Scriptum
Elementare Zahlentheorie

Prof. W. Hoffmann

1 Vielfache und Teiler

Wir verwenden die Bezeichnungen

$$\mathbb{N} = \{0, 1, 2, 3, \dots\}$$

für die Menge der natürlichen Zahlen und $\mathbb{Z}$ für die Menge der ganzen Zahlen und setzen die Grundaussagen der Arithmetik als bekannt voraus: Die Kommutativität und Assoziativität der Addition und der Multiplikation, das Distributivgesetz und die Rechengesetze für Ungleichungen.

Definition 1 *Eine ganze Zahl b heißt Vielfaches der ganzen Zahl a, wenn es eine ganze Zahl c gibt, so dass $b = ac$. Eine ganze Zahl a heißt Teiler der ganzen Zahl b (abgekürzt $a \mid b$), wenn b ein Vielfaches von a ist. Die Formulierung „b ist durch a teilbar“ bedeutet dasselbe.*

Beispiel. Es seien a, b ganze Zahlen sowie m und n natürliche Zahlen. Ist $m \mid n$, so gilt $a^m - b^m \mid a^n - b^n$. Dies folgt aus der zweiten binomischen Formel

$$x^k - y^k = (x - y)(x^{k-1} + x^{k-2}y + \cdots + xy^{k-2} + y^{k-1})$$

mit $n = km$, wenn wir $x = a^m$ und $y = b^m$ einsetzen.

Satz 1 *Es seien a, b, c und d ganze Zahlen.*

(i) *Ist $a \mid b$ und $c \mid d$, so gilt $ac \mid bd$.*

(ii) *Ist $a \mid b$ und $b \mid c$, so gilt $a \mid c$.*

(iii) *Ist $a \mid b$ und $a \mid c$, so gilt für alle ganzen Zahlen m und n, dass $a \mid mb + nc$.*

(iv) Ist $a \mid b$ und $b \mid a$, so gilt $a = b$ oder $a = -b$.

Beweis. (i) Nach Voraussetzung ist $b = ax$ und $d = cz$ mit ganzen Zahlen x und z. Es folgt $bd = (ax)(cz) = (ac)(xz)$, und xz ist eine ganze Zahl.

(iii) Nach Voraussetzung ist $b = ax$ und $c = ay$ mit ganzen Zahlen x und y. Es folgt $mb + nc = max + nay = a(mx + ny)$, und $mx + ny$ ist eine ganze Zahl.

Für den Beweis der übrigen Aussagen siehe Übungsaufgabe 1. □

Satz 2 (Division mit Rest) *Es seien a und b natürliche Zahlen, $b > 0$. Dann gibt es eindeutig bestimmte natürliche Zahlen q und r, wobei $r < b$, so dass*

$$a = qb + r.$$

Beweis. Zunächst beweisen wir die Existenz des Quotienten q und des Restes r mittels vollständiger Induktion nach a bei festgehaltenem b. Ist $a = 0$, so gilt die Behauptung mit $q = 0$ und $r = 0$. Dies ist der Induktionsanfang.

Im Induktionsschritt können wir annehmen, dass die Aussage bereits gilt, wenn wir a durch eine kleinere Zahl ersetzen. Wir nehmen eine Fallunterscheidung vor. Ist $a < b$, so gilt die Behauptung mit $q = 0$ und $r = a$. Ist hingegen $a \geq b$, so ist auch $a - b$ eine natürliche Zahl, nennen wir sie a_1, und wegen $b > 0$ ist $a_1 < a$. Nach Induktionsvoraussetzung gibt es q_1 und $r_1 < b$, so dass

$$a_1 = q_1 b + r_1.$$

Es folgt

$$a = b + a_1 = b + q_1 b + r_1 = (q_1 + 1)b + r_1,$$

also gilt die Behauptung auch für a mit $q = q_1 + 1$ und $r = r_1$.

Jetzt beweisen wir die Eindeutigkeit. Angenommen, wir haben natürliche Zahlen q, q', $r < b$ und $r' < b$, so dass

$$qbq + r = q'b + r'.$$

Ohne Beschränkung der Allgemeinheit sei $r \leq r'$. Dann ist

$$(q - q')b = r' - r.$$

Die rechte Seite ist eine natürliche Zahl kleiner als b. Also kann $q - q'$ nicht negativ sein. Aber $q - q'$ kann auch nicht positiv sein, da sonst die linke Seite mindestens b wäre. Folglich ist $q = q'$ und somit auch $r = r'$. □

Folgerung 1 *Eine natürliche Zahl a ist genau dann durch eine natürliche Zahl b teilbar, wenn der Rest von a bei Division durch b gleich Null ist. (Erst mit der Eindeutigkeitsaussage von Satz 2 können wir von „dem“ Rest sprechen.)*

Beispiel. Heute ist Dienstag. Welcher Wochentag ist in einer Million Tagen? Wegen $1000000 = 142857 \cdot 7 + 1$ wird Mittwoch sein.

Mit Hilfe der Division mit Rest kann man einen Bruch $\frac{a}{b}$ in eine gemischte Zahl $q + \frac{r}{b}$ umwandeln, z. B. $\frac{29}{9} = 3\frac{2}{9}$. Da $q \leq \frac{a}{b} < q + 1$, kann man umgekehrt mit Hilfe des Taschenrechners den Quotienten bei Division mit Rest bestimmen, also auch den Rest (vorausgesetzt, das Ergebnis wird nicht durch Rundungsfehler verfälscht).

2 Ziffernsysteme

Ziffernsysteme wurden erfunden von den Sumerern (abwechselnde Zehner- und Sechserziffern, also Grundzahl 60), den Indern (Grundzahl 10) und den Maya (Grundzahl 20, aber im Kalender vorletzte Ziffer Achtzehnerziffer). Computer rechnen im System mit der Grundzahl 2. Jede Grundzahl größer als 1 ist möglich:

Grundzahl	*lateinisch*	*grieschisch*
2	binär, dual	dyadisch
3	ternär	triadisch
4	quaternär	tetradisch
5	quinär	pentadisch
6	senär	hexadisch
7	septenär	heptadisch
8	octal	oktadisch
9	nonär	nonadisch
10	dezimal	dekadisch
16	hexadezimal	
20	vigesimal	
60	sexagesimal	
⋮		

Satz 3 *Es sei $g > 1$ eine natürliche Zahl. Unter einer Ziffer zur Grundzahl g verstehen wir eine natürliche Zahl kleiner als g. Zu jeder natürlichen Zahl n gibt es eindeutig bestimmte Ziffern c_0, c_1, ..., von denen nur endlich viele nicht Null sind, so dass*

$$n = c_0 + c_1 g + c_2 g^2 + \dots$$

Beispiel. Um die Zahl 625 ins triadische System umzuwandeln, dividieren wir fortgesetzt durch 3:

$$\begin{aligned} 625 &= 208 \cdot 3 + 1 \\ 208 &= 69 \cdot 3 + 1 \\ 69 &= 23 \cdot 3 + 0 \\ 23 &= 7 \cdot 3 + 2 \\ 7 &= 2 \cdot 3 + 1 \\ 2 &= 0 \cdot 3 + 2 \end{aligned}$$

Setzen wir jeweils eine Zeile in die vorhergehende ein, so erhalten wir

$$\begin{aligned} 625 &= ((((2 \cdot 3 + 1) \cdot 3 + 2) \cdot 3 + 0) \cdot 3 + 1) \cdot 3 + 1 \\ &= 2 \cdot 3^5 + 1 \cdot 3^4 + 2 \cdot 3^3 + 0 \cdot 3^2 + 1 \cdot 3 + 1. \end{aligned}$$

Die Reste ergeben also die triadischen Ziffern. Wie im Dezimalsystem kann man Zahlen einfach durch die Folge ihrer Ziffern notieren, aber wenn Zahlen in verschiedenen Systemen vorkommen, so müssen wir sie kenntlich machen, z. B. durch Anfügen der tiefgestellten Grundzahl:

$$625_{10} = 212011_3$$

Für $g > 10$ braucht man weitere Ziffern. In Programmiersprachen benutzt man beim Hexadezimalsystem z. B. die Ziffern $A = 10$, $B = 12$, …, $F = 15$.

Beweis von Satz 3 durch vollständige Induktion. Die Behauptung gilt für $n = 0$, wobei alle Ziffern gleich Null sein müssen.

Im Induktionsschritt können wir wieder annehmen, dass die Behauptung bereits gilt, wenn wir n durch eine kleinere natürliche Zahl ersetzen. Nach Satz 2 gibt es natürliche Zahlen q und $r < g$, so dass

$$n = qg + r.$$

Wegen $g > 1$ ist $n \geq qg > q$, also gibt es nach Induktionsvoraussetzung Ziffern d_0, d_1, …, von denen nur endlich viele nicht Null sind, so dass

$$q = d_0 + d_1 g + d_2 g^2 + \dots$$

Wir erhalten

$$n = r + (d_0 + d_1 g + d_2 g^2 + \dots)g = r + d_0 g + d_1 g^2 + d_2 g^3 + \dots$$

Also gilt die Behauptung auch für die Zahl n mit den Ziffern

$$c_0 = r, \quad c_1 = d_0, \quad c_2 = d_1, \quad c_3 = d_2, \dots$$

Zum Beweis der Eindeutigkeit betrachten wir eine Zifferndarstellung

$$n = c'_0 + c'_1 g + c'_2 g^2 + \dots$$

und setzen

$$q' = c'_1 + c'_2 g + \dots$$

Dann gilt $n = qg + c'_0$, und nach der Eindeutigkeitsaussage von Satz 2 ist $c'_0 = c_0$ und $q' = q$. Nach Induktionsvoraussetzung sind die Ziffern von q eindeutig bestimmt, also auch die Ziffern c_1, c_2, ... von n. □

Um im g-adischen System rechnen zu können, braucht man eine Additions- und eine Multiplikationstabelle (letztere auch kleines Einmaleins genannt). Wir wollen das am Beispiel des triadischen Systems erläutern. Wegen

$$1 + 2 = 3_{10} = 10_3, \quad 2 + 2 = 2 \cdot 2 = 4_{10} = 11_3$$

sehen diese Tabellen folgendermaßen aus, wobei wir die Zeilen und Spalten für die Ziffer 0 getrost weglassen können:

+	1	2
1	2	10
2	10	11

·	1	2
1	1	2
2	2	11

Wir haben uns hier erspart, jede triadische Zahl durch eine tiefgestellte 3 zu kennzeichnen. Nun kann man im triadischen System schriftlich addieren und multiplizieren, wie in der Schule gelernt:

$$\begin{array}{r} 212011 \cdot 122 \\ \hline 212011 \\ 1201022 \\ \quad 1201022 \\ \hline 112120112 \end{array}$$

Wir erhalten also

$$212011_3 \cdot 122_3 = 112120112_3.$$

Durch Rückverwandlung ins Dezimalsystem kann man die Probe machen:

$$625 \cdot 17 = 10625.$$

3 Der größte gemeinsame Teiler

Es ist klar, dass für ganze Zahlen a und b gilt: $a \mid b$ genau dann, wenn $-a \mid b$ genau dann, wenn $a \mid -b$. Darum kann man sich oft auf natürliche Zahlen beschränken. Da ein Teiler einer Zahl nicht größer sein kann (dem Betrage nach) als die Zahl selbst, hat jede Zahl nur endlich viele Teiler.

Die positiven Teiler einer nicht zu großen natürlichen Zahl kann man finden, indem man alle kleineren Zahlen durchprobiert. So hat z. B. 12 die Teiler 1, 2, 3, 4, 6 und 12, und die Zahl 20 hat die Teiler 1, 2, 4, 5, 10, 20. Die gemeinsamen Teiler von 12 und 20 sind 1, 2 und 4. Haben zwei Zahlen den einzigen (positiven) gemeinsamen Teiler 1, so heißen sie teilerfremd.

Für viele Fragen ist es wichtig, den größten gemeinsamen Teiler zweier natürlicher Zahlen a und b, abgekürzt $\mathrm{ggT}(a, b)$, zu kennen (z. B. zur Ermittlung des kleinsten gemeinsamen Nenners zweier Brüche). Wie findet man ihn möglichst effektiv? Es ist klar, dass $\mathrm{ggT}(a, a) = \mathrm{ggT}(a, 0) = a$.

Wir brauchen also nur den Fall $a > b > 0$ zu behandeln. Aus Satz 1(iii) wissen wir, dass jeder geminsame Teiler von a und b auch ein Teiler der natürlichen Zahl $c = a - b$ ist. Ebenso ist jeder gemeinsame Teiler von b und c auch ein Teiler von $b + c = a$. Es folgt, dass jeder gemeinsame Teiler von a und b ein gemeinsamer Teiler von b und c ist und umgekehrt, also $\mathrm{ggT}(a, b) = \mathrm{ggT}(b, c)$. Wir haben das Problem auf ein leichteres zurückgeführt, denn $\max(b, c) < \max(a, b)$. Wenn wir so fortfahren, kommen wir irgendwann zu einem Paar, bei dem eine Zahl gleich Null ist, und dann sind wir fertig.

Die eben beschriebene Mothode heißt Euklidischer Algorithmus. Beispiel:

$$\begin{aligned}\mathrm{ggT}(247, 91) &= \mathrm{ggT}(156, 91) = \mathrm{ggT}(91, 65) = \mathrm{ggT}(65, 26)\\ &= \mathrm{ggT}(39, 26) = \mathrm{ggT}(26, 13) = \mathrm{ggT}(13, 13) = 13.\end{aligned}$$

Zur Beschleunigung subtrahieren wir in einem Schritt die kleinere von der größeren Zahl so oft wie möglich, d. h. wir teilen mit Rest:

$$\begin{aligned}247 &= 2 \cdot 91 + 65\\ 91 &= 1 \cdot 65 + 26\\ 65 &= 2 \cdot 26 + 13\\ 26 &= 2 \cdot \underline{13}\end{aligned}$$

Haben wir $d = \mathrm{ggT}(a, b)$ mit dem Euklidischen Algorithmus berechnet, so können wir eine ganzzahlige Lösung der Gleichung

$$ax + by = d$$

finden. In unserem Beispiel:

$$\begin{aligned} 13 &= 65 - 2 \cdot 26 \\ &= 65 - 2(91 - 65) = 3 \cdot 65 - 2 \cdot 91 \\ &= 3(247 - 2 \cdot 91) - 2 \cdot 91 = 3 \cdot 247 - 8 \cdot 91 \end{aligned}$$

Die Gleichung $247x + 91y = 13$ hat also u. a. die Lösung $x = 3$, $y = -8$.

Weiteres Beispiel: Finde $\mathrm{ggT}(111, 77)$.

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

Es folgt $\mathrm{ggT}(111, 77) = 1$, d. h. 111 und 77 sind teilerfremd.

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

Die Gleichung $111x + 77y = 1$ hat also u. a. die Lösung $x = 34$, $y = -49$.

Satz 4 *Ist d der größte gemeinsame Teiler der natürlichen Zahlen $a_1, \ldots, a_n$, die nicht alle gleich Null sind, so gibt es ganze Zahlen $x_1, \ldots, x_n$, so dass*

$$d = a_1 x_1 + \cdots + a_n x_n.$$

Ist d' ein gemeinsamer Teiler von $a_1, \ldots, a_n$, so ist d' ein Teiler von d.

Beweis. Es sei I die Menge aller Zahlen der Form $a_1 x_1 + \cdots + a_n x_n$ mit irgendwelchen $x_1 \in \mathbb{Z}, \ldots, x_n \in \mathbb{Z}$. Dann gilt für beliebige a, $b \in I$ und x, $y \in \mathbb{Z}$, dass $ax + by \in I$. (Eine Teilmenge von $\mathbb{Z}$ mit dieser Eigenschaft heißt Ideal.) Ist d' ein gemeinsamer Teiler von $a_1, \ldots, a_n$, so teilt d' nach Satz 1(iii) jedes Element von I.

Nach Voraussetzung hat I positive Elemente. Wir bezeichnen das kleinste positive Element von I mit d. Für jedes i gibt es nach Satz 2 natürliche Zahlen q_i und $r_i < d$, so dass

$$a_i = q_i d + r_i.$$

Wegen $a_i \in I$ und $d \in I$ ist $r_i = a_i - q_i d \in I$. Wäre $r_i > 0$, so würde das der Minimalität von d widersprechen, also muss $r_i = 0$ und $d \mid a_i$ sein.

Wir sehen, dass d ein gemeinsamer Teiler von $a_1, \ldots, a_n$ ist. Da d von jedem anderen gemeinsamen Teiler d' geteilt wird, ist $d = \mathrm{ggT}(a_1, \ldots, a_n)$. □

Nebenbei haben wir bewiesen, dass jedes Ideal I in $\mathbb{Z}$ von der Form

$$d\mathbb{Z} = \{dm \mid m \in \mathbb{Z}\}$$

ist, also genau aus den Vielfachen einer Zahl d besteht. Unser konkretes Ideal

$$I = a_1\mathbb{Z} + \cdots + a_n\mathbb{Z}$$

ist das kleinste Ideal, das die Zahlen $a_1, \ldots, a_n$ enthält.

Man sollte den Euklidischen Algorithmus nicht mit dem Algorithmus zur Bestimmung der g-adischen Ziffern einer Zahl verwechseln. Bei letzterem wird immer der Quotient des vorigen Schrittes durch dieselbe Grundzahl g geteilt, beim Euklidischen Algorithmus hingegen wird der Quotient des vorigen Schrittes durch den Rest des vorigen Schrittes geteilt.

Satz 5 *Es seien a und b ganze Zahlen, nicht beide gleich Null.*

(i) Für jedes $n \in \mathbb{N}$ gilt $\mathrm{ggT}(na, nb) = n \cdot \mathrm{ggT}(a, b)$.

(ii) Die Zahlen a und b sind genau dann teilerfremd, wenn es ganze Zahlen x und y gibt, so dass $ax + by = 1$.

(iii) Sind a und b teilerfremd und gilt $a \mid bc$, so gilt $a \mid c$.

(iv) Sind a und b teilerfremd und gilt $a \mid c$ und $b \mid c$, so gilt $ab \mid c$.

Beweis. (i) Ist eine natürliche Zahl c gemeinsamer Teiler von a und b, so ist nach Satz 1(i) die Zahl nc gemeinsamer Teiler von na und nb. Nach Aufgabe 1(c) gilt auch die Umkehrung. Hieraus folgt die Behauptung.

(ii) Sind a und b teilerfremd, so ist $\mathrm{ggT}(a, b) = 1$, und nach Satz 4 existieren die behaupteten Zahlen x und y (die man mit Hilfe des Euklidischen Algorithmus finden kann). Umgekehrt gelte $ax + by = 1$ für ganze Zahlen x und y. Ist nun $c \in \mathbb{N}$ ein gemeinsamer Teiler von a und b, so ist nach Satz 1(iii) c auch Teiler von $ax + by$, also von 1. Daraus folgt $c = 1$.

(iii) Nach (ii) gibt es x, $y \in \mathbb{Z}$, so dass $ax + by = 1$. Multiplizieren wir mit c, so erhalten wir

$$a(cx) + (bc)y = c.$$

Wegen $a \mid bc$ folgt aus Satz 1(iii), dass $a \mid c$.

(iv) Nach Voraussetzung gibt es d, $e \in \mathbb{Z}$, so dass $c = ad = be$. Multiplizieren wir wieder die Gleichung $ax + by = 1$ mit c, so erhalten wir

$$c = acx + bcy = a(be)x + b(ad)y = ab(ex + dy).$$

Daraus folgt $ab \mid c$. □

Sind a und b positive natürliche Zahlen, so gibt es positive gemeinsame Vielfache (z. B. ab), und unter diesen gibt es ein kleinstes, abgekürzt $\mathrm{kgV}(a, b)$.

Satz 6 *Es gilt*

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

Jedes gemeinsame Vielfache ist ein Vielfaches des kleinsten gemeinsamen Vielfachen.

Beweis. Bezeichnen wir $\mathrm{ggT}(a, b)$ mit d, so gibt es x, $y \in \mathbb{N}$ mit $a = dx$ und $b = dy$. Natürlich ist die Zahl

$$\frac{ab}{d} = ay = bx$$

ein gemeinsames Vielfaches von a und b. Nach Satz 5(i) ist

$$d = \mathrm{ggT}(a, b) = d\,\mathrm{ggT}(x, y),$$

also sind x und y teilerfremd.

Ist nun z irgendein gemeinsames Vielfaches von a und b, so gibt es e und f, so dass $z = ae = bf$. Daraus folgt $(dx)e = (dy)f$, also $xe = yf$. Nach Satz 5(iii) folgt $y \mid e$, also gibt es ein h, so dass $e = hy$ und somit

$$z = a(hy) = \frac{ab}{d}\,h.$$

Somit ist z ein Vielfaches von $\frac{ab}{d}$. Jedes gemeinsame Vielfache ist also ein Vielfaches von $\frac{ab}{d}$ und ist insbesondere nicht kleiner als dieses gemeinsame Vielfache. □

Eine lineare Diophantische Gleichung in zwei Variablen x, y ist eine Gleichung der Form

$$ax + by = c \tag{1}$$

wobei ganze Zahlen a, b und c gegeben sind. Wir diskutieren hier nur den interessanten Fall, wenn $a \neq 0$ und $b \neq 0$. Es sei d der größte gemeinsame

Teiler von a und b. Man kann ihn mit Hilfe des Euklidischen Algorithmus ebenso bestimmen wie zwei ganze Zahlen x' und y', so dass

$$ax' + by' = d.$$

Wegen $d \mid a$ und $d \mid b$ gibt es e, $f \in \mathbb{Z}$, so dass $a = de$ und $b = df$, und die Gleichung (1) wird zu

$$d(ex + fy) = c.$$

Es kann natürlich nur dann eine Lösung geben, wenn d ein Teiler von c ist. Angenommen, diese Bedingung ist erfüllt, d. h. $c = nd$. Dann ist offenbar $x_0 = nx'$, $y_0 = ny'$ eine Lösung, aber wie findet man alle Lösungen? Die Gleichung (1) ist äquivalent zu

$$ex + fy = n,$$

und nach Satz 5(i) sind e und f teilerfremd. Ist x, y eine weitere Lösung, so gilt

$$ex + fy = ex_0 + fy_0, \qquad \text{also} \qquad e(x - x_0) = f(y_0 - y).$$

Mit Satz 5(iii) folgern wir, dass $f \mid x - x_0$, also $x - x_0 = kf$ mit $k \in \mathbb{Z}$. Setzen wir dies ein und dividieren durch f, so erhalten wir $ke = y_0 - y$. Zusammenfassend erhalten wir, dass jede Lösung der Gleichung (1) von der Form

$$x = x_0 + kf, \qquad y = y_0 - ke$$

für ein $k \in \mathbb{Z}$ ist, und man prüft leicht nach, dass alle solchen Zahlenpaare tatsächlich Lösungen sind.

4 Primzahlen

Definition 2 *Eine natürliche Zahl n heißt zusammengesetzte Zahl, wenn sie sich als Produkt $n = ab$ schreiben lässt, wobei $a \neq 1$ und $b \neq 1$. Eine natürliche Zahl p heißt Primzahl, wenn sie keine zusammengesetzte Zahl und nicht gleich 1 ist.*

Satz 7 *Jede natürliche Zahl größer als 1 lässt sich als Produkt von Primzahlen schreiben.*

Den Beweis kann man leicht mit Hilfe der vollständigen Induktion führen, denn für $n = ab$ mit $a \neq 1$ und $b \neq 1$ ist $a < n$ und $b < n$, so dass man die Induktionsbehauptung auf a und b anwenden kann. Wir können auch die Zahl 1 einschließen, wenn wir ein Produkt aus Null Faktoren zulassen.

Satz 8 *Es gibt unendlich viele Primzahlen.*

Beweis. Angenommen, $p_1, \ldots, p_k$ wären alle Primzahlen. Dann lässt die Zahl

$$N = p_1 p_2 \ldots p_k + 1$$

bei Division durch jede Primzahl den Rest 1, hat also keine Primteiler. Andererseits ist $N \neq 1$ (Widerspruch zu Satz 7). □

Eine natürliche Zahl $p > 1$ ist genau dann Primzahl, wenn ihre einzigen Teiler 1 und p sind. Man kann die Primzahlen aus der Menge $\{2, 3, 4, \ldots, n\}$ durch das Sieb des Erathosthenes aussondern.

Ist p eine Primzahl, so ist eine natürliche Zahl a genau dann zu p teilerfremd, wenn sie kein Vielfaches von p ist. Also erhalten wir:

Folgerung 2 (aus Satz 5(iii)) *Ist p eine Primzahl und $p \mid ab$, so gilt $p \mid a$ oder $p \mid b$.*

Dies lässt sich mittels vollständiger Induktion auf mehr als zwei Faktoren verallgemeinern.

Satz 9 *Die Primfaktorzerlegung einer positiven natürlichen Zahl ist eindeutig bis auf die Reihenfolge der Faktoren.*

Beweis durch vollständige Induktion. Für $n = 1$ gilt die Behauptung. Nun sei eine natürliche Zahl $n > 1$ gegeben, und die Behauptung gelte bereits für alle kleineren Zahlen. Angenommen, wir haben zwei Primfaktorzerlegungen

$$n = p_1 \ldots p_k = q_1 \ldots q_l,$$

Wegen $n > 1$ ist $k > 0$ und $l > 0$. Nun ist p_k ein Teiler des Produktes auf der rechten Seite, und wegen Folgerung 2 gibt es einen Index j, so dass $p_k \mid q_j$ und folglich, da beide Primzahlen sind, $p_k = q_j$. Wenn wir durch diese Zahl teilen, erhalten wir

$$p_1 \ldots p_{k-1} = q_1 \ldots \not{q}_j \ldots q_l.$$

Dies sind Primfaktorzerlegungen der Zahl n/p_k, die kleiner als n ist. Nach der Induktionsvoraussetzung stehen hier auf beiden Seiten dieselben Primfaktoren, möglicherweise in verschidener Reihenfolge. Insbesondere ist $k-1 = l-1$, also $k = l$. □

Wir können die Primfaktoren nach der Größe ordnen und gleiche Faktoren zusammenfassen:

$$n = 2^{e_2} 3^{e_3} 5^{e_5} \ldots$$

Natürlich sind nur endlich viele Exponenten nicht Null, und n ist durch die Gesamtheit der Exponenten bestimmt. Nach dem Satz sind umgekehrt die Exponenten eindeutig durch n bestimmt, wir können also $e_p = e_p(n)$ schreiben.

Satz 10 *Es seien a, b und c natürliche Zahlen.*

(i) Es gilt $b = ac$ genau dann, wenn $e_p(b) = e_p(a) + e_p(c)$ für alle p.

(ii) Es gilt $a \mid b$ genau dann, wenn $e_p(a) \leq e_p(b)$ für alle p.

(iii) Es gilt $d = \mathrm{ggT}(a, b)$ genau dann, wenn $e_p(d) = \min(e_p(a), e_p(b))$ für alle p.

(iv) Es gilt $m = \mathrm{kgV}(a, b)$ genau dann, wenn $e_p(m) = \max(e_p(a), e_p(b))$ für alle p.

Beweis. (i) Mit den Potenzgesetzen erhält man

$$ac = 2^{e_2(a)+e_2(c)} 3^{e_3(a)+e_3(c)} 5^{e_5(a)+e_5(c)} \dots$$

Aus der Eindeutigkeit der Exponenten folgt die Behauptung.

(ii) Ist $b = ac$, so folgt die Ungleichung aus (i) wegen $e_p(c) \geq 0$. Ist umgekehrt $e_p(a) \leq e_p(b)$ für alle p, so ist

$$c = 2^{e_2(b)-e_2(a)} 3^{e_3(b)-e_3(b)} 5^{e_5(b)-e_5(b)} \dots$$

eine natürliche Zahl, und $b = ac$.

(iii) Nach Satz 4 gilt $d = \mathrm{ggT}(a, b)$ genau dann, wenn d gemeinsamer Teiler von a und b ist und wenn jeder gemeinsame Teiler von a und b ein Teiler von d ist. Die Eigenschaft, gemeinsamer Teiler zu sein, können wir mit Hilfe von Teil (ii) umformulieren: d' ist ein gemeinsamer Teiler von a und b genau dann, wenn $e_p(d') \leq \min(e_p(a), e_p(b))$ für alle p. Die Zahl d mit den Exponenten $e_p(d) = \min(e_p(a), e_p(b))$ für alle p hat also die Eigenschaft, die den größten gemeinsamen Teiler charakterisiert.

(iv) siehe Aufgabe 13. □

Die alten Griechen nannten eine natürliche Zahl vollkommen, wenn sie gleich der Summe ihrer echten Teiler ist, wie z. B. $6 = 1 + 2 + 3$. Dies ist gleichbedeutend damit, dass die Summe aller Teiler gleich dem Doppelten der Zahl ist. Wie findet man vollkommene Zahlen?

Schon bei Euklid wird bewiesen: Ist $p = 2^q - 1$ eine Primzahl, so ist $n = 2^{q-1}p$ eine vollkommene Zahl. Die Teiler von n sind nämlich

$$1, 2, 4, \dots, 2^{q-1},$$
$$p, 2p, 4p, \dots, 2^{q-1}p,$$

und ihre Summe ist nach der Formel aus Beispiel 1

$$(p+1)(1 + 2 + 4 + \cdots + 2^{q-1}) = (p+1)\,\frac{2^q - 1}{2 - 1} = 2^q p = 2n.$$

Es gilt zumindest eine partielle Umkehrung dieser Aussage.

Satz 11 (Euler) *Jede gerade vollkomme Zahl ist von der Form $2^{q-1}p$, wobei $p = 2^q - 1$ eine Primzahl ist.*

Beweis. Es sei $q-1$ der Exponent von 2 in der Primfaktorzerlegung von n, so dass $n = 2^{q-1}p$ mit einer ungeraden Zahl p gilt. Wir müssen zeigen, dass p eine Primzahl und gleich $2^q - 1$ ist.

Für jeden Teiler d von p sind die Zahlen d, $2d$, $4d$, $\ldots$, $2^{q-1}d$ Teiler von n, und jeder Teiler von n entsteht auf diese Weise genau ein Mal. Bezeichnen wir die Summe der Teiler von p mit s, so ist die Summe der Teiler von n gleich

$$s(1 + 2 + 4 + \cdots + 2^{q-1}) = s(2^q - 1).$$

Da n vollkommen ist, gilt

$$s(2^q - 1) = 2n = 2^q p.$$

Die Zahlen 2^q und $2^q - 1$ sind teilerfremd, und aus Satz 5(iii) folgt, dass $2^q \mid s$ und $2^q - 1 \mid p$. Es gibt also eine natürliche Zahl m, so dass

$$p = m(2^q - 1), \qquad s = m2^q = p + m.$$

Da n gerade ist, gilt $q \geq 2$, also $2^q - 1 \neq 1$. Wäre $m \neq 1$, so wären 1, m und p verschiedene Teiler von p, so dass $s \geq 1 + m + p$ (Widerspruch). Folglich ist $m = 1$, $p = 2^q - 1$, und $s = p + 1$, so dass p keine weiteren Teiler außer p und 1 haben kann. □

Der Mönch Mersenne suchte nach Primzahlen Form $p = 2^q - 1$, die seither Mersennesche Primzahlen genannt werden. Es ist nicht bekannt, ob es unendlich viele davon gibt. Aus Beispiel 1 folgt, dass auch q eine Primzahl sein muss. Aber nicht für jede Primzahl q ist p prim, z. B. ist $2^{11} - 1 = 23 \cdot 89$. Die größte derzeit bekannte Primzahl ist übrigens die Mersennesche Primzahl $2^{32582657} - 1$, siehe The Prime Pages.

q	2	3	5	7	13
p	3	7	31	127	8191
n	6	28	496	8128	33550336

Bisher sind keine ungeraden vollkommenen Zahlen bekannt. Jedenfalls gibt es keine mit weniger als 200 Dezimalstellen.

5 Pythagoräische Tripel

Nach dem Satz des Pythagoras und seiner Umkehrung sind drei Zahlen a, b und c genau dann die Seitenlängen eines rechtwinkligen Dreiecks (mit c als

Länge der Hypothenuse), wenn sie die Gleichung

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

erfüllen. Dabei halten wir eine Längeneinheit fest, so dass Längen durch Zahlen gegeben sind. Schon im Altertum fragte man sich, wie man rechtwinklige Dreiecke mit ganzzahligen Seitenlängen finden kann. Eine Lösung (a, b, c) der Diophantischen Gleichung (2) in natürlichen Zahlen heißt Pythagoräisches Zahlentripel, wie z. B. das Tripel $(3, 4, 5)$. Kennt man diese, so kennt man alle ganzzahligen Lösungen, denn für jede Lösung (a, b, c) sind auch $(\pm a, \pm b, \pm c)$ Lösungen. Den trivialen Fall, wenn $a = 0$ oder $b = 0$, brauchen wir nicht weiter zu betrachten.

Haben wir ein Pythagoräisches Tripel (a, b, c) gefunden, so erhalten wir unendlich viele weitere in der Form (da, db, dc) mit $d \in \mathbb{N}$. Ein Tripel (a, b, c) ganzer Zahlen heiße primitiv, wenn die Zahlen a, b und c teilerfremd sind, d. h. $\mathrm{ggT}(a, b, c) = 1$. Es ist klar, dass man jedes Pythagoräische Zahlentripel als Vielfaches eines primitiven Pythagoräischen Zahlentripels erhält, und zwar auf genau eine Weise.

Um primitive Pythagoräische Tripel zu finden, untersuchen wir zunächst ihre Eigenschaften. Von den drei Zahlen a, b und c muss mindestens eine ungerade sein. Ist es möglich, dass nur eine ungerade ist? Es gelten folgende Regeln, wobei g für gerade und u für ungerade steht:

+	g	u
g	g	u
u	u	g

·	g	u
g	g	g
u	g	u

Von den drei Zahlen a^2, b^2 und c^2 kann nach diesen Regeln nicht nur eine ungerade sein. Nach den Regeln ist außerdem eine Zahl genau dann gerade, wenn ihr Quadrat gerade ist. Es folgt, dass von den drei Zahlen eines primitiven Pythagoräischen Tripels zwei ungerade sind und eine gerade ist. Wäre c die gerade Zahl, so wäre c^2 durch 4 teilbar, aber mit $a = 2r + 1$ und $b = 2s + 1$ erhalten wir $a^2 + b^2 = 4(r^2 + r + s^2 + s) + 2$ (Widerspruch). Somit muss eine der Zahlen a oder b gerade sein, sagen wir b, und dann sind a und c ungerade.

Die entscheidende Idee der alten Griechen bestand darin, in Gleichung (2) den Term a^2 auf die rechte Seite zu bringen und sie dann in der Form

$$b^2 = (c + a)(c - a)$$

zu schreiben. Es folgt

$$b = 2j, \qquad c + a = 2k, \qquad c - a = 2l$$

mit natürlichen Zahlen j, k und l, die die Gleichung

$$j^2 = kl$$

erfüllen und teilerfremd sind:

$$\begin{gathered}\mathrm{ggT}(j,k,l) = \mathrm{ggT}(j,k+l,l) = \mathrm{ggT}(j,c,l),\\ \mathrm{ggT}(j,k,l) \mid \mathrm{ggT}(2j,c,2l) = \mathrm{ggT}(b,c,c-a) = \mathrm{ggT}(b,c,a) = 1.\end{gathered}$$

Man kann a, b und c aus j, k und l zurückgewinnen:

$$b = 2j, \qquad c = k + l, \qquad a = k - l.$$

Ist umgekehrt $j^2 = kl$, so rechnet man leicht nach, dass (a, b, c) eine Lösung der Gleichung (2) ist.

Nach Aufgabe 14(b) sind k und l Quadratzahlen, also $k = m^2$, $l = n^2$ und $j = mn$ für natürliche Zahlen m, n, wobei natürlich m und n teilerfremd sind. Wir haben beweisen:

Satz 12 *Jedes primitive Pythagoräische Tripel (a, b, c) mit geradem b ist von der Form*

$$a = m^2 - n^2, \qquad b = 2mn, \qquad c = m^2 + n^2$$

mit teilerfremden natürlichen Zahlen m und n.

Ist nicht b, sondern a gerade, so vertauscht man die Rollen von a und b. Wenn m und n gemeinsame Teiler haben, so erhält man natürlich auch Pythagoräische Tripel, nur eben keine primitiven.

Es gibt noch einen moderneren Lösungsweg. Dazu teilen wir beide Seiten der Gleichung (2) durch c und schreiben $x = \frac{a}{c}$, $y = \frac{b}{c}$:

$$x^2 + y^2 = 1.$$

Wir suchen jetzt also nach Lösungen (x, y) dieser Gleichung in rationalen Zahlen, also nach Punkten (x, y) auf dem Einheitskreis mit rationalen Koordinaten. Wählen wir irgendein y und lösen die Gleichung nach x, so erhalten wir nach der Lösungsformel für quadratische Gleichungen im Allgemeinen keine rationalen Zahlen. Auch wenn wir die Schnittpunkte einer Geraden mit dem Einheitskreis suchen, wenn wir also eine Geradengleichung

$$y = tx + u$$

für y einsetzen, so erhalten wir wieder eine quadratische Gleichung. Haben die Schnittpunkte der Geraden mit dem Kreis rationale Koordinaten, so müssen

t und u rational sein, aber das ist nicht genug, da auch für rationale t und u irrationale Lösungen für x auftreten können. Wenn wir aber wissen, dass eine der beiden Lösungen rational ist, so muss auch die andere rational sein.

Wir wählen also beliebige Sekanten durch einen festen Punkt des Einheitskreises, sagen wir $(-1, 0)$; deren Gleichung ist

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

Setzen wir dies ein, so erhalten wir

$$x^2 + t^2(x^2 + 2x + 1) = 1.$$

Bringen wir alle Terme auf die linke Seite, so können wir $x+1$ ausklammern:

$$(x + 1)\big((t^2 + 1)x + t^2 - 1\big) = 0.$$

Eine Lösung ist offensichtlich $x = -1$, für die andere können wir durch $x+1$ teilen:

$$(1 + t^2)x = 1 - t^2.$$

Lösen wir nach x auf und setzen das Ergebnis in die Geradengleichung ein, so erhalten wir

$$x = \frac{1 - t^2}{1 + t^2}, \qquad y = \frac{2t}{1 + t^2}.$$

Lassen wir t alle rationalen Zahlen durchlaufen, so erhalten wir alle Lösungen außer $(-1, 0)$. (Man nennt dies eine rationale Parametrisierung des Einheitskreises.) Schreiben wir $t = \frac{n}{m}$ mit teilerfremden ganzen Zahlen m und n, so können wir mit m^2 erweitern:

$$x = \frac{m^2 - n^2}{m^2 + n^2}, \qquad y = \frac{2mn}{m^2 + n^2}.$$

Erinnern wir uns, dass $x = \frac{a}{c}$ und $y = \frac{b}{c}$, so erhalten wir von Neuem die Behauptung von Satz 12. Mit dieser Methode kann man Diophantische Gleichungen der Form $F(a, b, c) = 0$ behandeln, wobei F eine beliebige quadratische Form ist, z. B. $F(a, b, c) = 3a^2 + 2ab - ac + b^2 + 5ac + 4c^2$.

6 Zahlenkongruenzen

Die Rechenregeln für gerade und ungerade Zahlen waren recht nützlich. Betrachten wir aber die Teilbarkeit durch 3, so gibt es keine genauso einfache Regel für die Addition oder Multiplikation zweier nicht durch drei teilbarer Zahlen: 2+4 ist durch 3 teilbar, 1+4 aber nicht. Statt nur auf die Teilbarkeit

durch 3 zu schauen, muss man darauf achten, welchen Rest eine Zahl bei Division durch 3 lässt. Eine ähnliche Idee kam in der ersten Vorlesung vor: Zwei Kalendertage fallen auf denselben Wochentag, wenn die Differenz ihrer Nummern (in fortlaufender Zählung) ein Vielfaches von 7 ist.

Definition 3 *Es sei m eine positive natürliche Zahl. Zwei ganze Zahlen a und b heißen kongruent modulo m, wenn $m \mid a-b$. Zur Abkürzung schreiben wir dafür $a \equiv b \pmod{m}$.*

Diese Schreibweise ist natürlich nicht kürzer als $m \mid a-b$, aber intuitiver. So ist z. B. $a \equiv b \pmod{m}$ gleichbedeutend mit $b \equiv a \pmod{m}$. Aus den Aussagen $a \equiv b \pmod{m}$ und $b \equiv c \pmod{m}$ folgt $a \equiv c \pmod{m}$. Darum ist es sinnvoll, ähnlich wie bei Gleichungen fortlaufende Kongruenzen zu schreiben: $a \equiv b \equiv c \pmod{m}$.

Die auf Gauß zurückgehende lateinische Phrase „kongruent modulo m“ bedeutet „zusammenpassend bezüglich der Einheit m“. Sind die natürlichen Zahlen a und b kongruent modulo m, so lassen sie denselben Rest bei Division durch m.

Satz 13 *Es sei m eine positive natürliche Zahl. Dann gilt für alle ganzen Zahlen a, b und c:*

(i) Ist $a \equiv c$ und $b \equiv d \pmod{m}$, so ist $a+b \equiv c+d \pmod{m}$.

(ii) Ist $a \equiv c$ und $b \equiv d \pmod{m}$, so ist $a \cdot b \equiv c \cdot d \pmod{m}$.

Beweis. Die erste Aussage folgt mit Hilfe von Satz 1(iii) aus

$$(a+b)-(c+d) = (a-c)+(b-d),$$

die zweite aus

$$ab - cd = (a-c)b + c(b-d). \qquad \square$$

Beispiel. Welchen Rest lässt 7^{999} bei Division durch 15?

$$7^2 = 49 \equiv 4 \pmod{15}, \qquad 7^4 = (7^2)^2 \equiv 4^2 \equiv 1 \pmod{15},$$
$$7^{999} = 7^{4\cdot 249+3} = (7^4)^{249}7^3 \equiv 7^2 \cdot 7 \equiv 13 \pmod{15}.$$

Die Antwort ist 13.

Satz 2′ *Ist m eine positive natürliche Zahl und a eine ganze Zahl, so gibt es eindeutig bestimmte ganze Zahlen q und r, so dass $0 \le r < m$ und*

$$a = qm + r.$$

Beweis. Den Fall $a \geq 0$ haben wir bereits in Satz 2 erledigt. Sei also $a < 0$. Wenden wir Satz 2 auf die positive Zahl $-a$ an, so erhalten wir natürliche Zahlen q_1 und $r_1 < m$, so dass

$$-a = q_1 m + r_1, \qquad \text{also} \qquad a = -q_1 m - r_1.$$

Ist $r_1 = 0$, so können wir $q = -q_1$ und $r = 0$ setzen und sind fertig. Andernfalls schreiben wir

$$a = (-q_1 - 1)m + (m - r_1),$$

und wenn wir $q = -q_1 - 1$ und $r = m - r_1$ setzen, so ist $0 < r < m$. Die Eindeutigkeit beweist man wie in Satz 2. □

Wir werden die Zahl r als den Rest bei der Division von a durch m bezeichnen. Mit dieser Festlegung sind zwei ganze Zahlen (ganz gleich welchen Vorzeichens) genau dann kongruent modulo m, wenn sie bei Division durch m den gleichen Rest lassen.

Beispiel. Mit Hilfe von Zahlenkongruenzen kann man leicht die bekannten Teilbarkeitsregeln beweisen. Ist z. B. die Dezimaldarstellung

$$n = c_0 + c_1 \cdot 10 + c_2 \cdot 10^2 + \dots$$

einer natürlichen Zahl gegeben, so folgt aus der Tatsache $10 \equiv 1 \pmod 9$, dass

$$n \equiv c_0 + c_1 \cdot 1 + c_2 \cdot 1^2 + \dots \equiv c_0 + c_1 + c_2 + \dots \pmod 9,$$

d. h. eine Zahl lässt bei Division durch 9 denselben Rest wie ihre Quersumme. Analog kann man zeigen, dass die Zahl n bei Division durch 11 denselben Rest lässt wie ihre alternierende Quersumme $c_0 - c_1 + c_2 - c_3 + - \dots$ Dies ist die Grundlage für die Neunerprobe und die Elferprobe.

Aus der Eigenschaft $4 \mid 10^2$ folgt

$$n \equiv c_0 + c_1 \cdot 10 \pmod 4,$$

d. h. eine Zahl lässt bei Division durch 4 denselben Rest wie die aus Zehner- und Einerstelle gebildete Zahl.

Die Menge $\mathbb{Z}$ der ganzen Zahlen zerfällt in zwei Klassen, nämlich die Klasse der geraden und die Klasse der ungeraden Zahlen. Wenn wir eine positive natürliche Zahl m festhalten, so können wir analog die Menge $\mathbb{Z}$ in sogenannte Restklassen modulo m einteilen: Zwei Zahlen gehören zu derselben Klasse, wenn sie kongruent modulo m sind. Es gibt z. B. drei Restklassen modulo 3:

$$\{\dots, -6, -3, 0, 3, 6, \dots\},$$
$$\{\dots, -5, -2, 1, 4, 7, \dots\},$$
$$\{\dots, -7, -4, -1, 2, 5, \dots\}.$$

Ist a irgendein Vertreter einer Restklasse modulo m, so besteht die Restklasse aus allen Zahlen der Form $a+km$ mit $k \in \mathbb{Z}$. Wir bezeichnen diese Restklasse mit $[a]_m$. So ist z. B.

$$[1]_3 = \{\dots, -5, -2, 1, 4, 7, \dots\} = [4]_3 = [-5]_3 \dots$$

Man kann also in jeder Restklasse $[a]_m$ einen Vertreter r mit $0 \leq r < m$ finden, und es gibt genau m Restklassen modulo m, nämlich $[0]_m$, $[1]_m$, $\dots$, $[m-1]_m$.

Wir wollen die Rechenregeln für Restklassen modulo 2 (also gerade und ungerade) verallgemeinern.

Definition 4 *Es sei m eine positive natürliche Zahl. Wir setzen*

$$[a]_m + [b]_m = [a+b]_m, \qquad [a]_m \cdot [b]_m = [a \cdot b]_m.$$

Dies ist korrekt, denn wenn wir andere Zahlen c und d mit $[a]_m = [c]_m$ und $[b]_m = [d]_m$ nehmen, so erhalten wir dieselben Ergebnisse

$$[a+b]_m = [c+d]_m, \qquad [a \cdot b]_m = [c \cdot d]_m$$

nach Satz 6. Für $m = 4$ haben wir z. B. folgende Additions- und Multiplikationstabelle, wobei wir einfach a statt $[a]_4$ schreiben:

$+$	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

Beispiel. Für welche $n > 0$ ist $1 + 4 + 16 + \dots + 4^n$ eine Quadratzahl? Angenommen, diese Zahl ist gleich a^2. Dann gibt es wegen $[a^2]_4 = [a]_4 \cdot [a]_4$ folgende Möglichkeiten:

$[a]_4$	0	1	2	3
$[a^2]_4$	0	1	0	1

(Eigentlich müssten alle Zahlen in den Klammern $[\,.\,]_4$ stehen.) Wir sehen, dass nur $[0]_4$ und $[1]_4$ quadratische Restklassen[1] sind. Dies ergibt keinen Widerspruch zu $1 + 4 + 16 + \dots + 4^n = a^2$. Betrachten wir nun die Restklassen modulo 8. Zur Verringerung des Aufwandes wählen wir andere Vertreter:

$[a]_8$	0	± 1	± 2	± 3	4
$[a^2]_8$	0	1	4	1	0

[1] oder, wie man häufig sagt, quadratische Reste

Dies steht im Widerspruch zu

$$1 + 4 + 16 + \cdots + 4^n \equiv 5 \pmod 8.$$

Die Antwort lautet also: Für kein $n > 0$.

Wir beschäftigen uns nun mit der Lösung linearer Kongruenzen

$$ax \equiv c \pmod m,$$

wobei a und b gegebene ganze Zahlen sind. Die Kongruenz ist nach Definition gleichwertig zu der Aussage

$$m \mid ax - c,$$

und diese bedeutet wiederum, dass es eine ganze Zahl y gibt, so dass

$$-my = ax - c, \qquad \text{d. h.} \qquad ax + my = c.$$

Letzteres ist eine lineare Diophantische Gleichung, und wir wissen bereits, wie man ihre Lösungen findet. Jedenfalls existiert eine Lösung genau dann, wenn $\mathrm{ggT}(a, m) \mid c$.

Beispiel. Am heutigen Dienstag wird der Vorratstank eines Aggregats aufgefüllt, und dies soll alle 30 Tage wiederholt werden. Die wievielten Wiederholungen werden an Sonntagen stattfinden? Bis zum nächsten Sonntag dauert es 5 Tage, also ist die gesuchte Zahl eine Lösung der Kongruenz

$$30x \equiv 5 \pmod 7.$$

Sie führt auf die lineare Gleichung

$$30x + 7y = 5.$$

Der Euklidische Algorithmus liefert $\mathrm{ggT}(30, 7) = 1$ und $1 = 13 \cdot 7 - 3 \cdot 30$. Wir finden also die Lösung $(x, y) = (-15, 65)$, und die allgemeine Lösung ist von der Form $(x, y) = (7k - 15, 65 - 30k)$ mit $k \in \mathbb{Z}$. Da wir uns nur für x interessieren, lautet die Antwort $x \equiv -15 \pmod 7$ oder, was dasselbe ist,

$$x \equiv 6 \pmod 7.$$

Im vorliegenden Fall hätte man die kleinste positive Lösung noch durch Probieren finden können:

$[x]_7$	1	2	3	4	5	6	...
$[30x]_7$	2	4	6	1	3	5	...

Je größer aber die Zahlen, um so ineffektiver wird das Probieren im Vergleich zum Euklidischen Algorithmus.

Man hätte die Kongruenz auch als Gleichung von Restklassen modulo 7 formulieren können:

$$[30]_7 \cdot [x]_7 = [5]_7,$$

und die Lösung lautet

$$[x]_7 = [6]_7.$$

Beispiel. Man finde alle Lösungen der linearen Kongruenz

$$24x \equiv 15 \pmod{27}.$$

Sie führt auf die Gleichung

$$24x + 27y = 15.$$

Wir finden $\mathrm{ggT}(24, 27) = 3$ und $3 = 27 - 24$. Wegen $3 \mid 15$ existiert eine Lösung, nämlich $(x, y) = (-5, 5)$, und die Gleichung vereinfacht sich zu

$$8x + 9y = 5.$$

Die allgemeine Lösung ist $(x, y) = (9k - 5, 5 - 8k)$ mit $k \in \mathbb{Z}$. Die Lösung unserer Kongruenz ist also

$$x \equiv 4 \pmod{9}.$$

Formulieren wir unsere Aufgabe wieder als Gleichung von Restklassen

$$[24]_{27} \cdot [x]_{27} = [15]_{27},$$

so liefert uns obige Antwort $x \in [4]_9$. Dies ist aber keine Restklasse modulo 27, sondern die Vereinigung von drei Restklassen:

$$[4]_9 = [4]_{27} \cup [13]_{27} \cup [22]_{27}.$$

Wenn wir also nach den Restklassen modulo 27 fragen, die unsere Gleichung lösen, so lautet die Antwort

$$[x]_{27} \in \{[4]_{27}, [13]_{27}, [22]_{27}\}.$$

Allgemein gilt für positive Zahlen $n \mid m$, dass jede Restklasse $[a]_n$ eine Vereinigung von Restklassen modulo m ist. Es gilt nämlich

$$[a]_n = \{a + kn \,:\, k \in \mathbb{Z}\},$$

und wenn wir $m = dn$ schreiben, so gibt es nach Satz 2′ für jedes k ganze Zahlen q und r, so dass $0 \leq r < d$ und $k = qd + r$, also

$$[a]_n = \{a + qm + rn \,:\, q,\, r \in \mathbb{Z},\, 0 \leq r < d\}.$$

Nun ist aber

$$\{a + qm + rn \,:\, q \in \mathbb{Z}\} = [a + rn]_m,$$

also

$$= [a]_m \cup [a + n]_m \cup \cdots \cup [a + (d-1)n]_m.$$

Beispiel. Bei seinen Feldzügen soll Cäsar folgendes Verschlüsselungsverfahren angewandt haben. Man halte eine Zahl c fest und verschlüssle einen Buchstaben dadurch, dass man ihn durch denjenigen Buchstaben ersetzt, der im Alphabet c Plätze später kommt. Im Falle von $c = 2$ wird z. B. aus dem Wort CAESAR das Wort ECGVCT. (Im Lateinischen gab es das Schriftzeichen U noch nicht.) Dabei ordnet man die Buchstaben zyklisch an, so dass nach dem letzten Buchstaben X wieder A kommt, ähnlich wie beim Rommé, wo das As nach dem König, aber auch vor der Eins kommt. (Die Buchstaben J, Y und Z sind eigentlich griechische Buchstaben.) Die Entschlüsselung erfolgt einfach durch Verschiebung um c Schritte nach links.

Dieses Verfahren lässt sich rechnerisch beschreiben, wenn man den Buchstaben Zahlen zuordnet, z B.

A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	V	X
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

(Man könnte auch die Zahlen von 1 bis 21 benutzen.) Ist x die Zahl des unverschlüsselten Buchstaben, so ergibt sich die Zahl y des verschlüsselten Buchstaben als $y = x + c$, wenn $x + c \leq 20$, aber als $y = x + c - 21$, wenn $x + c \geq 21$. Übersichtlicher wird es, wenn man den Buchstaben nicht Zahlen, sondern Restklassen modulo 21 zuordnet; dann ergibt sich die Restklasse $[y]_{21}$ des verschlüsselten Buchstaben aus

$$y \equiv x + c \pmod{21}.$$

Ein weniger leicht zu knackender Code entsteht aus der Vorschrift

$$y \equiv ax + c \pmod{21}, \tag{3}$$

wobei wir a und c geeignet festlegen. Die Wahl von c ist beliebig, sie bedeutet nur, dass wir nach Multiplikation mit a noch eine Cäsar-Verschiebung als zweiten Verschlüsselungsschritt vornehmen. Nehmen wir z. B. $c = 5$. Hingegen ist nicht jede Zahl für a geeignet. Bei $a = 3$ würden die Restklassen

$[0]_{21}$ und $[7]_{21}$ durch dieselbe Restklasse $[c]_{21}$ verschlüsselt. Wir müssen a teilerfremd zu 21 wählen, z. B. $a = 2$, denn dann finden wir k und l, so dass

$$k \cdot 2 + l \cdot 21 = 1, \qquad \text{also} \qquad k \cdot 2 \equiv 1 \pmod{21}.$$

Im vorliegenden Fall können wir $k = 11$ wählen. Multiplizieren wir beide Seiten der Verschlüsselungsvorschrift (3) (in der wir $a = 2$ und $c = 5$ gesetzt haben) mit 11, so folgt

$$11y \equiv x + 55 \pmod{21},$$

und Umstellung nach x ergibt, wenn wir die Zahlen durch ihre Reste bei Division durch 21 ersetzen, die Entschlüsselungsvorschrift

$$x \equiv 11y + 8 \pmod{21}. \tag{4}$$

Mitunter ist es günstiger, nicht den Rest bei Division durch m als Vertreter der Restklasse zu wählen, sondern z. B. die betragsmäßig kleinste Zahl unter allen Elementen der Restklasse, also

$$x \equiv 8 - 10y \pmod{21}.$$

Zur Verschlüsselung des Wortes

CAESAR

wandelt man dieses mit obiger Tabelle in die Folge von Restklassen

2,0,4,17,0,16

um und errechnet nach der Verschlüsselungsvorschrift (3) die Folge

9,5,13,18,5,16,

woraus sich nach der Tabelle die verschlüsselte Nachricht

KFOTFR

ergibt. Empfängt man die verschlüsselte Nachricht

BORKAISOXLRAD

so wandelt man diese in die Folge

1,13,16,9,0,8,17,13,20,10,16,0,3

um, berechnet nach der Entschlüsselungsvorschrift (4) die Folge

19,4,16,2,8,12,6,4,18,13,16,8,20

und erhält die entschlüsselte Nachricht

VERCINGETORIX.

In der Praxis benötigt man zur Übermittlung von Nachrichten natürlich weitere Zeichen, vor allem das Leerzeichen. Statt Römischer Zahlen benutzt man heute lieber Dezimalzahlen, was 10 zusätzliche Zeichen erfordert.

7 Der chinesische Restsatz

Manche Pflanzen vermehren sich nur in bestimmten Jahren, sagen wir alle m Jahre. Wenn Jahr a ein solches Jahr ist, so geschieht die Vermehrung in den Jahren x mit der Eigenschaft

$$x \equiv a \pmod{m}.$$

Man sagt, dass diese Pflanzen dadurch besser den Parasiten entgehen, die auch einen festen Vermehrungszyklus, sagen wir von n Jahren, haben. Diese vermehren sich dann in den Jahren x, für die gilt

$$x \equiv b \pmod{n}.$$

In welchen Jahren treffen beide aufeinander? Wir suchen also nach den Lösungen des Systems von Kongruenzen

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$

Ist x_0 eine Lösung, so gilt für jede andere Lösung x, dass

$$m \mid x - x_0 \qquad \text{und} \qquad n \mid x - x_0.$$

Nehmen wir an, dass m und n teilerfremd sind. Dann folgt nach Satz 5(iv), dass $mn \mid x - x_0$. Natürlich gilt auch die Umkehrung. Haben wir also eine Lösung x_0, so bilden sämtliche Lösungen eine Restklasse $[x_0]_{mn}$ modulo mn. Aber für welche a und b existieren tatsächlich Lösungen?

Nehmen wir z. B. $m = 7$ und $n = 4$. Für eine Restklasse $[x]_{28}$ sind die Restklassen $[x]_7$ und $[x]_4$ unabhängig vom Vertreter x bestimmt. Also kann x nur für ein einziges Paar vorgegebener Restklassen $[a]_7$ und $[b]_4$ Lösung sein. Wir tragen alle Restklassen $[x]_{28}$ in eine Tabelle ein, wobei die Spalte durch die Restklasse von x modulo 7 und die Zeile durch die Restklasse modulo 4 bestimmt ist:

	0	1	2	3	4	5	6
0	0	8	16	24	4	12	20
1	21	1	9	17	25	5	13
2	14	22	2	10	18	26	6
3	7	15	23	3	11	19	27

Wie wir sehen, findet sich in jedem Feld genau eine Restklasse, und kein Feld bleibt leer. Also gibt es zu vorgegebenen a und b genau eine Restklasse modulo 28, die aus Lösungen besteht.

Wie kann man die Lösungen des Systems ohne Probieren zu finden? Die Lösungen der ersten Kongruenz sind die Zahlen $x = a+ym$ mit $y \in \mathbb{Z}$. Setzen wir dies in die zweite Kongruenz ein, so erhalten wir die lineare Kongruenz

$$my \equiv b - a \pmod{n}$$

mit der Unbekannten y. Diese Kongruenz können wir lösen, wenn m und n teilerfremd sind, und das Ergebnis in die Formel für x einsetzen. Wir haben folgenden Satz bewiesen, der bereits in einem chinesischen Manuskript der ersten Jahrhunderts auftaucht.

Satz 15 (Chinesischer Restsatz) *Sind m und n teilerfremde positive natürliche Zahlen, so hat das System von Kongruenzen*

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$

für beliebige ganze Zahlen a und b Lösungen, und diese sind gerade die Lösungen einer einzigen Kongruenz

$$x \equiv x_0 \pmod{mn}.$$

Beweis. Wir wollen den Existenzbeweis noch einmal in eleganterer Form aufschreiben. Da m und n teilerfremd sind, finden wir mit Hilfe des Euklidischen Algorithmus ganze Zahlen k und l, so dass

$$km + ln = 1.$$

Wir behaupten, dass

$$x_0 = bkm + aln$$

eine Lösung ist. Dies folgt sofort aus

$$ln \equiv 1 \pmod{m}, \qquad km \equiv 1 \pmod{n}.$$

□

Die Teilerfremdheit von m und n ist übrigens notwendig, damit das System für beliebige a und b lösbar ist. Eine Lösung für $a = 1$ und $b = 0$ hat nämlich die Eigenschaften $1 - x = lm$ und $x = kn$ mit k, $l \in \mathbb{Z}$, so dass $1 = km + ln$.

Satz 16 *Sind m und n positive natürliche Zahlen, so hat das System von Kongruenzen*

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$

genau dann Lösungen, wenn $a \equiv b \pmod{\text{ggT}(m,n)}$*, und diese sind dann gerade die Lösungen einer einzigen Kongruenz*

$$x \equiv x_0 \pmod{\text{kgV}(m,n)}.$$

Beweis. Es sei $d = \text{ggT}(m,n)$ und $v = \text{kgV}(m,n)$. Mit dem Euklidischen Algorithmus finden wir $k, l \in \mathbb{Z}$, so dass

$$km + ln = d.$$

Ist $a \equiv b \pmod{d}$, so gibt es $e \in \mathbb{Z}$, so dass

$$a - b = ed = ekm + eln.$$

Setzen wir

$$x_0 = a - ekm = b + eln,$$

so ist x_0 offensichtlich eine Lösung.

Ist umgekehrt x_0 eine Lösung, so gilt

$$\begin{cases} x_0 \equiv a \pmod{d}, \\ x_0 \equiv b \pmod{d}, \end{cases}$$

also $a \equiv b \pmod{d}$.

Kennen wir bereits eine Lösung x_0, so ist eine ganze Zahl x genau dann eine Lösung, wenn

$$\begin{cases} x \equiv x_0 \pmod{m}, \\ x \equiv x_0 \pmod{n}, \end{cases}$$

also genau dann, wenn $x - x_0$ ein gemeinsames Vielfaches von m und n ist. Nach Satz 6 ist dies genau dann der Fall, wenn $x - x_0$ ein Vielfaches von v ist, d. h. wenn $x \equiv x_0 \pmod{v}$. □

Sind m und n teilerfremd, so ist die Bedingung $a \equiv b \pmod{\text{ggT}(m,n)}$ automatisch erfüllt, und nach Satz 6 ist $\text{kgV}(m,n) = mn$. Somit ist Satz 15 ein Spezialfall von Satz 16.

Satz 16 zeigt, dass ein System aus zwei Kongruenzen äquivalent zu einer einzigen Kongruenz ist. Haben wir ein System aus beliebig vielen Kongruenzen, so können wir schrittweise zwei Kongruenzen durch eine ersetzen, bis wir eine Kongruenz erhalten, die äquivalent zum gesamten System ist.

Beispiel. Wenn sich die Schüler einer Klasse in Zweier-, Dreier- oder Vierreihen aufstellen, bleibt jedesmal ein Schüler übrig. Erst als sie sich in

Fünferreihen gruppieren, hat jeder seinen Platz. Wie viele Schüler hat die Klasse?

Die Anzahl der Schüler ist eine Lösung des Systems

$$\begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 1 \pmod 3 \\ x \equiv 1 \pmod 4 \\ x \equiv 0 \pmod 5 \end{cases}$$

Offensichtlich ist 1 eine Lösung des Teilsystems aus den ersten beiden Kongruenzen, wir können diese also nach Satz 15 durch die Kongruenz

$$x \equiv 1 \pmod 6$$

ersetzen. Um diese mit der dritten zu kombinieren, braucht man Satz 16 und erhält

$$x \equiv 1 \pmod{12}.$$

(Dies hätte man übrigens in einem Schritt sehen können, denn die erste Kongruenz des Ausgangssystems ist eine Folgerung aus der dritten.) Wir haben unser System also auf

$$\begin{cases} x \equiv 1 \pmod{12} \\ x \equiv 0 \pmod 5 \end{cases}$$

zurückgeführt. Mit Hilfe des Euklidischen Algorithmus finden wir

$$1 = 5 \cdot 5 - 2 \cdot 12,$$

also ist nach Satz 15 und seinem Beweis

$$x \equiv 25 \pmod{60}.$$

Die Klasse besteht offenbar aus 25 Schüler(innen), denn die anderen positiven Lösungen 85, 145, ... sind nicht realistisch.

8 Reduktion Diophantischer Gleichungen

Eine Diophantische Gleichung ist eine Gleichheit von zwei Termen, die aus ganzen Zahlen und Unbekannten (auch Variablen genannt) nur unter Verwendung der Operationen Addition und Multiplikation gebildet sind. Man könnte auch die Subtraktion zulassen, aber das ergibt nichts Neues, denn

$a - b = a + (-1) \cdot b$. Kommen in der Gleichung n Variablen vor, so versteht man unter einer Lösung der Diophantischen Gleichung ein n-Tupel von Zahlen, das beim Einsetzen an Stelle der Variablen die Gleichung in eine wahre Aussage verwandelt. Da keine Division vorkommt, laufen sämtliche Berechnungen im Bereich der ganzen Zahlen ab. Bisher sind uns Diophantische Gleichungen begegnet wie z. B.

$$4x + 7y = 9, \qquad a^2 + b^2 = c^2.$$

Formen wir einen Term unter Verwendung der Rechengesetze

- Kommutativgesetz der Addition und der Multiplikation
- Assoziativgesetz Addition und der Multiplikation
- Distributivgesetz

oder durch das Ausführen von Rechenoperationen zwischen Zahlen um, so erhalten wir einen neuen Term, der beim Einsetzen eines n-Tupels von Zahlen denselben Wert annimmt wie der ursprüngliche Ausdruck.

Definition 5 *Zwei Terme der oben genannten Art heißen äquivalent, wenn man den einen in den anderen unter Verwendung der genannten Schritte umformen kann. Eine Klasse äquivalenter Terme, in denen n Variablen vorkommen, nennt man Polynom in n Variablen.*

So stellen beispielsweise die Terme

$$(4x - 3)y + 2x \qquad \text{und} \qquad 2x(2y + 1) - 3y$$

dasselbe Polynom dar. Es ist üblich, für Polynome in ein, zwei, ... Variablen Bezeichnungen der Art $p(x)$, $q(x, y)$, ... zu verwenden.

Offensichtlich kann man jeden Term der genannten Art, in dem nur eine Variable x vorkommt, in die Form

$$p(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \dots$$

bringen, wobei die sogenannten Koeffizienten a_0, a_1, a_3, ... ganze Zahlen sind, von denen nur endlich viele ungleich Null sind. (Wir bezeichnen die Koeffizienten hier mit Variablen a_i, um allgemeine Aussagen über Polynone zu machen, aber für jedes konkrete Polynom stehen natürlich an ihrer Stelle Zahlen.) Man kann beweisen, dass die Koeffizienten eines Polynoms eindeutig bestimmt sind.

Analog kann man jeden Term der genannten Art, in dem zwei Variablen x und y vorkommen, in die Form

$$\begin{aligned} q(x,y) = b_{00} + b_{10}x + b_{20}x^2 + b_{30}x^3 + \ldots \\ + b_{01}y + b_{11}xy + b_{21}x^2y + \ldots \\ + b_{02}y^2 + b_{12}xy^2 + \ldots \end{aligned}$$

bringen, und Ähnliches gilt für Polynome in einer beliebigen Anzahl von Variablen. Auch hier sind die Koeffizienten eindeutig bestimmt. Man kann auch Polynome mit rationalen, reellen u. a. Koefizienten betrachten, aber die beiden Seiten einer Diophantischen Gleichung sind Polynome mit ganzzahligen Koeffizienten. Man kann mit Diophantischen Gleichungen äquivalente Umformungen vornehmen, z. B. Addition desselben Polynoms auf beiden Seiten oder Multiplikation beider Seiten mit einer von Null verschiedenen Zahl. Auf diese Weise kann man jede Diophantische Gleichungen so umformen, dass auf der rechten Seite Null steht.

Definition 6 *Es sei $f(x_1, \ldots, x_n)$ ein Polynom und m eine positive natürliche Zahl. Die Reduktion der Diophantischen Gleichung*

$$f(x_1, \ldots, x_n) = 0$$

modulo m ist die Kongruenz

$$f(x_1, \ldots, x_n) \equiv 0 \pmod{m}.$$

Die Reduktion modulo 1 ist natürlich nutzlos, denn zwei beliebige ganze Zahlen sind kongruent modulo 1.

Satz 17 *(i) Ist das n-Tupel $(c_1, \ldots, c_n)$ eine Lösung einer Diophantischen Gleichung, so ist es auch eine Lösung ihrer Reduktion modulo einer beliebigen positiven natürlichen Zahl m.*

(ii) Sind $(c_1, \ldots, c_n)$ und $(d_1, \ldots, d_n)$ zwei n-Tupel mit

$$d_1 \equiv c_1 \pmod{m}, \qquad \ldots, \qquad d_n \equiv c_n \pmod{m},$$

so gilt

$$f(c_1, \ldots, c_n) \equiv f(d_1, \ldots, d_n) \pmod{m}.$$

Ist also eines der n-Tupel eine Lösung, so auch das Andere.

Beweis. Die Aussage (i) ist offensichtlich.

Wir beweisen Aussage (ii) durch Induktion nach der Anzahl der Operationen, die in dem Term vorkommen, durch den f gegeben ist. Kommen keine Operationen vor, so ist $f(x_1, \ldots, x_n)$ eine Zahl oder eine der Variablen $x_1, \ldots, x_n$, und die Behauptung gilt. Kommen Operationen vor, so ist

$$f(x_1, \ldots, x_n) = g(x_1, \ldots, x_n) + h(x_1, \ldots, x_n) \qquad \text{oder}$$
$$f(x_1, \ldots, x_n) = g(x_1, \ldots, x_n) \cdot h(x_1, \ldots, x_n)$$

wobei die Behauptung für g und h nach Induktionsvoraussetzung bereits gilt. Damit folgt die Behauptung für f nach Satz 13. □

Als Lösungen einer Diophantischen Gleichung in n Unbekannten kommen also nur solche n-Tupel $(c_1, \ldots, c_n)$ in Frage, für die das entsprechende n-Tupel $([c_1]_m, \ldots, [c_n]_m)$ von Restklassen aus Lösungen der Reduktion modulo m besteht. Um aber alle Lösungen einer Kongruenz modulo m in n Unbekannten zu finden, braucht man im Prinzip nur alle n-Tupel von Restklassen durchzuprobieren. Ihre Anzahl ist m^n. Wir haben die Methode der Reduktion bereits im Zusammenhang mit Pythagoräischen Tripeln (modulo 2 und 4) und in dem Beispiel nach Definition 4 (modulo 4 und 8) benutzt.

Aus der Lösbarkeit der Reduktion einer Diophantischen Gleichung modulo beliebiger m folgt aber nicht die Lösbarkeit der Diophantischen Gleichung selbst.

Beispiel. Die Diophantische Gleichung

$$(2x - 1)(3y - 1) = 0$$

hat keine Lösungen, denn für jede Lösung müsste $2x = 1$ oder $3y = 1$ gelten. Ist nun m eine positive natürliche Zahl, so finden wir mit Hilfe der Primfaktorzerlegung teilerfremde natürliche Zahlen m_1 und m_2, so dass $m = m_1 m_2$ und dass m_1 nicht durch 2 und m_2 nicht durch 3 teilbar ist. Nach dem Chinesischen Restsatz ist das System

$$\begin{cases} 2x \equiv 1 \pmod{m_1} \\ 3y \equiv 1 \pmod{m_2} \end{cases}$$

lösbar. Für eine Lösung (x, y) gilt dann $m_1 \mid 2x - 1$ und $m_2 \mid 3y - 1$, also $m \mid (2x - 1)(3y - 1)$, d. h.

$$(2x - 1)(3y - 1) \equiv 0 \pmod{m}.$$

Zwischen den verschiedenen Reduktionen besteht folgender Zusammenhang: Ist d ein Teiler von m, so ist jede Lösung der Kongruenz

$$f(x_1, \ldots, x_n) \equiv 0 \pmod{m}$$

auch Lösung der Kongruenz

$$f(x_1, \ldots, x_n) \equiv 0 \pmod{d}.$$

Man kann also die Suche nach Lösungen der Kongruenz modulo m auf diejenigen Restklassen einschränken, deren Vertreter Lösungen der einfacher zu behandelnden Kongruenz modulo d sind. So hätten wir in dem Beispiel nach Definition 4 die Suche nach quadratischen Restklassen modulo 8 auf die Restklassen $[0]_8$, $[1]_8$, $[4]_8$ und $[5]_8$ einschränken können, nachdem wir schon wussten, dass nur die Restklassen $[0]_4$ und $[1]_4$ quadratisch sind.

Man kann die Arbeit noch weiter vereinfachen. Es sei $m = ab$ mit teilerfremden positiven natürlichen Zahlen a und b. Haben wir eine Kongruenz bereits modulo a und modulo b gelöst, gilt also

$$\begin{cases} f(c_1, \ldots, c_n) \equiv 0 \pmod{a}, \\ f(d_1, \ldots, d_n) \equiv 0 \pmod{b}, \end{cases}$$

so gewinnen wir die Lösungen der Kongruenz

$$f(x_1, \ldots, x_n) \equiv 0 \pmod{m},$$

indem wir die Systeme

$$\begin{cases} x_1 \equiv c_1 \pmod{a}, \\ x_1 \equiv d_1 \pmod{b}, \end{cases} \quad \ldots \quad \begin{cases} x_n \equiv c_n \pmod{a}, \\ x_n \equiv d_n \pmod{b}, \end{cases}$$

lösen. Dies folgt aus dem Chinesischen Restsatz.

Durch wiederholte Anwendung kann man das Problem also auf den Fall zurückführen, dass der Modul nur einen einzigen Primteiler besitzt, d. h. Potenz einer Primzahl ist.

Beispiel. Wir wollen die Kongruenz

$$x^3 - 3x^2 + 27 \equiv 0 \pmod{1125}$$

lösen. Die Primfaktorzerlegung von 1125 ist $3^2 \cdot 5^3$. Die weitestgehende Zerlegung in teilerfremde Faktoren ist also $1125 = 9 \cdot 125$, und unsere Kongruenz ist nach dem Chinesischen Restsatz äquivalent zu dem System

$$\begin{cases} x^3 - 3x^2 + 27 \equiv 0 \pmod{9}, \\ x^3 - 3x^2 + 27 \equiv 0 \pmod{125}. \end{cases}$$

Wir betrachten zunächst die erste Kongruenz, die sich zu

$$x^3 - 3x^2 \equiv 0 \pmod{9}$$

vereinfacht. Jede ihrer Lösungen ist auch Lösung von

$$x^3 - 3x^2 \equiv 0 \pmod 3, \qquad \text{d. h.} \qquad x^3 \equiv 0 \pmod 3.$$

Man prüft durch Einsetzen, dass von den drei Restklassen modulo 3 nur die Klasse $[0]_3$ eine Lösung ist, d. h. $x = 3k$. Betrachten wir nun die Kongruenz modulo 9, so kommen als Lösung nur die Klassen $[0]_9$, $[3]_9$ und $[6]_9$ in Frage. Man prüft wiederum durch Einsetzen, dass alle drei Lösungen sind. Die Lösung der ersten Kongruenz unseres Systems ist also

$$x \equiv 0 \pmod 3.$$

Nun muss man die zweite Kongruenz nach derselben Methode behandeln.

Eine Aufgabe dieser Art wird oft durch folgenden Spezialfall des Henselschen Lemmas erleichtert.

Satz 18 (Hensel) *Es sei p eine Primzahl, e eine positive natürliche Zahl und $f(x)$ ein Polynom in einer Variablen mit ganzzahligen Koeffizienten. Ist c eine Lösung der Kongruenz*

$$f(x) \equiv 0 \pmod{p^e}.$$

und ist $f'(c)$ nicht durch p teilbar, so gibt es genau eine Lösung $[x]_{p^{e+1}}$ der Kongruenz

$$f(x) \equiv 0 \pmod{p^{e+1}}$$

mit $x \equiv c \pmod{p^e}$, nämlich $x = c + kp^e$, wobei

$$\frac{f(c)}{p^e} + f'(c)k \equiv 0 \pmod p.$$

Beweis. Die Bedingung $x \equiv c \pmod{p^e}$ bedeutet

$$x = c + kp^e \qquad \text{mit} \qquad k \in \mathbb{Z}.$$

Schreiben wir

$$f(c + y) = a_0 + a_1 y + a_2 y^2 + \ldots,$$

so gilt $a_0 = f(c) \equiv 0 \pmod{p^e}$, also $a_0 = bp^e$. Einsetzen ergibt

$$f(x) = f(c + kp^e) = bp^e + a_1 kp^e + a_2 k^2 p^{2e} + \ldots$$

Wir suchen nach Lösungen der Kongruenz $f(x) \equiv 0 \pmod{p^{e+1}}$, d. h.

$$(b + a_1 k)p^e \equiv 0 \pmod{p^{e+1}}.$$

Schreiben wir diese Kongruenz nach Definition als Teilbarkeit um, so sehen wir mit Aufgabe 1(c), dass sie äquivalent ist zu

$$b + a_1 k \equiv 0 \pmod{p}.$$

(Man kann sich als allgemeine Regel merken, dass die Division beider Seiten einer Kongruenz *und* des Moduls durch dieselbe Zahl eine äquivalente Umformung ist.) Da $a_1 = f'(c)$ nicht durch p teilbar ist, hat diese lineare Kongruenz genau eine Lösung k modulo p, und durch Einsetzen erhalten wir für x genau eine Lösung modulo p^{e+1}. □

Der Satz liefert uns die Existenz einer Lösung, und der Beweis gibt uns eine Methode, sie zu finden (die auch ohne die Voraussetzung an $f'(c)$ anwendbar ist).

Beispiel. Wir setzen das vorige Beispiel fort und betrachten nun die zweite Kongruenz

$$x^3 - 3x^2 + 27 \equiv 0 \pmod{125}$$

unseres Systems. Jede Lösung ist auch Lösung von

$$x^3 - 3x^2 + 27 \equiv 0 \pmod{5}.$$

Durch Einsetzen der Restklassen modulo 5 findet man, dass nur

$$x \equiv 1 \pmod{5}$$

Lösung ist, also $x = 1 + 5k$.

Um die Kongruenz modulo der nächsthöheren Potenz von 5, also

$$x^3 - 3x^2 + 27 \equiv 0 \pmod{25}$$

zu lösen, setzen wir auf der linken Seite für x den Ausdruck $1 + 5k$ ein:

$$\begin{aligned}(1+5k)^3 - 3(1+5k)^2 + 27 \\ &= (1 + 15k + 75k^2 + 125k^3) - 3(1 + 10k + 25k^2) + 27 \\ &= 25 - 15k + 125k^3.\end{aligned}$$

Die Kongruenz wird zu

$$-15k \equiv 0 \pmod{25}.$$

Schreibt man diese Kongruenz als $25 \mid -15k$, so folgt aus Aufgabe 1(c), dass $5 \mid -3k$, d. h.

$$-3k \equiv 0 \pmod{5}.$$

Dies kann man übrigens ohne Rechnung aus dem Satz ablesen, denn in unserem Fall ist $p = 5$, $e = 1$, $f(1) = 25$ und $f'(1) = -3$. Die Lösung der letzten Kongruenz ist $k \equiv 0 \pmod 5$, und durch Einsetzen ergibt sich

$$x \equiv 1 \pmod{25}, \qquad \text{d. h.} \qquad x = 1 + 25l.$$

Nun gehen wir zur nächsten Potenz über und betrachten

$$x^3 - 3x^2 + 27 \equiv 0 \pmod{125}.$$

Setzt man hier für x den Ausdruck $1 + 125l$ ein, multipliziert alles aus und lässt die durch 125 teilbaren Summanden weg, so erhält man

$$25 + 5^2(-3)l \equiv 0 \pmod{125}.$$

Nach Division durch 25 ergibt sich

$$1 - 3l \equiv 0 \pmod 5.$$

(Dasselbe Ergebnis erhält man wieder schneller aus dem Satz, wobei diesmal $e = 2$ ist und für k ein l steht.) Die Lösung ist $l \equiv 2 \pmod 5$, und Einsetzen ergibt

$$x \equiv 1 + 25 \cdot 2 \equiv 51 \pmod{125}.$$

Diese Kongruenz ist äquivalent zur zweiten Kongruenz unseres Systems.

Wir hatten schon früher gesehen, dass die erste Kongruenz des Systems zu

$$x \equiv 0 \pmod 3$$

äquivalent ist. Mit Hilfe des Chinesischen Restsatzes finden wir, dass das gesamte System, also auch die anfangs betrachtete Kongruenz

$$x^3 - 3x^2 + 27 \equiv 0 \pmod{1125},$$

äquivalent ist zu

$$x \equiv 51 \pmod{3 \cdot 125}.$$

Will man die Lösung durch Restklassen modulo $1125 = 9 \cdot 125$ ausdrücken, so muss man $[51]_{1125}$, $[801]_{1125}$ und $[426]_{1125}$ angeben.

Die Methode aus dem Beweis des Satzes ähnelt dem Newtonschen Näherungsverfahren zur Bestimmung der Nullstellen eines Polynoms $f(x)$ mit reellen Koeffizienten, wo man ausgehend von einer Näherungslösung c der Gleichung $f(x) = 0$ eine neue Näherung

$$x = c - \frac{f(c)}{f'(c)}$$

findet. Durch Iteration findet man eine Folge, die gegen eine Lösung konvergiert.

Die Analogie geht noch viel weiter. Eine ganze p-adische Zahl ist eine Folge von Restklassen $[c_1]_p$, $[c_2]_{p^2}$, $[c_3]_{p^3}$, ..., so dass $c_i \equiv c_j \pmod{p^i}$ für alle $i \leq j$ gilt. Nach dem Satz ist unter gewissen Bedingungen eine Kongruenz $f(x) \equiv 0 \pmod{p^e}$ für alle e lösbar und liefert eine Lösung der Gleichung $f(x) = 0$ im Bereich $\mathbb{Z}_p$ der ganzen p-adischen Zahlen. Hensel hat eine Art Abstand p-adischer Zahlen definiert, bezüglich dessen die Folge seiner Näherungslösungen in $\mathbb{Z}_p$ konvergiert.

9 Prime Restklassen

Am Ende von Abschnitt 6 haben wir ein Verschlüsselungsverfahren kennengelernt, das jedem Buchstaben eine Codezeichen zuordnet, wobei verschiedenen Buchstaben verschiedene Codezeichen zugeordnet werden und kein Codezeichen unbenutzt bleibt. So etwas nennt man in der Mathematik eine eineindeutige Abbildung einer Menge auf eine andere. Unsere Codezeichen waren Restklassen modulo einer positiven natürlichen Zahl m. Man kann auch eineindeutige Abbildungen einer Menge auf sich selbst betrachten, diese nennt man Permutationen. Wir haben z. B. im zweiten Schritt Restklassen wiederum durch Restklassen kodiert. Eine Methode bestand darin, dass wir einer Restklasse $[x]_m$ diejenige Restklasse $[y]_m$ zuordneten, die sich aus der Kongruenz

$$y \equiv ax \pmod{m}$$

ergibt. Dadurch soll eine Permutation der Menge der Restklassen gegeben sein, d. h. die obige Kongruenz soll für jedes gegebene y eine eindeutige Lösung $[x]_m$ besitzen. Insbesondere muss dies für $y = 1$ gelten, d. h. es muss eine ganze Zahl k geben, so dass

$$1 \equiv ak \pmod{m},$$

und das bedeutet, dass es zudem eine ganze Zahl l geben muss, so dass

$$1 = ak + ml.$$

Nach Satz 5(ii) müssen a und m also teilerfremd sein.

Sind umgekehrt a und m teilerfremd, so liefert der Euklidische Algorithmus Zahlen k und l, die die obige Gleichung erfüllen, so dass $1 \equiv ak \pmod{m}$. Die eingangs gegebene Kongruenz hat dann für gegebenes y eine eindeutige Lösung, denn sie ist äquivalent zu der Kongruenz

$$ky \equiv x \pmod{m}.$$

Die erstere geht nämlich bei Multiplikation beider Seiten mit k in die letztere über, und jene geht bei Multiplikation mit a in erstere über.

Definition 7 *Eine prime Restklasse modulo m ist eine Restklasse $[a]_m$, wobei a zu m teilerfremd*[2] *ist.*

Ist b ein anderer Vertreter der Restklasse $[a]_m$, also $a \equiv b \pmod{m}$, so ist jeder gemeinsame Teiler von b und m nach Satz 1(iii) auch ein gemeinsamer Teiler von a und m. Mit a ist also auch b teilerfremd zu m, d. h. dies ist eine Eigenschaft der gesamten Restklasse und nicht eines einzelnen Vertreters.

Beispiel. Streichen wir von den Restklassen $[0]_{15}$, ..., $[14]_{15}$ alle Restklassen, deren Vertreter einen gemeinsamen Teiler mit 15 hat, so verbleiben die primen Restklassen modulo 15, nämlich

$$[1]_{15},\ [2]_{15},\ [4]_{15},\ [7]_{15},\ [8]_{15},\ [11]_{15},\ [13]_{15},\ [14]_{15}.$$

Einfacher stehen die Dinge, wenn der Modul eine Primzahl p ist. Eine ganze Zahl ist genau dann teilerfremd zu p, wenn sie nicht durch p teilbar ist. Die Restklassen modulo p sind $[0]_p$, $[1]_p$, ...,$[p-1]_p$, und natürlich ist 0 durch p teilbar. Alle anderen Restklassen sind prime Restklassen, denn die Zahlen 1, 2, ..., $p-1$ sind nicht durch p teilbar. Es gibt also genau $p-1$ prime Restklassen modulo einer Primzahl p.

Lemma 1 *Das Produkt zweier primer Restklassen modulo m ist eine prime Restklasse modulo m. Zu jeder primen Restklasse $[a]_m$ gibt es eine prime Restklasse $[k]_m$, so dass $[a]_m \cdot [k]_m = [1]_m$.*

Beweis. Hat ab einen gemeinsamen Teiler $d > 1$ mit m, so ist ein beliebiger Primfaktor p von d ebenfalls ein gemeinsamer Teiler. Nach Satz 5(iii) muss p dann a oder b teilen, d. h. eine der beiden Zahlen hat einen echten gemeinsamen Teiler mit m. Ist hingegen jede der beiden Zahlen a und b teilerfremd zu m, so kann dies nicht eintreten, also muss dann auch ab teilerfremd zu m sein.

Wie wir oben gesehen haben, gibt es zu einer ganzen Zahl a genau dann eine ganze Zahl k mit der Eigenschaft $ak \equiv 1 \pmod{m}$, wenn a zu m teilerfremd ist. In dieser Kongruenz kann man die Rollen von a und k vertauschen, also ist dann auch k teilerfremd zu m. □

Folgerung 3 *Die Multiplikation der Restklassen modulo m mit einer festen primen Restklasse definiert eine Permutation der Menge der primen Restklassen modulo m.*

[2]Statt „teilerfremd“ sagt man mitunter „relativ prim“, daher der Name. Wir werden den Begriff „relativ prim“ vermeiden, da er leicht mit „prim“ verwechselt werden kann.

Beispiel. Durch Multiplikation mit $[7]_{15}$ erhalten wir folgende Permutation der primen Restklassen modulo 15, wobei wir die Klammern der Einfachheit halber weglassen:

$[a]_{15}$	1	2	4	7	8	11	13	14
$[7]_{15} \cdot [a]_{15}$	7	14	13	4	11	2	1	8

Wegen $7 \cdot 13 \equiv 1 \pmod{15}$ macht die Multiplikation mit $[13]_{15}$ die Permutation wieder rückgängig.

Satz 19 (Fermat) *Ist p eine Primzahl, so gilt für jede ganze Zahl a, die nicht durch p teilbar ist, dass*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Beweis. Es sei $[n]_p$ das Produkt aller $p-1$ primen Restklassen modulo p. Ersetzen wir jeden Faktor $[b]_p$ durch $[a]_p \cdot [b]_p$, so können wir wegen der Kommutativität der Multiplikation von Restklassen alle Faktoren $[a]_p$ nach links bringen und erhalten $[a]_p^{p-1}[n]_p$. Wir können aber auch anders vorgehen und in jedem Faktor $[a]_p \cdot [b]_p$ die Multiplikation ausführen. Wegen obiger Folgerung stehen noch dieselben Faktoren da, wenn auch in anderer Reihenfolge, also ist das Produkt unverändert. Es folgt

$$[a]_p^{p-1}[n]_p = [n]_p.$$

Nach Lemma 1 ist $[n]_p$ eine prime Restklasse, also gibt es ein l, so dass $[n]_p \cdot [l]_p = [1]_p$. Multiplikation beider Seiten mit $[l]_p$ liefert

$$[a]_p^{p-1} = [1]_p,$$

und wegen $[a]_p^{p-1} = [a^{p-1}]_p$ ist dies gleichbedeutend mit der Behauptung. □

Beispiel (vgl. Aufgabe 17). Man finde den Rest von 19^{135} bei Division durch 13. Da 13 eine Primzahl ist, gilt nach dem Satz

$$19^{12} \equiv 1 \pmod{13}, \qquad 19^{12k} = (19^{12})^k \equiv 1 \pmod{13}.$$

Durch Division mit Rest finden wir $135 = 12 \cdot 11 + 3$, also

$$19^{135} = (19^{12})^{11} \cdot 19^3 \equiv 19^3 \equiv 6^3 \equiv 8 \pmod{13}.$$

Die Antwort ist also 8.

Folgerung 4 *Ist p eine Primzahl, so gilt für alle ganzen Zahlen a*

$$a^p \equiv a \pmod{p}.$$

Bemerkung. Die Verwendung algebraischer Begriffe macht Argumente wie im Beweis von Satz 19 übersichtlicher. Auf der Menge der Restklassen modulo m haben wir in Definition 4 zwei Operationen (Addition und Multiplikation) eingeführt. Diese haben folgende Eigenschaften:

- Kommutativität der Addition und der Multiplikation,
- Assoziativität der Addition und der Multiplikation,
- Distributivität,
- es gibt ein neutrales Element bezüglich der Addition, nämlich $[0]_m$, und zu jedem Element $[a]_m$ gibt es ein eingegengesetztes Element, d. h. ein solches Element $[b]_m$, dass $[a]_m + [b]_m = [0]_m$,
- es gibt ein neutrales Element bezüglich der Multiplikation, nämlich $[1]_m$.

Eine Menge mit zwei Operationen, die diese Eigenschaften haben, nennt man einen kommutativen Ring mit Einselement. Wir kennen bereits den Ring $\mathbb{Z}$ der ganzen Zahlen, den Ring $\mathbb{Q}$ der rationalen Zahlen und den Ring $\mathbb{R}$ der reellen Zahlen. Der Bereich $\mathbb{N}$ der natürlichen Zahlen ist kein Ring, weil es nicht zu jeder natürlichen Zahl eine entgegengesetzte Zahl in $\mathbb{N}$ gibt. Den Ring der Restklassen modulo m bezeichnet man mit $\mathbb{Z}/m\mathbb{Z}$. (Es gibt allgemein für ein Ideal I in einem kommutativen Ring R den Quotientenring R/I, vgl. Satz 4.) Es gibt auch nichtkommutative Ringe, z. B. den Ring der $n \times n$-Matrizen mit Koeffizienten in einem anderen Ring wie $\mathbb{Z}$ oder $\mathbb{Q}$.

Nach Lemma 1 sind die primen Restklassen $[a]_m$ genau diejenigen Elemente des Restklassenrings $\mathbb{Z}/m\mathbb{Z}$, die ein inverses Element besitzen, d. h. ein Element $[k]_m$, so dass $[a]_m \cdot [k]_m = [1]_m$. Im Ring $\mathbb{Z}$ besitzen nur die Elemente 1 und -1 Inverse, in $\mathbb{Q}$ wie auch in $\mathbb{R}$ besitzt hingegen jedes von Null verschiedene Element ein Inverses, das hier Kehrwert genannt wird. Ein Ring, in dem jedes von Null verschiedene Element ein Inverses besitzt, heißt Körper. Wir haben also den Körper $\mathbb{Q}$ der rationalen Zahlen und den Körper $\mathbb{R}$ der reellen Zahlen, aber $\mathbb{Z}$ ist kein Körper.

Wir erinnern daran, dass man die Lösungen einer quadratischen Gleichung, z. B.

$$x^2 - 5x + 4 = 0,$$

in $\mathbb{Q}$ oder $\mathbb{R}$ durch Bildung der quadratischen Ergänzung finden kann, in

unserem Beispiel

$$\begin{aligned} x^2 - 5x + 4 = x^2 - 2 \cdot \frac{5}{2}\, x + 4 &= \left(x - \frac{5}{2}\right)^2 - \frac{25}{4} + 4 \\ &= \left(x - \frac{5}{2}\right)^2 - \frac{9}{4} = \left(x - \frac{5}{2} + \frac{3}{2}\right)\left(x - \frac{5}{2} - \frac{3}{2}\right) \\ &= (x-1)(x-4). \end{aligned}$$

Das Produkt zweier von Null verschiedener Zahlen ist nicht Null. Da unsere Gleichung die Form

$$(x-1)(x-4) = 0$$

angenommen hat, muss beim Einsetzen einer Lösung wenigstens einer der Faktoren Null werden. Die Lösungen sind also genau die Zahlen 1 und 4. Betrachten wir aber die Gleichung

$$x^2 - 5x - 1 = 0,$$

so führt die Bildung der quadratischen Ergänzung auf die Gleichung

$$\left(x - \frac{5}{2}\right)^2 = \frac{29}{4},$$

die zwar Lösungen in $\mathbb{R}$ hat, aber nicht in $\mathbb{Q}$, weil $\frac{29}{4}$ kein Quadrat in $\mathbb{Q}$ ist (siehe Aufgabe 12).

Ist p eine Primzahl, so ist der Restklassenring $\mathbb{Z}/p\mathbb{Z}$ ein Körper. Man kann in ihm fast so rechnen wie in $\mathbb{Q}$ oder $\mathbb{R}$. Um z. B. die Gleichung

$$X^2 - [5]_7\, X - [1]_7 = [0]_7$$

(wobei X eine gesuchte Restklasse ist) mit Hilfe der quadratischen Ergänzung zu lösen, braucht man das Inverse von $[2]_7$, das in diesem Körper natürlich nicht $\frac{1}{2}$, sondern $[4]_7$ ist (vgl. Lemma 1). Wir erhalten $[5]_7 = [2]_7 \cdot [4]_7 \cdot [5]_7 = [2]_7 \cdot [-1]_7$, so dass

$$X^2 - [5]_7\, X - [1]_7 = X^2 + [2]_7\, X - [1]_7 = \big(X + [1]_7\big)^2 - [1]_7^2 - [1]_7.$$

Beim Durchprobieren der Restklassen modulo 7 findet man, dass $[1]_7^2 + [1]_7 = [2]_7$ ein Quadrat ist, nämlich $[\pm 3]_7^2$, so dass

$$X^2 - [5]_7\, X - [1]_7 = \big(X + [1]_7 - [3]_7\big)\big(X + [1]_7 + [3]_7\big).$$

Unsere quadratische Gleichung wird also zu

$$\big(X - [2]_7\big)\big(X - [3]_7\big) = [0]_7.$$

Da nach Lemma 1 das Produkt zweier von $[0]_7$ verschiedener Restklassen nicht $[0]_7$ ist, können wir wieder schließen, dass die Gleichung genau die Lösungen $[2]_7$ und $[3]_7$ hat. Auf ähnliche Weise kann man auch die Gleichung

$$X^2 - [5]_7 X + [4]_7 = 0$$

behandeln, aber hier wissen wir sowieso aus Satz 17(i), dass $[1]_7$ und $[4]_7$ Lösungen sind. Jedenfalls zeigt unsere Methode, dass eine quadratische Gleichung in einem Körper höchstens zwei Lösungen haben kann.

Man kann die gesuchte Restklasse als $X = [x]_7$ mit einer ganzen Zahl x schreiben, und die letztgenannte quadratische Gleichung in $\mathbb{Z}/7\mathbb{Z}$ ist dann äquivalent zu der Kongruenz

$$x^2 - 5x + 4 \equiv 0 \pmod 7.$$

Es ist Geschmackssache, welche Schreibweise man bevorzugt.

Satz 20 (Wilson) *Ist p eine Primzahl, so gilt*[3]

$$(p-1)! \equiv -1 \pmod p.$$

Beweis. Wir betrachten das Produkt aller primen Restklassen modulo p, also

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

Nach Lemma 1 hat jede prime Restklasse eine eindeutig bestimmte inverse Restklasse, und wenn diese beiden Restklassen voneinander verschieden sind, so kann man sie in dem Produkt wegkürzen. Die Restklassen, die mit ihren Inversen übereinstimmen, sind die Lösungen der Gleichung

$$X^2 = [1]_p, \qquad \text{d. h.} \qquad (X + [1]_p)(X - [1]_p) = [0]_p.$$

Diese Gleichung hat nur die Lösungen $[1]_p$ und $[-1]_p$, also erhalten wir

$$[(p-1)!]_p = [1]_p \cdot [-1]_p,$$

was zu der Behauptung des Satzes äquivalent ist. □

[3]Wenn eine natürliche Zahl $n > 0$ gegeben ist, so bezeichnet man mit $n!$ (gelesen n Fakultät) das Produkt aller natürlichen Zahlen von 1 bis n, und man setzt $0! = 1$.

10 Die Eulersche Funktion

Nach Leonhard Euler bezeichnet man die Anzahl der primen Restklassen modulo m mit $\varphi(m)$. Die Eulersche Funktion φ hat als Definitionsbereich die Menge der positiven natürlichen Zahlen. Wir können ihre Werte durch Abzählen bestimmen, z. B. $\varphi(15) = 8$ (vgl. das Beispiel nach Definition 7).

Satz 21 (Euler) *Ist m eine positive natürliche Zahl, so gilt für alle ganzen Zahlen a, die teilerfremd zu m sind,*

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

Der Beweis ist identisch mit dem des Satzes von Fermat: Man bildet das Produkt aller primen Restklassen und multipliziert jeden Faktor mit $[a]_m$. Einerseits werden die primen Restklassen dabei permutiert, so dass das Produkt unverändert bleibt, andererseits multipliziert sich das Produkt mit $[a]_m^{\varphi(m)}$.

Für jede Primzahl p gilt $\varphi(p) = p - 1$, so dass sich der Satz von Fermat als Spezialfall des Satzes von Euler ergibt. Eulers Verallgemeinerung ist natürlich nur von Nutzen, wenn man $\varphi(m)$ effektiv bestimmen kann. Im Fall einer Primzahlpotenz $m = p^e$ ist das einfach. Eine Zahl a ist genau dann teilerfremd zu p^e, wenn sie nicht durch p teilbar ist. Von den $m = p^e$ Restklassen

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

müssen wir alle Vielfachen von p wegstreichen, also alle $[kp]_m$ mit $0 \le k < \frac{m}{p}$. Es verbleiben $m - \frac{m}{p}$ prime Restklassen, so dass

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

Satz 22 *Sind m und n teilerfremd, so gilt*

$$\varphi(mn) = \varphi(m)\varphi(n).$$

Beweis. Ist $[a]_{mn}$ eine Restklasse modulo mn, so ist die Restklasse $[a]_m$ unabhängig von der Wahl des Vertreters a. Wir ordnen so jeder Restklasse modulo mn eine Restklasse modulo m zu. (Diese Zuordnung haben wir bereits bei der Reduktion einer Diophantischen Gleichung bezüglich verschiedener Moduln betrachtet.) Analog können wir der Restklasse $[a]_{mn}$ eine Restklasse modulo n zuordnen, nämlich $[a]_n$. Aus einer Restklasse $[a]_{mn}$ erhalten wir also ein geordnetes Paar $([a]_m, [a]_n)$ von Restklassen. (Das lässt sich durch eine Tabelle wie in Abschnitt 7 veranschaulichen.)

Jedes Paar $([b]_m, [c]_n)$ bestehend aus einer Restklasse modulo m und einer Restklasse modulo n entsteht auf diese Weise aus einer eindeutig bestimmten Restklasse $[a]_{mn}$. Dies folgt aus dem Chinesischen Restsatz, denn a ist Lösung des Systems von Kongruenzen

$$\begin{cases} x \equiv b \pmod{m}, \\ x \equiv c \pmod{n}. \end{cases}$$

Ist a teilerfremd zu mn, so ist a offensichtlich teilerfremd zu m und zu n. Einer primen Restklasse wird also ein Paar primer Restklassen zugeordnet. Umgekehrt sei a teilerfremd zu m und zu n. Dann ist a auch teilerfremd zu mn, wie schon im Beweis von Lemma 1 bemerkt (mit vertauschten Rollen von Modul und Element). Jedes Paar primer Restklassen entsteht also aus einer eindeutig bestimmten primen Restklasse modulo mn.

Die Anzahl aller geordneten Paare bestehend aus einer primen Restklasse modulo m und einer primen Restklasse modulo n ist $\varphi(m)\varphi(n)$. □

Bemerkung. Sind X und Y Mengen, so bezeichnet man die Menge aller geordneten Paare (x, y) mit $x \in X$ und $y \in Y$ als das Kartesische Produkt $X \times Y$. Der chinesische Restsatz liefert also eine eineindeutige Abbildung

$$\mathbb{Z}/mn\mathbb{Z} \to (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}).$$

Die Menge der invertierbaren Elemente eines Ringes R bezeichnet man oft mit $R^\times$, weil auf dieser Menge nur noch die Operation $\times$ möglich ist. Wir haben im obigen Beweis gezeigt, dass sich die Abbildung des Chinesischen Restsatzes zu einer eineindeutigen Abbildung

$$(\mathbb{Z}/mn\mathbb{Z})^\times \to (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$$

einschränkt.

Die Formel des Satzes lässt sich durch vollständige Induktion auf eine beliebige Anzahl von Faktoren verallgemeinern: Sind $m_1, \ldots, m_r$ paarweise teilerfremd, so gilt

$$\varphi(m_1 \ldots m_r) = \varphi(m_1) \ldots \varphi(m_r).$$

Damit können wir die Eulersche Funktion für eine beliebige Zahl berechnen, z. B.

$$\varphi(240) = \varphi(2^3 \cdot 3^2 \cdot 5) = \varphi(2^3)\varphi(3^2)\varphi(5) = 2^2(2-1)3(3-1)(5-1) = 96.$$

Allgemein gilt: Ist $m = p_1^{e_1} \ldots p_r^{e_r}$ mit verschiedenen Primzahlen $p_1, \ldots, p_r$, so gilt

$$\varphi(m) = p_1^{e_1-1}(p_1-1) \ldots p_r^{e_r-1}(p_r-1) = m\left(1 - \frac{1}{p_1}\right) \ldots \left(1 - \frac{1}{p_r}\right).$$

Auch die Folgerung aus dem Satz von Fermat lässt sich begrenzt verallgemeinern.

Folgerung 5 *Sind k und $m > 0$ natürliche Zahlen, so dass $k \equiv 1 \pmod{\varphi(m)}$, so gilt für alle ganzen Zahlen a, die teilerfremd zu m sind,*

$$a^k \equiv a \pmod{m}.$$

Es ist nämlich $k - 1 = l\varphi(m)$ mit $l \in \mathbb{N}$, so dass

$$a^k = a^{l\varphi(m)+1} = (a^l)^{\varphi(m)} a \equiv a \pmod{m}$$

nach Satz 21. Im Unterschied zur Folgerung aus dem Satz von Fermat gilt dies nicht für alle ganzen Zahlen, wie das Beispiel $\varphi(12) = 4$, aber

$$2^5 = 32 \not\equiv 2 \pmod{12}$$

zeigt. Beschränkt man sich auf quadratfreie m, so gilt die Behauptung doch für alle a:

Satz 23 *Sind k und $m > 0$ natürliche Zahlen, so dass m quadratfrei ist und $k \equiv 1 \pmod{\varphi(m)}$, so gilt für alle ganzen Zahlen a*

$$a^k \equiv a \pmod{m}.$$

Beweis. Eine quadratfreie natürliche Zahl ist ein Produkt von verschiedenen Primzahlen, d. h.

$$m = p_1 \dots p_r.$$

Nach Satz 22 ist

$$\varphi(m) = (p_1 - 1) \dots (p_r - 1).$$

Für jeden Primfaktor p_i von m gilt $p_i - 1 \mid \varphi(m) \mid k - 1$, also $k = l_i(p_i - 1) + 1$. Ist a teilerfremd zu p_i, so gilt nach dem Satz von Fermat

$$a^k = (a^{l_i})^{p_i - 1} a \equiv a \pmod{p_i}.$$

Ist a nicht teilerfremd zu p_i, so gilt ebenfalls

$$a^k \equiv a \pmod{p_i},$$

denn in diesem Fall sind beide Seiten kongruent zu Null. Die Zahl $a^k - a$ ist also durch die paarweise teilerfremden Zahlen p_i teilbar und somit nach Satz 5(iv) auch durch m. □

Pohlig und Hellmann haben Ende der siebziger Jahre ein Verschlüsselungsverfahren durch Potenzieren vorgeschlagen. Zunächst wird der Klartext in eine Folge von Restklassen modulo einer quadratfreien natürlichen Zahl m umgewandelt. Damit Zeichen nicht anhand ihrer Häufigkeit erkannt werden

können, verschlüsselt man nicht Zeichen für Zeichen, sondern setzt die Zahlencodes eines Textabschnitts zu einer einzigen Zahl zusammen, die natürlich kleiner als m sein muss. Im zweiten Schritt werden die so entstandenen Restklassen nicht wie in Abschnitt 6 mit einer festen Restklasse multipliziert, sondern mit einem festen Exponenten d potenziert. Der Restklasse $[x]_m$ wird also die Restklasse $[y]_m$ mit

$$y \equiv x^d \pmod{m}$$

zugeordnet. Zum Entschlüsseln braucht man eine natürliche Zahl e, so dass

$$de \equiv 1 \pmod{\varphi(m)}$$

ist, denn für alle x und die zugehörigen y gilt

$$y^e \equiv x^{de} \equiv x \pmod{m}$$

nach Satz 23, weil m quadratfrei ist.

Damit ein Entschüsselungsexponent e existiert, muss man natürlich d teilerfremd zu $\varphi(m)$ wählen. Wenn man d durch einen anderen Vertreter derselben Restklasse modulo $\varphi(m)$ ersetzt, so ergibt sich nach Satz 23 die selbe Verschlüsselung. Es kommt beim Verschlüsselungsexponenten also darauf an, eine prime Restklasse modulo $\varphi(m)$ zu wählen. Dafür gibt es im Prinzip $\varphi(\varphi(m))$ verschiedene Möglichkeiten. Man sollte aber nicht $d \equiv 1 \pmod{\varphi(m)}$ wählen, weil dann die Verschlüsselung gar nichts bewirken würde.

Bei allen Geheimcodes besteht die Gefahr, dass der Schlüssel in unbefugte Hände gerät. Man braucht den möglichen Absendern geheimer Nachrichten natürlich nur die Zahlen m und d mitteilen und kann den Entschlüsselungsexponenten e geheimhalten. (Dabei sollte man nicht den Verschlüsselungsexponenten $d \equiv -1 \pmod{\varphi(m)}$ wählen, weil d dann auch der Entschlüsselungsexponent wäre.) Ist m eine Primzahl, so nützt die Geheimhaltung von e nichts, denn wenn ein Codeknacker von einem unachtsamen Absender die Zahlen m und e in Erfahrung gebracht hat, ist es für ihn ein Leichtes, $\varphi(m) = m - 1$ zu berechnen und die Kongruenz

$$de \equiv 1 \pmod{(m-1)}$$

nach e aufzulösen.

Ende der siebziger Jahre bemerkten Rivest, Shamir und Adlemann, dass bei zusammengesetzten quadratfreien Zahlen m die Dinge völlig anders liegen und man die Zahlen m und d getrost der ganzen Welt bekanntgeben kann. Dadurch wurde die “public key cryptography” (man spricht auch von

RSA-Verschlüsselung) praktisch interessant und ist heute bei der sicheren Datenübertragung im Internet weit verbreitet.

Will man einen öffentlichen Schlüssel herstellen, so wählt man zwei große Primzahlen p und q und setzt $m = pq$. Dann wählt man d teilerfremd zu $\varphi(m) = (p-1)(q-1)$ und veröffentlicht m und d (aber weder p noch q noch $\varphi(m)$). Für den eigenen Gebrauch findet man den Entschlüsselungsexponenten e als Lösung der Kongruenz

$$de \equiv 1 \pmod{(p-1)(q-1)}.$$

Ohne die Kenntnis von p und q kann ein potentieller Codeknacker diese Rechnung nicht nachvollziehen. Zwar wurden immer schnellere Algorithmen gefunden, um eine gegebene zusammengesetzte Zahl in ihre Primfaktoren zu zerlegen (man sagt auch „zu faktorisieren“), aber sie sind immer noch um Größenordnungen langsamer als Algorithmen (sogenannte Primzahltests), die püfen, ob eine Zahl Primzahl ist. Die Sicherheit des Verfahrens beruht auf der Vermutung, dass es keine Faktorisierungsalgorithmen geben kann, die ähnlich schnell wie Primzahltests arbeiten. Allerdings kann das bisher niemand mathematisch beweisen.

11 Die Ordnung modulo m

Es sei m eine positive natürliche Zahl. Um den Rest einer Potenz bei Division durch m möglichst effektiv zu bestimmen, kann man den Satz von Euler benutzen (wenn man $\varphi(m)$ kennt, was für den Absender beim RSA-Verfahren natürlich nicht der Fall ist). Um z. B. den Rest von 4^{2006} bei Division durch $91 = 7{\cdot}13$ zu bestimmen, kann man zunächst $\varphi(7{\cdot}13) = 6{\cdot}12 = 72$ berechnen. Durch Division mit Rest findet man $2006 = 72 \cdot 27 + 62$, so dass

$$4^{2006} = (4^{72})^{27}4^{62} \equiv 4^{62} \pmod{91}.$$

Wenn man aber bemerkt, dass $4^6 \equiv 1 \pmod{91}$, so findet man durch Division mit Rest $2006 = 6 \cdot 334 + 2$, und man kommt schneller auf das Ergebnis

$$4^{2006} = (4^6)^{334}4^2 \equiv 4^2 \equiv 16 \pmod{91}.$$

Definition 8 *Es sei m eine positive natürliche Zahl und a eine zu m teilerfremde ganze Zahl. Die Ordnung von a modulo m ist die kleinste positive natürliche Zahl n, so dass*

$$a^n \equiv 1 \pmod{m}.$$

Zur Abkürzung schreiben wir $n = \mathrm{ord}_m(a)$.

Es ist klar, dass $\mathrm{ord}_m(a) \leq \varphi(m)$ und dass die Ordnung von a modulo m nur von der (primen) Restklasse $[a]_m$ abhängt, denn sie ist die kleinste positive natürliche Zahl n, so dass $[a]_m^n = [1]_m$.

Beispiel. Es sei $m = 15$, so dass $\varphi(m) = 8$. Zur Bestimmung der Ordnungen der primen Restklassen modulo m berechnen wir ihre Potenzen:

k	0	1	2	3	4	5	6	7
$[2^k]_{15}$	1	2	4	8	1	2	4	8
$[7^k]_{15}$	1	7	4	13	1	7	4	13
$[11^k]_{15}$	1	11	1	11	1	11	1	11
$[14^k]_{15}$	1	14	1	14	1	14	1	14

Die Zahlen 2, 7 und 8 haben also die Ordnung 4, die Zahlen 4, 11 und 14 haben die Ordnung 2, und die Zahl 1 hat die Ordnung 1 modulo 15.

Lemma 2 *(i) Ist $ab \equiv 1 \pmod m$, so gilt*

$$\mathrm{ord}_m(a) = \mathrm{ord}_m(b).$$

(ii) Es sei $n = \mathrm{ord}_m(a)$. Für beliebige k, $l \in \mathbb{N}$ gilt:

$$a^k \equiv a^l \pmod m \qquad \Longleftrightarrow \qquad k \equiv l \pmod n.$$

Beweis. (i) Für alle k gilt $a^k b^k \equiv 1 \pmod m$. Ist $a^k \equiv 1 \pmod m$, so ist auch $b^k \equiv 1 \pmod m$, und umgekehrt.

(ii) Wir können annehmen, dass $k \geq l$. Wegen der Existenz von b wie oben ist die gegebene Kongruenz äquivalent zu

$$a^{k-l} \equiv 1 \pmod m.$$

Damit wird der Beweis auf den Fall $l = 0$ zurückgeführt.

Durch Division mit Rest finden wir natürliche Zahlen q und $r < e$, so dass $k = nq + r$. Nach der Definition der Ordnung gilt

$$a^k = (a^n)^q a^r \equiv a^r \pmod m.$$

Ist $n \mid k$, so ist $r = 0$, und es folgt $a^k \equiv 1 \pmod m$. Ist umgekehrt diese Kongruenz erfüllt, so folgt $a^r \equiv 1 \pmod m$, aber dann kann r nicht größer als Null sein, weil das der Minimalität von n widersprechen würde, also $n \mid k$. □

Aus dem Lemma folgt übrigens $\mathrm{ord}_m(a) \mid \varphi(m)$.

Satz 24 *(i) Ist* $\operatorname{ord}_m(a) = n$*, so gilt für alle* $l \in \mathbb{N}$

$$\operatorname{ord}_m(a^l) = \frac{n}{\operatorname{ggT}(n,l)}.$$

(ii) Ist $a \equiv a_1 a_2 \pmod m$ *und* $\operatorname{ord}_m(a) = n$, $\operatorname{ord}_m(a_1) = n_1$, $\operatorname{ord}_m(a_2) = n_2$*, so gilt*

$$n \mid \operatorname{kgV}(n_1, n_2).$$

Sind die Exponenten einer Primzahl p *in den Primfaktorzerlegungen von* n_1, n_2 *und* n *gleich* e_1, e_2 *bzw.* e*, so gilt*

$$e_1 \neq e_2 \qquad \Longleftrightarrow \qquad e = \max(e_1, e_2).$$

Sind insbesondere n_1 *und* n_2 *teilerfremd, so ist* $n = n_1 n_2$.

Beweis. (i) Nach dem Lemma gilt $(a^l)^k \equiv 1 \pmod m$ genau dann, wenn $n \mid kl$, wenn also kl gemeinsames Vielfaches von n und l ist, d. h. wenn $\operatorname{kgV}(n,l) \mid kl$. Schreiben wir $\operatorname{kgV}(n,l) = nl/\operatorname{ggT}(n,l)$ nach Satz 6, so folgt die Behauptung mit Aufgabe 1(c).

(ii) Ist k ein gemeinsames Vielfaches von n_1 und n_2, so gilt $a^k \equiv a_1^k a_2^k \equiv 1 \pmod m$, und die erste Behauptung folgt.

Da a_1 teilerfremd zu m ist, gibt es ein a_1', so dass $a_1 a_1' \equiv 1 \pmod m$, also $a a_1' \equiv a_2 \pmod m$, und aus dem Bewiesenen folgt

$$n_2 \mid \operatorname{kgV}(n_1, n), \qquad \text{und analog} \qquad n_1 \mid \operatorname{kgV}(n_2, n).$$

Für jede Primzahl p gilt also nach Aufgabe 13(a)

$$e \leq \max(e_1, e_2), \qquad e_2 \leq \max(e, e_1), \qquad e_1 \leq \max(e, e_2).$$

Hieraus folgt die Formel für e im Fall $e_1 \neq e_2$. Sind n_1 und n_2 teilerfremd, so gilt sie in jedem Fall, da dann eine der Zahlen e_1 und e_2 gleich Null ist. □

Satz 25 *Sind* a *und* g *teilerfremd zu der natürlichen Zahl* m *und hat* g *die maximal mögliche Ordnung modulo* m*, so ist* $\operatorname{ord}_m(a) \mid \operatorname{ord}_m(g)$.

Beweis. Es sei p eine Primzahl, e ihr Exponent in der Primfaktorzerlegung von $n = \operatorname{ord}_m(a)$ und f ihr Exponent in $l = \operatorname{ord}_m(g)$. Schreiben wir $n = p^e n'$ und $l = p^f l'$, so ist nach Satz 24(i)

$$\operatorname{ord}_m(a^{n'}) = p^e, \qquad \operatorname{ord}_m(g^{p^f}) = l',$$

und nach Satz 24(ii) folgt

$$\mathrm{ord}_m(a^{n'}g^{p^f}) = p^e l'.$$

Wegen der Maximalität von l folgt $p^e \leq p^f$, also $e \leq f$. Da p beliebig war, folgt $n \mid l$. □

Jetzt betrachten wir genauer den Fall, dass $m = p$ eine Primzahl ist. Es sei n die maximal mögliche Ordnung modulo p. Nach Satz 25 gilt für alle nicht durch p teilbaren Zahlen a, dass

$$a^n \equiv 1 \pmod{p}.$$

Wie bei der Folgerung aus dem Satz von Fermat schließen wir, dass für alle ganzen Zahlen a gilt

$$a^{n+1} \equiv a \pmod{p},$$

oder anders ausgedrückt

$$[a]_p^{n+1} = [a]_p,$$

d. h. jede Restklasse modulo p ist eine Nullstelle[4] des Polynoms

$$X^{n+1} - X, \qquad \text{also} \qquad X^{n+1} + [-1]_p X$$

mit Koeffizienten im Körper $\mathbb{Z}/p\mathbb{Z}$.

Satz 26 *Ist $f(X)$ ein Polynom mit Koeffizienten in einem Körper und ist das Element C des Körpers eine Nullstelle (oder Wurzel) von $f(X)$, so ist $f(X)$ ein Vielfaches des Polynoms $X - C$.*

Beweis. Wir können das Polynom in der Form

$$f(X) = A_0 + A_1 X + A_2 X^2 + \dots$$

mit Körperelementen A_0, A_1, A_2, … schreiben. Es gilt

$$f(X) = f(X) - f(C) = A_1(X - C) + A_2(X^2 - C^2) + \dots$$

Aus jedem Term können wir $X - C$ ausklammern, denn

$$X^k - C^k = (X - C)(X^{k-1} + X^{k-2}C + \dots + C^{k-1}).$$

Es folgt, dass

$$f(X) = (X - C)g(X)$$

[4]Die Nullstellen nennt man traditionell auch Wurzeln des Polynoms, weil man sie für Polynome bis zum Grad 4 durch wiederholtes Ziehen von Wurzeln finden kann.

mit einem Polynom $g(X)$. □

Die Koeffizienten A_i des Polynoms $f(X)$ sind eindeutig bestimmt, und das höchste i, für das $A_i \neq 0$ ist, nennt man den Grad des Polynoms. Der Grad von $g(X)$ ist um eins kleiner als der von $f(X)$. Durch Induktion zeigt man:

Folgerung 6 *Ein Polynom vom Grad k mit Koeffizienten in einem Körper hat in diesem Körper höchstens k Nullstellen.*

Daraus ergibt sich ein erstaunlicher Fakt:

Satz 27 *Ist p eine Primzahl, so gibt es eine Zahl g mit* $\mathrm{ord}_p(g) = p - 1$.

(Die primen Restklassen modulo p sind dann $[1]_p$, $[g]_p$, $[g^2]_p$, …, $[g^{p-1}]_p$.)

Beweis. Ist n die maximale Ordnung modulo p, so ist jedes Element des Körpers $\mathbb{Z}/p\mathbb{Z}$ eine Wurzel des Polynoms $X^{n+1} - X$. Die Anzahl der Wurzeln ist aber durch den Grad des Polynoms, nämlich $n + 1$, beschränkt, d. h. $p \leq n + 1$. Andererseits wissen wir, dass $n \leq \varphi(p) = p - 1$, also $n = p - 1$. □

Man nennt eine Zahl g mit $\mathrm{ord}_m(g) = \varphi(m)$ eine Primitivwurzel modulo m. Leider gibt es kein besseres Verfahren zur Auffindung einer Primitivwurzel als bloßes Durchprobieren. Man kann übrigens zeigen, dass es genau dann eine Primitivwurzel modulo m gibt, wenn m gleich 2 oder 4 oder einer ungerade Primzahlpotenz oder dem Doppelten einer solchen ist.

Man kann das Polynom $X^{n+1} - X = X(X^n - 1)$ über jedem Körper betrachten, und seine Wurzeln sind 0 und die $n$ten Einheitswurzeln, d. h. die Elemente C mit $C^n = 1$. Die $n$ten Einheitswurzeln sind abgeschlossen unter Multiplikation und Inversenbildung (man sagt, sie bilden eine Gruppe), und es gilt ein Analogon von Satz 25. Genau wie oben folgt, dass es eine n-te Einheitswurzel gibt (eine sogenannte Primitivwurzel), so dass alle anderen ihre Potenzen sind.

12 Brüche in Ziffernsystemen

Bekanntlich lässt sich jede reelle Zahl als unendlicher Dezimalbruch schreiben, z. B.

$$\frac{15}{13} = 1{,}15384\ldots, \qquad \sqrt{2} = 1{,}41421\ldots, \qquad \pi = 3{,}14159\ldots$$

Dies gilt auch für Ziffernsysteme mit anderer Grundzahl g. Ist $g > 1$ eine natürliche Zahl und sind Ziffern $c_k \in \{0, 1, \ldots, g-1\}$ für alle $k \in \mathbb{Z}$ gegeben,

wobei c_k für genügend große positive k gleich Null sind, so hat die nach rechts unendliche Reihe

$$\cdots + c_2 g^2 + c_1 g + c_0 + c_{-1} g^{-1} + c_{-2} g^{-2} + \ldots$$

einen Sinn: Man kann zeigen, dass die Folge der Teilsummen

$$x_n = \cdots + c_2 g^2 + c_1 g + c_0 + c_{-1} g^{-1} + c_{-2} g^{-2} + \cdots + c_{-n} g^{-n}$$

gegen eine reelle Zahl x konvergiert und sich so jede positive reelle Zahl auf eindeutige Weise darstellen lässt, wenn man Ziffernfolgen, bei denen die Ziffern c_k für alle genügend großen negativen k gleich $g-1$ sind, nicht benutzt.

Satz 28 *Die Darstellung einer reellen Zahl x im Ziffernsystem mit der Grundzahl g ist genau dann periodisch, wenn x eine rationale Zahl ist. Dabei ist die Periodenlänge von $\frac{a}{b}$ kleiner als $|b|$.*

Beweis. Ist m eine ganze Zahl, so ergibt sich die Ziffernfolge von $g^m x$ aus der Ziffernfolge von x durch Verschiebung um m Stellen. Ist also eine reelle Zahl x durch einen periodischen g-adischen Bruch gegeben, so können wir zum Beweis ihrer Rationalität annehmen, dass x keine Vorperiode hat, d. h. dass die Periode sofort nach dem Komma beginnt. Die Periodenlänge sei l. Die Stellen vor dem Komma stellen eine natürliche Zahl dar, die wir von x abziehen können. Wir brauchen also nur den Fall zu betrachten, dass

$$x = c_{-1} g^{-1} + c_{-2} g^{-2} + \ldots,$$

wobei $c_{-k} = c_{-k-l}$ für alle k gilt. Nun fassen wir jeweils l Summanden zusammen und klammern eine geeignete Potenz von g aus:

$$x = (c_{-1} g^{-1} + \cdots + c_{-l} g^{-l}) + (c_{-l-1} g^{-1} + \cdots + c_{-2l} g^{-l}) g^{-l} + \ldots$$

Wegen der Periodizität sind die Ausdrücke in allen Klammern gleich. Bezeichnen wir diese mit

$$q = c_{-1} g^{-1} + c_{-2} g^{-2} + \cdots + c_{-l} g^{-l},$$

so folgt

$$x_{kl} = q(1 + g^{-l} + g^{-2l} + \cdots + g^{-(k-1)l}).$$

Mit der Formel aus Beispiel 1 können wir die geometrische Reihe auf der rechten Seite berechnen:

$$x_{kl} = q \, \frac{1 - (g^{-l})^k}{1 - g^{-l}}.$$

Da eine Teilfolge einer konvergenten Folge gegen denselben Grenzwert konvergiert, ist

$$x = \lim_{k\to\infty} x_{kl}.$$

Nach den Rechenregeln für Grenzwerte gilt

$$x = q\,\frac{1 - \lim_{k\to\infty}(g^{-l})^k}{1 - g^{-l}},$$

und wegen $g^{-l} < 1$ folgt

$$x = \frac{q}{1-g^{-l}} = \frac{qg^l}{g^l - 1} = \frac{c_{-1}g^{l-1} + c_{-2}g^{l-2} + \cdots + c_{-l}}{g^l - 1},$$

was eine gebrochene Zahl ist.

Umgekehrt sei eine rationale Zahl x gegeben. Durch Subtraktion einer geeigneten natürlichen Zahl können wir den Beweis auf den Fall $0 \le x < 1$ zurückführen, d. h. $x = \frac{a}{b}$ mit ganzen Zahlen $0 \le a < b$. Praktisch bestimmt man die Ziffernfolge von $\frac{a}{b}$ durch schriftliche Division im Ziffernsystem mit der Grundzahl g. Ohne Zuhilfenahme der Regeln der schriftlichen Division lässt sich dies wie folgt beschreiben. Nach Satz 2 gibt es ganze Zahlen q_1 und r_1, so dass

$$ga = q_1 b + r_1, \qquad 0 \le r_1 < b. \tag{5}$$

Dabei gilt

$$0 \le q_1 b \le ga < gb, \qquad \text{also} \qquad 0 \le q_1 < g.$$

Wir können nun mit q_1 anstelle von a fortfahren und erhalten nacheinander natürliche Zahlen $q_k < g$ und $r_k < b$, so dass

$$\begin{aligned} ga &= q_1 b + r_1, \\ gr_1 &= q_2 b + r_2, \\ gr_2 &= q_3 b + r_3, \\ &\dots \end{aligned}$$

Wir dividieren alle Gleichungen durch gb und erhalten

$$\begin{aligned} \frac{a}{b} &= \left(q_1 + \frac{r_1}{b}\right) g^{-1}, \\ \frac{r_1}{b} &= \left(q_2 + \frac{r_2}{b}\right) g^{-1}, \\ \frac{r_2}{b} &= \left(q_3 + \frac{r_3}{b}\right) g^{-1}, \\ &\dots \end{aligned}$$

Durch fortlaufendes Einsetzen folgt

$$\begin{aligned}\frac{a}{b} &= \left(q_1 + \frac{r_1}{b}\right) g^{-1} = q_1 g^{-1} + \left(q_2 + \frac{r_2}{b}\right) g^{-2} = \dots \\ &= q_1 g^{-1} + q_2 g^{-2} + \dots + \left(q_n + \frac{r_n}{b}\right) g^{-n}.\end{aligned}$$

Die Folge

$$x_n = q_1 g^{-1} + q_2 g^{-2} + \dots + q_n g^{-n}$$

konvergiert gegen $\frac{a}{b}$, denn

$$0 \le \frac{a}{b} - x_n = \frac{r_n}{b} g^{-n} < g^{-n},$$

und die Konvergenz folgt aus dem Einschließungskriterium.

Tritt irgendwann der Rest $r_n = 0$ auf, so sind von da an alle Reste (und folglich auch alle Ziffern q_k) gleich Null. Andernfalls gibt es nur $b-1$ Möglichkeiten für die Reste, also tritt irgendwann ein Rest r_n auf, der schon früher vorgekommen ist, d. h. $r_n = r_{n-l}$ mit $l < n$. Dann folgt $r_{n+1} = r_{n-l+1}$, $r_{n+2} = r_{n-l+2}$ usw., und wir haben eine Periode der Länge l. Da die Reste $r_1, \dots, r_{n-1}$ verschieden sind, gilt $n \le b$. □

Es ist klar, dass für periodische Reste r_k auch die Ziffern q_k periodisch sind, aber die Umkehrung ist nicht so offensichtlich. Sie stimmt trotzdem, denn die Reste sind eindeutig durch die nachfolgenden Ziffern bestimmt:

$$\frac{r_n}{b} = q_{n+1} g^{-1} + q_{n+2} g^{-2} + \dots$$

Satz 29 *Die natürlichen Zahlen a und $g > 1$ seien teilerfremd zu der natürlichen Zahl b. Dann ist die minimale Periodenlänge von $\frac{a}{b}$ im Ziffernsystem mit der Grundzahl g gleich* $\operatorname{ord}_b(g)$*, und es tritt keine Vorperiode auf.*

Beweis. Nach Gleichung (5) gilt

$$ga \equiv r_1 \pmod{b},$$

und wegen der Teilerfremdheit von g und a zu b folgt, dass auch r_1 teilerfremd zu b ist. Analog zeigt man durch vollständige Induktion, dass alle r_k teilerfremd zu b sind.

Weiter gilt für $k > l$

$$r_k \equiv g r_{k-1} \equiv g^2 r_{k-2} \equiv \dots \equiv g^l r_{k-l} \pmod{b}.$$

Setzen wir $r_0 = a$, so gilt das sogar für $k \ge l$. Wegen $r_k \in \{0, 1, \dots, b-1\}$ ist

$$r_k = r_{k-l} \qquad \Longleftrightarrow \qquad r_k \equiv r_{k-l} \pmod{b},$$

und wegen der Teilerfremdheit der r_k zu b ist dies genau dann der Fall, wenn $g^l \equiv 1 \pmod{b}$, also wenn l ein Vielfaches von $\mathrm{ord}_b(g)$ ist. □

Die Periodenlänge eines unkürzbaren Bruches $\frac{a}{b}$ ist somit nicht größer als $\varphi(b)$, und sie erreicht diesen Wert, wenn die Grundzahl g eine Primitivwurzel modulo b ist.

Zsigmondy hat im Jahre 1892 gezeigt, dass es für gegebene natürliche Zahlen $g > 1$ und $n \geq 1$ (außer für $g = 2$, $n = 6$) mindestens eine Primzahl p mit $\mathrm{ord}_p(g) = n$ gibt. Also kommt bei den Brüchen mit Primzahlnenner in einem beliebigen Ziffernsystem mit einer Ausnahme jede beliebige Periodenlänge vor.

Artin hat vermutet, dass es für jede natürliche Zahl $g > 1$, die keine Quadratzahl ist, eine Primzahl p gibt, so dass g eine Primitivwurzel modulo p ist, d. h. dass die Periode von $\frac{1}{p}$ im Zahlensystem mit der Grundzahl g gleich $p - 1$ ist.

Beispiel. Es gilt

$$\begin{aligned}
\frac{1}{7} &= 0{,}\overline{142857}, & 142 + 857 &= 999,\\
\frac{1}{13} &= 0{,}\overline{076923}, & 067 + 932 &= 999,\\
\frac{1}{17} &= 0{,}\overline{0588235294117647}, & 05882352 + 94117647 &= 99999999.
\end{aligned}$$

Wir wollen für eine beliebige Primzahl p zeigen, dass der Bruch $\frac{1}{p}$ in jedem Ziffernsystem, wo seine minimale Periodenlänge l gerade ist, diese Eigenschaft hat. In den Bezeichnungen aus dem Beweis von Satz 28 ist

$$\frac{1}{p} = \frac{qg^l}{g^l - 1}.$$

Wir zerlegen wir die Periode der Länge $l = 2k$ in zwei Halbperioden, das heißt

$$\begin{aligned}
qg^l &= c_{-1}g^{l-1} + c_{-2}g^{-2} + \cdots + c_{-l}\\
&= (c_{-1}g^{k-1} + \cdots + c^{-k})g^k + (c_{-k-1}g^{k-1} + \cdots + c_{-2k}).
\end{aligned}$$

Die Klammerausdrücke sind k-stellige natürliche Zahlen

$$e = c_{-1}g^{k-1} + \cdots + c_{-k}, \qquad f = c_{-k-1}g^{k-1} + \cdots + c_{-2k}.$$

Durch Einsetzen ergibt sich

$$\frac{1}{p} = \frac{eg^k + f}{g^{2k} - 1}, \qquad \text{d. h.} \qquad p(eg^k + f) = g^{2k} - 1 = (g^k - 1)(g^k + 1).$$

Als Primzahl muss p einen der beiden Faktoren teilen. Wäre $p \mid g^k - 1$, so wäre $g^k \equiv 1 \pmod{p}$, was der Aussage $\mathrm{ord}_p(g) = 2k$ von Satz 29 widerspricht. Somit ist

$$p \mid g^k + 1, \qquad g^k - 1 \mid eg^k + f.$$

Wegen $eg^k + f = e(g^k - 1) + (e + f)$ folgt

$$g^k - 1 \mid e + f.$$

Die Zahlen e und f sind höchstens k-stellig im Ziffernsystem bezüglich der Grundzahl g, also höchstens gleich $g^k - 1$, so dass

$$e + f \leq 2(g^k - 1),$$

wobei Gleichheit nur für $e = f = g^k - 1$ eintreten kann. Dies kann aber nicht sein, weil sonst auch k eine Periode wäre, die kleiner als l ist. Wir sehen also, dass $e + f$ ein Vielfaches von $g^k - 1$, aber kleiner als das Doppelte ist, und somit folgt

$$e + f = g^k - 1,$$

wie behauptet.

13 Quadratische Reste

Es sei $m > 1$ eine natürliche Zahl und a eine zu m teilerfremde ganze Zahl. Traditionell sagt man, dass a ein quadratischer Rest modulo m ist, wenn die Kongruenz

$$x^2 \equiv a \pmod{m}$$

lösbar ist. Dies ist natürlich genau dann der Fall, wenn die prime Restklasse $[a]_m$ das Quadrat einer anderen Restklasse ist. Natürlich wird eine Lösung x auch teilerfremd zu m sein. Manchmal benutzt man den Ausdruck „quadratischer Rest“ auch für die Restklasse von a. Um alle quadratischen Reste modulo m zu finden, muss man sämtliche Restklassen quadrieren.

Beispiel. $m = 36$.

$[x]_{36}$	± 1	± 5	± 7	± 11	± 13	± 17
$[x^2]_{36}$	1	25	13	13	25	1

Die Zahlen (besser: Restklassen) in der zweiten Zeile sind die quadratischen Reste modulo 36.

Wie kann man feststellen, ob eine gegebene prime Restklasse quadratischer Rest ist, ohne eine vollständige Liste zu berechnen? Dieses Problem

wird uns eine ganze Weile beschaftigen, wobei wir uns aber auf den Fall beschränken, dass $m = p$ eine Primzahl ist. Eine erste Antwort lautet wie folgt.

Satz 30 (Euler) *Es sei $p \neq 2$ eine Primzahl und a teilerfremd zu p. Dann ist a genau dann ein quadratischer Rest modulo p, wenn*

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Man beachte, dass der Exponent wegen $p \neq 2$ eine natürliche Zahl ist. *Beweis.* Es sei a ein quadratischer Rest, so dass es eine ganze Zahl x mit $x^2 \equiv a \pmod{p}$ gibt. Dann gilt

$$a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod{p}$$

nach dem Satz von Fermat.

Umgekehrt sei die Kongruenz aus dem Satz erfüllt. Nach Satz 27 gibt es eine Primitivwurzel g modulo p, so dass

$$a \equiv g^k \pmod{p}$$

für eine geeignete natürliche Zahl k. Es folgt

$$g^{k\,\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \equiv 1 \pmod{p},$$

und nach Lemma 2 ist $k\,\frac{p-1}{2}$ ein Vielfaches von $\mathrm{ord}_p(g) = p - 1$, also

$$2(p-1) \mid k(p-1).$$

Nach Aufgabe 1(c) muss k gerade sein, also $k = 2n$ und

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

d. h. a ein quadratischer Rest modulo p. □

Es herrscht eine gewisse Ordnung in der Verteilung von quadratischen und nichtquadratischen[5] Resten.

Satz 31 *Modulo einer Primzahl $p \neq 2$ gilt: Das Produkt zweier quadratischer Reste wie auch zweier nichtquadratischer Reste ist ein quadratischer Rest. Das Produkt eines quadratischen mit einem nichtquadratischen Rest ist ein nichtquadratischer Rest.*

Es gibt genausoviele quadratische wie nichtquadratische Reste, nämlich $\frac{p-1}{2}$.

[5] Anstelle von „nichtquadratischer Rest“ hat sich auch die absurde Bezeichnung „quadratischer Nichtrest“ eingebürgert.

Beweis. Ist $a \equiv x^2$ und $b \equiv y^2 \pmod{p}$, so gilt $ab \equiv (xy)^2 \pmod{p}$, also ist das Produkt zweier quadratischer Reste ein quadratischer Rest.

Um zu beweisen, dass das Produkt eines quadratischen Restes a und eines nichtquadratischen Restes c ein nichtquadratischer Rest ist, nehmen wir das Gegenteil an, also $a \equiv x^2$ und $ac \equiv y^2 \pmod{p}$. Da x teilerfremd zu p ist, gibt es ein z mit $xz \equiv 1 \pmod{p}$, so dass

$$(yz)^2 \equiv acz^2 \equiv (xz)^2 c \equiv c \pmod{p},$$

aber c sollte ja nichtquadratisch sein (Widerspruch).

Bisher wissen wir nicht, ob es überhaupt nichtquadratische Reste modulo p gibt. Die Gleichung $X^2 = [a]_p$ hat nach Folgerung 6 im Körper der Restklassen modulo p höchstens 2 Lösungen, und wenn $[x]_p$ eine Lösung ist, so ist auch $[-x]_p$ eine Lösung. Da p ungerade ist, gilt $x \not\equiv -x \pmod{p}$, also gibt es entweder zwei oder keine Lösung. Wir haben somit jeder der $p-1$ primen Restklassen $[x]_p$ eine quadratische Restklasse $[a]_p$ zugeordnet, und dabei wird jede quadratische Restklasse $[a]_p$ immer zwei primen Restklassen zugeordnet. Es gibt also genau $\frac{p-1}{2}$ quadratische Restklassen, und die verbleibenden $\frac{p-1}{2}$ primen Restklassen sind nichtquadratisch.

Die Multiplikation mit einem festen nichtquadratischen Rest permutiert die primen Restklassen und ordnet nach dem bereits Bewiesenen jedem quadratischen Rest einen nichtquadratischen Rest zu. Weil es von beiden gleichviele gibt, muss sie jedem nichtquadratischen Rest einen quadratischen zuordnen. Also ist das Produkt von zwei nichtquadratischen Resten ein quadratischer Rest. □

Man kann auch einen Beweis mit Hilfe einer Primitivwurzel g geben. Die primen Restklassen sind $[g^0]_p$, $[g^1]_p$, $\ldots$, $[g^{p-1}]_p$, und im Beweis von Satz 30 haben wir gesehen, das g^k genau dann quadratischer Rest ist, wenn k gerade ist. Somit folgen die Multiplikationsregeln für quadratische und nichtquadratische Reste

×	q	n
q	q	n
n	n	q

aus den Additionsregeln für gerade und ungerade Zahlen.

Satz 32 *Es sei $p \neq 2$ eine Primzahl.*

(i) Die Zahl -1 ist genau dann quadratischer Rest modulo p, wenn

$$p \equiv 1 \pmod{4}.$$

(ii) Die Zahl 2 *ist genau dann quadratischer Rest modulo* p*, wenn*

$$p \equiv 1 \quad \textit{oder} \quad p \equiv -1 \pmod 8.$$

Beweis. (i) Es sei $r = \frac{p-1}{2}$. Nach Satz 30 ist -1 genau dann quadratischer Rest, wenn $(-1)^r \equiv 1 \pmod p$, was wegen $p > 2$ genau dann eintritt, wenn $(-1)^r = 1$. Man prüft leicht nach, dass

$$\begin{aligned} p \equiv 1 \pmod 4 &\iff r \text{ gerade}, \\ p \equiv 3 \pmod 4 &\iff r \text{ ungerade}, \end{aligned}$$

und die Behauptung folgt.

(ii) Es sei

$$n = 2 \cdot 4 \cdots (p-3)(p-1).$$

Der Faktor, der am nächsten bei $\frac{p}{2}$ liegt, ist entweder $r < \frac{p}{2}$ oder $r + 1 = p - r > \frac{p}{2}$, je nachdem, welche dieser beiden Zahlen gerade ist. Ziehen wir aus jedem der r Faktoren eine 2 heraus, so erhalten wir

$$n = 2^r r!.$$

Ersetzen wir hingegen jeden Faktor der Form $p-k$, der größer als $\frac{p}{2}$ ist, durch $-k$, so erhalten wir

$$n \equiv 2 \cdot 4 \cdots (-3)(-1) \pmod p.$$

Durch Umordnen ergibt sich

$$\begin{aligned} n &\equiv (-1)2(-3)4 \cdots (-1)^r r \\ &\equiv (-1)^1 1 \cdot (-1)^2 2 \cdots (-1)^r r \equiv (-1)^s r! \pmod p, \end{aligned}$$

wobei

$$s = 1 + 2 + \cdots + r = \frac{r(r+1)}{2} = \frac{p^2 - 1}{8}.$$

Vergleichen wir beide Ausdrücke für n, so können wir den Faktor $r!$ kürzen, weil er teilerfremd zu p ist:

$$2^r \equiv (-1)^s \pmod p.$$

Nach Satz 30 ist 2 genau dann quadratischer Rest, wenn s gerade ist, und wegen

$$\frac{(8k \pm 1)^2 - 1}{8} = 2k(4k \pm 1), \qquad \frac{(8k \pm 3)^2 - 1}{8} = 2k(4k \pm 3) + 1$$

folgt, dass

$$\begin{aligned} p &\equiv \pm 1 \pmod 8 \quad \Longleftrightarrow \quad s \text{ gerade,} \\ p &\equiv \pm 3 \pmod 8 \quad \Longleftrightarrow \quad s \text{ ungerade.} \end{aligned}$$

□

Als Anwendung untersuchen wir die Frage, welche natürlichen Zahlen sich als Summe von zwei Quadraten schreiben lassen, d. h. für welche n die Diophantische Gleichung

$$x^2 + y^2 = n$$

lösbar ist. Durch Reduktion modulo 4 erhält man die Kongruenz

$$x^2 + y^2 \equiv n \pmod 4.$$

Die quadratischen Restklassen modulo 4 sind $[0]_4$ und $[1]_4$, die linke Seite ist also kongruent zu 0, 1 oder 2 modulo 4. Es folgt, dass sich eine natürliche Zahl n mit $n \equiv 3 \pmod 4$ sicher nicht als Summe von zwei Quadraten darstellen lässt.

Satz 33 *Eine Primzahl $p \neq 2$ lässt sich genau dann als Summe von zwei Quadraten schreiben, wenn $p \equiv 1 \pmod 4$ ist.*

Beweis. Lässt sich eine ungerade Primzahl als Summe von zwei Quadraten darstellen, so muss nach den Vorbetrachtungen $p \equiv 1 \pmod 4$ sein.

Umgekehrt sei p irgendeine Primzahl, die dieser Kongruenz genügt. Es sei r die größte natürliche Zahl mit der Eigenschaft $r^2 \leq p$ und M die Menge aller Paare (x, y), wobei $x,\ y \in \{0, 1, \ldots, r\}$. Die Anzahl der Paare in M ist $(r+1)^2 > p$.

Nach Satz 32 gibt es eine ganze Zahl a, so dass

$$a^2 \equiv -1 \pmod p.$$

Die Restklassen der Zahlen $x - ay$ modulo p, wobei (x, y) die Menge M durchläuft, können nicht alle verschieden sein, da es nur p Restklassen gibt. Folglich existieren verschiedene Paare (x_1, y_1) und (x_2, y_2) in M, so dass

$$x_1 - ay_1 \equiv x_2 - ay_2 \pmod p.$$

Setzen wir $x = x_1 - x_2$ und $y = y_1 - y_2$, so ist

$$x \equiv ay \pmod p,$$

und wegen der Wahl von a folgt

$$x^2 \equiv -y^2 \pmod{p},$$

das heißt, $x^2 + y^2$ ist ein Vielfaches von p.

Da die Paare (x_1, y_1) und (x_2, y_2) verschieden sind, ist $x^2 + y^2 > 0$, und wegen $-r \le x \le r$, $-r \le y \le r$ folgt $x^2 < p$ und $y^2 < p$, also $x^2 + y^2 < 2p$. Somit muss $x^2 + y^2 = p$ sein. □

Die Primzahl 2, die wir bisher ausgeschlossen haben, ist natürlich als Summe von zwei Quadraten darstellbar, nämlich $2 = 1^2 + 1^2$.

Satz 34 *Eine natürliche Zahl ist genau dann als Summe von zwei Quadraten darstellbar, wenn jeder Primfaktor q mit der Eigenschaft $q \equiv -1 \pmod 4$ mit geradem Exponenten vorkommt.*

Beweis. Es sei

$$n = p_1^{e_1} \dots p_r^{e_r} q_1^{f_1} \dots q_s^{f_s}$$

die Zerlegung der gegebenen Zahl in Potenzen verschidener Primzahlen, wobei für alle i und j gelte

$$p_i = 2 \quad \text{oder} \quad p_i \equiv 1 \pmod 4, \qquad q_j \equiv -1 \pmod 4.$$

Nach Satz 33 gibt es für jedes i natürliche Zahlen a_i, b_i, so dass $p_i = a_i^2 + b_i^2$. Sind alle f_j gerade, also $f_j = 2k_j$, so folgt

$$n = (a_1^2 + b_1^2)^{e_1} \dots (a_r^2 + b_r^2)^{e_1} (q_1^2 + 0^2)^{k_1} \dots (q_s^2 + 0^2)^{k_s}.$$

Sind zwei Zahlen als Summe von Quadraten darstellbar, so auch ihr Produkt, denn wie wir bei der Lösung von Aufgabe 16 gesehen haben, gilt

$$(a_1^2 + b_1^2)(a_2^2 + b_2^2) = (a_1 a_2 - b_1 b_2)^2 + (a_1 b_2 + b_1 a_2)^2.$$

Dies lässt sich durch vollständige Induktion auf eine beliebige Zahl von Faktoren verallgemeinern.

Umgekehrt sei $n = a^2 + b^2$. Schreiben wir $d = \mathrm{ggT}(a, b)$, so ist $a = da'$, $b = db'$ und $n = d^2 n'$, also $n' = a'^2 + b'^2$. Es genügt zu beweisen, dass in n' keine Primfaktoren q mit $q \equiv -1 \pmod 4$ vorkommen. Es sei also p irgendein Primfaktor von n', so dass

$$a'^2 + b'^2 \equiv 0 \pmod{p}.$$

Wäre b' durch p teilbar, so auch a', aber $\mathrm{ggT}(a', b') = 1$. Also gibt es ein c' mit $b'c' \equiv 1 \pmod p$, und es folgt

$$(a'c')^2 + 1 \equiv 0 \pmod{p},$$

d. h. -1 ist quadratischer Rest modulo p. Nach Satz 33 ist dann $p \equiv 1 \pmod 4$ oder $p = 2$. □

14 Das Jacobi-Symbol

In diesem Abschnitt sei m eine ungerade natürliche Zahl, also $m = 2r + 1$. Ist $a \equiv -a \pmod{m}$, so ist $a \equiv 0 \pmod{m}$. Durch Multiplikation mit -1 werden also die von $[0]_m$ verschiedenen Restklassen paarweise vertauscht.

Definition 9 *Eine Menge $\{h_1, \ldots, h_r\}$ heißt Halbsystem modulo m, wenn die Zahlen 0, h_1, $-h_1$, …, h_r, $-h_r$ paarweise inkongruent modulo m sind.*

Ist a teilerfremd zu m, so gibt es für jedes $i \in \{0, \ldots, r\}$ ein eindeutig bestimmtes $j \in \{0, \ldots, r\}$, so dass $ah_i \equiv \pm h_j \pmod{m}$, wobei auch das Vorzeichen eindeutig bestimmt ist. Es gibt also genau ein $e_i \in \{1, -1\}$, so dass

$$ah_i \equiv e_i h_j \pmod{m}. \tag{6}$$

Wir definieren das Jacobi-Symbol durch

$$\left(\frac{a}{m}\right) = e_1 e_2 \ldots e_r.$$

Es ist klar, dass es nur von der Restklasse von a abhängt.

Beispiel. Die Menge $\{1, 2, 3, 4, 5, 6, 7\}$ ist ein Halbsystem modulo 15.

h	1	2	3	4	5	6	7
$[-h]_{15}$	-1	-2	-3	-4	-5	-6	-7
$[2h]_{15}$	2	4	6	-7	-5	-3	-1
$[7h]_{15}$	7	-1	6	-2	5	-3	4

Es folgt

$$\left(\frac{-1}{15}\right) = -1, \qquad \left(\frac{2}{15}\right) = 1, \qquad \left(\frac{7}{15}\right) = -1.$$

Was passiert, wenn wir ein anderes Halbsystem, z. B. $\{2, 4, 6, 8, 10, 12, 14\}$, benutzen?

Lemma 3 *(i) Das Jacobi-Symbol hängt nicht von der Wahl des Halbsystems ab.*

(ii) Sind a und b teilerfremd zu m, so gilt

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

Beweis. (i) Es sei $\{h'_1, \ldots, h'_r\}$ ein anderes Halbsystem. Durch geeignete Numerieren können wir erreichen, dass für alle i gilt $h'_i \equiv g_i h_i \pmod{m}$ mit $g_i \in \{1, -1\}$. Um die entsprechenden Vorzeichen e'_i für das neue Halbsystem zu bestimmen, multiplizieren wir die Kongruenz (6) mit g_i und erhalten

$$ah'_i \equiv e_i g_i h_j \pmod{m}.$$

Wegen $h_j \equiv g_j h'_j \pmod{m}$ erhalten wir

$$ah'_i \equiv e'_i h'_j \pmod{m}$$

mit

$$e'_i = e_i g_i g_j.$$

Die j ergeben sich aus den i durch eine Permutation der Menge $\{1, \ldots, r\}$. Bilden wir also das Produkt über alle i, so ergibt sich

$$e_1 \ldots e_r = (e'_1 \ldots e'_r)(g_1 \ldots g_r)^2.$$

(ii) Für jedes j gibt es ein k und ein $f_j \in \{1, -1\}$, so dass

$$bh_j \equiv f_j h_k \pmod{m}.$$

Nun gilt

$$abh_i \equiv be_i h_j \equiv e_i f_j h_k \pmod{m}.$$

Die Vorzeichen für ab sind also $g_i = e_i f_j$, wobei sich die j durch eine Permutation der i ergeben. Es folgt

$$g_1 \ldots g_r = (e_1 \ldots e_r)(f_1 \ldots f_r).$$

□

Wir betrachten nun den Fall, dass $m = p$ eine Primzahl ist. In diesem Fall wurde das Symbol schon füher von Legendre eingefhrt und heißt darum Legendre-Symbol.

Satz 35 *Es sei $p \neq 2$ eine Primzahl und a nicht durch p teilbar. Ist a ein quadratischer Rest, so ist $\left(\frac{a}{p}\right) = 1$, andernfalls ist $\left(\frac{a}{p}\right) = -1$.*

Beweis. Wir multiplizieren wir die Kongruenzen (6) miteinander, wobei nun $m = 2r + 1 = p$ ist. Da die Indizes j durch Permutation aus den Indizes i entstehen, erhalten wir

$$a^r h_1 \ldots h_r \equiv (e_1 \ldots e_r)(h_1 \ldots h_r) \pmod{p}.$$

Weil p eine Primzahl ist, sind alle h_i teilerfremd zu p, also

$$a^r \equiv \left(\frac{a}{p}\right) \pmod{p}.$$

Nun ergibt sich die Behauptung aus Satz 30. □

Die Voraussetzung, dass p eine Primzahl sei, ist wesentlich. So ist z. B. 2 kein quadratischer Rest modulo 15, obwohl das Jacobi-Symbol den Wert 1 hat (siehe Beispiel).

15 Das quadratische Reziprozitätsgesetz

Mit diesem Namen bezeichnete Gauß folgenden tiefliegenden Satz:

Satz 36 (Gauß) *Es seien m und n teilerfremde ungerade natürliche Zahlen. Dann gilt*

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

Da alle Faktoren gleich 1 oder -1 sind, kann man die Formel wie folgt umstellen:

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

Dazu gibt es den ersten und zweiten Ergänzungssatz, die wir hier zusammenfassen:

Satz 37 *Ist m eine ungerade natürliche Zahl, so gilt*

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

Beweis von Satz 37. Wir setzen wieder $m = 2r + 1$ und verwenden das Halbsystem $\{1, 2, \ldots, r\}$. Die erste Aussage folgt direkt aus der Definition des Jacobi-Symbols.

Ist h in unserem Halbsystem, so ist auch $2h$ im Halbsystem, falls $h \le \frac{r}{2}$, während $-h$ im Halbsystem liegt, falls $h > \frac{r}{2}$. Wir erhalten den Faktor $e = 1$ im ersten Fall und den Faktor $e = -1$ im zweiten Fall. Bilden wir das Produkt dieser Faktoren für alle h im Halbsystem, so erhalten wir nach Definition

$$\left(\frac{2}{m}\right) = \begin{cases} (-1)^{\frac{r}{2}} & \text{falls } r \text{ gerade,} \\ (-1)^{\frac{r+1}{2}} & \text{falls } r \text{ ungerade.} \end{cases}$$

Der Wert einer ganzzahligen Potenz von -1 ändert sich nicht, wenn wir den Exponenten mit einer ungeraden Zahl multiplizieren, z. B. mit $r+1$ im ersten Fall bzw. mit r im zweiten Fall. Es gilt also

$$\left(\frac{2}{m}\right) = (-1)^{\frac{r(r+1)}{2}},$$

wie behauptet (vgl. den Beweis von Satz 32). □

Bevor wir das quadratische Reziprozitätsgesetz beweisen, wollen wir seine Anwendung und Bedeutung diskutieren.

Beispiel. Wir wollen bestimmen, ob 5683 ein quadratischer Rest modulo 7919 ist. Da 5683 teilerfremd zu 7919 ist und letztere eine Primzahl ist (denn sie ist durch keine Primzahl kleiner als 89 teilbar, und $89^2 > 7919$), brauchen wir dazu nur das Legendre-Symbol $\left(\frac{5683}{7919}\right)$ zu berechnen. Übrigens ist auch 5683 eine Primzahl. Nach dem quadratischen Reziprozitätsgesetz gilt

$$\left(\frac{5683}{7919}\right) = (-1)^{2841\cdot 3959}\left(\frac{7919}{5683}\right) = -\left(\frac{2236}{5683}\right),$$

denn

$$7919 \equiv 2236 \pmod{5683}.$$

Hätten wir das Reziprozitätsgesetz nur für das Legendre-Symbol formuliert, so müssten wir die Zahl 2236 in Primfaktoren zerlegen, um das Symbol nach Lemma 3(ii) zu zerlegen und das Reziprozitätsgesetz auf jeden Faktor anwenden zu können. Da wir aber über das Jacobi-Symbol verfügen, genügt es, die Zahl 2236 in eine Zweierpotenz und eine ungerade Zahl zu zerlegen:

$$-\left(\frac{2236}{5683}\right) = -\left(\frac{2^2\cdot 559}{5683}\right) = -\left(\frac{2}{5683}\right)^2\left(\frac{559}{5683}\right).$$

Normalerweise würde man das Jacobi-Symbol von 2 mit dem zweiten Ergänzungssatz behandeln, aber sein Quadrat ist sowieso gleich 1. Durch zwei weitere Anwendungen des quadratischen Reziprozitätsgesetzes erhalten wir

$$\begin{aligned} -(-1)^{279\cdot 2841}\left(\frac{5683}{559}\right) &= \left(\frac{93}{559}\right) \\ &= (-1)^{46\cdot 279}\left(\frac{559}{93}\right) = \left(\frac{1}{93}\right), \end{aligned}$$

denn $5683 \equiv 93 \pmod{559}$ und $559 \equiv 1 \pmod{93}$. Unsere Rechnung ergibt also

$$\left(\frac{5683}{7919}\right) = 1,$$

und nach Satz 35 ist die Zahl 5683 ein quadratischer Rest modulo 7919.

Auf diese Weise kann man für eine gegebene Zahl a effektiv bestimmen, ob sie quadratischer Reste modulo einer gegebenen Primzahl p ist. Das Auffinden einer Lösung der Kongruenz $x^2 \equiv a \pmod{p}$ ist allerdings weitaus aufwendiger.

Folgerung 7 *Sind a, m und n ungerade natürliche Zahlen, ist a teilerfremd zu m und zu n, und ist $m \equiv n \pmod{4a}$, so gilt*

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

Beweis. Nach Satz 36 ist

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

Wegen $m \equiv n \pmod{a}$ stimmen die Jacobi-Symbole auf der rechten Seite überein, und wegen $m \equiv n \pmod{4}$ ist

$$\frac{m-1}{2} \equiv \frac{n-1}{2} \pmod{2}.$$

□

Wenn wir für eine feste Zahl a bestimmen wollen, modulo welcher Primzahlen $p \neq 2$ sie quadratischer Rest ist, so hängt die Antwort also nur von der Restklassen von p modulo $4a$ ab. Die Antwort lässt sich explizit bestimmen, indem man die Legendre-Symbole $\left(\frac{a}{m}\right)$ für Vertreter m aller primen Restklassen modulo $4a$ berechnet. Die Antwort für $a = -1$ und $a = 2$ kennen wir bereits aus Satz 32.

Der Fall $a = -1$ wurde in Satz 33 und 34 auf die Darstellbarkeit von natürlichen Zahlen n als Summe von zwei Quadraten angewendet, also auf die Lösbarkeit der Diophantischen Gleichung

$$x^2 + y^2 = n$$

für vorgegebenes n. Der allgemeine Fall hat eine ähnliche Anwendung auf die Lösbarkeit von Diophantischen Gleichungen der Form

$$ax^2 + bxy + cy^2 = n$$

bei vorgegebenen a, b, c und n. Dies war für Gauß die Motivation zum Studium quadratischer Reste.

Folgerung 8 *Sind a, m und n ungerade natürliche Zahlen und ist a teilerfremd zu m und zu n, so gilt*

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

Beweis. Im Fall einer ungeraden natürlichen Zahl a ist die Behauptung nach dem quadratischen Reziprozitätsgesetz äquivalent zu

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

Da m und n ungerade sind, gilt

$$(m-1)(n-1) \equiv 0 \pmod 4,$$

also

$$\begin{aligned}(m-1)+(n-1) &\equiv mn-1 \pmod 4,\\ \frac{m-1}{2}+\frac{n-1}{2} &\equiv \frac{mn-1}{2} \pmod 2,\end{aligned}$$

und die Behauptung folgt aus dem Satz 35.

Im Fall $a = -1$ folgt die Behauptung aus dem ersten Ergänzungssatz und der eben angeführten Kongruenz.

Im Fall $a = 2$ folgt die Behauptung aus dem zweiten Ergänzungssatz und

$$(m^2-1)(n^2-1) = (m+1)(m-1)(n+1)(n-1) \equiv 0 \pmod{16},$$

also

$$\begin{aligned}(m^2-1)+(n^2-1) &\equiv (mn)^2-1 \pmod{16},\\ \frac{m^2-1}{8}+\frac{n^2-1}{8} &\equiv \frac{(mn)^2-1}{8} \pmod 2.\end{aligned}$$

Eine beliebige Zahl a lässt sich in ein Produkt von Faktoren der betrachteten Art zerlegen, also ergibt sich die Behauptung aus Satz 35. (Da die vorkommenden Jacobi-Symbol nur von der Restklasse von a modulo mn abhängen, ist die Betrachtung des Falles $a = -1$ eigentlich nicht nötig.) □

Wir sehen also, dass das Jacobi-Symbol auch bezüglich des unteren Eintrages multiplikativ ist. Wir haben diese Eigenschaft aus Zeitgründen aus dem tiefliegenden quadratischen Reziprozitätsgesetz gefolgert. Sie lässt sich auch direkt beweisen, wobei die Betrachtung verschiedener Halbsysteme wichtig wird.

Beweis von Satz 36. Wir schreiben $m = 2r + 1$ und $n = 2s + 1$. Nach Definition ist

$$\left(\frac{m}{n}\right) = (-1)^k,$$

wobei k die Anzahl der Zahlen x in dem Halbsystem $\{1, 2, \ldots, s\}$ modulo m bezeichnet, für die es eine Zahl z in demselben Halbsystem gibt, so dass

$$mx \equiv -z \pmod{n}.$$

Letzteres bedeutet, dass es eine Zahl y gibt, so dass

$$-s \leq mx - ny < 0,$$

wobei dann $-z = mx - ny$, also auch y, eindeutig bestimmt ist. Außerdem folgt

$$ny \geq mx + 1 \geq 1, \qquad ny \leq mx + s \leq (m + 1)s = 2(r + 1)s < (r + 1)n,$$

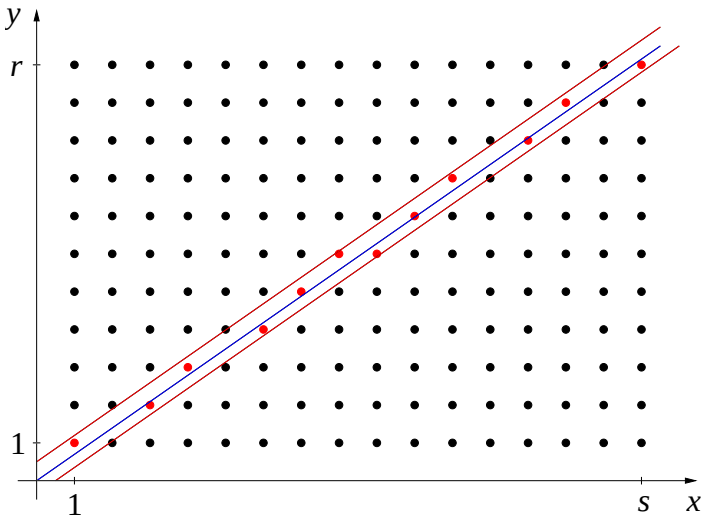
so dass

$$1 \leq y \leq r.$$

Bezeichnen wir also mit M die Menge der Paare (x, y) ganzer Zahlen mit der Eigenschaft $x \in \{1, 2, \ldots, s\}$, $y \in \{1, 2, \ldots, r\}$, so ist k gleich der Anzahl der Paare (x, y) in M, für die gilt

$$-s \leq mx - ny < 0.$$

Die Paare in M kann man als Menge von Gitterpunkten in einem Rechteck anschaulich darstellen, aus dem die angegebenen Ungleichungen einen Streifen ausschneiden.



Vertauschen wir die Rollen von m und n sowie von x und y, so sehen wir, dass

$$\left(\frac{n}{m}\right) = (-1)^l,$$

wobei l gleich der Anzahl der Paare (x, y) in M mit der Eigenschaft

$$-r \leq ny - mx < 0$$

ist. Die letzte Gleichung lässt sich auch als

$$0 < mx - ny \leq r$$

schreiben.

Da m und n teilerfremd sind, könnte $mx - ny$ höchstens dann Null sein, wenn $n \mid x$ und $m \mid y$, was jedoch für Elemente der jeweiligen Halbsysteme unmöglich ist. Wir sehen somit, dass

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{k+l},$$

wobei $k + l$ gleich der Anzahl der Paare $(x, y) \in M$ mit der Eigenschaft

$$-s \leq mx - ny \leq r$$

ist. Diese Paare bilden eine Teilmenge M_0 von M. Bezeichnen wir mit M_1 die Menge aller Paare in M mit der Eigenschaft

$$mx - ny \leq -s$$

sowie mit M_2 die Menge der Paare in M mit der Eigenschaft

$$mx - ny \geq r,$$

so folgt

$$M = M_0 \cup M_1 \cup M_2,$$

wobei die drei Teilmengen disjunkt sind.

Wir ordnen nun jedem Paar (x, y) ganzer Zahlen das Paar (x', y') zu, das sich durch

$$x' = s + 1 - x, \qquad y' = r + 1 - y$$

ergibt. Liegt (x, y) in M, dann liegt auch (x', y') in M, und umgekehrt. (Geometrisch bedeutet die Zuordnung eine Punktspiegelung im Mittelpunkt unseres Rechtecks.) Außerdem ist

$$\begin{aligned} mx' - ny' + s &= m(s + 1 - x) - n(r + 1 - y) + s \\ &= ny - mx + (2r + 1)(s + 1) - (2s + 1)(r + 1) + s \\ &= ny - mx + r. \end{aligned}$$

Es gilt also $(x', y') \in M_1$ genau dann, wenn $(x, y) \in M_2$. Wir haben somit eine umkehrbar eindeutige Zuordnung zwischen M_1 und M_2 gefunden, und folglich haben diese Mengen die gleiche Anzahl von Elementen. Die Zahl der Elemente in M ist rs, also

$$k + l \equiv rs \pmod 2, \qquad (-1)^{k+l} = (-1)^{rs},$$

was zu beweisen war. □

16 Unendlicher Abstieg

Wir wollen die Lösungen der Diophantischen Gleichung

$$x^4 + y^4 = z^2 \tag{7}$$

bestimmen. Lösungen, in denen eine der Variablen x oder y den Wert Null annimmt, heißen triviale Lösungen, sie sind von der Form $(a, 0, \pm a^2)$ oder $(0, b, \pm b^2)$.

Angenommen, das Tripel (a, b, c) ist eine Lösung, d. h.

$$a^4 + b^4 = c^2.$$

Ist d ein gemeinsamer Teiler von a und b, also $a = da_1$, $b = db_1$, so ist d^4 ein Teiler von c^2, und nach Aufgabe 14(a) ist d^2 ein Teiler von c. Es folgt $c = d^2c_1$, wobei auch (a_1, b_1, c_1) eine Lösung unserer Diophantischen Gleichung ist. Es genügt also, die primitiven Lösungen zu bestimmen, d. h. solche, bei denen a und b teilerfremd sind.

Ist (a, b, c) eine Lösung, so gilt

$$(a^2)^2 + (b^2)^2 = c^2,$$

also ist (a^2, b^2, c) ein Pythagoräisches Tripel. Wir nehmen nun an, dass unsere Lösung primitiv ist. Dann ist auch das entsprechende Pythagoräische Tripel primitiv. Wie wir wissen, ist dann von den Zahlen a^2 und b^2 genau eine gerade. Wir nehmen ohne Beschränkung der Allgemeinheit an, dass a^2 ungerade und b^2 gerade ist, d. h. dass a ungerade und b gerade ist. Nach Satz 12 gibt es teilerfremde ganze Zahlen m und n, so dass

$$a^2 = m^2 - n^2, \qquad b^2 = 2mn, \qquad c = m^2 + n^2.$$

Aus der ersten Gleichung sieht man, dass (a, n, m) wiederum ein Pythagoräisches Tripel ist! Wegen der Teilerfremdheit von m und n ist es ebenfalls

primitiv. Um Satz 12 noch einmal anwenden zu können, müssen wir wissen, welche der Zahlen a und n gerade ist. Wäre n ungerade, so müsste m gerade sein, denn b^2 ist durch 4 teilbar. Daraus würde aber folgen, dass $a^2 \equiv -1 \pmod 4$ im Widerspruch zu der Tatsache, dass -1 kein quadratischer Rest modulo 4 ist. Also ist n gerade und a ungerade, und wir finden teilerfremde Zahlen k und l, so dass

$$a = k^2 - l^2, \qquad n = 2kl, \qquad m = k^2 + l^2.$$

Die Zahlen k und l sind weiteren Einschränkungen unterworfen. Wegen

$$\left(\frac{b}{2}\right)^2 = m\,\frac{n}{2}$$

ist das Produkt der teilerfremden Zahlen m und $\frac{n}{2}$ eine Quadratzahl.[6] Nach Aufgabe 14(b) sind beide selbst Quadratzahlen, d. h.

$$m = t^2, \qquad n = 2v^2$$

für geeignete Zahlen t und v. Setzen wir den Ausdruck für n ein, so können wir eine 2 kürzen:

$$v^2 = kl.$$

Da k und l teilerfremd sind, folgt wiederum nach Aufgabe 14(b), dass es Zahlen r und s gibt, so dass

$$k = r^2, \qquad l = s^2,$$

und auch r und s sind teilerfremd. Setzen wir alles in die Formel für m ein, so folgt

$$t^2 = r^4 + s^4,$$

d. h. (r, s, t) ist ebenfalls eine primitive Lösung unserer Diophantischen Gleichung. Ist die Ausgangslösung nichttrivial, so ist $m \neq 0$ und $n \neq 0$, so dass $k \neq 0$, $l \neq 0$, also $r \neq 0$, $s \neq 0$, und

$$t^2 = m \leq m^2 < m^2 + n^2 = c \leq c^2, \qquad \text{also} \qquad |t| < |c|.$$

Auf diese Weise gewinnt man aus jeder primitiven nichttrivialen Lösung (a, b, c) eine neue primitive nichttriviale Lösung (r, s, t), bei der t dem Betrage nach kleiner ist als c. Verfährt man mit dieser Lösung ebenso, so müsste man zu immer neuen Lösungen kommen (unendlicher Abstieg). Dies widerspricht

[6] Auf der linken Seite ist natürlich kein Jacobi-Symbol gemeint, sondern das Quadrat eines Bruches!

aber der Tatsache, dass es zu einer natürlichen Zahl nur endlich viele kleinere gibt. Unsere Annahme, dass es eine primitive nichttriviale Lösung gibt, war also falsch. Jede nichttriviale Lösung entsteht aber aus einer primitiven nichttrivialen Lösung. Wir haben somit bewiesen:

Satz 38 (Fermat) *Die Diophantische Gleichung (7) hat nur triviale Lösungen.*

Es folgt, dass auch die Diophantische Gleichung

$$x^4 + y^4 = z^4$$

nur triviale Lösungen hat, denn für jede Lösung (a, b, c) dieser Gleichung wäre (a, b, c^2) eine Lösung von Gleichung (7).

In einer postum überlieferten Randnotiz in einer Ausgabe des Diophant bemerkte Fermat (1601-1665), er habe einen wunderbaren Beweis dafür gefunden, dass die Diophantische Gleichung

$$x^n + y^n = z^n$$

für beliebiges $n > 2$ nur triviale Lösungen hat. Diese Aussage wurde (im Unterschied zu Satz 19) oft als großer Satz von Fermat bezeichnet, obwohl ein Beweis von Fermat nicht überliefert ist und wahrscheinlich auch nicht existierte. Erste Fortschritte stammen von Euler, Sophie Germain, Dirichlet, Legendre and Lamé, aber mit elementaren Methoden gelang es nur, einzelne Exponenten zu behandeln oder Lösungen auszuschließen, deren Komponenten teilerfremd zu n sind. Das Fermat-Problem stimulierte die Entwicklung von Methoden der algebraischen Zahlentheorie und ihre Verbindung mit analytischen Methoden über drei Jahrhunderte. Nach Vorarbeiten von Barry Mazur erkannte Gerhard Frey 1986, dass die Fermat-Vermutung aus der sogenannten Shimura-Taniyama-Vermutung folgen würde. Diese bewies Andrew Wiles in den erforderlichen Fällen 1994 durch unter Benutzung einer Vielzahl von Resultaten anderer Forscher.