufgabe 4.6.2

Berechne mit dem Euler-Kriterium die Legendre-Symbole

$$\left(\frac{5}{23}\right), \qquad \left(\frac{241}{257}\right) \qquad \text{und} \qquad \left(\frac{17}{31}\right)$$

Lösung

Durch geschicktes Ausrechnen erhalten wir

$$\begin{aligned} 5^{\frac{23-1}{2}} &= 5^{11} \equiv -1 \,(\bmod\ 23\,), \\ 241^{\frac{257-1}{2}} &= 241^{128} \equiv 1 \,(\bmod\ 257\,), \\ 17^{\frac{31-1}{2}} &= 17^{15} \equiv -1 \,(\bmod\ 31\,), \end{aligned}$$

somit folgt direkt

$$\left(\frac{5}{23}\right) = -1, \qquad \left(\frac{241}{257}\right) = 1 \qquad \text{und} \qquad \left(\frac{17}{31}\right) = -1.$$

Aufgabe 4.6.3

Berechne mit dem quadratischen Reziprozitätsgesetz das Legendre-Symbol

$$\left(\frac{17}{31}\right).$$

Lösung

Es gilt

$$\begin{aligned} \left(\frac{17}{31}\right) &= (+1)\left(\frac{31}{17}\right) = \left(\frac{14}{17}\right) = \left(\frac{2}{17}\right)\cdot\left(\frac{7}{17}\right) \\ &= (+1)\left(\frac{17}{7}\right) = \left(\frac{3}{7}\right) = (-1)\left(\frac{7}{3}\right) = (-1)\left(\frac{1}{3}\right) = -1. \end{aligned}$$

Aufgabe 4.6.4

Zeige, dass die quadratische Kongruenz

$$x^2 \equiv 166 \,(\bmod\ 221\,)$$

mindestens eine Lösung besitzt.

Lösung

Zunächst berechnen wir das Jacobi-Symbol $\left(\frac{166}{221}\right)$:

$$\left(\frac{166}{221}\right) = \left(\frac{2}{221}\right)\cdot\left(\frac{83}{221}\right) = (-1)(+1)\left(\frac{221}{83}\right) = (-1)\left(\frac{55}{83}\right)$$

$$
\begin{aligned}
&= (-1)\left(\frac{5}{83}\right)\cdot\left(\frac{11}{83}\right) = (-1)(+1)(-1)\left(\frac{83}{5}\right)\cdot\left(\frac{83}{11}\right)\\
&= \left(\frac{3}{5}\right)\cdot\left(\frac{6}{11}\right) = (+1)\left(\frac{5}{3}\right)\cdot\left(\frac{2}{11}\right)\cdot\left(\frac{3}{11}\right)\\
&= (-1)(-1)\left(\frac{2}{3}\right)\cdot\left(\frac{11}{3}\right) = (-1)\left(\frac{2}{3}\right) = (-1)(-1) = 1.
\end{aligned}
$$

Somit ist das Jacobi-Symbol gleich 1 und damit ist eine notwendige Bedingung dafür, dass

$$x^2 \equiv 166 \,(\bmod\ 221)$$

eine Lösung hat, gegeben. Als Lösungsmenge ergibt sich nach einiger Rechnung

$$M = \{a + 221 \cdot k \mid a = 59, 110, 111, 162 \text{ und } k \in \mathbb{N}\},$$

somit ist zum Beispiel $x = 59$ eine Lösung der gegebenen Kongruenz:

$$59^2 = 3481 \equiv 166 \,(\bmod\ 221).$$

Aufgabe 4.6.5

Berechne mit dem quadratischen Reziprozitätsgesetz und den Ergänzungssätzen das Legendre-Symbol

$$\left(\frac{40097}{65539}\right).$$

Als Hinweis sei gegeben, dass die Zahlen 101, 397 sowie 65539 Primzahlen sind.

Lösung

Der erste Lösungsweg nur mit dem quadratischen Reziprozitätsgesetz ist mühsam und aufwendig:

$$
\begin{aligned}
\left(\frac{40097}{65539}\right) &= \left(\frac{101}{65539}\right)\cdot\left(\frac{397}{65539}\right) = (+1)\left(\frac{65539}{101}\right)\cdot(+1)\left(\frac{65539}{397}\right)\\
&= \left(\frac{91}{101}\right)\cdot\left(\frac{34}{397}\right) = \left(\frac{7}{101}\right)\cdot\left(\frac{13}{101}\right)\cdot\left(\frac{2}{397}\right)\cdot\left(\frac{17}{397}\right)\\
&= (+1)\left(\frac{101}{7}\right)\cdot(+1)\left(\frac{101}{13}\right)\cdot(-1)\cdot(+1)\left(\frac{397}{17}\right)\\
&= (-1)\left(\frac{3}{7}\right)\cdot\left(\frac{10}{13}\right)\cdot\left(\frac{6}{17}\right)\\
&= (-1)(-1)\left(\frac{7}{3}\right)\cdot\left(\frac{2}{13}\right)\cdot\left(\frac{5}{13}\right)\cdot\left(\frac{2}{17}\right)\cdot\left(\frac{3}{17}\right)
\end{aligned}
$$

$$\begin{aligned}
&= (+1)\left(\frac{1}{3}\right)\cdot(-1)\left(\frac{13}{5}\right)\cdot(+1)\cdot(+1)\left(\frac{17}{3}\right)\\
&= (-1)\cdot(+1)\left(\frac{3}{5}\right)\cdot\left(\frac{2}{3}\right) \;=\; (-1)\cdot(+1)\left(\frac{5}{3}\right)\cdot(-1)\\
&= (+1)\left(\frac{2}{3}\right) \;=\; (-1).
\end{aligned}$$

Bei der Berechnung des Legendre-Symbols bei derart großen Zahlen sollte versucht werden, den Zähler betragsmäßig möglichst klein zu halten. Daher wäre in der zweiten Zeile die Umformung

$$\left(\frac{91}{101}\right) \;=\; \left(\frac{-10}{101}\right) \;=\; \left(\frac{-1}{101}\right)\cdot\left(\frac{10}{101}\right) \;=\; (+1)\left(\frac{10}{101}\right)$$

sinnvoller gewesen. Aber natürlich führen hier wie immer viele Wege zum Ziel.

Ein wenig einfacher ist der Rechenweg durch *umkippen* des Jacobi-Symbols:

$$\begin{aligned}
\left(\frac{40097}{65539}\right) &= (+1)\left(\frac{65539}{40097}\right) \;=\; \left(\frac{25442}{40097}\right) \;=\; \left(\frac{2}{40097}\right)\cdot\left(\frac{12721}{40097}\right)\\
&= (+1)\left(\frac{40097}{12721}\right) \;=\; \left(\frac{1934}{12721}\right) \;=\; \left(\frac{2}{12721}\right)\cdot\left(\frac{967}{12721}\right)\\
&= (+1)\left(\frac{12721}{967}\right) \;=\; \left(\frac{150}{967}\right) \;=\; \left(\frac{2}{967}\right)\cdot\left(\frac{75}{967}\right)\\
&= (+1)(-1)\left(\frac{967}{75}\right) \;=\; (-1)\left(\frac{67}{75}\right) \;=\; (-1)(-1)\left(\frac{75}{67}\right)\\
&= \left(\frac{8}{67}\right) \;=\; \left(\frac{2}{67}\right)^3 \;=\; \left(\frac{2}{67}\right) \;=\; (-1).
\end{aligned}$$

Hierbei wurde anders als bei der Berechnung zuvor keine Primfaktorenzerlegung verwendet, was einen großen Vorteil bei der algorithmischen Berechnung von Legendre-Symbolen darstellt.

Aufgabe 4.6.6

Sei $p = 2n + 1$ eine ungerade Primzahl. Folgere aus dem Satz von Wilson, dass

$$(n!)^2 \;\equiv\; (-1)^{n+1} \,(\bmod\; p\,)$$

gilt. Folgere daraus wiederum den ersten Ergänzungssatz zum quadratischen Reziprozitätsgesetz sowie die beiden Gleichungen

$$\begin{aligned}
&2^2\cdot 4^2\cdot\ldots\cdot(p-3)^2\cdot(p-1)^2 \;\equiv\; (-1)^{\frac{p+1}{2}}\,(\bmod\; p\,) \qquad \text{und}\\
&1^2\cdot 3^2\cdot\ldots\cdot(p-4)^2\cdot(p-2)^2 \;\equiv\; (-1)^{\frac{p+1}{2}}\,(\bmod\; p\,).
\end{aligned}$$

Lösung

Der Satz von Wilson besagt

$$(p-1)! \equiv -1 \,(\bmod\ p).$$

Damit erhalten wir direkt

$$\begin{aligned}
(n!)^2 &\equiv 1^2 \cdot 2^2 \cdot \ldots \cdot (n-1)^2 \cdot n^2 \,(\bmod\ p) \\
&\equiv n! \cdot 1 \cdot 2 \cdot \ldots \cdot (n-1) \cdot n \,(\bmod\ p) \\
&\equiv n! \cdot (-1)(2n) \cdot (-1)(2n-1) \cdot \ldots \cdot (-1)(n+1) \,(\bmod\ p) \\
&\equiv (-1)^n \cdot n! \cdot (n+1) \cdot (n+2) \cdot \ldots \cdot (2n-1) \cdot (2n) \,(\bmod\ p) \\
&\equiv (-1)^n \cdot (2n)! \,(\bmod\ p) \\
&\equiv (-1)^n \cdot (p-1)! \,(\bmod\ p) \\
&\equiv (-1)^n \cdot (-1) \,(\bmod\ p) \\
&\equiv (-1)^{n+1} \,(\bmod\ p).
\end{aligned}$$

Damit wissen wir nun auch, dass

$$x^2 \equiv -1 \,(\bmod\ p)$$

genau dann eine Lösung hat (nämlich $x = n!$), wenn n gerade ist. Weiter hat

$$x^2 \equiv 1 \,(\bmod\ p)$$

genau dann eine Lösung, wenn n ungerade ist. Damit folgt auch, dass

$$x^2 \equiv -1 \,(\bmod\ p)$$

genau dann keine Lösung hat,wenn n ungerade ist. Dies zeigt geraden den ersten Ergänzungssatz zum quadratischen Reziprozitätsgesetz:

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{falls} \quad p \equiv 1 \,(\bmod\ 4) \\ -1 & \text{falls} \quad p \equiv 3 \,(\bmod\ 4) \end{cases}.$$

Wir haben damit sogar auch die Lösung $n!$ für eine Kongruenz der Form

$$x^2 \equiv -1 \,(\bmod\ p)$$

für eine Primzahl p mit $p \equiv 1 \,(\bmod\ 4)$ berechnet.

Nach dem Satz von Wilson folgt auch

$$\begin{aligned}
& 2^2 \cdot 4^2 \cdot \ldots \cdot (p-3)^2 \cdot (p-1)^2 \\
\equiv\ & 2 \cdot 4 \cdot \ldots \cdot (p-1) \cdot (-1)(p-2) \cdot (-1)(p-4) \cdot \ldots \cdot (-1) \,(\bmod\ p) \\
\equiv\ & (-1)^{\frac{p-1}{2}} \cdot (2n)! \,(\bmod\ p) \\
\equiv\ & (-1)^{\frac{p-1}{2}} \cdot (p-1)! \,(\bmod\ p) \\
\equiv\ & (-1)^{\frac{p-1}{2}} \cdot (-1) \,(\bmod\ p) \\
\equiv\ & (-1)^{\frac{p+1}{2}} \,(\bmod\ p).
\end{aligned}$$

Die Gleichung

$$1^2 \cdot 3^2 \cdot \ldots \cdot (p-4)^2 \cdot (p-2)^2 \equiv (-1)^{\frac{p+1}{2}} \,(\bmod\ p\,)$$

zeigt man ganz analog.

5 Diophantische Gleichungen

In diesen Kapitel wollen wir auf die schon in der Einleitung angesprochenen ***diophantischen Gleichungen*** einleitend eingehen.

Allgemein betrachtet man s Polynomgleichungen

$$\begin{aligned} p_1(x_1, \ldots, x_t) &= 0 \\ &\vdots \\ p_s(x_1, \ldots, x_t) &= 0 \end{aligned}$$

mit ganzen Koeffizienten. Gesucht sind dann ganze oder rationale Zahlen $x_1, \ldots, x_t$, die dieses Gleichungssystem lösen. Auch nach mehreren Jahrhunderten andauernden Bemühungen gibt es keinen Algorithmus, der derartige Gleichungssysteme löst.

5.1 Beispiele einiger diophantischer Gleichungen

Satz 5.1.1

Seien $x, y, z \in \mathbb{N} - \{0\}$ so gewählt, dass

$$x^2 + y^2 = z^2$$

gilt. Dann gibt es ein $d > 0$ und teilerfremde $a, b \in \mathbb{N}$ mit

$$x = 2abd, \qquad y = (a^2 - b^2)d \qquad \text{und} \qquad z = (a^2 + b^2)d$$

oder mit

$$y = 2abd, \qquad z = (a^2 - b^2)d \qquad \text{und} \qquad z = (a^2 + b^2)d.$$

Da $\mathrm{ggT}(a, b) = 1$ gilt, müssen auch x, y und z paarweise teilerfremd sein oder sie haben den gemeinsamen Faktor 2.

Beispiele

Es gilt

$$\begin{aligned} 3^2 + 4^2 &= 5^2 \qquad \text{mit} \quad a = 2, \quad b = 1, \quad d = 1, \\ 5^3 + 12^2 &= 13^2 \qquad \text{mit} \quad a = 3, \quad b = 2, \quad d = 1. \end{aligned}$$

Bemerkung 5.1.2

Weiterhin können wir $x^2 + y^2 = z^2$ auch so verstehen, dass

$$\left(\frac{x}{z}\right)^2 + \left(\frac{y}{z}\right)^2 = 1$$

gilt, wir suchen also rationale Zahlen ξ und ζ mit

$$\xi^2 + \zeta^2 = 1,$$

dies veranschaulicht Abbildung 5.1.

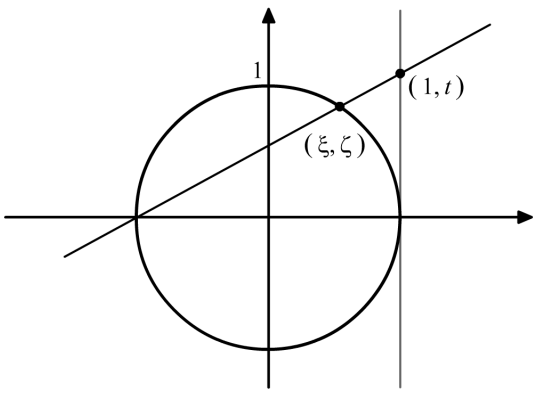


Abbildung 5.1: Modifikation zur Bestimmung von Lösungen zu $x^2+y^2 = z^2$.

Ist hier t rational, so sind auch die Koeffizienten der Geraden durch $(-1, 0)$ sowie $(1, t)$ rational. Daraus folgt, dass auch ξ und ζ rational sind.

Wir kommen nun zu einer weiteren Aussage zu einer speziellen Art von Gleichungen:

Satz 5.1.3

Es gibt keine Zahlen $x, y, z > 0$ mit

$$x^4 + y^4 = z^2.$$

Damit folgt auch, dass

$$x^4 + y^4 \;=\; z^4$$

keine Lösung für $x, y, z > 0$ besitzt.

In Beweisen zu derartigen Sätzen werden im Wesentlichen zwei Tatsachen ausgenutzt:

(1) Sind a und b teilerfremd mit $ab = x^n$, so folgt nach dem Hauptsatz der Arithmetik, dass $a = x_1^n$ und $b = x_2^n$ gelten muss.

(2) Ist eine Gleichung $f(x, y) = 0$ lösbar, dann besitzt auch

$$f(x, y) \;\equiv\; 0 \,(\bmod\; n\,)$$

für jedes n (mindestens) eine Lösung.

Wesentlich schwieriger ist der Beweis zum folgenden Satz, der erst vor zehn Jahren bewiesen wurde:

Satz 5.1.4

Es gibt keine Zahlen $x, y, z > 0$, so dass für $n > 2$

$$x^n + y^n \;=\; z^n$$

gilt.

5.2 Summe von zwei Quadraten

Wir wollen uns nun mit dem Problem beschäftigen, wann eine natürliche Zahl n als Summe von zwei Quadratzahlen dargestellt werden kann.

Dieses Problem betrachten wir allgemein im Ring der ***Gaußschen Zahlen***

$$R \;:=\; \{a + bi \mid a, b \in \mathbb{Z}\} \qquad \text{mit} \quad i^2 \;=\; -1.$$

Für $\alpha = a + bi \in R$ sei

$$N(\alpha) \;:=\; a^2 + b^2$$

die ***Norm*** von α. Mit $\alpha, \beta \in R$ folgt sofort

$$N(\alpha) \;\in\; \mathbb{N} \qquad \text{und} \qquad N(\alpha \cdot \beta) \;=\; N(\alpha) \cdot N(\beta).$$

Wir wollen nun den Restsatz auch im Ring R der Gaußschen Zahlen betrachten:

Satz 5.2.1 (Restsatz)

Seien $\alpha, \beta \in R$ mit $\beta \neq 0$.

Dann gibt es $\gamma, \delta \in R$ mit

$$\alpha \;=\; \gamma \cdot \beta + \delta \qquad \text{und} \qquad N(\delta) \;\leq\; \frac{1}{2} N(\beta).$$

Mit Hilfe des Restsatzes erhalten wir auch die folgende Aussage:

Satz 5.2.2

Der Ring R der Gaußschen Zahlen ist ein Hauptidealring.

Nach der Algebra sei bekannt, dass wir in jedem Hauptidealring Primelemente definieren können. Damit können wir nicht nur den größten gemeinsamen Teiler und so weiter definieren, wir erhalten sogar eine Primfaktorenzerlegung der Elemente aus R:

Definition 5.2.3

Eine Elemente α aus R heißt ***Primelement***, wenn aus $\alpha = \beta \cdot \gamma$ mit $\beta, \gamma \in R$ entweder $N(\beta) = 1$ oder $N(\gamma) = 1$ folgt.

Damit entsprechen gerade die Primelemente im Ring R den Primzahlen im Ring der ganzen Zahlen. Zur Unterscheidung werden wir aber weiterhin der Bezeichnung Primelement in R nachgehen.

Satz 5.2.4

Für jedes von Null verschiedene $\xi \in R$ gibt es eine Darstellung

$$\xi \;=\; \varepsilon \cdot \pi_1^{e_1} \cdot \ldots \cdot \pi_s^{e_s}$$

wobei π_i Primelemente aus R sind, $e_i \in \mathbb{N} - \{0\}$ und $N(\varepsilon) = 1$ gilt. Diese Darstellung ist bezüglich der Normen der Primelementen π_i eindeutig.

Die Bedingung $N(\varepsilon) = 1$ wird nur von vier Elementen aus R erfüllt:

$$\varepsilon \;\in\; \{1, -1, i, -i\}.$$

Diese vier Zahlen nennen wir die ***Einheiten*** in R.

Beispiel 5.2.5

Zunächst sind die vier Elemente

$$1+2i, \qquad 1-2i, \qquad 2+i \qquad \text{und} \qquad 2-i$$

Primelemente in R: Mit $1+2i = \alpha \cdot \beta$ folgt nach

$$5 \;=\; N(1+2i) \;=\; N(\alpha \cdot \beta) \;=\; N(\alpha) \cdot N(\beta),$$

dass $N(\alpha) = 1$ oder $N(\beta) = 1$ und so weiter. Nun gilt

$$5 \;=\; 2^2 + 1^1 \;=\; (2+i) \cdot (2-i) \;=\; (1+2i) \cdot (1-2i).$$

Damit haben wir zwei unterschiedliche Primfaktorenzerlegungen von $5 \in R$, wobei sich die Primfaktoren nur um den Faktor einer Einheit unterscheiden. Somit sind die Normen der Primelemente alle gleich.

Wir wollen uns nun damit befassen, wie wir Primelemente in R berechnen können:

Satz 5.2.6

Zunächst sind die Elemente $1+i$ sowie $1-i$ Primelemente in R.

Weiter sei $p \in \mathbb{N}$ eine Primzahl mit

$$p \;\equiv\; 3 \,(\bmod\; 4\,).$$

Dann ist $p = p + 0i$ auch ein Primelement in R.

Nun sei $p \in \mathbb{N}$ eine Primzahl mit

$$p \;\equiv\; 1 \,(\bmod\; 4\,).$$

Dann gibt es zwei unterschiedliche Zahlen $x+yi$ und $x-yi$ in R mit

$$p \;=\; (x+yi) \cdot (x-yi) \;=\; x^2 + y^2.$$

Diese Zahlen sind sogar Primelement in R.

Damit folgt direkt:

Korollar 5.2.7

Jede Primzahl p mit

$$p \;\equiv\; 1 \,(\bmod\; 4\,)$$

kann als Summe von zwei Quadratzahlen dargestellt werden.

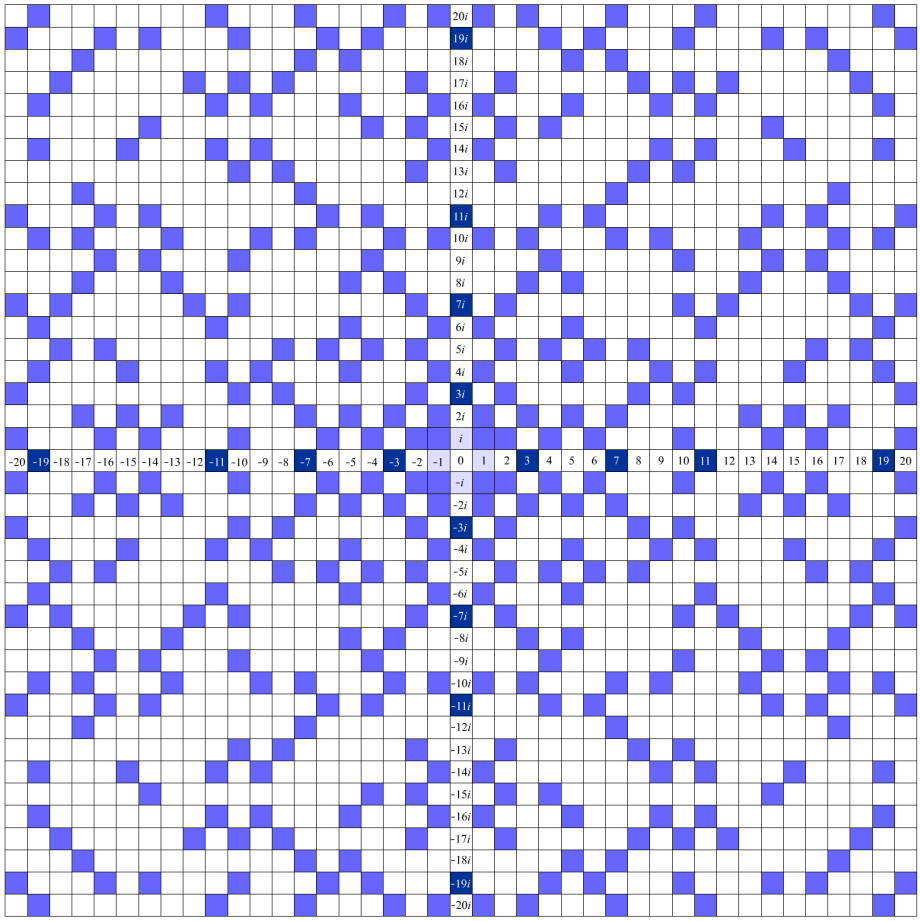


Abbildung 5.2: Veranschaulichung aller Primelemente $x + yi$ im Ring der Gaußschen Zahlen R mit $-20 \leq x, y \leq 20$.

Korollar 5.2.8

Sei $n \in \mathbb{N}$ mit

$$n \;=\; 2^{e_0} \cdot p_1^{e_1} \cdot \ldots \cdot p_s^{e_s},$$

wobei die p_i Primzahlen sind mit

$$p_i \;\equiv\; 1 \,(\bmod\; 4\,).$$

Dann ist n Summe von zwei Quadratzahlen.

Weiterhin ist die Anzahl dieser Darstellungen genau

$$4 \cdot (e_1 + 1) \cdot \ldots \cdot (e_s + 1).$$

Bemerkung 5.2.9

Für eine Primzahl p und ein $e \in \mathbb{N}$ definieren wir

$$r(p^e) \;=\; e + 1$$

und r sei eine multiplikative Funktion. Weiter definieren wir

$$\chi(n) \;:=\; \begin{cases} 1 & \text{für} \quad n = 1 \\ 0 & \text{für} \quad n \text{ gerade} \\ 1 & \text{für} \quad n \equiv 1 \,(\bmod\; 4\,) \\ -1 & \text{für} \quad n \equiv 3 \,(\bmod\; 4\,) \end{cases}.$$

Dann gilt

$$\sum_{d \le e} \chi(p^d) \;=\; e + 1$$

und wir erhalten insgesamt das wichtige Resultat

$$r(n) \;=\; \sum_{d \mid n} \chi(d).$$

Die Anzahl der Darstellungen von n als Summe von zwei Quadratzahlen ist somit

$$4 \cdot \sum_{d \mid n} \chi(d).$$

Für einige kleine $N \in \mathbb{N}$ kann man eine ähnliche Formel auch für die Anzahl von Darstellungen von n als

$$n \;=\; x^2 + Ny^2$$

angeben. Für allgemeine N ist dies jedoch sehr, sehr kompliziert.

Bemerkung 5.2.10

Wir wollen an dieser Stelle abschließend noch eine weitere diophantische Gleichung präsentieren, die nur eine triviale Lösung besitzt, was wieder mit den Gaußschen Zahlen gezeigt werden kann.

Die einzigen natürlichen Zahlen, die die Gleichung

$$x^3 \;=\; y^2 + 1$$

lösen, sind $x = 1$ und $y = 0$. Dazu schreiben wir

$$x^3 \;=\; y^2 + 1 \;=\; (y + i)(y - i).$$

Es lässt sich zeigen, dass $y^2 + 1$ ungerade ist und dass $(y + i)$ sowie $(y - i)$ teilerfremd sind. Daher gibt es ein $\xi \in R$ und Einheiten ε sowie ε' mit

$$y + i \;=\; \varepsilon' \xi^3 \;=\; (\varepsilon\xi)^3.$$

Nun sei $\varepsilon\xi = u + vi$ und damit

$$y + i \;=\; (u + vi)^3 \;=\; (u^3 - 3uv^2) + (2u^2v - v^3)i.$$

Das Gleichungssystem

$$y \;=\; u^3 - 3uv^2 \qquad \text{und} \qquad 1 \;=\; 2u^2v - v^3$$

wird jedoch nur von $u = 0$ und $v = -1$ gelöst, somit muss

$$y + i \;=\; (0 - i)^3 \;=\; i$$

und damit $y = 0$ gelten. Dies zeigt, dass die Gleichung

$$x^3 \;=\; y^2 + 1$$

nur durch $x = 1$ und $y = 0$ gelöst wird.

Die Gleichung

$$x^3 + 1 \;=\; y^2$$

wird nur durch $x = 0$ und $y = 1$ sowie $x = 2$ und $y = 3$. Auch dies kann mit den Gaußschen Zahlen bewiesen werden, was jedoch deutlisch schwieriger ist.

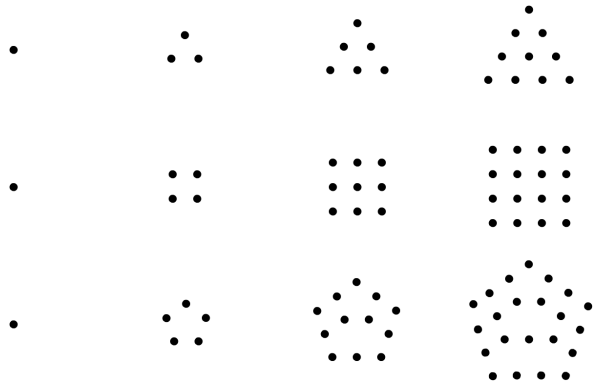


Abbildung 5.3: Dreieckzahlen, Viereckzahlen und Fünfeckzahlen.

5.3 Summe von vier Quadraten

Wir wollen nun die Darstellung von natürlichen Zahlen als Summe von ***Vieleckzahlen*** betrachten, siehe dazu Abbildung 5.3.

Für Vieleckzahlen gilt also:

(1) ***Dreieckzahlen***: $1,\ 3,\ 6,\ 10,\ 15,\ 21, \ldots$ oder allgemein

$$\frac{1}{2} \cdot (1 \cdot n + 1) \ = \ \frac{1}{2} \cdot (n + 1).$$

(2) ***Viereckzahlen***: $1,\ 4,\ 9,\ 16,\ 25,\ 36, \ldots$ oder allgemein

$$\frac{1}{2} \cdot (2 \cdot n + 0) \ = \ n^2.$$

(3) ***Fünfeckzahlen***: $1,\ 5,\ 12,\ 22,\ 35,\ 51, \ldots$ oder allgemein

$$\frac{1}{2} \cdot (3 \cdot n - 1).$$

Fermat behauptete, dass alle natürlichen Zahlen als Summe von drei Dreieckszahlen, als Summe von vier Viereckszahlen, als Summe von fünf Fünfeckszahlen und so weiter darstellbar sind. Diese Aussagen konnten alle nacheinander bewiesen werden.

Wir sind hier vor allem am Beispiel von Viereckzahlen interessiert, also an der Summe von vier Quadraten.

Sei $N_j(n)$ die Anzahl der Darstellungen von n als Summe von j Quadraten

$$x_1^2 + \ldots + x_j^2$$

mit $x_k > 0$ und x_k ungerade für $k = 1, \ldots, j$. In Abschnitt 5.2.8 bei den Summen von zwei Quadraten haben wir bereits gesehen, dass

$$N_2(n) \;=\; 4 \cdot \sum_{d|n} \chi(d)$$

gilt, wobei hierbei die x_k auch gerade sein durften.

Für die Summe von vier Quadraten erhalten wir die folgenden Aussagen:

Satz 5.3.1

Für $n \equiv 4 \,(\mathrm{mod}\ 8)$ gilt

$$N_4(n) \;=\; \sum_{\substack{d|n \\ d \text{ ungerade}}} d.$$

Korollar 5.3.2

Jede Primzahl p ist Summe von vier Quadraten.

Satz 5.3.3

Jede natürliche Zahl n ist Summe von vier Quadraten.

Beweis

Zunächst ist das Produkt von zwei Summen aus vier Quadraten wieder eine Summe aus vier Quadraten:

$$\begin{aligned} & (x_1^2 + x_2^2 + x_3^2 + x_4^2) \cdot (y_1^2 + y_2^2 + y_3^2 + y_4^2) \\ = \;& (x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4)^2 \;+\; (x_1y_2 + x_2y_1 + x_3y_4 - x_4y_3)^2 \\ + \;& (x_1y_3 - x_2y_4 + x_3y_1 + x_4y_2)^2 \;+\; (x_1y_4 + x_2y_3 - x_3y_2 + x_4y_1)^2. \end{aligned}$$

Die Aussage folgt nun direkt aus dem Hauptsatz der Arithmetik, also aus der Primfaktorzerlegung mit dem Korollar zuvor. □

5.4 Aufgaben

Aufgabe 5.4.1

Finde alle Teiler von $4 + 7i$ im Ring der Gaußschen Zahlen.

Lösung

Die Norm von $4+7i$ ist $N(4+7i) = 16+49 = 65$. Die Norm eines möglichen nicht trivialen Teiler von $4+7i$ in R muss ein Teiler von 65 sein, also entweder die Norm 5 oder die Norm 13 haben. Damit kommen in R die Primelemente aus der Menge

$$\begin{aligned} A &= \{(3+2i),\,(3-2i),\,(-3+2i),\,(-3-2i),\,(2+3i),\\ &\quad (2-3i),\,(-2+3i),\,(-2-3i)\} \end{aligned}$$

sowie aus der Menge

$$\begin{aligned} B &= \{(2+i),\,(2-i),\,(-2+i),\,(-2-i),\,(1+2i),\\ &\quad (1-2i),\,(-1+2i),\,(-1-2i)\} \end{aligned}$$

als Teiler von $4+7i$ in Frage. Damit gilt $4+7i = a \cdot b$ für geeignete Paare $(a,b) \in A \times B$. Wir erhalten die Möglichkeiten

$$\begin{aligned} 4+7i &= (3+2i)\cdot(2+i) \;=\; (-3-2i)\cdot(-2-i)\\ &= (2-3i)\cdot(-1+2i) \;=\; (-2+3i)\cdot(1-2i), \end{aligned}$$

somit ist

$$\begin{aligned} C &= \{1,\,(4+7i),\,(-1),\,(-4-7i),\,i,\,(7-4i),\,(-i),\,(-7+4i),\\ &\quad (3+2i),\;(2+i),\;(-3-2i),\;(-2-i),\\ &\quad (2-3i),\;(-1+2i),\;(-2+3i),\;(1-2i)\} \end{aligned}$$

die Menge der Teiler von $4+7i$ im Ring der Gaußschen Zahlen R.

Aufgabe 5.4.2

Finde alle Primfaktorzerlegungen von 13, 21 und $7+12i$ im Ring der Gaußschen Zahlen.

Lösung

Es gilt $13 \equiv 1 \pmod 4$, somit ist 13 Summe von zwei Quadraten. In den Gaußschen Zahlen erhalten wir

$$\begin{aligned} 13 &= (3+2i)\cdot(3-2i) \;=\; (-3+2i)\cdot(-3-2i)\\ &= (2+3i)\cdot(2-3i) \;=\; (-2+3i)\cdot(-2-3i), \end{aligned}$$

damit sind dies die vier möglichen Primfaktorenzerlegungen von 13 in R.

Es ist $3 \cdot 7 = 21$ und es gilt

$$3 \equiv 3 \,(\mathrm{mod}\ 4) \qquad \text{sowie} \qquad 7 \equiv 3 \,(\mathrm{mod}\ 4).$$

Somit sind 3 und 7 bzw. -3 und -7 auch Primelemente in R und damit sind

$$21 \;=\; 3 \cdot 7 \;=\; (-3) \cdot (-7) \;=\; (-3i) \cdot (7i) \;=\; (3i) \cdot (-7i)$$

die vier möglichen Primfaktorenzerlegungen von 21 in R.

Die Norm von $7+12i$ ist $N(7+12i) = 193$. Die Norm eines möglichen Teiler von $7 + 12i$ in R müsste ein Teiler von 193 sein, da 193 aber eine Primzahl ist, hat $7 + 12i$ keinen Teiler in R und ist damit selbst ein Primelement.

Aufgabe 5.4.3

Finde alle Primteiler von 29, 57 und $5 + 6i$ im Ring der Gaußschen Zahlen.

Lösung

Zunächst ist 29 auch eine Primzahl in $\mathbb{N}$ und es gilt

$$29 \equiv 1 \,(\mathrm{mod}\ 4),$$

daher ist 29 Summe von zwei Quadraten. Es gilt

$$\begin{aligned} 29 \;&=\; (5 + 2i) \cdot (5 - 2i) \;=\; (-5 + 2i) \cdot (-5 - 2i) \\ &=\; (2 + 5i) \cdot (2 - 5i) \;=\; (-2 + 5i) \cdot (-2 - 5i). \end{aligned}$$

Somit sind diese acht Zahlen die Primteiler von 29 im Ring der Gaußschen Zahlen.

Weiter gilt $57 = 3 \cdot 19$ und 3 sowie 19 sind Primzahlen in $\mathbb{N}$ mit

$$3 \equiv 3 \,(\mathrm{mod}\ 4) \qquad \text{und} \qquad 19 \equiv 3 \,(\mathrm{mod}\ 4),$$

somit sind 3 und 19 auch Primzahlen in Ring der Gaußschen Zahlen. Alle gesuchen Primteiler ergeben sich daher wie folgt:

$$57 \;=\; 3 \cdot 19 \;=\; (-3) \cdot (-19) \;=\; (3i) \cdot (-19i) \;=\; (-3i) \cdot (19i).$$

Des Weiteren ist 61 eine Primzahl in $\mathbb{N}$ und es gilt

$$61 \equiv 1 \,(\mathrm{mod}\ 4).$$

Da nun gerade

$$61 \;=\; (5 + 6i) \cdot (5 - 6i)$$

gilt, ist $5+6i$ ein Primelement im Ring der Gaußschen Zahlen und damit ergeben sich durch Multiplikation mit den Einheiten die folgenden Primteiler:

$$\begin{array}{llll}(5+6i), & (-5-6i), & (-6+5i), & (6-5i),\\ (5-6i), & (-5+6i), & (6+5i), & (-6-5i).\end{array}$$

Aufgabe 5.4.4

Zeige die beiden Gleichungen

$$x^2+\left(\frac{x^2-1}{2}\right)^2 \;=\; \left(\frac{x^2+1}{2}\right)^2 \quad \text{und} \quad x^2+\left(\frac{x^2}{4}-1\right)^2 \;=\; \left(\frac{x^2}{4}+1\right)^2$$

und untersuche, ob man damit alle phythagoräische Tripel erhalten kann.

Lösung

Zunächst einmal gilt sofort

$$\begin{aligned} x^2+\left(\frac{x^2-1}{2}\right)^2 &= x^2+\frac{1}{4}x^4-\frac{1}{2}x^2+\frac{1}{4}\\ &= \frac{1}{4}x^4+\frac{1}{2}x^2+\frac{1}{4} \;=\; \left(\frac{x^2+1}{2}\right)^2\end{aligned}$$

und ähnlich auch direkt

$$\begin{aligned} x^2+\left(\frac{x^2}{4}-1\right)^2 &= x^2+\frac{1}{16}x^4-\frac{1}{2}x^2+1\\ &= \frac{1}{16}x^4+\frac{1}{2}x^2+1 \;=\; \left(\frac{x^2}{4}+1\right)^2.\end{aligned}$$

Für ungerade x erhalten wir damit nach der ersten Gleichung ein phythagoräisches Tripel und für gerade x mit der zweiten Gleichung.

Nun gilt mit Hinblick auf die erste Gleichung

$$\left|x-\frac{x^2-1}{2}\right| \;=\; \frac{1}{2}\cdot\left|-x^2+2x+1\right| \;=\; \frac{1}{2}\cdot\left|x^2-2x-1\right| \;>\; 1$$

für alle $x\geq 3$. Mit Hinblick auf die zweite Gleichung ergibt sich

$$\left|x-\frac{x^2}{4}+1\right| \;=\; \frac{1}{4}\cdot\left|-x^2+4x+4\right| \;=\; \frac{1}{4}\cdot\left|x^2-4x-4\right| \;>\; 1$$

für alle $x \geq 6$. Außerdem gilt

$$x \;<\; \frac{x^2-1}{2} \;<\; \frac{x^2+1}{2} \qquad \text{und} \qquad x \;<\; \frac{x^2}{4}-1 \;<\; \frac{x^2}{4}+1.$$

Dies zeigt, dass zum Beispiel die beiden phythagoräische Tripel zu

$$20^2+21^2 \;=\; 19^2 \qquad \text{und} \qquad 119^2+120^2 \;=\; 169^2$$

nicht mit den gegebenen beiden Gleichungen dargestellt werden können, da $21-20 = 120-119 = 1$ gilt und da $20, 119 \geq 6$ ist.

6 Binäre quadratische Formen

In diesem Abschnitt untersuchen wir eine weitere Klasse von diophantischen Gleichungen, nämlich Gleichungen der Form

$$f(x,y) \;=\; ax^2 + bxy + cy^2.$$

6.1 Grundlagen

Definition 6.1.1

Eine Funktion der Form

$$f(x,y) \;=\; ax^2 + bxy + cy^2 \qquad \text{mit} \qquad a,b,c \in \mathbb{Z}$$

heißt ***binäre quadratische Form***. Die ***Diskriminante*** $d(f)$ von f sei

$$d(f) \;:=\; b^2 - 4ac.$$

Mit dieser Definition gilt $d(f) \equiv 0 \,(\bmod\ 4)$ oder $d(f) \equiv 1 \,(\bmod\ 4)$.

Wir werden nun einige Probleme mit diophantischen Gleichungen betrachten.

Ein Problem wie im Abschnitt zuvor ist es, ob es zu gegebenen a, b und c sowie einem $n \in \mathbb{N}$ auch natürliche Zahlen x und y mit

$$f(x,y) \;=\; ax^2 + bxy + cy^2 \;=\; n$$

gibt. Einige bekannte Beispiele hierzu sind die folgenden:

(1) $f(x,y) = x^2 + y^2 = n \qquad \text{mit} \qquad d(f) = -4.$

(2) $f(x,y) = x^2 + xy + y^2 = n \qquad \text{mit} \qquad d(f) = -3.$

(3) $f(x,y) = x^2 - 2y^2 = n \qquad \text{mit} \qquad d(f) = 8.$

(4) $f(x,y) = x^2 - Ny^2 = 1 \qquad \text{mit} \qquad d(f) = 4N.$

Ein weiteres Problem ist die Frage nach der Gesamtheit der Zahlen n, die durch eine gegebene binäre quadratische Form f dastellbar sind. Auch dies haben wir bereits am Beispiel $f(x,y) = x^2 + y^2$ untersucht.

Wir können $f(x,y) = ax^2 + bxy + cy^2$ auch schreiben als

$$f(x,y) \;=\; (x,y)^T \cdot \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix}.$$

Damit erhalten wir

$$d(f) \;=\; -4 \cdot \det \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}.$$

Definition 6.1.2

Sei f eine binäre quadratische Form.

Wir sagen n ist durch f ***darstellbar***, wenn es $x, y \in \mathbb{Z}$ gibt, so dass $f(x,y) = n$ gilt.

Weiter heißt n durch f ***primitiv darstellbar***, wenn es teilerfremde $x, y \in \mathbb{Z}$ gibt, so dass $f(x,y) = n$ gilt.

Satz 6.1.3

Sei f eine binäre quadratische Form mit $d := d(f) \neq 0$ und sei n so gewählt, dass n durch f primitiv darstellbar ist.

Dann gilt für jede Primzahl $p > 2$ mit $p \mid n$

$$\left(\frac{d}{p}\right) \;=\; 1,$$

also ist d ein quadratischer Rest modulo p und die Gleichung

$$z^2 \;\equiv\; d \,(\bmod\; p)$$

ist für ein $z \in \mathbb{Z}$ lösbar.

Definition 6.1.4

Seien f und g zwei binäre quadratische Formen.

Dann heißen f und g ***äquivalent***, wenn es $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$ mit $\alpha\delta - \beta\gamma = \pm 1$ gibt, so dass

$$f(x, y) \;=\; g(\alpha x + \beta y,\, \gamma x + \delta y)$$

gilt. Wir schreiben dafür $f \sim g$.

Gilt dabei $\alpha\delta - \beta\gamma = +1$, so heißen f und g ***streng äquivalent***, darauf werden wir aber nicht weiter eingehen.

Satz 6.1.5

Es gilt:

(1) Die zuvor definierte Äquivalenz bildet eine Äquivalenzrelation.

(2) Sind f und g äquivalent, dann gilt $d(f) = d(g)$.

(3) Sind f und g äquivalent und ist n durch f darstellbar, dann ist n auch durch g darstellbar.

6.2 Allgemeine Reduktionstheorie

Definition 6.2.1

Eine binäre quadratische Form mit $d := d(f) \neq 0$ heißt ***reduziert***, falls

$$0 \;\leq\; b \;\leq\; |a| \;\leq\; |c|$$

gilt.

Mit dieser Definition kommen wir nun zur Hauptaussage dieses Abschnitts. Damit wird es uns möglich sein zu einer vorgegebenen Diskriminante alle binären quadratischen Formen mit dieser Diskriminante zu finden.

Satz 6.2.2

(1) Jede binäre quadratische Form f mit $d := d(f) \neq 0$ ist zu einer reduzierten Form äquivalent.

(2) Die Anzahl der reduzierten binären quadratischen Formen f mit einer Diskriminante $d(f) \neq 0$ ist endlich, ferner gilt

$$b^2 \;\leq\; |ac| \;\leq\; \frac{|d(f)|}{3}.$$

(3) Sei $d < 0$ und seien f und g äquivalente reduzierten binäre quadratische Formen mit $d(f) = d(g) = d$.

Dann gilt $f = g$.

Vor allem die zweite Aussage dieses Satzes liefert uns nun interessante Beispiele. Es folgen daher eine ganze Reihe von Ergebnissen, die wir alle erhalten, wenn wir die reduzierten binären quadratischen Formen zu einer vorgegebenen Diskriminanten betrachten.

Beispiel 6.2.3

Wir suchen binären quadratischen Formen f mit der Diskriminanten $d(f) = -4$.

Für eine reduzierte binäre quadratische Form muss

$$b^2 \;\leq\; |ac| \;\leq\; \frac{|d(f)|}{3} \;=\; \frac{4}{3}$$

gelten, also $|ac| \leq 1$. Weiter folgt aus $d(f) = b^2 - 4ac$ gerade

$$0 \;\leq\; b^2 \;=\; 4ac - 4 \;=\; 4(ac - 1),$$

somit muss entweder $a = c = 1$ oder $a = c = -1$ gelten und jeweils ergibt sich dazu $b = 0$.

Wir erhalten also die beiden binären quadratischen Formen

$$f(x, y) \;=\; x^2 + y^2 \qquad \text{und} \qquad g(x, y) \;=\; -x^2 - y^2.$$

Nach Satz 6.2.2 sind damit alle binären quadratischen Formen mit einer Diskriminante von -4 zu diesen beiden Formen äquivalent. Offensichtlich sind f und g nicht äquivalent, da f nur positive und g nur negative Zahlen darstellen kann.

Auch mit der Theorie zu binären quadratischen Formen und diesem Beispiel lässt sich zeigen, dass jede Primzahl p mit $p \equiv 1 \,(\bmod\, 4)$ Summe von zwei Quadratzahlen ist. Allerdings erhalten wir hier anders als beim Ansatz mit den Gaußschen Zahlen keine Eindeutigkeit.

Beispiel 6.2.4

Wir interessieren uns nun für binäre quadratische Formen f mit der Diskriminanten $d(f) = -23$.

Zunächst gilt

$$b^2 \;\leq\; |ac| \;\leq\; \frac{|d(f)|}{3} \;=\; \frac{23}{3},$$

also $|ac| \leq 7$. Weiter folgt aus $d(f) = b^2 - 4ac$ gerade

$$0 \;\leq\; b^2 \;=\; 4ac - 23.$$

Dies zeigt aber auch, dass $ac \geq 6$ gelten muss, also zusammen $ac = 6$ oder $ac = 7$.

Für $ac = 7$ müsste aber $b^2 = 5$ gelten, das kann nicht sein.

Für $ac = 6$ folgt $b = 1$. Aus Symmetriegründen betrachten wir nur die reduzierte binären quadratischen Formen mit $|a| < |c|$. Mit dieser Einschränkung erhalten wir die beiden Lösungen

$$f(x,y) \;=\; 2x^2 + xy + 3y^2 \qquad \text{und} \qquad g(x,y) \;=\; x^2 + xy + 6y^2.$$

Die reduzierte binäre quadratische Form f stellt dabei zum Beispiel die Zahl 2 dar, f hingegen nicht.

Beispiel 6.2.5

Wir untersuchen nun reduzierte binäre quadratische Formen f mit $d(f) = -3$. Es gilt

$$b^2 \;\leq\; |ac| \;\leq\; \frac{|d(f)|}{3} \;=\; 1.$$

Mit $d(f) = b^2 - 4ac = -3$ folgt $ac = 1$. Wir untersuchen nur den positiven Fall und erhalten damit die einzig mögliche reduzierte binäre quadratische Form

$$f(x,y) \;=\; x^2 + xy + y^2 \;=\; (x+y)^2.$$

Mit der dritten Einheitswurzel $\omega = (-1 + \sqrt{-3})/2$ erhalten wir ähnlich wie unter Abschnitt 5.2 bei den Gaußschen Zahlen $R = \mathbb{Z}[i]$ auch mit $\mathbb{Z}[\omega]$ einen Hauptidealring. Es stellt sich also die Frage, ob für jede Primzahl p mit $p \equiv 3 \,(\bmod\ 4)$ bzw. mit $p \equiv 1 \,(\bmod\ 4)$ auch

$$\mathbb{Z}[(-1 + \sqrt{-p})/2] \qquad \text{bzw.} \qquad \mathbb{Z}[\sqrt{-p}]$$

ein Hauptidealring ist. Mit der Theorie über binäre quadratische Formen lässt sich zeigen, dass $p = 163$ die größte Primzahl ist, für die wir einen Hauptidealring erhalten.

Beispiel 6.2.6

Wir wollen nun die Beispiele betrachten, bei denen die Diskriminante eine Quadratzahl ist, also $d(f) = D^2$. Ist dies der Fall, dann gilt für die binäre quadratische Form $f(x, y) = ax^2 + bxy + cy^2$ mit $D^2 = b^2 - 4ac$ gerade

$$\begin{aligned} 4a \cdot (ax^2 + bxy + cy^2) &= (4ax)^2 + 4abxy + 4acy^2 \\ &= (4ax)^2 + 4abxy + (b^2 - D^2)y^2 \\ &= (4ax)^2 + 4abxy + (by)^2 - (Dy)^2 \\ &= (2ax + by)^2 - (Dy)^2 \\ &= (2ax + by - Dy) \cdot (2ax + by + Dy). \end{aligned}$$

Zunächst sei $a \neq 0$. Wenn wir dann bestimmen wollen, ob n durch eine binäre quadratische Form $f(x, y) = ax^2 + bxy + cy^2$ darstellbar ist deren Diskriminante eine Quadratzahl ist, so müssen wir nur überprüfen, ob es zwei Teiler d_1 und d_2 von $4an$ mit $4an = d_1 \cdot d_2$ gibt, die die Gleichungen

$$2ax + by - Dy = d_1 \qquad \text{und} \qquad 2ax + by + Dy = d_2$$

lösen.

Der einfache Spezialfall $f(x, y) = xy$ mit $d(f) = 1$ ist leicht zu untersuchen. Hier ist jedes n durch f darstellbar und wir erhalten mit $x, y \in \mathbb{Z}$ genau $2d(n)$ mögliche Darstellungen. Hierbei ist $d(n)$ als Anzahl der Teiler von n zu verstehen.

Dieses Beispiel begründet, wieso wir bei Beispielen mit positiven Diskriminanten keine Quadratzahlen mehr betrachten werden.

Beispiel 6.2.7

In diesem Beispiel interessieren wir uns für binäre quadratische Formen f mit der Diskriminante $d(f) = 5$.

Zunächst gilt

$$b^2 \leq |ac| \leq \frac{|d(f)|}{3} = \frac{5}{3}$$

gelten, also $|ac| \leq 1$. Weiter folgt aus $d(f) = b^2 - 4ac = 5$, dass $ac = -1$ gelten muss, denn für $ac = 0$ müsste $b^2 = 5$ gelten und für $ac = 1$ wäre $b = 3 > |a|$. Es ergeben sich somit die beiden reduzierten binären quadratischen Formen

$$f(x, y) = x^2 + xy - y^2 \qquad \text{und} \qquad g(x, y) = -x^2 + xy + y^2.$$

Diese beiden reduzierten Formen sind äquivalent, da $f(x,y) = g(y,x)$ gilt.

Zu diesem Beispiel betrachten wir die Folge der ***Fibonacci-Zahlen***

$$1, \quad 1, \quad 2, \quad 3, \quad 5, \quad 8, \quad 13, \quad 21, \quad 34, \quad \ldots,$$

die durch

$$F_n \;=\; F_{n-1} + F_{n-2}$$

definiert ist. Zunächst stellen wir fest, dass

$$\begin{aligned} f(F_0, F_1) &= 1, \\ f(F_1, F_2) &= -1, \\ f(F_2, F_3) &= 1, \\ f(F_3, F_4) &= -1 \end{aligned}$$

gilt. Wir wollen nun zeigen, dass sich sogar

$$f(F_n, F_{n+1}) \;=\; (-1)^n$$

ergibt. Dies ergibt sich iterativ aber sofort aus

$$\begin{aligned} f(F_n, F_{n+1}) &= F_n^2 + F_n \cdot (F_n + F_{n-1}) - (F_n + F_{n-1})^2 \\ &= F_n^2 + F_n^2 + F_n F_{n-1} - F_n^2 - 2F_n^2 F_{n-1} - F_{n-1}^2 \\ &= F_n^2 - F_n F_{n-1} - F_{n-1}^2 \;=\; -f(F_{n-1}, F_n). \end{aligned}$$

Es gibt also unendliche viele Darstellungen von 1 und von -1 durch $f(x,y) = -x^2 + xy + y^2$.

Beispiel 6.2.8

Sei nun $d(f) = 8$ vorgegeben. Für eine reduzierte binäre quadratische Form f mit $d(f) = 8$ muss

$$b^2 \;\leq\; |ac| \;\leq\; \frac{|d(f)|}{3} \;=\; \frac{8}{3}$$

gelten, also $|ac| \leq 2$. Weiter folgt aus $d(f) = b^2 - 4ac$ gerade

$$0 \;\leq\; b^2 \;=\; 4ac + 8$$

und da $0 \leq b \leq |a|$ gelten soll, folgt $ac = -2$ und damit $b = 0$. Wir erhalten die beiden reduzierten binären quadratischen Formen

$$f(x,y) \;=\; x^2 - 2y^2 \qquad \text{und} \qquad g(x,y) \;=\; -x^2 + 2y^2.$$

Auch diese beiden Formen sind äquivalent. Mit

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \;=\; \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}$$

folgt

$$f(\alpha x + \beta y,\, \gamma x + \delta y) \;=\; f(x + 2y,\, x + y) \;=\; g(x, y).$$

Wir beschäftigen uns im Folgenden mit

$$f(x, y) \;=\; x^2 - 2y^2 \;=\; (x + \sqrt{2}y) \cdot (x - \sqrt{2}y).$$

In dieser Darstellung gilt für $(x, y) = (1, 1)$

$$f(1, 1) \;=\; x^2 - 2y^2 \;=\; (1 + \sqrt{2}) \cdot (1 - \sqrt{2}) \;=\; -1$$

und es ergibt sich mit

$$(1 + \sqrt{2})^2 \;=\; 3 + 2\sqrt{2} \qquad \text{sowie} \qquad (1 - \sqrt{2})^2 \;=\; 3 - 2\sqrt{2}$$

sofort

$$f(3, 2) \;=\; (3 + 2\sqrt{2}) \cdot (3 - 2\sqrt{2}) \;=\; 1.$$

Somit erhalten wir auch

$$\begin{aligned} f(x, y) \;&=\; x^2 - 2y^2 \;=\; (x + \sqrt{2}y) \cdot (x - \sqrt{2}y) \cdot \Big((3 + 2\sqrt{2}) \cdot (3 - 2\sqrt{2})\Big)^n \\ &=\; \Big((x + \sqrt{2}y) \cdot (3 - 2\sqrt{2})^n\Big) \cdot \Big((x - \sqrt{2}y) \cdot (3 + 2\sqrt{2})^n\Big)\,. \end{aligned}$$

Wir definieren nun die Folgen $(s_n)_{n\in\mathbb{N}}$ und $(s_n)_{n\in\mathbb{N}}$ durch

$$(3 + 2\sqrt{2})^2 \;=:\; s_n + t_n\sqrt{2}$$

und es folgt damit insgesamt nach kurzer Rechnung

$$f(s_n x + 2t_n y,\, t_n x + s_n y) \;=\; f(x, y).$$

Weiter ergibt sich auch

$$\det \begin{pmatrix} s_n & 2t_n \\ t_n & s_n \end{pmatrix} \;=\; s_n^2 - 2t_n^2 \;=\; 1^n \;=\; 1$$

und wir erhalten damit zwei Ergebnisse:

(1) Wenn eine Zahl $n \neq 0$ durch $f(x, y)$ dargestellt werden kann, dann gibt es unendlich viele Darstellungen.

(2) Es gibt eine unendliche Gruppe von 2×2-Matrizen $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ mit

$$f(\alpha x + \beta y,\, \gamma x + \delta y) \;=\; f(x, y).$$

Weitere Ergebnisse zur Diskriminanten $d(f) = 8$ sind in Aufgabe 6.4.3 zu finden. Hier weden auch unendliche viele Lösungen von $f(x, y) = \pm 1$ berechnet.

Für ein $N \in \mathbb{N}$ heißen Gleichungen der Form

$$p(x, y) \;=\; x^2 - Ny^2 \;=\; 1$$

Pellsche Gleichungen. Ist N keine Quadratzahl, dann hat die zugehörige Pellsche Gleichung unendlich viele Lösungen.

Für $N = 5$ gilt zum Beispiel

$$p(2, 1) \;=\; 4 - 5 \;=\; (2 + \sqrt{5}) \cdot (2 - \sqrt{5}) \;=\; -1$$

und aus

$$(2 + \sqrt{5})^2 \cdot (2 - \sqrt{5})^2 \;=\; (-1)^2 \;=\; 1$$

folgt, dass $(x, y) = (9, 4)$ die kleinsten Zahlen sind, mit

$$p(x, y) \;=\; x^2 - 5y^2 \;=\; 1.$$

Beispiel 6.2.9

In diesem Beispiel untersuchen wir reduzierte binäre quadratische Formen f mit $d(f) = -20$. Aus

$$b^2 \;\leq\; |ac| \;\leq\; \frac{|d(f)|}{3} \;=\; \frac{20}{3}$$

folgt $|ac| \leq 6$. Weiter ergibt sich mit $d(f) = b^2 - 4ac$ gerade

$$0 \;\leq\; b^2 \;=\; 4ac - 20,$$

also $|ac| = 5$ mit $b = 0$ oder $|ac| = 6$ mit $b = 2$. Betrachten wir nur positive a und c, so erhalten wir mit der Bedingung $b^2 \leq a \leq c$ wieder zwei binäre quadratische Formen:

$$f(x, y) \;=\; x^2 + 5y^2 \qquad \text{und} \qquad g(x, y) \;=\; 2x^2 + 2xy + 3y^2.$$

Die Zahlen 1 und 5 werden offenbar durch f, jedoch nicht durch g dargestellt. Umgekehrt werden die Zahlen 2 und 3 durch g dargestellt, jedoch nicht durch f. Somit können g und f nicht äquivalent sind.

Es lässt sich zeigen, dass jedes n mit

$$n \equiv 1 \,(\mathrm{mod}\ 20) \qquad \text{oder} \qquad n \equiv 9 \,(\mathrm{mod}\ 20)$$

durch f, jedoch nicht durch g darstellbar ist. Für jedes n mit

$$n \equiv 3 \,(\mathrm{mod}\ 20) \qquad \text{oder} \qquad n \equiv 7 \,(\mathrm{mod}\ 20)$$

liegt der umgekehrte Fall vor.

Durch Kongruenzrechnung lässt sich damit genau feststellen, welche Zahlen n durch f und welche Zahlen n durch g darstellbar sind.

Beispiel 6.2.10

Zur Diskriminanten $d(f) = -71$ erhalten wir die folgenden vier reduzierten binären quadratischen Formen:

(1) $f_1(x, y) = x^2 + xy + 18y^2$.

(2) $f_2(x, y) = 2x^2 + xy + 9y^2$.

(3) $f_3(x, y) = 3x^2 + xy + 6y^2$.

(4) $f_4(x, y) = 4x^2 + 3xy + 5y^2$.

Wir bemerken, dass wir hier gleich vier reduzierte Formen erhalten, da $72 = 71 + 1$ so viele Teiler hat.

Die drei kleinsten Zahlen, die primitiv durch eine allgemeine reduzierte Form $f(x, y) = ax^2 + bxy + cy^2$ dargestellt werden können, sind a, c und $a + c - b$.

In unserem Falle gilt damit:

(1) $n = 1$ wird nur durch $f_1(x, y)$ dargestellt.

(2) $n = 2$ wird nur durch $f_2(x, y)$ dargestellt.

(3) $n = 3$ wird nur durch $f_3(x, y)$ dargestellt.

(4) $n = 4$ wird primitiv nur durch $f_4(x, y)$ dargestellt, mit $f_1(2, 0) = 4$ jedoch auch (nicht primitiv) durch $f_1(x, y)$.

(5) $n = 5$ wird nur durch $f_4(x, y)$ dargestellt.

(6) $n = 6$ hingegeben wird durch $f_3(x, y)$ und $f_4(x, y)$ dargestellt.

Dies zeigt also, dass es möglich ist, dass eine Zahl n durch zwei reduzierte binäre quadratische Formen mit einer Diskriminanten $d(f) = -p$ dargestellt werden kann. Dies erhält man jedoch erst für *größere* Primzahlen p, in diesem Beispiel haben wir $p = 71$.

Beispiel 6.2.11

Abschließend betrachten wir noch einmal das Beispiel $d(f) = -23$. Wir erhalten hier die reduzierten Formen

$$f(x, y) \;=\; 2x^2 + xy + 3y^2 \qquad \text{und} \qquad g(x, y) \;=\; x^2 + xy + 6y^2.$$

Ähnlich wie bei der Darstellung einer Zahl N als Summe von zwei Quadratzahlen lässt sich auch hier eine Formel zur Berechnung der endlichen Anzahl der Darstellungen von n durch $f(x, y)$ bzw. $g(x, y)$ angeben.

Weiter hatten wir definiert, dass f und g äquivalent sind, wenn es $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$ mit $\alpha\delta - \beta\gamma = \pm 1$ gibt, so dass

$$f(x, y) \;=\; g(\alpha x + \beta y,\, \gamma x + \delta y)$$

gilt. Damit erhalten wir, dass

$$f(x, y) \;=\; 2x^2 + xy + 3y^2 \qquad \text{und} \qquad \overline{f}(x, y) \;=\; 2x^2 - xy + 3y^2$$

äquivalent sind. Lassen wir hingegen nur Koeffizienten mit $\alpha\delta - \beta\gamma = +1$ zu, so sind

$$f(x, y) \;=\; 2x^2 + xy + 3y^2 \qquad \text{und} \qquad \overline{f}(x, y) \;=\; 2x^2 - xy + 3y^2$$

nicht mehr äquivalent, die beiden Formen

$$g(x, y) \;=\; x^2 + xy + 6y^2 \qquad \text{und} \qquad \overline{g}(x, y) \;=\; x^2 - xy + 6y^2$$

jedoch schon.

6.3 Reduktionstheorie nach Gauß

Wir beschäftigen uns weiterhin mit binären quadratischen Formen, genauer mit dessen Reduktion auf eine reduzierte Form. Für ***indefinite*** Formen, also für binären quadratischen Formen f, bei denen es (x, y) mit $f(x, y) > 0$ und (u, v) mit $f(u, v) < 0$ gibt, treten zwei Probleme auf:

(1) Es gibt keine eindeutige reduzierte Form.

(2) Es gibt eine unendliche Automorphismengruppe von 2×2-Matrizen $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ mit

$$f(\alpha x + \beta y,\, \gamma x + \delta y) \;=\; f(x, y).$$

Dies haben wir bereits in Beispiel 6.2.8 mit der binären Form

$$f(x, y) \;=\; x^2 - 2y^2$$

kennen gelernt. Um mit derartigen Problemen besser umgehen zu können, wird eine weitere Theorie benötigt. Wir verwenden dazu einen weiteren Reduktionsbegriff, der auf Gauß zurückgeht. An dieser Stelle soll ein kurzer Einblick in diese Theorie gegeben werden, mit der wir in der Lage sind eine reduzierte Form recht einfach algorithmisch zu berechnen. Dazu betrachten wir zunächst den Spezialfall von positiv definiten Formen, bevor wir zum allgemeinen Fall zurückkehren.

Positiv definite binäre quadratische Formen

Sei

$$f(x, y) \;=\; ax^2 + bxy + cy^2$$

eine positiv definite binäre quadratische Form auf $\mathbb{R}$, es gelte also $f(x, y) > 0$ für alle $x, y \in \mathbb{R} - \{0\}$. Wir fordern damit also auch $a, c > 0$ und die Diskriminante von f sei $d := d(f) < 0$. Weiter sei

$$g \;=\; \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \qquad \text{und} \qquad \alpha\delta - \beta\gamma \;=\; \pm 1$$

und zu einem derartigen g sei

$$(f \circ g)(x, y) \;:=\; f(\alpha x + \beta y,\, \gamma x + \delta y).$$

Mit der komplexen Zahl

$$z \;=\; \frac{-b + \sqrt{d}}{2a} \qquad \text{sowie} \qquad \overline{z} \;=\; \frac{-b - \sqrt{d}}{2a}$$

ergibt sich mit $d = b^2 - 4ac$ direkt

$$f(x, y) \;=\; ax^2 + bxy + cy^2 \;=\; a \cdot (x - zy) \cdot (x + \overline{z}y).$$

Die Bedingung an eine reduzierte Form zu einer positiv definiten binären quadratischen Form ist

$$0 \;\leq\; b \;\leq\; a \;\leq\; c,$$

da hier $a, c > 0$ gelten muss. Wir erhalten mit $\operatorname{Re} z = -b/(2a)$ gerade

$$-\frac{1}{2} \;\leq\; \operatorname{Re} z \;\leq\; \frac{1}{2}$$

und mit $c = (b^2 - d)/(4a) = |z|^2 a$ gerade

$$|z|^2 \;\geq\; 1.$$

Um nun zu einem $z \in \mathbb{C}$ eine positiv definite binäre quadratische Form zu erhalten, müssen wir nur die Menge

$$Z \;:=\; \left\{ z \in \mathbb{C} \;\middle|\; |z| \;\geq\; 1,\;\; -\frac{1}{2} \;\leq\; \operatorname{Re} z \;\leq\; \frac{1}{2} \right\}$$

betrachten.

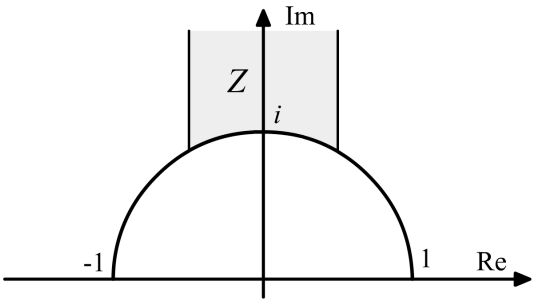


Abbildung 6.1: Veranschaulichung der Menge Z.

Indefinite binäre quadratische Formen

Wir kommen nun zum allgemeinen Fall zurück und betrachten indefinite Formen:

Sei

$$f(x, y) \;=\; ax^2 + bxy + cy^2$$

eine indefinite binäre quadratische Form auf $\mathbb{R}$, es gebe also $(x, y), (u, v) \in \mathbb{R}^2$ mit $f(x, y) > 0$ und $f(u, v) < 0$. Die Diskriminante von f ist dabei also gegeben durch $d := d(f) > 0$. Auch hier faktorisieren wir f zu

$$f(x, y) \;=\; ax^2 + bxy + cy^2 \;=\; a \cdot (x - \theta y) \cdot (x + \theta' y),$$

wobei θ und θ' mit

$$\theta \;=\; \frac{-b + \sqrt{d}}{2|a|} \qquad \text{sowie} \qquad \theta' \;=\; \frac{-b - \sqrt{d}}{2|a|}$$

gerade die Nullstellen von

$$|a|\xi^2 + b\xi + c$$

sind. Hier gilt $\theta + \theta' = -b/|a|$ und mit der Bedingung

$$0 \ \leq \ b \ \leq \ |a| \ \leq \ |c|$$

an eine reduzierte Form also

$$-1 \ \leq \ \theta + \theta' \ \leq \ 0.$$

Dies führt uns zu dem bereits angesprochenen neuen Reduktionsbegriff:

Definition 6.3.1

Sei

$$f(x, y) \ = \ ax^2 + bxy + cy^2$$

eine indefinite binäre quadratische Form mit positiver Diskriminante, die kein Quadrat ist. Es gelte also $d := d(f) > 0$ mit $\sqrt{d} \notin \mathbb{N}$.

Die Form f heißt ***Gauß reduziert***, wenn

$$0 \ \leq \ b \ < \ \sqrt{d} \qquad \text{und} \qquad \sqrt{d} - b \ < \ 2|a| \ < \ \sqrt{d} + b$$

gilt.

Wieder können wir zu jeder indefinite binäre quadratische Form f mit $d = d(f) > 0$ und $\sqrt{d} \notin \mathbb{N}$ eine Gauß reduzierte Form mit gleicher Diskriminante d finden.

Der folgende Algorithmus basiert auf der Idee, dass der Abstand $|\theta - \theta'|$ möglichst groß werden soll. Dies bedeutet nämlich gerade, dass

$$|\theta - \theta'| \ = \ \frac{\sqrt{d}}{|a|}$$

möglich groß und damit $|a|$ möglichst klein werden soll.

Nach der Definition von Gauß reduzierten Formen ist auch sofort klar, dass es nur endlich viele Gauß reduzierte Formen geben kann.

Gauß-Algorithmus

Gegeben sei eine indefinite binäre quadratische Form

$$f(x,y) \;=\; ax^2 + bxy + cy^2$$

mit $d := d(f) > 0$ und $\sqrt{d} \notin \mathbb{N}$.

Bestimme $b_1 \equiv -b \,(\bmod\ 2|c|\,)$ mit

$$\sqrt{d} - 2|c| \;<\; b_1 \;<\; \sqrt{d}$$

und setze

$$a_1 \;=\; c \qquad \text{und} \qquad c_1 \;=\; \frac{b_1^2 - d}{4a_1}.$$

Als Ergebnis erhalten wir den ***Nachfolger***

$$f_1(x,y) \;=\; a_1x^2 + b_1xy + c_1y^2.$$

Zu diesem Algorithmus lässt sich zeigen, dass sich in jedem Schritt der Abstand $|\theta - \theta'|$ vergrößert. Außerdem erhalten wir stets nach endlich vielen Schritten eine Gauß reduzierte Form, allerdings ist diese nicht eindeutig bestimmt.

Eine weitere Eigenschaft der Gauß Reduktion ist es, dass wir etwas einfacher überprüfen können, ob eine Zahl n durch eine gegebene indefinite binäre quadratische Form mit positiver Diskriminante, die kein Quadrat ist, darstellbar ist oder nicht. Zudem lässt sich diese Theorie auch anschaulich erklären.

Zykel aus Gauß reduzierten Formen

Sind wir nach endlich vielen Schritten bei einer Gauß reduzierten Form angekommen, so ist auch jeder Nachfolger eine Gauß reduzierte Form.

Wir laufen also durch einen ***Zykel*** von Gauß reduzierten Formen. Trotzdem kann es zu Formen mit einer vorgegebenen Diskriminanten mehrere Zykel aus Gauß reduzierten Formen geben. Jeder Zykel besteht also aus äquivalenten Formen, die dieselben Zahlen darstellen können. Die Formen aus unterschiedlichen Zykel sind dagegen nicht äquivalent.

Wir wollen abschließend einige Beispiele diskutieren.

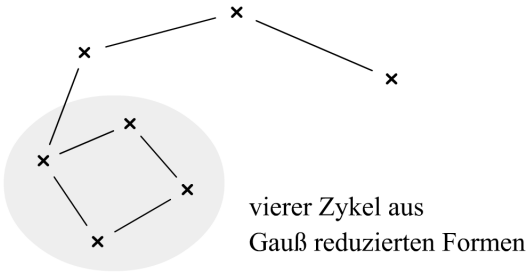


Abbildung 6.2: Vierer Zykel aus Gauß reduzierten Formen.

Beispiel 6.3.2

Wir betrachten das Beispiel $a = 1$, $b = 0$ und $c = -2$, also

$$f(x, y) \;=\; x^2 - 2y^2.$$

Diese Form ist offenbar indefinit und die Diskriminante $d := d(f) = 8$ ist kein Quadrat. Zudem ist diese Form aus Beispiel 6.2.8 reduziert, jedoch nicht Gauß reduziert, da die Bedingung

$$\sqrt{d} - b \;<\; 2|a| \;<\; \sqrt{d} + b$$

verletzt wird. Wenden wir den Gauß-Algorithmus an, so erfüllt $b_1 = 0$ gerade $b_1 \equiv -b \,(\bmod\; 2|c|\,)$ mit

$$\sqrt{d} - 2|c| \;<\; b_1 \;<\; \sqrt{d}$$

und wir erhalten

$$a_1 \;=\; c \;=\; -2 \qquad \text{und} \qquad c_1 \;=\; \frac{b_1^2 - d}{4a_1} \;=\; 1,$$

also den Nachfolger

$$f_1(x, y) \;=\; -2x^2 + y^2.$$

Auch hier ist die Bedingung

$$\sqrt{d} - b_1 \;<\; 2|a_1| \;<\; \sqrt{d} + b_1$$

verletzt, sodass auch f_1 nicht Gauß reduziert ist. Im nächsten Schritt erfüllt gerade $b_2 = 2$ die Bedingung $b_2 \equiv -b_1 \,(\bmod\; 2|c_1|\,)$ mit

$$\sqrt{d} - 2|c_1| \;<\; b_2 \;<\; \sqrt{d}.$$

Es ergibt sich dazu

$$a_2 \;=\; c_1 \;=\; 1 \qquad \text{und} \qquad c_2 \;=\; \frac{b_2^2 - d}{4a_2} \;=\; -1,$$

also

$$f_2(x,y) \;=\; x^2 + 2xy - y^2.$$

Diese Form ist nun Gauß reduziert. Im vierten Schritt folgt

$$f_3(x,y) \;=\; -x^2 + 2xy + y^2$$

und im fünften Schritt wieder f_2. Wir haben in diesem Beispiel also einen zweier Zykel aus den beiden äquivalenten Gauß reduzierten Formen f_2 und f_3.

Bevor wir zum nächsten Beispiel übergehen, führen wir eine Definition zur kürzeren Schreibweise von binären quadratischen Formen ein:

Definition 6.3.3

Die Kurzschreibweise der binären quadratischen Form

$$f(x,y) \;=\; ax^2 + bxy + cy^2$$

sei gegeben durch

$$f \;:=\; (a,b,c).$$

Beispiel 6.3.4

Wir untersuchen nun als Beispiel binäre quadratische Formen f mit der Diskriminanten $d = d(f) = 65$.

Zunächst wollen wir alle Gauß reduzierten Formen mit dieser Diskriminanten finden. Es gilt $8 < \sqrt{d} < 9$, somit erhalten wir als Bedingung

$$0 \;\leq\; b \;\leq\; 8.$$

Die zweite Bedingung aus der Definition einer Gauß reduzierten Form lautet

$$\sqrt{d} - b \;<\; 2|a| \;<\; \sqrt{d} + b \qquad \Rightarrow \qquad 8 - b \;<\; 2|a| \;\leq\; 8 + b$$

und mit $d = b^2 - 4ac$ ergibt sich, dass b ungerade sein muss. Wir erhalten die gesuchten Gauß reduzierten Formen nun einfach durch Betrachtung dieser Bedingungen. Für $b = 1$ muss $ac = -16$, für $b = 3$ muss $ac = -14$, für $b = 5$ muss $ac = -10$ und für $b = 7$ muss $ac = -4$ gelten. Unter Berücksichtigung aller Bedingungen ergeben sich 12 Gauß reduzierte Formen, nämlich:

$$\begin{array}{llll} (4,1,-4), & (-4,1,4), & (2,5,-5), & (-2,5,5), \\ (5,5,-2), & (-5,5,2), & (1,7,-4), & (-1,7,4), \\ (2,7,-2), & (-2,7,2), & (4,7,-1), & (-4,7,1). \end{array}$$

Um nun festzustellen, welcher dieser Formen äquivalent sind, berechnen wir dessen Nachbarn und damit den oder die Zykel. Beginnen wir mit $(a, b, c) = (4, 1, -4)$, so gilt mit $2|c| = 8$ und mit $0 < b_1 \leq 8$

$$b_1 \equiv -b \,(\mathrm{mod}\ 8)$$

gerade für $b_1 = 7$. Wir setzen

$$a_1 = c = -4 \qquad \text{und} \qquad c_1 = \frac{b_1^2 - d}{4a_1} = 1.$$

Der Nachbar von $(4, 1, -4)$ ist also $(-4, 7, 1)$. Führen wir dies weiter fort, so erhalten wir den folgenden Zykel:

$$\begin{array}{ccccc} (4,1,-4) & \longrightarrow & (-4,7,1) & \longrightarrow & (1,7,-4) \\ \uparrow & & & & \downarrow \\ (-1,7,4) & \longleftarrow & (4,7,-1) & \longleftarrow & (-4,1,4) \end{array} .$$

Als zweiten Zykel ergibt sich

$$\begin{array}{ccccc} (2,5,-5) & \longrightarrow & (-5,5,2) & \longrightarrow & (2,7,-2) \\ \uparrow & & & & \downarrow \\ (-2,7,2) & \longleftarrow & (5,5,-2) & \longleftarrow & (-2,5,5) \end{array} .$$

Mit $(1, 7, -4)$ und $(-1, 7, 4)$ aus dem ersten Zykel und mit $(x, y) = (1, 0)$ erkennen wir, dass alle äquivalenten Formen aus dem ersten Zykel die Zahlen 1 und -1 darstellen.

Die Formen aus dem zweiten Zykel können die Zahl 1 zum Beispiel nicht darstellen: Nach dem Euler-Kriterium folgt mit

$$2^2 \equiv -1 \,(\mathrm{mod}\ 5),$$

dass 2 ein quadratischer Nichtrest modulo 5 ist. Damit haben die Kongruenzen

$$x^2 \equiv 2 \,(\mathrm{mod}\ 5) \qquad \text{und} \qquad 2x^2 \equiv 1 \,(\mathrm{mod}\ 5)$$

keine Lösung. Dies zeigt, dass die Gauß reduzierte Form

$$f(x, y) = 2x^2 + 5xy + 5y^2$$

aus dem zweiten Zykel die Zahl 1 nicht darstellen kann und damit keine Form aus diesem Zykel.

Zum Beispiel stellt die binäre quadratische Form

$$f(x,y) \;=\; x^2 + xy - 16y^2$$

die Zahl 1 dar, ist aber nicht Gauß reduziert. Wenn wir diese Form reduzieren, landen wir nach zwei Schritten wie erwartet im ersten Zykel:

$$\begin{array}{ccccccc} & & & & & & (1,1,-16) \\ & & & & & & \downarrow \\ (4,1,-4) & \longrightarrow & (-4,7,1) & \longrightarrow & (1,7,-4) & \longleftarrow & (-16,-1,1)\ . \\ \uparrow & & & & \downarrow & & \\ (-1,7,4) & \longleftarrow & (4,7,-1) & \longleftarrow & (-4,1,4) & & \end{array}$$

Interessant an diesem Beispiel war auch die Tatsache, dass es zwei Zykel gab. Daher ist die *Klassenzahl* von $d = 65$ gerade 2:

Definition 6.3.5

Die ***Klassenzahl*** $A(d)$ einer gegebenen Diskriminante $d > 0$ mit $\sqrt{d} \notin \mathbb{N}$ sei die Anzahl der Zykel in Gauß reduzierten Formen.

Die Klassenzahl lässt sich alleine aus der vorgegebenen Diskriminanten d berechnen, darauf wollen wir aber nicht weiter eingehen.

Zudem gibt es nur endlich viele Diskriminanten d, die die Klassenzahl $A(d) = 1$ haben. Die größte dieser Zahlen ist $d = 163$. Tabelle 6.1 zeigt die Klassenzahlen zu den möglichen Diskriminanten $d \leq 30$.

d	5	8	12	13	17	20	21	24	28	29
$A(d)$	1	1	2	1	1	3	2	2	2	1

Tabelle 6.1: Die Klassenzahl zu einigen Diskriminanten.

Bemerkung

Wir können auch die Methode der Zykel verwenden, um für eine Gauß reduzierte Form f mit der Diskriminanten d ein T zu finden, so dass

$$f(T(x,y)) \;=\; f(x,y)$$

gilt. Ist die Zykellänge t, so ist T von der Form

$$T \;=\; \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \;=\; \begin{pmatrix} 0 & 1 \\ 1 & n_1 \end{pmatrix} \cdot \ldots \cdot \begin{pmatrix} 0 & 1 \\ 1 & n_t \end{pmatrix}.$$

Dabei gilt $\det(T) = \pm 1$, wie untersuchen jedoch nur $\det(T) = 1$, denn für $\det(T) = -1$ verwenden wir T^2 mit $\det(T^2) = 1$. Als Bedingung an T erhalten wir nach kurzer Rechnung

$$\left(\frac{\alpha+\delta}{2}\right)^2 - d \cdot \left(\frac{\alpha-\delta}{2}\right)^2 = 1.$$

Damit können wir also auch eine Lösung für die Pellsche Gleichung

$$x^2 - dy^2 = 1$$

berechnen.

6.4 Aufgaben

Aufgabe 6.4.1

Bestimme die Menge aller Zahlen ≤ 100, die durch die binäre quadratische Form $f(x, y) = x^2 + 5y^2$ dargestellt werden können.

Lösung

Löst (x, y) die gegebenen binäre quadratische Form, dann auch $(-x, -y)$. Somit untersuchen wir nur natürliche Zahlen x und y, da es für negative ganze Zahlen offenbar unendlich viele Lösungen mit $x, y \leq 100$ gibt.

Wählen wir $y = 0$, so erhalten wir mit $x = 0, \ldots, 10$ alle Quadratzahlen und diese können damit durch $f(x, y)$ dargestellt werden:

$$\{0, 1, 4, 9, 16, 25, 36, 49, 64, 81, 100\}.$$

Wählen wir $y = 1$, so erkennen wir, dass auch alle $x^2 + 5$ durch $f(x, y)$ dargestellt werden können:

$$\{5, 6, 9, 14, 21, 30, 41, 54, 69, 86\}.$$

Für $y = 2$ erhalten wir alle $x^2 + 20$:

$$\{20, 21, 24, 29, 36, 45, 56, 69, 84\}.$$

Für $y = 3$ alle $x^2 + 45$:

$$\{45, 46, 49, 54, 61, 70, 81, 94\}.$$

Und für $y = 4$ schließlich alle $x^2 + 80$:

$$\{80, 81, 84, 89, 96\}.$$

Da $5 \cdot 5^2 > 100$ gilt, können wir hier aufhören. Insgesamt erhalten wir die Lösungsmenge

$$\begin{aligned} A \;=\; \{&0,\,1,\,4,\,5,\,6,\,9,\,14,\,16,\,20,\,21,\,24,\,25,\,29,\,30,\,36,\,41,\,45,\,46,\,49,\\ &54,\,56,\,61,\,64,\,69,\,70,\,80,\,81,\,84,\,86,\,89,\,94,\,96,\,100\}. \end{aligned}$$

Damit enthält die Menge A 33 Elemente und zwischen 70 und 80 lässt sich keine Zahl durch $x^2 + 5y^2$ darstellen. Zu zwei beliebigen Zahlen aus dieser Menge ist auch das Produkt in der Menge enthalten, sofern dieses die Bedingung ≤ 100 erfüllt. Für jedes Element $a \in A$ gilt außerdem

$$a \;\equiv\; 0,\,1 \,\text{oder}\, -1 \,(\bmod\, 5\,).$$

Aufgabe 6.4.2

Reduziere die binäre quadratische Form $f(x, y) = 23x^2 + 73xy + 58y^2$ und finde alle Lösungen von $f(x, y) = 11$.

Lösung

Es gilt $d(f) = -7$, somit ist f zu einer reduzierten Form g mit $d(g) = d(f) = -7$ äquivalent. Für die reduzierte binäre quadratische Form g mit $d(g) = -7$ muss

$$b^2 \;\leq\; |ac| \;\leq\; \frac{|d(f)|}{3} \;=\; \frac{7}{3}$$

gelten, also $|ac| \leq 2$. Weiter folgt aus $d(g) = b^2 - 4ac$ gerade

$$0 \;\leq\; b^2 \;=\; 4ac - 7,$$

somit muss $ac = 2$ gelten und es ergibt sich dazu $b = 1$. Wir erhalten

$$g(x, y) \;=\; x^2 + xy + 2y^2$$

als reduzierte binäre quadratische Form mit $d(g) = -7$.

Wir wollen nun zeigen, dass g und f äquivalent sind. Dazu müssen wir $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$ mit $\alpha\delta - \beta\gamma = \pm 1$ finden, so dass

$$g(\alpha x + \beta y,\, \gamma x + \delta y) \;=\; f(x, y)$$

gilt. Aus

$$\begin{aligned} g(\alpha x + \beta y,\, \gamma x + \delta y) \;=\; &(\alpha^2 + 2\gamma^2 + \alpha\gamma) \cdot x^2 \;+\; (\beta^2 + 2\delta^2 + \beta\delta) \cdot y^2 \\ &+ (2\alpha\beta + 4\gamma\delta + \alpha\delta + \beta\gamma) \cdot xy \end{aligned}$$

folgen die beiden Bedingungen

$$\alpha^2 + 2\gamma^2 + \alpha\gamma \;=\; 23 \qquad \text{und} \qquad \beta^2 + 2\delta^2 + \beta\delta \;=\; 58.$$

Die erste Bedingung wird für $\alpha = 3$ und $\gamma = 2$ und die zweite Bedingung durch $\beta = 5$ und $\delta = 3$ erfüllt. Für diese Lösungen gilt $\alpha\delta - \beta\gamma = -1$ sowie

$$g(3x + 5y,\, 2x + 3y) \;=\; 23x^2 + 73xy + 58y^2 \;=\; f(x, y),$$

also sind g und f äquivalent. Somit lassen sich die gleichen Zahlen durch f darstellen, die auch durch g darstellbar sind. Es gilt

$$g(x, y) \;=\; x^2 + xy + 2y^2 \;=\; 11$$

nur für die vier Lösungen

$$(1,\, 2), \quad (-1,\, -2), \quad (-3,\, 2) \quad \text{und} \quad (3,\, -2).$$

Um diese vier Lösungen von $g(x, y) = 11$ auch auf $f(x, y) = 11$ übertragen zu können, müssen wir die Gleichungssystem

$$A \cdot \begin{pmatrix} x \\ y \end{pmatrix} \;=\; \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \qquad A \cdot \begin{pmatrix} x \\ y \end{pmatrix} \;=\; \begin{pmatrix} -1 \\ -2 \end{pmatrix},$$
$$A \cdot \begin{pmatrix} x \\ y \end{pmatrix} \;=\; \begin{pmatrix} 3 \\ -2 \end{pmatrix}, \qquad A \cdot \begin{pmatrix} x \\ y \end{pmatrix} \;=\; \begin{pmatrix} -3 \\ 2 \end{pmatrix}.$$

mit

$$A \;=\; \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \;=\; \begin{pmatrix} 3 & 5 \\ 2 & 3 \end{pmatrix}$$

lösen. Wir erhalten damit die folgenden Lösungen für $f(x, y) = 11$:

$$(7,\, -4), \quad (-7,\, 4), \quad (-19,\, 12) \quad \text{und} \quad (19,\, -12).$$

Da es nur 4 Lösungen für $g(x, y) = 11$ gibt, kann es auch für $f(x, y) = 11$ nur diese vier Lösungen geben.

Aufgabe 6.4.3

Reduziere die binäre quadratische Form $f(x, y) = 17x^2 + 56xy + 46y^2$ und zeige, dass $f(x, y) = 1$ sowie $f(x, y) = -1$ jeweils unendliche viele Lösungen haben.

Lösung

Es gilt $d(f) = 8$, somit ist f zu einer reduzierten Form g mit $d(g) = d(f) = 8$ äquivalent. Für die reduzierte binäre quadratische Form g mit $d(g) = 8$ muss

$$b^2 \;\leq\; |ac| \;\leq\; \frac{|d(f)|}{3} \;=\; \frac{8}{3}$$

gelten, also $|ac| \leq 2$. Weiter folgt aus $d(g) = b^2 - 4ac$ gerade

$$0 \;\leq\; b^2 \;=\; 4ac + 8$$

und da $0 \leq b \leq |a|$ gelten soll, folgt $ac = -2$. Wählen wir $a = 1$ und $c = -2$, so muss $b = 0$ sein und wir erhalten

$$g(x, y) \;=\; x^2 - 2y^2$$

als reduzierte binäre quadratische Form mit $d(g) = 8$.

Wir wollen nun zeigen, dass g und f äquivalent sind. Dazu müssen wir $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$ mit $\alpha\delta - \beta\gamma = \pm 1$ finden, so dass

$$g(\alpha x + \beta y,\, \gamma x + \delta y) \;=\; f(x, y)$$

gilt. Aus

$$g(\alpha x + \beta y,\, \gamma x + \delta y) \;=\; (\alpha^2 - 2\gamma^2) \cdot x^2 + (\beta^2 - 2\delta^2) \cdot y^2 + (2\alpha\beta - 4\gamma\delta) \cdot xy$$

folgen die beiden Bedingungen

$$\alpha^2 - 2\gamma^2 \;=\; 17 \qquad \text{und} \qquad \beta^2 - 2\delta^2 \;=\; 46.$$

Die erste Bedingung wird für $\alpha = 5$ und $\gamma = 2$ und die zweite Bedingung durch $\beta = 8$ und $\delta = 3$ erfüllt. Für diese Lösungen gilt $\alpha\delta - \beta\gamma = -1$ sowie

$$g(5x + 8y,\, 2x + 3y) \;=\; 17x^2 + 56xy + 46y^2 \;=\; f(x, y),$$

also sind g und f äquivalent. Somit lassen sich die gleichen Zahlen durch f darstellen, die auch durch g darstellbar sind.

Wir wollen nun zeigen, dass es unendliche viele Lösungen von $g(x, y) = 1$ bzw. $g(x, y) = -1$ gibt. Zunächst gilt

$$\begin{aligned}
g(1, 1) &= 1^2 - 2 \cdot 1^2 = -1, \\
g(3, 2) &= 3^2 - 2 \cdot 2^2 = 1, \\
g(7, 5) &= 7^2 - 2 \cdot 5^2 = -1, \\
g(17, 12) &= 17^2 - 2 \cdot 12^2 = 1, \\
g(41, 29) &= 41^2 - 2 \cdot 29^2 = -1, \\
g(99, 70) &= 99^2 - 2 \cdot 10^2 = 1.
\end{aligned}$$

Wir definieren nun

$$(x_0, y_0) \;=\; (1,1) \qquad \text{und} \qquad (x_1, y_1) \;=\; (3,2).$$

Weiter sei

$$(x_k, y_k) \;:=\; (3y_{k-1} + y_{k-2},\, 2y_{k-1} + y_{k-2}),$$

damit gilt stets $x_{k-2} = y_{k-1} - y_{k-2}$. Wir nehmen nun an, es gilt

$$\begin{aligned} g(x_{k-2}, y_{k-2}) &= x_{k-2}^2 - 2y_{k-2}^2 \;=\; 1 \qquad \text{und} \\ g(x_{k-1}, y_{k-1}) &= x_{k-1}^2 - 2y_{k-1}^2 \;=\; -1, \end{aligned}$$

dann erhalten wir

$$\begin{aligned} g(x_k, y_k) &= x_k^2 - 2y_k^2 \;=\; (3y_{k-1} + y_{k-2})^2 - 2 \cdot (2y_{k-1} + y_{k-2})^2 \\ &= 9y_{k-1}^2 + 6y_{k-1}y_{k-2} + y_{k-2}^2 - 8y_{k-1}^2 - 8y_{k-1}y_{k-2} - 2y_{k-2}^2 \\ &= y_{k-1}^2 - 2y_{k-1}y_{k-2} - y_{k-2}^2 \;=\; (y_{k-1} - y_{k-2})^2 - 2y_{k-2}^2 \\ &= x_{k-2}^2 - 2y_{k-2}^2 \;=\; 1. \end{aligned}$$

Somit haben wir eine Rekursionsformel berechnet und erhalten insgesamt

$$g(x_{2k}, y_{2k}) \;=\; -1 \qquad \text{und} \qquad g(x_{2k+1}, y_{2k+1}) \;=\; 1$$

für alle $k \in \mathbb{N}$.

Diese Lösungen können wir auch auf die äquivalente Form $f(x, y)$ übertragen. Dazu müssen wir das Gleichungssystem

$$A \cdot \begin{pmatrix} x \\ y \end{pmatrix} \;=\; \begin{pmatrix} x_k \\ y_k \end{pmatrix}$$

mit

$$A \;=\; \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \;=\; \begin{pmatrix} 5 & 8 \\ 2 & 3 \end{pmatrix}$$

lösen. Wir erhalten damit

$$\begin{aligned} f(5,3) &= -1, \\ f(7,-4) &= 1, \\ f(19,-11) &= -1, \\ f(45,-26) &= 1, \\ f(109,-63) &= -1, \\ f(263,-152) &= 1. \end{aligned}$$

Literaturverzeichnis

[1] Patterson, S. : *Übungen zur Vorlesung Zahlen und Zahlentheorie.* – Übungszettel zur Vorlesung im Wintersemester 2006 / 2007 von S.J. Patterson, Universität Göttingen

[2] Scholz, D. : *Zahlen und Zahlentheorie.* – Vorlesungsmitschrift im Wintersemester 2006 / 2007 zur Vorlesung von S.J. Patterson, Universität Göttingen

[3] Wikipedia: *Zermelo-Fraenkel-Mengenlehre.* 30. Oktober 2006. – Siehe `http://de.wikipedia.org/wiki/Zermelo-Fraenkel-Mengenlehre`

[4] Wulkau, M. : *Zahlen und Zahlentheorie.* Oktober 2006. – Vorlesungsmitschriften von M. Wulkau im Sommersemester 2005 zur Vorlesung von S.J. Patterson, Universität Göttingen

Stichwortverzeichnis

S

T

V

W

Z