Zahlentheorie

Vorbereitungskurs zur Österreichischen Mathematischen Olympiade

Clemens Heuberger

Inhaltsverzeichnis

Auflage 2.7 11.04.2012

Vorwort

Diese Unterlagen decken die zahlentheoretischen Grundlagen ab, die bei Mathematik-Olympiaden immer wieder erforderlich sind.

Um das Erarbeiten des Stoffes in verschiedenen Etappen zu erleichtern, wurde versucht, die „Wichtigkeit“ der einzelnen Themen typographisch zu kennzeichnen — wohl wissend, dass eine solche Wertung immer subjektiv und damit gefährlich ist.

Der Stoff, der bereits beim ersten Teil des Bundeswettbewerbs erforderlich sein kann, wurde als „unmarkierter“ Text gesetzt.

In kleinerer Schriftart wurden Stoffgebiete gesetzt, die typischerweise erst beim zweiten Teil des Bundeswettbewerbs und bei internationalen Bewerben auftreten.

Zusätzlich gekennzeichnet wurden manchmal nützliche Resultate sowie längere Beweise von Sätzen, die man notfalls auch ohne Kenntnis der Beweise bei Bewerben anwenden können sollte. Dennoch lohnt sich ein Durcharbeiten dieser Beweise, weil dies jedenfalls das Verständnis verbessert.

Graz, April 2005 Clemens Heuberger

1 Teilbarkeit

1.1 Grundbegriffe

Definition 1.1.1. Es seien a und b ganze Zahlen. Man sagt: *a teilt b*, wenn es eine ganze Zahl q gibt, sodass $a \cdot q = b$, und schreibt dafür $a \mid b$. Man nennt alle Zahlen a, die b teilen, *Teiler* von b.

Der folgende Satz hält einige einfache Tatsachen fest, die fast unmittelbar einsichtig sind — dementsprechend kurz lassen sich die Beweise führen.

Satz 1.1. *Für alle ganzen Zahlen a, b, a_1, a_2, b_1, b_2 und t gilt:*

1. $a \mid 0$;
2. $a \mid b \iff a \mid -b$;
3. $a \mid b \iff ta \mid tb$ *mit* $t \neq 0$;
4. *aus* $a_1 \cdot a_2 \mid b$ *folgt* $a_1 \mid b$;
5. *aus* $a \mid b$ *folgt* $a \mid tb$;
6. *aus* $a \mid b$ *und* $b \mid c$ *folgt* $a \mid c$;
7. *aus* $a \mid b_1$ *und* $a \mid b_2$ *folgt* $a \mid (b_1 \pm b_2)$;
8. *aus* $a \mid (b_1 + b_2)$ *und* $a \mid b_1$ *folgt* $a \mid b_2$;
9. *aus* $a \mid b$ *und* $b \neq 0$ *folgt* $|a| \leq |b|$.

Beweis. 1. $a \cdot 0 = 0 \Rightarrow a \mid 0$ (wegen $0 \in \mathbb{Z}$).

2. $aq = b \iff a \cdot (-q) = -b \iff a \mid -b$ (wegen $(-q) \in \mathbb{Z}$).

3. $aq = b \iff (ta)q = (tb) \iff ta \mid tb$.

4. $a_1 a_2 q = b \Rightarrow a_1(a_2 q) = b \Rightarrow a_1 \mid b$ (wegen $a_2 q \in \mathbb{Z}$).

5. Für $t = 0$ folgt die Behauptung aus (1), sonst aus (3) und (4): $a \mid b \Rightarrow ta \mid tb \Rightarrow a \mid tb$.

6. $b = aq$. Aus $aq \mid c$ folgt nach (4) auch $a \mid c$.

7. $aq_1 = b_1$ und $aq_2 = b_2 \Rightarrow b_1 \pm b_2 = a(q_1 \pm q_2)$, wobei $(q_1 \pm q_2) \in \mathbb{Z}$.

8. $aq = b_1 + b_2, aq_1 = b_1 \Rightarrow b_2 = b_2 + b_1 - b_1 = a(q - q_1)$, wobei $(q - q_1) \in \mathbb{Z}$.

9. Aus $aq = b$ folgt $|aq| = |b|$, also $|a| \cdot |q| = |b|$. Wegen $b \neq 0$ gilt $q \neq 0$, somit $|q| \geq 1$ und dadurch folgt aus $|a| \cdot |q| = |b|$, dass $|a| \leq |b|$.

□

Man sieht aus (9), dass es für $b \neq 0$ nur endlich viele Teiler von b geben kann, weil nur endlich viele ganze Zahlen die notwendige Bedingung $|a| \leq |b|$ erfüllen.

Allein die Kombination der Teilbarkeitsregeln in Satz 1.1 mit Größenordnungsüberlegungen führt bei vielen Olympiadeaufgaben zum Ziel.

Aufgabe 1.1.2. Finden Sie alle Paare ganzer Zahlen (x, y), die der Gleichung

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

genügen. *(Großbritannien 2001/2002, Zweite Runde, Beispiel 2.)*

Lösung. Da y nur linear in der Gleichung vorkommt, können wir die Gleichung zu einer Teilbarkeitsaufgabe umschreiben, indem wir y herausheben:

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

Daher teilt $x^2 - 2x - 1$ die Zahl $x^2 + 2x - 1$. Für große x sind $x^2 - 2x - 1$ und $x^2 + 2x - 1$ etwa gleich groß. Wir betrachten daher deren Differenz, die laut Satz 1.1 auch von $x^2 - 2x - 1$ geteilt wird:

$$(x^2 - 2x - 1) \mid \big((x^2 + 2x - 1) - (x^2 - 2x - 1)\big) = 4x.$$

Somit erhalten wir $4x = 0$ (und damit die Lösung $(x, y) = (0, 1)$) oder

$$\left|x^2 - 2x - 1\right| \leq |4x|.$$

Die linke Seite $x^2 - 2x - 1 = (x - 1)^2 - 2$ ist für $x \in \{0, 1, 2\}$ negativ, sonst positiv. Wir überprüfen daher die x-Werte 1 und 2 und erhalten Lösungen $(x, y) \in \{(1, -1), (2, -7)\}$. Für $x > 3$ gilt

$$x^2 - 2x - 1 \leq 4x,$$

woraus $(x-3)^2 \leq 10$ folgt. Es kommen daher nur $x \in \{3,4,5,6\}$ in Frage. Für negative x gilt

$$x^2 - 2x - 1 \leq -4x,$$

also $(x+1)^2 \leq 2$, es kommen also nur $x \in \{-2,-1\}$ in Frage.

Durch Überprüfen dieser endlich vielen Möglichkeiten erhält man die Lösungsmenge

$$\{(-1,-1),(0,1),(1,-1),(2,-7),(3,7)\}.$$

□

In $\mathbb{Z}$ ist die Division bekanntlich nicht immer ausführbar, weshalb man eine Division mit Rest einführen kann, die im Bereich der ganzen Zahlen stets durchführbar ist.

Satz 1.2 (Division mit Rest)**.** *Sei a eine ganze und b eine positive ganze Zahl. Dann existiert genau ein Paar von ganzen Zahlen (q,r), sodass $0 \leq r < b$ und $a = b \cdot q + r$ gilt.*

Beweis. Zunächst wird die Existenz gezeigt: Sei q die größte ganze Zahl kleiner oder gleich $\frac{a}{b}$, also $q = \left\lfloor \frac{a}{b} \right\rfloor$, d.h.

$$q \leq \frac{a}{b} < q+1.$$

Multiplikation mit $b > 0$ ergibt

$$bq \leq a < bq + b \iff 0 \leq a - bq < b.$$

Setzt man $r = a - bq$, erhält man das gewünschte $0 \leq r < b$. Zu zeigen bleibt die Eindeutigkeit. Sei (q', r') ein weiteres Paar ganzer Zahlen, das den Bedingungen genügt. Dann gilt

$$bq + r = a = bq' + r' \iff b(q - q') = r' - r.$$

Aus $0 \leq r,\ r' < b$ folgt $|r' - r| < b$, somit auch $|b(q-q')| < b$, woraus $q = q'$ und damit $r = r'$ folgt. □

Man nennt die Zahl q Quotient und die Zahl r Rest von a bei der Division durch b und sagt auch: a lässt den Rest r bei Division durch b.

1.2 Größter gemeinsamer Teiler

Definition 1.2.1. Seien a und b ganze Zahlen. Die ganze Zahl c heißt *gemeinsamer Teiler* von a und b, wenn $c \mid a$ und $c \mid b$ gilt.

Da es nur endlich viele Teiler von a bzw. b gibt (falls nicht beide 0 sind), gibt es auch nur endlich viele gemeinsame Teiler, weshalb es einen größten gemeinsamen Teiler gibt:

Definition 1.2.2. Seien a und b ganze Zahlen, die nicht beide 0 sind. Dann nennt man die größte ganze Zahl, die gemeinsamer Teiler von a und b ist, den *größten gemeinsamen Teiler* von a und b und schreibt dafür $\mathrm{ggT}(a,b)$.

Es gilt $\mathrm{ggT}(a,b) = \mathrm{ggT}(|a|,|b|)$, weil nach Satz 1.1(2) jeder Teiler von a bzw. b auch Teiler von $(-a)$ bzw. $(-b)$ ist, daher auch von $|a|$ bzw. $|b|$.

Da $1 \mid a$ und $1 \mid b$, gilt sicher $\mathrm{ggT}(a,b) \geq 1$.

Definition 1.2.3. Ganze Zahlen a und b, für die $\mathrm{ggT}(a,b) = 1$ gilt, heißen *teilerfremd* oder *relativ prim.*

Beispiel 1.2.4. 3 ist ein gemeinsamer Teiler von 30 und 45; der größte gemeinsame Teiler von 30 und 45 ist $\mathrm{ggT}(30,45) = 15$; die Zahlen 15 und 16 sind teilerfremd.

Euklid gab in seinen „Elementen“ eine Möglichkeit an, den ggT zweier natürlicher Zahlen einfach zu bestimmen. Sie wird nach ihm „Euklidscher Algorithmus“ genannt. Basis ist der folgende Satz:

Satz 1.3. *Seien a und b ganze Zahlen, nicht beide 0. Für alle ganzen Zahlen k gilt*

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

Beweis. Sei $r = a - bk$, $d_1 = \mathrm{ggT}(a,b)$ und $d_2 = \mathrm{ggT}(b,r)$. Da $d_1 \mid a$ und $d_1 \mid bk$, gilt nach Satz 1.1 (7) $d_1 \mid r = a - bk$. Da d_1 gemeinsamer Teiler von b und r ist, gilt $d_2 \geq d_1$. Es gilt aber auch $a = bk + r$. Daher gilt analog wie oben $d_2 \mid a$, also gilt $d_2 \leq d_1$. Zusammen gilt $d_1 = d_2$. □

Wählt man für k den auf die nächste ganze Zahl (kaufmännisch) gerundeten Quotienten von a und b (bezeichnet als $\lfloor a/b \rceil$), so kommt man besonders schnell zum Ziel.

Aufgabe 1.2.5. Man finde den größten gemeinsamen Teiler von 2005 und 197 (ohne Primfaktorzerlegung).

Lösung.

$$\begin{aligned}
\mathrm{ggT}(2005,197) &= \mathrm{ggT}\left(197, 2005 - \left\lfloor \frac{2005}{197} \right\rceil \cdot 197\right) = \mathrm{ggT}(197, 2005 - \lfloor 10.1\ldots \rceil \cdot 197) \\
&= \mathrm{ggT}(197, 2005 - 10 \cdot 197) \\
= \mathrm{ggT}(197,35) &= \mathrm{ggT}\left(35, 197 - \left\lfloor \frac{197}{35} \right\rceil \cdot 35\right) = \mathrm{ggT}(35, 197 - \lfloor 5.6\ldots \rceil \cdot 35) \\
&= \mathrm{ggT}(35, 197 - 6 \cdot 35) = \mathrm{ggT}(35,-13) = \\
= \mathrm{ggT}(35,13) &= \mathrm{ggT}(13, 35 - 3 \cdot 13) = \mathrm{ggT}(13,-4) \\
= \mathrm{ggT}(13,4) &= \mathrm{ggT}(4, 13 - 3 \cdot 4) \\
= \mathrm{ggT}(4,1) &= \mathrm{ggT}(1, 4 - 4 \cdot 1) = \mathrm{ggT}(1,0) = 1.
\end{aligned}$$

□

Aufgabe 1.2.6. Man zeige, dass je zwei aufeinanderfolgende ganze Zahlen teilerfremd sind.

Lösung. Für jede ganze Zahl x gilt $\mathrm{ggT}(x+1,x) = \mathrm{ggT}(x,(x+1)-x) = \mathrm{ggT}(x,1) = 1$, also sind zwei aufeinanderfolgende ganze Zahlen stets teilerfremd. □

Man kann bei der Durchführung des euklidschen Algorithmus einfach zusätzliche Informationen berechnen, die sich in späterer Folge als nützlich herausstellen werden. Man nennt dies den *erweiterten* EUKLIDschen Algorithmus.

Satz 1.4. *Seien $a > b$ positive ganze Zahlen. Setze*

k	d_k	x_k	y_k
0	a	1	0
1	b	0	1

und für $k \geq 1$ rekursiv $q_k := \lfloor d_{k-1}/d_k \rfloor$ und

d_{k+1}	x_{k+1}	y_{k+1}
$d_{k-1} - q_k d_k$	$x_{k-1} - q_k x_k$	$y_{k-1} - q_k y_k$.

Dann gibt es ein $K \geq 1$, sodass $d_{K+1} = 0$. Es gilt $\mathrm{ggT}(a,b) = d_K = x_K a + y_K b$.

Beweis. Da $0 \leq d_{k-1} - q_k d_k < d_k$ folgt, dass $0 \leq d_{k+1} < d_k$ für $k \geq 0$. Damit gibt es ein $K \geq 1$, sodass $d_{K+1} = 0$. Nach Satz 1.3 gilt $\mathrm{ggT}(d_{k-1}, d_k) = \mathrm{ggT}(d_k, d_{k+1})$ und damit induktiv $\mathrm{ggT}(a,b) = \mathrm{ggT}(d_K, d_{K+1}) = \mathrm{ggT}(d_K, 0) = d_K$. Weiters gilt $d_k = ax_k + by_k$ für alle $k \geq 0$, wie man leicht durch vollständige Induktion zeigen kann. Daher gilt auch $d_K = x_K a + y_K b$. □

Das obige Verfahren berechnet also nicht nur den größten gemeinsamen Teiler von a und b, sondern auch zwei ganze Zahlen („Kofaktoren“) x und y, sodass $\mathrm{ggT}(a,b) = xa + yb$, was später immer wieder nützlich sein wird. Benötigt man x und y jedoch nicht, so muss man natürlich nur die d_k, $k \geq 0$, berechnen. Man kann natürlich statt der Abrundung $q_k = \lfloor d_{k-1}/d_k \rfloor$ auch wieder kaufmännisch runden, dadurch wird die Rechnung meist kürzer, man bezahlt mit dem vermehrten Auftreten negativer Vorzeichen.

Aufgabe 1.2.7. Bestimme den $\mathrm{ggT}(2005, 197)$ mit den Kofaktoren.

Lösung.

k	d_k	x_k	y_k	
0	2005	1	0	
1	197	0	1	$\cdot(-10)$
2	35	1	-10	$\cdot(-6)$
3	-13	-6	61	$\cdot(+3)$
4	-4	-17	173	$\cdot(-3)$
5	-1	45	-458	$\cdot(-4)$
6	0			

,

also gilt $\mathrm{ggT}(2005, 197) = 1$ und $-1 = 45 \cdot 2005 + (-458) \cdot 197$ und daher

$$1 = -45 \cdot 2005 + 458 \cdot 197.$$

□

Definition 1.2.8. Unter dem *kleinsten gemeinsamen Vielfachen* $\mathrm{kgV}(a,b)$ zweier Zahlen a und b (nicht beide 0) versteht man die kleinste positive Zahl, die sowohl von a als auch von b geteilt wird.

Bei der Bestimmung des größten gemeinsamen Teilers von zwei Binomen $x^a - y^a$ und $x^b - y^b$ kann man einfach den größten gemeinsamen Teiler der Exponenten bilden, wie die folgende manchmal nützliche Proposition zeigt.

Proposition 1.2.9. *Seien x, y teilerfremde ganze Zahlen und a, b positive ganze Zahlen mit $d = \mathrm{ggT}(a,b)$. Dann gilt*

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

Beweis. Es gibt ganze Zahlen r und s, sodass

$$ra - sb = d.$$

Ohne Beschränkung der Allgemeinheit können wir annehmen, dass r und s positiv sind.

Wir setzen

$$u = \frac{(x^a)^r - (y^a)^r}{x^a - y^a}, \qquad v = x^d \frac{(x^b)^s - (y^b)^s}{x^b - y^b}.$$

Offensichtlich sind u und v ganze Zahlen. Es gilt

$$u(x^a - y^a) - v(x^b - y^b) = x^{ar} - y^{ar} - x^d(x^{bs} - y^{bs}) = y^{bs}(x^d - y^d).$$

Somit ist $\mathrm{ggT}(x^a - y^a, x^b - y^b)$ ein Teiler von $y^{bs}(x^d - y^d)$. Da x und y teilerfremd sind, ist auch y^{bs} zu $\mathrm{ggT}(x^a - y^a, x^b - y^b)$ teilerfremd, und wir erhalten (streng genommen verwenden wir hier Satz 1.6, der erst im nächsten Abschnitt bewiesen wird)

$$\mathrm{ggT}(x^a - y^a, x^b - y^b) \mid (x^d - y^d).$$

Da aber $x^d - y^d$ ein gemeinsamer Teiler von $x^a - y^a$ und $x^b - y^b$ ist, folgt die Aussage des Lemmas. □

1.3 Primfaktordarstellung

Eine der wichtigsten Eigenschaften der Zahlentheorie ist der Satz über die eindeutige Primfaktordarstellung.

Satz 1.5 (Eindeutige Primfaktorzerlegung)**.** *Jede positive ganze Zahl n lässt sich eindeutig als Produkt*

$$n = \prod_{p|n} p^{\alpha_p}, \text{ mit } \alpha_p \geq 1$$

aller ihrer zu einer bestimmten Potenz erhobenen Primteiler darstellen.

So vertraut dieser Satz auch sein mag, ist er dennoch keineswegs eine ganz einfache Konsequenz aus den vorangegangenen Definitionen und erfordert daher einen Beweis. Die Teilschritte des Beweises bestehen aus kleinen Resultaten, die immer wieder nützlich sind. Möchte man bei der ersten Lektüre die eindeutige Primfaktordarstellung einfach „glauben“, so überlege man sich dennoch, wie sich diese Teilresultate aus der eindeutigen Primfaktordarstellung ableiten lassen.

Beispiel 1.3.1. $2004 = 4 \cdot 3 \cdot 167 = 2^2 \cdot 3 \cdot 167$.

Satz 1.6. *Seien a, b und c ganze Zahlen und es gelte $c \mid ab$ sowie $\mathrm{ggT}(a,c) = 1$, dann gilt $c \mid b$.*

Beweis. Wegen Satz 1.4 gibt es ganze x und y, sodass

$$\mathrm{ggT}(a,c) = 1 = ax + cy \iff b = abx + bcy.$$

Aus $c \mid abx$ und $c \mid bcy$ folgt nach Satz 1.1 (7), dass $c \mid (abx + bcy)$, also $c \mid b$. □

Ist nun c eine Primzahl p (im Folgenden stehe p immer für eine Primzahl, wenn nicht ausdrücklich anders angemerkt), so schreibt sich dieser Satz als

$$p \mid ab \wedge p \nmid a \Rightarrow p \mid b, \tag{1.3.1}$$

denn $\mathrm{ggT}(a,p) = 1$ ist zu $p \nmid a$ äquivalent, weil die positiven Teiler einer Primzahl nach Definition nur 1 und p sind.

Was nun für zwei Faktoren gezeigt wurde, lässt sich verallgemeinern:

Satz 1.7. *Es seien p eine Primzahl und a_1, a_2,..., a_n ganze Zahlen und es gelte $p \mid a_1 a_2 \cdots a_n$. Dann gibt es ein i, sodass $1 \leq i \leq n$ und $p \mid a_i$.*

Beweis. Dieser Satz kann mit vollständiger Induktion über n bewiesen werden.

Basis: Für $n = 1$ ist die Aussage äquivalent zu $p \mid a_1 \Rightarrow p \mid a_1$, was eine wahre Aussage ist.

Annahme: Der Satz gelte für $n = k - 1$, d. h. aus $p \mid a_1 a_2 \cdots a_{k-1}$ folgt die Existenz eines i mit $1 \leq i \leq k-1$ und $p \mid a_i$.

Schluss von $k-1$ auf k: Es gelte $p \mid (a_1 a_2 \cdots a_{k-1}) a_k$. Gilt nun $p \mid a_k$, so existiert ein i mit der geforderten Eigenschaft, nämlich $i = k$. Gilt allerdings $p \nmid a_k$, so folgt nach (1.3.1), dass $p \mid a_1 a_2 \cdots a_{k-1}$, woraus nach der Induktionsannahme folgt, dass ein i existiert, sodass $1 \leq i \leq k-1$ und $p \mid a_i$. In jedem der beiden Fälle wurde die Existenz eines i mit der geforderten Eigenschaft gezeigt, weshalb der Satz auch für $n = k$ gilt. □

Schließlich können wir nun den Satz über die eindeutige Primfaktordarstellung beweisen.

Beweis von Satz 1.5. Für $n = 1$ gibt es keinen Faktor, der der Bedingung $p \mid n$ genügt, daher ist das Produkt auf der rechten Seite leer, womit es nach Definition gleich 1 ist.

Zunächst wird die Existenz einer Darstellung gezeigt: Für $n = 2$ gilt $n = 2^1$. Sei nun k die kleinste Zahl, für die es keine Primfaktordarstellung gibt. Dieses k ist also insbesondere keine Primzahl. Damit gibt es $1 < d_1 \leq d_2 < k$, sodass $k = d_1 \cdot d_2$. Da diese d_1 und d_2 kleiner als k sind, besitzen sie nach Induktionsannahme eine Primfaktordarstellung, also

$$d_1 = \prod_{p \mid n} p^{\beta_p}, \qquad d_2 = \prod_{p \mid n} p^{\gamma_p},$$

wobei $\beta_p \geq 0$ und $\gamma_p \geq 0$ (wir haben möglicherweise einige zusätzliche Faktoren p^0 eingefügt, was aber nichts ausmacht). Multipliziert man die beiden Darstellungen, erhält man (mit $\alpha_p := \beta_p + \gamma_p$) eine Primfaktordarstellung von k.

Die Eindeutigkeit ergibt sich folgendermaßen: Für $n = 2$ kann keine höhere Potenz von 2 oder ein anderer Primfaktor als 2 im Produkt auftreten, weil dieses damit größer als 2 würde. Sei nun wieder k die kleinste Zahl, für die es (nicht nur durch die Anordnung) verschiedene Primfaktorzerlegungen gibt:

$$k = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n} = q_1^{\beta_1} q_2^{\beta_2} \ldots q_m^{\beta_m}, \text{ mit } p_i, q_i \text{ Primzahlen und } \alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m \geq 1$$

Es gilt nun

$$p_1 \mid q_1^{\beta_1} q_2^{\beta_2} \ldots q_m^{\beta_m},$$

weshalb es nach Satz 1.7 ein q_i gibt, sodass $p_1 \mid q_i$. Daraus folgt aber, dass $p_1 = q_i$, weshalb $\frac{k}{p_1} = \frac{k}{q_i} < k$ zwei verschiedene Primfaktorzerlegungen haben müsste, was ein Widerspruch zur Annahme ist, dass k die kleinste Zahl mit dieser Eigenschaft ist. □

Konsequenzen aus der eindeutigen Primfaktordarstellung

Manchmal lässt man das Produkt über alle Primzahlen laufen und setzt bei den überflüssigen Primfaktoren $\alpha_p = 0$:

$$n = \prod_{p \text{ prim}} p^{\alpha_p}.$$

Man schreibt auch $v_p(n) = \alpha_p$, wenn p genau mit dem Exponenten α_p in der Primfaktordarstellung von n auftritt.

Teilbarkeit, gemeinsame Teiler und gemeinsame Vielfache lassen sich nun ganz einfach durch die Primfaktordarstellung ausdrücken.

Satz 1.8. *Seien a und b positive ganze Zahlen mit den Primfaktordarstellungen*

$$a = \prod_{p\ prim} p^{\alpha_p}, \qquad b = \prod_{p\ prim} p^{\beta_p}$$

mit α_p, $\beta_p \geq 0$.
Dann gilt:

$$a \mid b \iff \forall\, p : \alpha_p \leq \beta_p,$$
$$\mathrm{ggT}(a,b) = \prod_{p\ prim} p^{\min(\alpha_p,\beta_p)},$$
$$\mathrm{kgV}(a,b) = \prod_{p\ prim} p^{\max(\alpha_p,\beta_p)}.$$

Beweis. Wir betrachten zunächst die erste Äquivalenz und nehmen an, dass $a \mid b$. Gäbe es eine Primzahl q mit $\alpha_q \geq \beta_q$, so folgte nach Satz 1.1(3)

$$q \,\Big|\, \prod_{p \neq q} p^{\beta_p},$$

was wegen Satz 1.7 zu einem Widerspruch führt. Die Umkehrung ist selbstverständlich.

Daraus folgen sofort auch die Darstellungen von ggT und kgV. □

Aufgabe 1.3.2. Finden Sie alle ganzen Zahlen x, y und z, sodass

$$\frac{13}{x^2} + \frac{1996}{y^2} = \frac{z}{1997}.$$

(Griechenland 1997)

Lösung. Durch Ausmultiplizieren erhalten wir

$$1997(13y^2 + 1996x^2) = x^2y^2z. \tag{1.3.2}$$

Daraus folgt sofort

$$x^2 \mid 13 \cdot 1997 \cdot y^2.$$

Sei p eine Primzahl. Da 13 und 1997 prim sind, gilt $2v_p(x) = v_p(x^2) \leq v_p(13 \cdot 1997 \cdot y^2) = v_p(13 \cdot 1997) + v_p(y^2) \leq 1 + 2v_p(y)$. Da $v_p(x)$ und $v_p(y)$ ganzzahlig sind, folgt daraus $v_p(x) \leq v_p(y)$ für alle p. Daher ist x ein Teiler von y und wir schreiben $y = ux$ für ein ganzzahliges u. Somit schreibt sich (1.3.2) nach Kürzen von x^2 als

$$1997(13u^2 + 1996) = u^2x^2z.$$

Daraus folgt, dass u^2 ein Teiler von $1996 \cdot 1997 = 2^2 \cdot 499 \cdot 1997$ ist; nach demselben Argument wie oben folgt, dass $u \mid 2$, also $u^2 \in \{1, 4\}$. Im Fall $u^2 = 1$ (also $y = \pm x$) folgt

$$1997 \cdot 2009 = 7^2 \cdot 41 \cdot 1997 = x^2z,$$

also (wieder nach demselben Argument) $x \mid 7$, somit $x \in \pm\{1, 7\}$ und $y = \pm x$. Im anderen Fall $u^2 = 4$ erhalten wir

$$1997 \cdot 2048 = 2^{11} \cdot 1997 = x^2z,$$

weshalb x ein Teiler von 2^5 ist.

Somit ergibt sich als Lösung

$$\begin{aligned}(x, y, z) \in \{&(\pm1, \pm1, 1997 \cdot 2009), (\pm7, \pm7, 41 \cdot 1997), (\pm1, \pm2, 1997 \cdot 2048),\\ &(\pm2, \pm4, 1997 \cdot 512), (\pm4, \pm8, 1997 \cdot 128), (\pm8, \pm16, 1997 \cdot 32),\\ &(\pm16, \pm32, 1997 \cdot 8), (\pm32, \pm64, 1997 \cdot 2)\}.\end{aligned}$$

□

Mit der eindeutigen Primfaktordarstellung lassen sich auch folgende Resultate leicht beweisen.

Satz 1.9. *Aus $a \mid c$ und $b \mid c$ folgt* $\mathrm{kgV}(a, b) \mid c$.

Beweis. Wir schreiben $c = \prod_{p \text{ prim}} p^{\gamma_p}$. Nach Satz 1.8 gilt für alle p, dass $\gamma_p \geq \alpha_p$ und $\gamma_p \geq \beta_p$, woraus $\gamma_p \geq \max(\alpha_p, \beta_p)$ und mit Satz 1.8 die Behauptung folgt. □

Satz 1.10. *Aus* $\mathrm{ggT}(a, c) = 1$ *und* $\mathrm{ggT}(b, c) = 1$ *folgt* $\mathrm{ggT}(ab, c) = 1$.

Beweis. Sei $p \mid ab$ und $p \mid c$. Nach Satz 1.6 folgt daraus $p \mid a$ oder $p \mid b$. Das ist ein Widerspruch zu $\mathrm{ggT}(a, c) = \mathrm{ggT}(b, c) = 1$. □

Die letzten beiden Sätze lassen sich mit vollständiger Induktion auf n Faktoren verallgemeinern.

Wir haben $v_p(a)$ als die Potenz der Primzahl p in der Primfaktordarstellung einer ganzen Zahl a definiert. Für diese Funktion v_p gelten folgende nützliche Rechenregeln, wobei die ersten beiden an Rechenregeln für Logarithmen erinnern.

Satz 1.11. *Sei p eine Primzahl, a und b ganze Zahlen und n eine natürliche Zahl. Dann gilt:*

1. $v_p(a \cdot b) = v_p(a) + v_p(b)$,
2. $v_p(a^n) = n \cdot v_p(a)$,
3. $v_p(a + b) \geq \min(v_p(a), v_p(b))$,
4. $v_p(a + b) = \min(v_p(a), v_p(b))$, *falls* $v_p(a) \neq v_p(b)$.

Beweis. Wir schreiben $\alpha = v_p(a)$ und $\beta = v_p(b)$. Es gilt also $a = p^\alpha \cdot c$ und $b = p^\beta \cdot d$ für ganze Zahlen c und d, die nicht durch p teilbar sind.

1. Es gilt $a \cdot b = p^{\alpha+\beta} \cdot c \cdot d$ und $c \cdot d$ ist nicht durch p teilbar. Damit gilt $v_p(a \cdot b) = \alpha + \beta = v_p(a) + v_p(b)$.
2. Das folgt aus dem ersten Teil durch Induktion nach n.
3. Wir nehmen ohne Beschränkung der Allgemeinheit an, dass $\alpha \leq \beta$. Dann ist $a + b = p^\alpha(c + p^{\beta-\alpha}d)$, womit $a + b$ jedenfalls durch p^α teilbar ist, d.h., $v_p(a + b) \geq \alpha = \min(v_p(a), v_p(b))$.
4. Wir können jetzt ohne Beschränkung der Allgemeinheit annehmen, dass $\alpha < \beta$ gilt. Wir wissen aus dem vorigen Punkt, dass $v_p(a + b) \geq \alpha$, dass also $a + b$ durch p^α teilbar ist. Falls $a + b$ durch $p^{\alpha+1}$ teilbar wäre, so wäre auch $a = (a + b) - b$ als Differenz zweier durch $p^{\alpha+1}$ teilbarer Zahlen durch $p^{\alpha+1}$ teilbar (da b durch p^β teilbar ist und $\beta \geq \alpha + 1$, ist b auch durch $p^{\alpha+1}$ teilbar), was ein Widerspruch ist.

□

2 Kongruenzen

2.1 Grundbegriffe

Definition 2.1.1. Sei m eine positive ganze Zahl. Zwei ganze Zahlen a und b heißen *kongruent modulo m*, wenn $m \mid a - b$. Man schreibt

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

Zahlen a und b, die nicht kongruent modulo m sind, heißen inkongruent, wofür man

$$a \not\equiv b \pmod{m}$$

schreibt.

Satz 2.1. *Sei m eine positive ganze Zahl. Dann ist jede ganze Zahl a zu genau einer der m Zahlen $0, \ldots, m-1$ kongruent.*

Beweis. Durch Division mit Rest (Satz 1.2) gibt es ganze Zahlen q und $0 \leq r < m$, sodass $a = qm + r$. Daraus folgt sofort $a \equiv r \pmod{m}$ mit einem passenden r. Angenommen, a wäre zu zwei Zahlen r_1 und r_2 mit $0 \leq r_1, r_2 < m$ kongruent. Dann gilt $m \mid (a - r_1)$ und $m \mid (a - r_2)$, also nach Satz 1.1 auch $m \mid (r_1 - r_2)$. Da $-m < r_1 - r_2 < m$, folgt daraus $r_1 - r_2 = 0$, also waren r_1 und r_2 gleich. □

Man bezeichnet die Menge aller zu a (modulo m) kongruenten ganzen Zahlen als die *Restklasse von a modulo m* und schreibt

$$\bar{a} := \{x \in \mathbb{Z} : a \equiv x \pmod{m}\}.$$

Wir haben eben gesehen, dass es genau die m Restklassen $\bar{0}$, $\bar{1}$, $\ldots$, $\overline{m-1}$ gibt.

2.2 Rechenregeln für Kongruenzen

Satz 2.2. *Seien a, b, c, d, e, f und t ganze Zahlen und k eine positive ganze Zahl und es gelte $a \equiv b \pmod{m}$ und $c \equiv d \pmod{m}$, so gilt:*

1. *$a + c \equiv b + d \pmod{m}$ sowie $a - c \equiv b - d \pmod{m}$.*
2. *$ac \equiv bd \pmod{m}$.*
3. *Gilt $k \mid m$, so folgt aus $a \equiv b \pmod{m}$ auch $a \equiv b \pmod{k}$.*
4. *$t \cdot a \equiv t \cdot b \pmod{|t| \cdot m}$, wobei $t \neq 0$.*
5. *Gilt $\mathrm{ggT}(k, m) = 1$ und $ke \equiv kf \pmod{m}$, so gilt auch $e \equiv f \pmod{m}$.*

Beweis.

1. Nach Satz 1.1 (7) folgt aus $m \mid (a-b)$ und $m \mid (c-d)$, dass $m \mid (a-b) \pm (c-d)$ und somit $m \mid [(a \pm c) - (b \pm d)]$.

2. Nach Satz 1.1 (5) folgt aus $m \mid (a - b)$ und $m \mid (c - d)$, dass $m \mid c \cdot (a - b)$ und $m \mid b \cdot (c-d)$, woraus nach Satz 1.1 (7) $m \mid (ac - bc + bc - bd)$ und somit $m \mid (ac - bd)$ folgt.

3. Aus $k \mid m$ und $m \mid (a - b)$ folgt nach Satz 1.1 (6) $k \mid (a - b)$.

4. $m \mid (a - b) \Rightarrow tm \mid t(a - b) \Rightarrow |t| \cdot m \mid (ta - tb)$

5. Aus $m \mid k \cdot (e - f)$ und $\mathrm{ggT}(k, m) = 1$ folgt nach Satz 1.6 $m \mid (e - f)$.

□

Die Rechenregeln (1) und (2) lassen sich durch Induktion auf n Summanden bzw. Faktoren verallgemeinern:

Aus $a_i \equiv b_i \pmod{m}$ für $1 \leq i \leq n$ folgt

$$\sum_{i=1}^{n} a_i \equiv \sum_{i=1}^{n} b_i \pmod{m}$$

und

$$\prod_{i=1}^{n} a_i \equiv \prod_{i=1}^{n} b_i \pmod{m}.$$

Insbesondere folgt aus $a \equiv b \pmod{m}$ für alle natürlichen Zahlen n, dass $a^n \equiv b^n \pmod{m}$.

Aufgabe 2.2.1. Zeigen Sie, dass für jede positive ganze Zahl n die Zahl

$$121^n - 25^n + 1900^n - (-4)^n$$

durch 2000 teilbar ist. *(Großbritannien, 2000).*

Lösung. Es gilt $2000 = 2^4 \cdot 5^3$ und eine Zahl ist genau dann durch 2000 teilbar, wenn sie durch 2^4 und durch 5^3 teilbar ist (Satz 1.9). Wir setzen $x_n = 121^n - 25^n + 1900^n - (-4)^n$.

Modulo $2^4 = 16$ gilt für $n \geq 2$

$$x_n = 121^n - 25^n + 1900^n - (-4)^n \equiv 9^n - 9^n + 0 - 0 \equiv 0 \pmod{16},$$

weil $121 = 112 + 9 = 7 \cdot 16 + 9 \equiv 9 \pmod{16}$ und $16 \mid 1900^n$ und $16 \mid (-4)^n$. Für $n \geq 2$ ist x_n daher durch 16 teilbar.

Modulo $5^3 = 125$ gilt für $n \geq 2$

$$x_n = 121^n - 25^n + 1900^n - (-4)^n \equiv (-4)^n - 0 + 0 - (-4)^n \equiv 0 \pmod{5^3},$$

die Zahl x_n ist also durch 5^3 teilbar.

Nach der Vorbemerkung ist also die Behauptung für $n \geq 2$ bewiesen. Für $n = 1$ sieht man durch Einsetzen, dass $x_1 = 2000$, was klarerweise auch durch 2000 teilbar ist. □

Satz 2.3. *Stellt man eine natürliche Zahl a als*

$$a = a_n 10^n + a_{n-1} 10^{n-1} + \ldots + a_2 10^2 + a_1 10^1 + a_0$$

im Dezimalsystem dar und schreibt dafür kurz

$$a = (a_n a_{n-1} \ldots a_2 a_1 a_0)_{10},$$

so gilt:

1. $a \equiv a_0 \pmod{2 \text{ bzw. } 5}$
2. $a \equiv (a_1 a_0)_{10} \pmod 4$
3. $a \equiv (a_2 a_1 a_0)_{10} \pmod 8$
4. $a \equiv a_n + a_{n-1} + \ldots + a_2 + a_1 + a_0 \pmod{3 \text{ bzw. } 9}$
5. $a \equiv a_0 - a_1 + a_2 - + \ldots \pm a_n \pmod{11}$
6. $a \equiv (a_2 a_1 a_0)_{10} - (a_5 a_4 a_3)_{10} + (a_8 a_7 a_6)_{10} - + \ldots \pmod{7 \text{ bzw. } 13}$

Beweis.

1. Wegen $10 \equiv 0 \pmod{2 \text{ bzw. } 5}$ gilt $a_k 10^k \equiv 0 \pmod{2 \text{ bzw. } 5}$ für alle $k \geq 1$. Daher gilt $a = a_n 10^n + \cdots + a_1 10^1 + a_0 \equiv 0 + \cdots + 0 + a_0 \pmod{2 \text{ bzw. } 5}$.

2. Wegen $4 \mid 100$ und $100 \mid 10^k$ für alle $k \geq 2$ gilt $a_k 10^k \equiv 0 \pmod 4$ für alle $k \geq 2$. Daher gilt $a \equiv 0 + 0 + \cdots + 10a_1 + a_0 = (a_1 a_0)_{10} \pmod 4$.

3. $8 \mid 1000$ und dann weiter wie bei 2.

4. Wegen $10 \equiv 1 \pmod{3 \text{ bzw. } 9}$ gilt $10^k \equiv 1^k = 1 \pmod{3 \text{ bzw. } 9}$ für alle $k \geq 1$. $a = a_n 10^n + \cdots + a_1 10^1 + a_0 \equiv a_n + a_{n-1} + \cdots + a_2 + a_1 + a_0 \pmod{3 \text{ bzw. } 9}$.

5. Wegen $10 \equiv -1 \pmod{11}$ gilt $10^k \equiv (-1)^k \pmod{11}$, also $a = a_0 + a_1 10^1 + \cdots + a_n 10^n \equiv a_0 - a_1 + a_2 - + \cdots \pm a_n \pmod{11}$.

6. Wegen $1000 \equiv -1 \pmod{7 \text{ bzw. } 13}$ gilt: $10^{3k} \equiv (-1)^k \pmod{7 \text{ bzw. } 13}$, daher $a = (a_2 a_1 a_0)_{10} + 10^3 (a_5 a_4 a_3)_{10} + 10^{3 \cdot 2} (a_8 a_7 a_6)_{10} + \cdots \equiv (a_2 a_1 a_0)_{10} - (a_5 a_4 a_3)_{10} + (a_8 a_7 a_6)_{10} - + \cdots \pmod{13 \text{ bzw. } 7}$.

□

Daraus folgen unmittelbar die bekannten *Teilbarkeitsregeln*:

Eine Zahl ist genau dann durch ... teilbar,	wenn es ... ist.
2 bzw. 5	ihre letzte Ziffer
4	die Zahl aus ihren letzten beiden Ziffern
8	die Zahl aus ihren letzten drei Ziffern
3 bzw. 9	ihre Ziffernsumme
11	ihre alternierende Ziffernsumme (Querdifferenz)
7 bzw. 13	die alternierende Summe ihrer Dreierblöcke

3 Lösen von Kongruenzen

3.1 Lineare Kongruenzen

Unter einer linearen Kongruenz versteht man einen Ausdruck der Form

$$ax \equiv b \pmod{m}, \tag{3.1.1}$$

wobei die ganzen Zahlen a und b sowie der Modul m gegeben sind und alle ganzen x gesucht werden, die obige Aussage erfüllen.

Es sind notwendige und hinreichende Bedingungen für die Lösbarkeit einer solchen linearen Kongruenz sowie die Anzahl der inkongruenten Lösungen modulo m interessant.

Wir setzen $d := \mathrm{ggT}(a, m)$. Nehmen wir zunächst an, dass (3.1.1) eine Lösung x besitzt. Da $d \mid a$ und $d \mid m \mid ax - b$ folgt nach Satz 1.1 auch $d \mid b$. Letztere Bedingung ist also notwendig für die Lösbarkeit der Kongruenz.

Wir nehmen jetzt umgekehrt $d \mid b$ an. Nach Satz 1.4 gibt es ganze Zahlen x' und y, sodass

$$d = \mathrm{ggT}(a, m) = ax' - my. \tag{3.1.2}$$

Schreiben wir $b' := b/d$, was ja nach Annahme eine ganze Zahl ist. Multiplizieren wir die Gleichung (3.1.2) mit b', so erhalten wir $b = db' = a(b'x') - m(yb')$, es ist damit $x = b'x'$ eine Lösung von (3.1.1).

Daher ist $d \mid b$ auch hinreichende Bedingung für die Lösung. Es bleibt noch die Frage nach der Anzahl der Lösungen. Dabei ist klar, dass mit x auch jedes Element der Restklasse $\bar{x}$ eine Lösung ist. Interessant ist also die Anzahl inkongruenter Lösungen modulo m.

Sei x_0 eine (fixe) Lösung, zum Beispiel die oben gefundene, und x eine weitere Lösung von (3.1.1). Dann gilt $ax \equiv b \equiv ax_0 \pmod{m}$, woraus $m \mid a \cdot (x - x_0)$ folgt. Wir schreiben $a' = a/d$ und $m' = m/d$. Nach Satz 1.1 (3) gilt auch $m' \mid a' \cdot (x - x_0)$ und wegen $\mathrm{ggT}(a', m') = 1$ folgt nach Satz 1.6

$$m' \mid (x - x_0) \iff x \equiv x_0 \pmod{m'}.$$

Alle Lösungen haben daher die Form $x_k = x_0 + km'$ mit einem ganzen k. Jedes dieser x_k, $k \in \mathbb{Z}$, ist auch tatsächlich Lösung, denn $ax_k = a'd(x_0 + km') = (a'd)x_0 + ka'(m'd) = ax_0 + ka'm \equiv b \pmod{m}$.

Zwei Lösungen x_i und x_j sind genau dann kongruent modulo m, wenn $im' \equiv jm' \pmod{dm'}$, also $i \equiv j \pmod{d}$. Es gibt damit genau d inkongruente Lösungen modulo m, nämlich $x_0, x_1, \ldots, x_{d-1}$.

Zusammenfassend gilt:

Satz 3.1. *Die lineare Kongruenz* $ax \equiv b \pmod{m}$ *ist genau dann lösbar, wenn* $\mathrm{ggT}(m,a) \mid b$. *In diesem Fall gibt es genau* $\mathrm{ggT}(m,a)$ *inkongruente Lösungen modulo* m.

Im wichtigen Spezialfall $b = 1$ gilt $\mathrm{ggT}(m,a) \mid b$ natürlich genau dann, wenn $\mathrm{ggT}(m,a) = 1$. Wir erhalten also:

Korollar 3.1.1. *Seien* a *und* $m \geq 1$ *ganze Zahlen. Es gibt genau dann ein ganzes* x *mit*

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

wenn $\mathrm{ggT}(a,m) = 1$. *In diesem Fall gibt es genau eine Lösung* x *modulo* m.

Diese eindeutige Lösung x wird manchmal auch als a^{-1} oder $1/a$ bezeichnet.

Aufgabe 3.1.2. Man bestimme alle Lösungen der Kongruenz

$$10x \equiv 46 \pmod{128}.$$

Lösung. Da $\mathrm{ggT}(128,10) = 2 \mid 46$, besitzt die Kongruenz Lösungen, und zwar genau $\mathrm{ggT}(128,10) = 2$ modulo 128. Wir dividieren die gesamte Kongruenz (inklusive des Moduls) durch 2 und erhalten

$$5x \equiv 23 \pmod{64}.$$

Wir führen nun den Euklidschen Algorithmus für 64 und 5 aus:

$$\begin{aligned} 4 &= 1 \cdot 64 + \ \ 0 \cdot 5 \\ 5 &= 0 \cdot 64 + \ \ 1 \cdot 5 \mid \cdot(-13) \\ \hline -1 &= 1 \cdot 64 - 13 \cdot 5. \end{aligned}$$

Offensichtlich gilt $13 \cdot 5 \equiv 1 \pmod{64}$, also $23 \cdot 13 \cdot 5 \equiv 23$. Wir erhalten damit als Lösung $x \equiv 23 \cdot 13 \equiv 299 \equiv 43 \pmod{64}$.

Die Lösungen modulo 128 sind daher 43 und $43 + 64 = 107$. □

3.2 Simultane Kongruenzen

Unter einer simultanen Kongruenz versteht man ein System von linearen Kongruenzen

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_n \pmod{m_n}, \end{aligned} \tag{3.2.1}$$

für die alle Lösungen $x \in \mathbb{Z}$ bestimmt werden sollen, die sämtliche Kongruenzen gleichzeitig lösen.

Ein solches System kann, muss aber keine Lösungen haben. Beispielsweise gibt es für das System

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 1 \pmod 9 \end{aligned}$$

keine Lösung, da aus $x \equiv 1 \pmod 9$ auch $x \equiv 1 \pmod 3$ folgt, weshalb $2 \equiv x \equiv 1 \pmod 3$ gelten müsste. Daher ist es sinnvoll, nur paarweise teilerfremde Moduln zuzulassen.

Satz 3.2 (Chinesischer Restsatz)**.** *Seien $m_1, \ldots, m_n$ paarweise teilerfremde positive Zahlen und $a_1, \ldots, a_n$ ganze Zahlen. Dann gibt es genau ein x modulo $m_1 m_2 m_3 \cdots m_n$, sodass*

$$x \equiv a_j \pmod{m_j} \qquad \textit{für } j = 1, \ldots, n$$

gilt.

Beweis. Wir beweisen die Existenz einer Lösung durch Induktion nach n. Für $n = 1$ ist nichts zu zeigen. Wir zeigen nun den Schritt von n auf $n+1$. Setze $M := m_1 \cdots m_n$. Nach Induktionsvoraussetzung gibt es ein $A \in \mathbb{Z}$ mit $A \equiv a_j \pmod{m_j}$ für $j = 1, \ldots, n$. Wir wählen den Ansatz $x = A + y \cdot M$ mit einem unbekannten $y \in \mathbb{Z}$. Dieses x erfüllt wegen der Wahl von A jedenfalls die Kongruenz

$$x = A + y \cdot M \equiv A \equiv a_j \pmod{a_j}, \qquad \text{für } j = 1, \ldots, n.$$

Wir haben also alle Freiheiten bei der Wahl von y, um die letzte Kongruenz

$$x = A + y \cdot M \equiv a_{n+1} \pmod{m_{n+1}}$$

zu erfüllen. Diese ist aber äquivalent zu

$$y \cdot M \equiv a_{n+1} - A \pmod{m_{n+1}},$$

und diese Kongruenz ist laut Satz 3.1 lösbar, weil laut Voraussetzung $\operatorname{ggT}(M, m_{n+1}) = \operatorname{ggT}(m_1 \cdots m_n, m_{n+1}) = 1$ gilt.

Zum Beweis der Eindeutigkeit nehmen wir an, dass ein $x' \in \mathbb{Z}$ ebenfalls die Kongruenzen $x' \equiv a_j \pmod{m_j}$ für $j = 1, \ldots, n$ erfüllt. Daraus folgt aber $x' \equiv a_j \equiv x \pmod{m_j}$, also

$$m_j \mid (x - x')$$

für $j = 1, \ldots, n$. Da die Moduln paarweise teilerfremd sind, schließen wir, dass

$$m_1 \cdots m_n \mid (x - x'),$$

die Zahlen x und x' sind daher modulo $m_1 \cdots m_n$ kongruent. □

Aufgabe 3.2.1. Bestimme alle ganzen Zahlen x, die die simultanen Kongruenzen

$$\begin{aligned} x &\equiv 1 \pmod 2 \\ x &\equiv 3 \pmod 5 \\ x &\equiv 2 \pmod 7 \end{aligned}$$

erfüllen.

Lösung. Wir setzen $x_2 = 1 + 2 \cdot y_2$ (dies erfüllt offensichtlich die erste Kongruenz) und stellen fest, dass y_2 so gewählt werden muss, dass

$$2y_2 \equiv 2 \pmod 5.$$

Diese Kongruenz hat offensichtlich die Lösung $y_2 = 1$ und wir erhalten $x_2 = 3$.

Nun setzen wir $x_3 = x_2 + 2 \cdot 5 \cdot y_3 = 3 + 10y_3$ an und müssen

$$3 + 10y_3 \equiv 2 \pmod 7 \iff 3y_3 \equiv -1 \pmod 7$$

lösen. Die Lösung $y_3 = 2$ kann man erraten (oder den Euklidschen Algorithmus anwenden!). Somit erhielten wir $x = x_3 = 23$. Diese Lösung ist Modulo $2 \cdot 5 \cdot 7 = 70$ eindeutig. □

Die Bedeutung des chinesischen Restsatzes liegt nicht nur in der konkreten Lösung eines Systems simultaner Kongruenzen, sondern er erlaubt auch, Fragestellung modulo $m = p_1^{\alpha_1} \cdots p_r^{\alpha_j}$ auf r simultane Kongruenzen modulo $p_1^{\alpha_1}$, …, $p_r^{\alpha_r}$ zu zerlegen, dort die geforderte Untersuchung durchzuführen, und am Schluss das Resultat mit Hilfe des chinesischen Restsatzes wieder modulo m zusammenzusetzen.

4 Zahlentheoretische Funktionen

4.1 Eulersche φ-Funktion

Definition 4.1.1. Sei $m \geq 2$ eine ganze Zahl. Die Anzahl der $0 \leq a < m$ mit $\mathrm{ggT}(a, m) = 1$ bezeichnet man mit $\varphi(m)$. Weiters definiert man $\varphi(1) := 1$.

Man bezeichnet die $0 \leq a_1 < \ldots < a_{\varphi(m)} < m$, für die $\mathrm{ggT}(a_i, m) = 1$ gilt, als *prime Reste modulo m*. Da nach Satz 1.3 $\mathrm{ggT}(a, m) = \mathrm{ggT}(x, m)$ für alle $x \in \bar{a}$, bezeichnet man $\overline{a_1}, \ldots, \overline{a_{\varphi(m)}}$ als *prime Restklassen modulo m*.

Satz 4.1. *Sei p eine Primzahl und $\alpha \geq 1$. Dann gilt*

$$\varphi(p^\alpha) = p^{\alpha-1}(p-1).$$

Beweis. Zu p^α sind alle Zahlen $\leq p^\alpha$ teilerfremd, die nicht von p geteilt werden. Vielfache von p, die $\leq p^\alpha$ sind, sind $1 \cdot p, 2 \cdot p, \ldots, p^{\alpha-1} \cdot p$ und ihre Anzahl beträgt $p^{\alpha-1}$. Daher gilt:

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1).$$

□

Satz 4.2. *Die φ-Funktion ist multiplikativ, das heißt:*

$$\varphi(mn) = \varphi(m)\varphi(n) \text{ für } \operatorname{ggT}(m,n) = 1.$$

Beweis. Seien $0 \leq a < m$ und $0 \leq b < n$. Nach dem chinesischen Restsatz 3.2 gibt es genau ein $1 \leq x < mn$, sodass $x \equiv a \pmod{m}$ und $x \equiv b \pmod{n}$.

Wir behaupten nun, dass

$$\operatorname{ggT}(x, mn) = 1 \iff \operatorname{ggT}(a,m) = 1 \text{ und } \operatorname{ggT}(b,n) = 1. \tag{4.1.1}$$

Nehmen wir an, dass $1 \neq d \mid a$ und $d \mid m$. Dann folgt wegen $x \equiv a \pmod{m}$ auch $d \mid x$, wir haben also einen gemeinsamen Teiler von x und mn gefunden. Ist andererseits p ein Primteiler von x und von mn, so folgt nach Satz 1.7, dass $p \mid m$ oder $p \mid n$. Ohne Beschränkung der Allgemeinheit gelte Ersteres. Wegen $p \mid x$, $p \mid m$ und $a \equiv x \pmod{m}$ gilt auch $p \mid a$. Wir haben also einen gemeinsamen Teiler von a und m gefunden. Somit ist (4.1.1) bewiesen.

Somit ist die Anzahl der zu mn teilerfremden Zahlen x mit $0 \leq x < mn$ gleich der Anzahl der Paare (a,b) mit $\operatorname{ggT}(a,m) = \operatorname{ggT}(b,n) = 1$, $0 \leq a < m$ und $0 \leq b < n$. Letztere Anzahl ist aber genau $\varphi(m)\varphi(n)$. □

Dieser Satz lässt sich durch Induktion auf k paarweise teilerfremde Zahlen $m_1, \ldots, m_k$ verallgemeinern:

$$\varphi(m_1 m_2 m_3 \cdots m_k) = \varphi(m_1)\varphi(m_2)\varphi(m_3)\cdots\varphi(m_k).$$

Wir erhalten also zusammenfassend:

Satz 4.3. *Gilt für m die kanonische Darstellung*

$$m = \prod_{p \mid m} p^{\alpha_p},$$

so gilt:

$$\varphi(m) = \prod_{p \mid m} p^{\alpha_p - 1}(p-1) = m \cdot \prod_{p \mid m} \left(1 - \frac{1}{p}\right).$$

Insbesondere gilt: $\varphi(p) = p - 1$, wenn p Primzahl.

Beweis.

$$\begin{aligned}\varphi(m) &= \varphi(p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_n^{\alpha_n}) = \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2})\varphi(p_3^{\alpha_3})\cdots\varphi(p_n^{\alpha_n}) = \\ &= p_1^{\alpha_1 - 1}(p-1)p_2^{\alpha_2 - 1}(p_2 - 1)p_3^{\alpha_3 - 1}(p_3 - 1)\cdots p_n^{\alpha_n - 1}(p_n - 1) = \prod_{p \mid m} p^{\alpha_p - 1}(p-1).\end{aligned}$$

□

Die φ-Funktion wird sich später bei der Untersuchung von Potenzresten (beim Satz von Euler-Fermat) als nützlich herausstellen.

4.2 Anzahl der Teiler $\tau(n)$

Definition 4.2.1. Sei n eine positive ganze Zahl. Dann bezeichnet $\tau(n)$ die Anzahl der positiven Teiler von n.

Satz 4.4. *Sei n eine positive ganze Zahl mit Primfaktordarstellung*

$$n = \prod_{p|n} p^{\alpha_p} \text{ mit } \alpha_p \geq 1.$$

Dann gilt

$$\tau(n) = \prod_{p|n} (\alpha_p + 1). \tag{4.2.1}$$

Insbesondere ist τ eine multiplikative Funktion, also gilt $\tau(m \cdot n) = \tau(m) \cdot \tau(n)$ für teilerfremde Zahlen m und n.

Beweis. Sei d eine positive Zahl mit Primfaktordarstellung $d = \prod_p p^{\beta_p}$. Nach Satz 1.8 ist d genau dann ein Teiler von n, wenn

$$0 \leq \beta_p \leq \alpha_p$$

für alle Primzahlen p gilt. Für jeden Primteiler p von n haben wir also die $\alpha_p + 1$ Möglichkeiten $0, \ldots, \alpha_p$ für die Wahl von β_p. Daraus folgt (4.2.1).

Die Multiplikativität von τ sieht man entweder aus (4.2.1) oder argumentiert direkt: Jeder Teiler d von $m \cdot n$ für teilerfremde m und n kann eindeutig in ein Produkt $d = a \cdot b$ zerlegt werden, wobei a ein Teiler von m und b ein Teiler von n ist. Umgekehrt ergibt sich für jedes Paar (a, b), wobei a ein Teiler von a und b ein Teiler von b ist, genau ein Teiler $a \cdot b$ von $m \cdot n$. Somit gilt $\tau(m \cdot n) = \tau(m) \cdot \tau(n)$. □

Aufgabe 4.2.2. Bestimmen Sie alle positiven ganzen Zahlen n mit der Eigenschaft, dass $n = \big(\tau(n)\big)^2$. *(Kanada 1999/3)*

Lösung. Sei $\alpha_p := v_p(n)$. Da $\tau(n) = \prod_{p|n}(\alpha_p + 1)$ (Satz 4.6), folgt

$$\prod_{p|n} p^{\alpha_p} = n = \tau(n)^2 = \prod_{p|n} (\alpha_p + 1)^2.$$

Da n offensichtlich eine Quadratzahl ist, ist α_p stets gerade, und damit n als Produkt $\prod_{p|n}(\alpha_p+1)^2$ ungerade. Nun ist $(\alpha_p+1)^2$ im Allgemeinen deutlich kleiner als p^{α_p}, wodurch diese Gleichung nur in Ausnahmefällen stimmen wird. Präziser gilt für $p \geq 3$ und $\alpha_p \geq 2$ nach dem binomischen Lehrsatz, dass

$$\begin{aligned} p^{\alpha_p} &= ((p-1)+1)^{\alpha_p} \geq 1 + \alpha_p(p-1) + \frac{\alpha_p(\alpha_p-1)}{2}(p-1)^2 \geq 1 + 2\alpha_p + 2\alpha_p(\alpha_p-1) \\ &= 2\alpha_p^2 + 1 \geq (\alpha_p+1)^2. \end{aligned}$$

Dabei gilt Gleichheit genau für $p = 3$ und $\alpha_3 = 2$. Damit sind die einzigen Lösungen $n = 1$ und $n = 9$. □

4.3 Summe der Teiler $\sigma(n)$

Definition 4.3.1. Sei n eine positive ganze Zahl. Dann bezeichnet $\sigma(n)$ die Summe der positiven Teiler von n.

Satz 4.5. *Sei p eine Primzahl und $\alpha \geq 1$. Dann gilt*

$$\sigma(p^\alpha) = \frac{p^{\alpha+1}-1}{p-1}.$$

Beweis. Die Teiler von p^α sind genau $1 = p^0$, $p = p^1$, $\ldots$, p^α. Damit gilt

$$\sigma(p^\alpha) = 1 + p + \cdots + p^\alpha = \frac{p^{\alpha+1}-1}{p-1}$$

nach der Summenformel für die endliche geometrische Reihe. □

Satz 4.6. *Die Funktion σ ist* multiplikativ, *d.h. $\sigma(mn) = \sigma(m)\sigma(n)$ für teilerfremde m und n.*

Beweis. Sei d ein Teiler von mn und $d_1 = \mathrm{ggT}(d, m)$ und $d_2 = d/d_1$. Dann folgt aus $d_2 \mid mn$ nach Satz 1.6, dass $d_2 \mid n$. Jeder Teiler d von mn kann somit als Produkt $d = d_1 \cdot d_2$ eines Teilers d_1 von m und eines Teilers d_2 von n geschrieben werden. Nach der eindeutigen Primfaktordarstellung ist diese Darstellung eindeutig.

Damit haben wir

$$\sigma(mn) = \sum_{d \mid mn} d = \sum_{d_1 \mid m} \sum_{d_2 \mid n} d_1 d_2 = \sum_{d_1 \mid m} d_1 \Big(\sum_{d_2 \mid n} d_2 \Big) = \sum_{d_1 \mid m} d_1 \sigma(n) = \sigma(n) \sum_{d_1 \mid m} d_1 = \sigma(n)\sigma(m).$$

(Es wurde also die Summation so umgeordnet, dass jeweils d_1 herausgehoben werden konnte.) □

Wie im Fall der φ-Funktion erhält man somit eine Formel für $\sigma(n)$:

Satz 4.7. *Sei n eine positive ganze Zahl mit Primfaktordarstellung*

$$n = \prod_{p \mid n} p^{\alpha_p} \text{ mit } \alpha_p \geq 1.$$

Dann gilt

$$\sigma(n) = \prod_{p \mid n} \frac{p^{\alpha+1}-1}{p-1}.$$

4.4 Primfaktorzerlegung von Fakultäten

In diesem Abschnitt soll die Primfaktorzerlegung von $n! = 1 \cdot 2 \cdots (n-1) \cdot n$ für $n \geq 1$ angegeben werden.

Satz 4.8 (Legendre). *Sei $n \geq 1$ und p eine Primzahl. Dann gilt*

$$v_p(n!) = \sum_{k=1}^{\left\lfloor \frac{\ln n}{\ln p} \right\rfloor} \left\lfloor \frac{n}{p^k} \right\rfloor .$$

Beweis. Nach der eindeutigen Primfaktorzerlegung gilt

$$v_p(n!) = v_p\left(\prod_{\ell=1}^{n} \ell\right) = \sum_{\ell=1}^{n} v_p(\ell).$$

Zu dieser Summe tragen alle Zahlen $1 \leq \ell \leq n$, die durch p teilbar sind, 1 bei, weiters alle durch p^2 teilbaren Zahlen noch einen weiteren Summanden 1 usw. Durch p teilbar sind die Zahlen $p, 2p, \ldots, \lfloor n/p \rfloor \cdot p$ (also $\lfloor n/p \rfloor$ Stück), durch p^2 teilbar sind die Zahlen $p^2, 2p^2, \ldots, \lfloor n/p^2 \rfloor \cdot p^2$ (also $\lfloor n/p^2 \rfloor$ Stück) usw. Da unter den Zahlen von 1 bis n nur Vielfache von p^k mit $p^k \leq n$ vorkommen können, wobei letzteres äquivalent mit $k \leq \ln n / \ln p$ ist, brauchen wir nur Exponenten k kleiner oder gleich $\lfloor \ln n / \ln p \rfloor$ zu betrachten.

In Formeln:

$$\sum_{\ell=1}^{n} v_p(\ell) = \sum_{k=1}^{\infty} \sum_{\substack{\ell=1 \\ v_p(\ell)=k}}^{n} k = \sum_{k=1}^{\infty} \sum_{\substack{\ell=1 \\ v_p(\ell)\geq k}}^{n} 1 = \sum_{k=1}^{\infty} \sum_{\substack{\ell=1 \\ p^k \mid \ell}}^{n} 1 = \sum_{k=1}^{\infty} \sum_{m:1 \leq m p^k \leq n} 1$$

$$= \sum_{k=1}^{\infty} \sum_{1 \leq m \leq n/p^k} 1 = \sum_{k=1}^{\infty} \sum_{1 \leq m \leq \lfloor n/p^k \rfloor} 1 = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor = \sum_{\substack{k=1 \\ n/p^k \geq 1}}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor = \sum_{k=1}^{\left\lfloor \frac{\ln n}{\ln p} \right\rfloor} \left\lfloor \frac{n}{p^k} \right\rfloor .$$

□

Aufgabe 4.4.1. Für natürliche Zahlen a und b sei

$$Z(a,b) = \frac{(3a)!(4b)!}{(a!)^4 (b!)^3}.$$

Man zeige: Für $a \leq b$ ist $Z(a,b)$ eine natürliche Zahl. *(35. Österreichische Mathematische Olympiade 2004, Bundeswettbewerb für Fortgeschrittene, Teil 1)*

Lösung. Sei p eine beliebige Primzahl und k eine positive ganze Zahl. Es gilt

$$\frac{3a}{p^k} \geq 3 \left\lfloor \frac{a}{p^k} \right\rfloor , \qquad \frac{4b}{p^k} \geq 4 \left\lfloor \frac{b}{p^k} \right\rfloor ,$$

daher auch

$$\left\lfloor \frac{3a}{p^k} \right\rfloor \geq 3 \left\lfloor \frac{a}{p^k} \right\rfloor, \qquad \left\lfloor \frac{4b}{p^k} \right\rfloor \geq 4 \left\lfloor \frac{b}{p^k} \right\rfloor.$$

Summiert man über alle $k \geq 1$, so erhält man

$$v_p((3a)!) = \sum_{k\geq 1} \left\lfloor \frac{3a}{p^k} \right\rfloor \geq 3 \sum_{k\geq 1} \left\lfloor \frac{a}{p^k} \right\rfloor = 3v_p(a!) = v_p((a!)^3),$$
$$v_p((4b)!) = \sum_{k\geq 1} \left\lfloor \frac{4b}{p^k} \right\rfloor \geq 4 \sum_{k\geq 1} \left\lfloor \frac{b}{p^k} \right\rfloor = 4v_p(b!) = v_p((b!)^4),$$

daher teilt $(a!)^3(b!)^4$ die Zahl $(3a)!(4b)!$. Wegen $b \geq a$ teilt $(a!)^4(b!)^3$ die Zahl $(a!)^3(b!)^4$ und daher ebenfalls $(3a)!(4b)!$.

Variante: Man kann $(3a)!/(a!)^3$ auch als Multinomialkoeffizient deuten, d.h. die Anzahl der Möglichkeiten, $3a$ Elemente in drei Klassen zu je a Elementen einzuteilen. Diese Anzahl ist offensichtlich ganzzahlig. Analog geht man für $(4b)!/(b!)^4$ vor und benutzt dann wieder die Annahme $a \leq b$. □

5 Potenzreste

5.1 Ordnung eines Elements

Wir versuchen hier, Regelmäßigkeiten bei den Potenzen a^k modulo m festzustellen.

Beispiel 5.1.1. Wir betrachten den Modul $m = 9$ und erhalten (wenn wir nur die Reste modulo 9 betrachten) die in Tabelle 1 wiedergegebene „Potenzierungstabelle“ modulo 9.

a	a^0	a^1	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	$\cdots$
0		0	0	0	0	0	0	0	0	0	0	0	0	0	$\cdots$
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	$\cdots$
2	1	2	4	−1	−2	−4	1	2	4	−1	−2	−4	1	2	$\cdots$
3	1	3	0	0	0	0	0	0	0	0	0	0	0	0	$\cdots$
4	1	4	−2	1	4	−2	1	4	−2	1	4	−2	1	4	$\cdots$
−4	1	−4	−2	−1	4	2	1	−4	−2	−1	4	2	1	−4	$\cdots$
−3	1	−3	0	0	0	0	0	0	0	0	0	0	0	0	$\cdots$
−2	1	−2	4	1	−2	4	1	−2	4	1	−2	4	1	−2	$\cdots$
−1	1	−1	1	−1	1	−1	1	−1	1	−1	1	−1	1	−1	$\cdots$

Tabelle 1: Potenzen modulo 9.

Die Zeilen für die Reste $a = 0$, 3 und -3 führen rasch zu 0. Jede Multiplikation davon mit einem weiteren Faktor a führt klarerweise wieder zu einem Rest von 0. Diese Zeilen sind „schließlich periodisch“, d.h., nach einer Vorperiode (in unserem Fall der Länge höchstens

1) tritt Periodizität mit der Periode 1 auf. Man beachte, dass diese Zeilen genau jenen a entsprechen, die nicht zu 9 teilerfremd sind.

Interessanter sind die Zeilen, die zu 9 teilerfremden Zahlen entsprechen. Hier tritt ein reinperiodisches Muster auf, die Periodenlängen sind 1, 2, 3 und 6, sind also Teiler von 6. Schließlich steht in den Spalten für a^0, a^6, a^{12} in diesen Zeilen ein Rest von 1.

Zunächst beweisen wir die Periodizität für allgemeine Moduln.

Satz 5.1. *Seien m und a teilerfremde ganze Zahlen. Dann gilt:*

1. *Die Folge der Reste von a^k modulo m ist rein periodisch.*

   Die primitive Periodenlänge (d.h. die kleinste positive ganze Zahl ℓ mit $a^{k+\ell} \equiv a^k \pmod{m}$ für alle positiven ganzen Zahlen k) wird als die Ordnung von a modulo m *bezeichnet, wir schreiben $\ell = \mathrm{ord}_m(a)$.*

2. *Die Ordnung $\mathrm{ord}_m(a)$ ist die kleinste positive ganze Zahl ℓ, sodass $a^\ell \equiv 1 \pmod{m}$.*

3. *Es gilt $a^j \equiv a^k \pmod{m}$ für positive ganze Zahlen j und k genau dann, wenn $j \equiv k \pmod{\mathrm{ord}_m(a)}$.*

4. *Insbesondere gilt $a^k \equiv 1 \pmod{m}$ für eine positive ganze Zahl k genau dann, wenn $\mathrm{ord}_m(a)$ ein Teiler von k ist.*

Beweis. 1. Für die unendlich vielen Potenzen $a^0, a^1, a^2, a^3, \ldots$ stehen nur $m-1$ Reste zur Verfügung (der Rest 0 kann wegen $\mathrm{ggT}(a, m) = 1$ nicht auftreten). Daher muss es eine Wiederholung geben.

Es sei ℓ die kleinste positive ganze Zahl, sodass es eine nicht-negative ganze Zahl j mit

$$a^{j+\ell} \equiv a^j \pmod{m}$$

gibt.

Es gilt also

$$a^j a^\ell \equiv a^j \pmod{m}.$$

Da $\mathrm{ggT}(a^j, m) = 1$, gilt nach Satz 2.2 (5)

$$a^\ell \equiv a^0 = 1 \pmod{m}. \tag{5.1.1}$$

Durch Multiplikation mit a^k für eine beliebige ganze Zahl k folgt

$$a^{k+\ell} \equiv a^k \pmod{m},$$

somit ist die Folge der Potenzen von a modulo m periodisch mit Periodenlänge ℓ. Aufgrund der Wahl von ℓ handelt es sich auch um die kürzest mögliche Periodenlänge, das heißt, ℓ ist die primitive Periodenlänge.

2. Laut (5.1.1) gilt jedenfalls $a^{\operatorname{ord}_m(a)} \equiv 1 \pmod{m}$.

   Aufgrund der Minimalität von ℓ kann es keine ganze Zahl i mit $0 < i < \operatorname{ord}_m(a)$ und $a^i \equiv 1 = a^0 \pmod{m}$ geben.

4. Sei zunächst k ein Vielfaches der Ordnung von a, also $k = \operatorname{ord}_m(a) \cdot q$ für eine passende ganze Zahl q. Dann gilt

   $$a^k \equiv (a^{\operatorname{ord}_m(a)})^q \equiv 1^q \equiv 1 \pmod{m},$$

   was zu zeigen war.

   Es gelte umgekehrt $a^k \equiv 1 \pmod{m}$. Wir dividieren k durch $\operatorname{ord}_m(a)$ mit Rest und erhalten $k = q \cdot \operatorname{ord}_m(a) + r$ für passende ganze Zahlen q und r mit $0 \leq r < m$. Wir wissen aus dem ersten Teil, dass $a^{q \operatorname{ord}_m(a)} \equiv 1 \pmod{m}$, somit erhalten wir

   $$1 \equiv a^k \equiv a^{q \operatorname{ord}_m(a)} \cdot a^r \equiv a^r \pmod{m}.$$

   Aus Punkt 2. und $r < \operatorname{ord}_m(a)$ folgt $r = 0$. Somit ist k ein Vielfaches von $\operatorname{ord}_m(a)$.

3. Seien $j < k$ positive ganze Zahlen. Da $\operatorname{ggT}(a^j, m) = 1$, ist $a^j \equiv a^k \pmod{m}$ äquivalent zu $1 \equiv a^{k-j} \pmod{m}$. Nach dem bereits bewiesenen Teil 4. ist das äquivalent zu $k - j \equiv 0 \pmod{\operatorname{ord}_m(a)}$, also $k \equiv j \pmod{\operatorname{ord}_m(a)}$.

□

Wenn man die Ordnung von a modulo m kennt, so kennt man auch die Ordnung beliebiger Potenzen von a modulo m:

Satz 5.2. *Seien a und m teilerfremd und j eine ganze Zahl. Dann gilt*

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

Beweis. Für ein $k \in \mathbb{Z}$ gilt $a^{jk} = (a^j)^k \equiv 1 \pmod{m}$ genau dann, wenn die Ordnung $\operatorname{ord}_m(a)$ ein Teiler von jk ist. Das ist genau dann der Fall, wenn $\operatorname{ord}_m(a)/\operatorname{ggT}(j, \operatorname{ord}_m(a))$ ein Teiler von k ist. Somit ist die Ordnung von a^j modulo m genau $\operatorname{ord}_m(a)/\operatorname{ggT}(j, \operatorname{ord}_m(a))$. □

5.2 Satz von Euler-Fermat

In Beispiel 5.1.1 wurde bemerkt, dass $a^6 \equiv 1 \pmod{9}$ für alle zu 9 teilerfremden a gilt. In Bezug auf diese Beobachtung fand Pierre Simon de Fermat (1601–1665) den folgenden grundlegenden Satz:

Satz 5.3 (Kleiner Satz von Fermat)**.** *Für eine Primzahl p und eine nicht durch p teilbare ganze Zahl a gilt*

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

Leonhard Euler bewies dann die Verallgemeinerung dieses Satzes:

Satz 5.4 (Euler-Fermat)**.** *Seien a und $m \geq 2$ teilerfremde ganze Zahlen. Dann gilt*

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

Tatsächlich gilt: $\varphi(9) = 6$.

Der kleine Satz von Fermat ist eine direkte Konsequenz des Satzes von Euler-Fermat, weil für eine Primzahl p die Beziehung $\varphi(p) = p - 1$ gilt.

Beweis von Satz 5.4. Seien $1 \leq x_1 < \cdots < x_{\varphi(m)} < m$ die $\varphi(m)$ primen Reste modulo m. Sei weiters $y_i := ax_i$ für $1 \leq i \leq \varphi(m)$. Da $\mathrm{ggT}(a, m) = \mathrm{ggT}(x_i, m) = 1$, muss auch $\mathrm{ggT}(y_i, m) = 1$ gelten. Weiters sind die y_i wegen Satz 2.2 (5) paarweise inkongruent modulo m. Damit durchläuft y_i, $1 \leq i \leq \varphi(m)$, genau die primen Restklassen modulo m. Daher gilt $y_1 \dots y_{\varphi(m)} \equiv x_1 \dots x_{\varphi(m)} \pmod{m}$. Setzt man die Definition der y_i ein, so erhält man

$$a^{\varphi(m)} x_1 \dots x_{\varphi(m)} = (ax_1) \dots (ax_{\varphi(m)}) \equiv x_1 \dots x_{\varphi(m)} \pmod{m}.$$

Da $\mathrm{ggT}(x_1 \dots x_{\varphi(m)}, m) = 1$ gilt, folgt daraus nach Satz 2.2 (5), dass $a^{\varphi(m)} \equiv 1 \pmod{m}$. □

Aufgabe 5.2.1. Für welche Primzahlen p (ungleich 2 oder 5) gibt es ein Vielfaches von p, dessen Ziffern alle 9 sind? Zum Beispiel: $999999 = 13 \cdot 76923$. *(Spanien 2003)*

Lösung. Sei p eine Primzahl ungleich 2 oder 5. Dann gilt nach dem kleinen Satz von Fermat, dass

$$10^{p-1} \equiv 1 \pmod{p},$$

also ist p ein Teiler der Zahl $10^{p-1} - 1 = 999 \cdots 999$, wobei letztere Zahl aus $p - 1$ Ziffern 9 besteht.

Somit gibt es für jede Primzahl $p \notin \{2, 5\}$ ein Vielfaches, dessen Ziffern alle 9 sind. □

Aus Sätzen 5.1 und 5.4 folgt sofort:

Satz 5.5. *Seien a und m teilerfremd. Dann gilt* $\mathrm{ord}_m(a) \mid \varphi(m)$.

Das erklärt, warum in Beispiel 5.1.1 alle Periodenlängen Teiler von 6 waren.

5.3 Carmichael-Funktion und Primitivwurzeln

Beispiel 5.3.1. Wir betrachten Potenzreste modulo 24. Es gibt $\varphi(24) = \varphi(3)\varphi(8) = 2 \cdot 4 = 8$ zu 24 relativ prime Reste, nämlich ± 1, ± 5, ± 7, ± 11. Wir erhalten Tabelle 2.

Offensichtlich haben alle relativ primen Reste Ordnung 1 oder 2 und es gilt bereits $a^2 \equiv 1 \pmod{24}$ für alle zu 24 teilerfremden ganzen Zahlen. Der Exponent $\varphi(24) = 8$ im Satz von Euler-Fermat (Satz 5.4) ist hier offensichtlich nicht bestmöglich.

Definition 5.3.2. Sei m eine ganze Zahl. Die kleinste positive ganze Zahl λ, sodass $a^\lambda \equiv 1 \pmod{m}$ für alle zu m teilerfremden ganzen Zahlen a gilt, wird mit $\lambda(m)$ bezeichnet. Die dadurch erklärte Funktion $\lambda(m)$ nennt man die *Carmichael-Funktion*.

a	a^0	a^1	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	$\cdots$
1	1	1	1	1	1	1	1	1	1	1	$\cdots$
5	1	5	1	5	1	5	1	5	1	5	$\cdots$
7	1	7	1	7	1	7	1	7	1	7	$\cdots$
11	1	11	1	11	1	11	1	11	1	11	$\cdots$
-11	1	-11	1	-11	1	-11	1	-11	1	-11	$\cdots$
-7	1	-7	1	-7	1	-7	1	-7	1	-7	$\cdots$
-5	1	-5	1	-5	1	-5	1	-5	1	-5	$\cdots$
-1	1	-1	1	-1	1	-1	1	-1	1	-1	$\cdots$

Tabelle 2: Potenzen modulo 24.

Nach dem Satz von Euler-Fermat (Satz 5.4) gilt $\lambda(m) \leq \varphi(m)$ für alle m. Weiters ist für alle zu m teilerfremden a die Ordnung $\mathrm{ord}_m(a)$ ein Teiler von $\lambda(m)$, also gilt insbesondere $\mathrm{ord}_m(a) \leq \lambda(m)$. Falls in beiden Abschätzungen Gleichheit gilt, vergeben wir eine eigene Bezeichnung:

Definition 5.3.3. Eine zu m teilerfremde Zahl a heißt *Primitivwurzel* modulo m, wenn $\mathrm{ord}_m(a) = \varphi(m)$ gilt.

Beispiel 5.3.4. Aus Tabelle 1 sieht man, dass 2 und -4 die einzigen Primitivwurzeln modulo 9 sind: Beide haben Ordnung 6.

Nach Tabelle 2 gibt es keine Primitivwurzeln modulo 24, weil $2 = \lambda(24) < 8 = \varphi(24)$.

Wie für die φ-Funktion bestimmt man $\lambda(m)$ zunächst für Primzahlpotenzen und setzt dann das Ergebnis unter Verwendung des chinesischen Restsatzes zusammen.

Die folgenden beiden Resultate erfordern etwas aufwändigere Beweise, die wir erst im nächsten Abschnitt erbringen.

Lemma 5.3.5. *Sei p eine ungerade Primzahl und α eine positive ganze Zahl. Dann gibt es eine Primitivwurzel modulo p^α.*

Für Zweierpotenzen (ungleich 2 oder 4) gibt es keine Primitivwurzeln, in der Tat gilt:

Lemma 5.3.6. *Sei $\alpha \geq 3$ und a ungerade. Dann gilt*

$$a^{2^{\alpha-2}} \equiv 1 \pmod{2^\alpha}. \tag{5.3.1}$$

Diese Aussage ist bestmöglich, weil

$$\mathrm{ord}_{2^\alpha}(3) = 2^{\alpha-2}. \tag{5.3.2}$$

Nun können wir $\lambda(m)$ vollständig bestimmen.

Satz 5.6. *Für Primzahlpotenzen ergibt sich λ durch*

$$\begin{aligned}
\lambda(2) &= \varphi(2) = 1, \\
\lambda(4) &= \varphi(4) = 2, \\
\lambda(2^\alpha) &= \frac{\varphi(2^\alpha)}{2} = 2^{\alpha-2}, && \alpha \geq 3, \\
\lambda(p^\alpha) &= \varphi(p^\alpha) = (p-1)p^{\alpha-1}, && p \geq 3 \text{ prim}, \ \alpha \geq 1.
\end{aligned}$$

Für paarweise verschiedene Primzahlen $p_1, \ldots, p_k$ und positive ganze Zahlen $\alpha_1, \ldots, \alpha_k$ gilt

$$\lambda(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) = \mathrm{kgV}(\lambda(p_1^{\alpha_1}), \ldots, \lambda(p_k^{\alpha_k})). \tag{5.3.3}$$

Beweis. Offensichtlich gilt $a^1 \equiv 1 \pmod 2$ für alle zu 2 teilerfremden a, es handelt sich gerade um die ungeraden Zahlen a. Somit gilt $\lambda(2) = 1$.

Modulo 4 gilt $a^2 \equiv 1 \pmod 4$ für alle ungeraden a, aber nicht $a^1 \equiv 1 \pmod 4$ für alle ungeraden a, somit gilt $\lambda(4) = 2$.

Die Aussage von Lemma 5.3.6 ist gerade, dass $\lambda(2^\alpha) = 2^{\alpha-2}$.

Da es laut Lemma 5.3.5 für eine ungerade Primzahlen p eine Primitivwurzel modulo p^α gibt, gilt in diesem Fall $\lambda(p^\alpha) = \varphi(p^\alpha) = (p-1)p^{\alpha-1}$.

Es bleibt nur mehr der Fall zusammengesetzter Moduln zu behandeln, die keine Primzahlpotenzen sind. Sei $m := p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Nach dem chinesischen Restsatz 3.2 gilt $a^e \equiv 1 \pmod m$ genau dann für ein a, wenn $a^e \equiv 1 \pmod{p_j^{\alpha_j}}$ für alle j gilt. Somit gilt $a^e \equiv 1 \pmod m$ genau dann für alle zu m (und damit für alle zu allen p_j) teilerfremden a, wenn für alle j die Kongruenz $a^e \equiv 1 \pmod{p_j^{\alpha_j}}$ für alle zu p_j teilerfremden a gilt. Letzteres ist aber äquivalent dazu, dass $\lambda(p_j^{\alpha_j}) \mid e$ für alle j. Das kann man zu

$$\mathrm{kgV}(\lambda(p_1^{\alpha_1}), \ldots, \lambda(p_k^{\alpha_k})) \mid e$$

umschreiben. Damit ist das kleinste positive e, für das $a^e \equiv 1 \pmod m$ für alle zu m teilerfremden a gilt, genau $\mathrm{kgV}(\lambda(p_1^{\alpha_1}), \ldots, \lambda(p_k^{\alpha_k}))$. □

Aufgabe 5.3.7. Man bestimme die größte ganze Zahl k, sodass k für alle natürlichen Zahlen n ein Teiler von $n^{37} - n$ ist. *(ÖMO 1991, Bundeswettbewerb, Beispiel 3.)*

Lösung. Sei p ein Primteiler von k. Laut Annahme ist p ein Teiler von $n^{37} - n = n(n^{36} - 1)$ für alle natürlichen Zahlen n. Somit ist p ein Teiler von $n^{36} - 1$ für alle n, die zu p teilerfremd sind. Damit ist $\lambda(p) = p - 1$ ein Teiler von 36, also gilt

$$(p-1) \in \{1, 2, 3, 4, 6, 9, 12, 18, 36\},$$

also

$$p \in \{2, 3, 5, 7, 13, 19, 37\}.$$

Nehmen wir nun an, dass p^2 ein Teiler von k ist und wählen $n = p$. Dann ist p^2 ein Teiler von $(p^{37} - p)$ und trivialerweise von p^{37}, daher auch von p, ein Widerspruch. Daher enthält k jeden Primfaktor höchstens einmal.

Die größte noch mögliche Wahl für k ist somit $k = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 19 \cdot 37$. Nach obigen Überlegungen ist $n^{37} - n = n(n^{36} - 1)$ für alle Primzahlen p mit $p \mid k$ durch p teilbar, somit auch durch k

Daher gilt $k = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 19 \cdot 37$. □

Wir können nun auch die Frage, zu welchen Moduln es Primitivwurzeln gibt, endgültig klären.

Satz 5.7. *Es gibt genau dann Primitivwurzeln modulo $m \geq 2$, wenn $m = p^\alpha$, $m = 2 \cdot p^\alpha$, $m = 2$ oder $m = 4$, wobei α eine positive ganze Zahl und p eine ungerade Primzahl ist.*

Beweis. Lemma 5.3.5 besagt bereits, dass es modulo p^α für eine ungerade Primzahl p und $\alpha \geq 1$ eine Primitivwurzel gibt.

Sei g eine Primitivwurzel modulo p^α. Wir zeigen, dass dann g auch eine Primitivwurzel modulo $2 \cdot p^\alpha$ ist. Sei k eine positive ganze Zahl mit $g^k \equiv 1 \pmod{2 \cdot p^\alpha}$. Dann gilt klarerweise auch $g^k \equiv 1 \pmod{p^\alpha}$, weshalb $\varphi(p^\alpha) = \mathrm{ord}_{p^\alpha}(g)$ laut Satz 5.1 ein Teiler von k ist. Da allerdings $\varphi(2 \cdot p^\alpha) = \varphi(2) \cdot \varphi(p^\alpha) = 1 \cdot \varphi(p^\alpha) = \varphi(p^\alpha)$ gilt, gilt $\mathrm{ord}_{2 \cdot p^\alpha}(g) \geq k = \varphi(2 \cdot p^\alpha)$. Somit ist g eine Primitivwurzel modulo $2 \cdot p^\alpha$.

Die Zahl 3 ist eine Primitivwurzel modulo 2 sowie modulo 4, wie man sofort nachprüft.

Es verbleibt zu zeigen, dass es für andere Moduln keine Primitivwurzeln geben kann. Notwendig für die Existenz von Primitivwurzeln modulo m ist, dass $\lambda(m) = \varphi(m)$. Somit gibt es modulo 2^α für $\alpha \geq 3$ laut Satz 5.3.6 keine Primitivwurzel. Wir müssen noch zusammengesetzte Zahlen $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ mit $k \geq 2$ untersuchen. Wegen (5.3.3) und Satz 4.3 ist dafür erforderlich, dass die $\lambda(p_j^{\alpha_j})$ paarweise teilerfremd sind, weil sonst das kleinste gemeinsame Vielfache der Carmichael-Funktionen kleiner als ihr Produkt ist. Insbesondere kann höchstens ein $\lambda(p_j^{\alpha_j})$ gerade sein. Für eine ungerade Primzahl p_j ist aber laut Satz 5.6 $\lambda(p_j^{\alpha_j})$ gerade, somit kann es höchstens ein ungerades p_j geben. Weiters ist $\lambda(2^\alpha)$ gerade, außer wenn $\alpha \in \{0, 1\}$. Damit gilt $m = 2 \cdot p^\alpha$ für ein ungerades α. □

Wenn es modulo m Primitivwurzeln gibt, so kann man weitere Aussagen treffen.

Satz 5.8. *Sei m ein Modul, bezüglich dessen es eine Primitivwurzel g gibt.*

1. *Für jedes zu m teilerfremde a gibt es ein $x \in \mathbb{Z}$, sodass*

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

   Dieses x ist eindeutig modulo $\varphi(m)$.

2. *Es gibt genau $\varphi(\varphi(m))$ Primitivwurzeln modulo m*

Beweis.

1. Nach Satz 5.1 sind $g^0, g^1, \ldots, g^{\varphi(m)-1}$ paarweise inkongruent modulo m. Weiters sind diese Zahlen auch zu m teilerfremd. Da es nur $\varphi(m)$ zu m teilerfremde Zahlen modulo m gibt, folgt daraus, dass $g^0, g^1, \ldots, g^{\varphi(m)-1}$ jede Restklasse modulo m genau einmal erreicht. Somit gibt es ein x mit $a \equiv g^x \pmod{m}$. Nach Satz 5.1 ist dieses x modulo $\mathrm{ord}_m(g) = \varphi(m)$ eindeutig.

2. Nach dem ersten Teil des Satzes können Primitivwurzeln modulo m nur die Gestalt g^x für passendes x haben. Nach Satz 5.2 ist g^x genau dann eine Primitivwurzel modulo m, wenn $1 = \mathrm{ggT}(x, \mathrm{ord}_m(g)) = \mathrm{ggT}(x, \varphi(m))$ gilt. Es gibt genau $\varphi(\varphi(m))$ solche Zahlen x modulo $\varphi(m)$ und damit ebensoviele Primitivwurzeln modulo m.

□

5.4 Existenz von Primitivwurzeln

Wir zeigen zunächst, dass es für jede Primzahl $m = p$ eine Primitivwurzel gibt. Dazu sind drei Hilfssätze erforderlich.

Lemma 5.4.1. *Sei $P(x) = a_0 + a_1x + \cdots + a_dx^d$ ein Polynom mit ganzen Koeffizienten a_i und p eine Primzahl. Weiters gelte $p \nmid a_d$.*

Dann gibt es höchstens d Lösungen x von $P(x) \equiv 0 \pmod{p}$, die paarweise inkongruent modulo p sind.

Beweis. Wir beweisen die Behauptung durch Induktion nach dem Grad d. Für $d = 0$ gibt es tatsächlich keine Lösung $P(x) = a_0 \equiv 0 \pmod{p}$, und für $d = 1$ die Behauptung aus Satz 3.1.

Sei nun der Satz für alle Grade bis einschließlich $d-1$ bewiesen. Sei $x = x_0$ eine Lösung von $P(x) \equiv 0 \pmod{p}$. Durch Division mit Rest (von Polynomen) erhalten wir ein Polynom $Q(x)$ vom Grad $d-1$ und eine ganze Zahl r, sodass $P(x) = (x - x_0)Q(x) + r$. Da $0 \equiv P(x_0) \equiv 0 \cdot Q(x_0) + r \pmod{p}$, folgt $r \equiv 0 \pmod{p}$.

Sei jetzt $x_1 \not\equiv x_0 \pmod{p}$ eine weitere Lösung von $P(x) \equiv 0 \pmod{p}$. Dann gilt $0 \equiv P(x_1) \equiv (x_1 - x_0)Q(x_1) \pmod{p}$, also ist x_1 eine Lösung von $Q(x) \equiv 0 \pmod{p}$. Da $Q(x)$ den Grad $d-1$ hat, gibt es nach Induktionsannahme höchstens $d-1$ Lösungen von $Q(x) \equiv 0 \pmod{p}$, zusammen mit unserer fixen Lösung x_0 also höchstens d Lösungen von $P(x) \equiv 0 \pmod{p}$. □

Lemma 5.4.2. *Sei p eine Primzahl und d ein Teiler von $p-1$. Dann hat die Kongruenz $x^d \equiv 1 \pmod{p}$ genau d Lösungen x, die paarweise inkongruent modulo m sind.*

Beweis. Sei $p - 1 = kd$. Nach der Summationsformel für die endliche geometrische Reihe gilt

$$(x^{p-1} - 1) = ((x^d)^k - (1^d)^k) = (x^d - 1)(1 + x^d + x^{2d} + \cdots + x^{(k-1)d}).$$

Das Polynom auf der linken Seite dieser Gleichungskette hat nach dem Satz von Fermat 5.3 genau die $p-1$ Lösungen $1, \ldots, p-1$ modulo p. Der rechte Faktor der rechten Seite der Gleichungskette hat nach Lemma 5.4.1 höchstens $(k-1)d$ Lösungen. Somit muss die Kongruenz $x^d - 1 \equiv 0 \pmod{p}$ mindestens $p - 1 - (k-1)d = kd - (k-1)d = d$ Lösungen haben. Mehr kann sie nach Lemma 5.4.1 nicht haben, also hat sie genau d Lösungen, wie behauptet wurde. □

Lemma 5.4.3. *Für alle positiven ganzen Zahlen n gilt*

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

Beweis. Betrachte die n rationalen Zahlen

$$\frac{1}{n}, \frac{2}{n}, \ldots, \frac{n-1}{n}, \frac{n}{n}.$$

Wir kürzen alle diese Brüche soweit als möglich, das heißt, dass nach dem Kürzen Zähler und Nenner jeweils teilerfremd sind. Sei k/d ein solcher gekürzter Bruch. Nach Konstruktion muss d ein Teiler von n sein (sonst hätte dieser Bruch nicht durch Kürzen entstehen können), weiters gilt $0 < k \leq d$ (sonst ist der Wert des Bruches nicht zwischen 0 und 1, was aber der Fall war), und schließlich muss $\mathrm{ggT}(k, d) = 1$ gelten, weil der Bruch sonst nicht gekürzt wäre.

Sei nun d ein Teiler von n und $0 < k \leq d$ mit $\mathrm{ggT}(k, d) = 1$. Dann gilt

$$\frac{k}{d} = \frac{k \cdot \frac{n}{d}}{d \cdot \frac{n}{d}} = \frac{k \cdot \frac{n}{d}}{n}.$$

Da (nach der eindeutigen Primfaktorzerlegung) jeder Bruch i/n eine eindeutige gekürzte Darstellung hat, ist k/d die gekürzte Darstellung des Bruches auf der rechten Seite obiger Gleichungskette. Jeder Bruch i/n mit $0 \leq i < n$ gehört also zu genau einem Bruch k/d mit $d \mid n$ und $0 < k \leq d$ und $\mathrm{ggT}(k, d) = 1$.

Da es zu jedem Teiler d von n genau $\varphi(d)$ gekürzte Brüche k/d gibt, entsprechen den n Brüchen in ungekürzter Darstellung

$$\sum_{d|n} \varphi(d)$$

Brüche in gekürzter Darstellung. □

Lemma 5.4.4. *Sei p eine Primzahl. Dann gibt es eine Primitivwurzel modulo p.*

Beweis. Für $d \mid p-1$ sei $\psi(d)$ die Anzahl der $1 \leq a \leq p-1$ mit $\mathrm{ord}_p(a) = d$. Wir behaupten, dass $\psi(d) = \varphi(d)$ und beweisen dies durch Induktion nach d. Für $d = 1$ gibt es genau ein a mit $\mathrm{ord}_p(a) = 1$, nämlich $a = 1$. Daher gilt $\psi(1) = 1$, was auch mit $\varphi(1) = 1$ übereinstimmt.

Wir bezeichnen mit L die Menge der Lösungen von $x^d - 1 \equiv 0 \pmod{p}$. Nach Lemma 5.4.2 hat L genau d Elemente. Laut Satz 5.1 gilt $a \in L$ genau dann, wenn $\mathrm{ord}_p(a) \mid d$. Somit gilt

$$d = \sum_{a \in L} 1 = \sum_{d'|d} \sum_{\substack{a=1 \\ \mathrm{ord}_p(a)=d'}}^{p-1} 1 = \sum_{d'|d} \psi(d').$$

Andererseits gilt nach Induktionsannahme für $d' < d$, dass $\psi(d') = \varphi(d')$. Verwenden wir noch Lemma 5.4.3, so folgt

$$d = \sum_{\substack{d'|d \\ d' \neq d}} \varphi(d') + \psi(d) = (d - \varphi(d)) + \psi(d),$$

also $\varphi(d) = \psi(d)$ wie behauptet.

Daher gibt es $\psi(p-1) = \varphi(p-1)$ Elemente a mit $\mathrm{ord}_p(a) = p - 1 = \varphi(p)$. Da $\varphi(p-1)$ für alle Primzahlen eine positive Zahl ist, wurde damit die Existenz einer Primitivwurzel modulo p gezeigt. □

Für den Beweis von Lemma 5.3.5 soll jetzt gezeigt werden, wie Primitivwurzeln modulo p auf Primzahlpotenzmoduln „hochgezogen“ werden können. Wesentliches Hilfsmittel ist folgendes Lemma.

Lemma 5.4.5. *Für $p \geq 3$ prim und $k \geq 1$ gilt*

$$(1+p)^{p^{k-1}} \equiv 1 + p^k \mod p^{k+1} \tag{5.4.1}$$

und $\mathrm{ord}_{p^{k+1}}(1+p) = p^k$.

Beweis. Induktion nach k. Für $k = 1$ lautet die Aussage $1 + p \equiv 1 + p \pmod{p^2}$, was sicherlich wahr ist.

Wir nehmen jetzt die Gültigkeit der Behauptung für ein $k \geq 1$ an. Dann gibt es ein ganzes a, sodass

$$(1+p)^{p^{k-1}} = 1 + p^k + ap^{k+1}.$$

Daher gilt

$$(1+p)^{p^k} = (1 + p^k + ap^{k+1})^p = 1 + p \cdot p^k(1+ap) + \frac{p \cdot (p-1)}{2} p^{2k}(1+ap)^2 + cp^{3k}$$

für ein ganzes c. Da $3k \geq 2k + 1 \geq k + 2$, folgt

$$(1+p)^{p^k} \equiv 1 + p^{k+1} \mod p^{k+2}. \tag{5.4.2}$$

Damit ist die erste Behauptung bewiesen. Aus (5.4.2) folgt auch

$$(1+p)^{p^k} \equiv 1 \mod p^{k+1}.$$

Das heißt, dass $\mathrm{ord}_{p^{k+1}}(1+p) \mid p^k$. Da aber laut (5.4.1) $\mathrm{ord}_{p^{k+1}}(1+p) \nmid p^{k-1}$, folgt auch die zweite Behauptung. □

Wir sind nun in der Lage, Lemma 5.3.5 zu beweisen.

Beweis von Lemma 5.3.5. Sei g eine Primitivwurzel modulo p. Wir behaupten, dass

$$x := g^{p^{k-1}}(1+p)$$

eine Primitivwurzel modulo p^k ist. Sei $s := \mathrm{ord}_{p^k}(x)$, also $x^s \equiv 1 \mod p^k$. Dann gilt

$$1 \equiv 1^{p-1} \equiv x^{s(p-1)} \equiv g^{sp^{k-1}(p-1)}(1+p)^{s(p-1)} \equiv (1+p)^{s(p-1)} \mod p^k,$$

also $p^{k-1} = \mathrm{ord}_{p^k}(1+p) \mid s(p-1)$, woraus $p^{k-1} \mid s$ wegen $\mathrm{ggT}(p, p-1) = 1$ folgt. Anderseits gilt auch

$$1 \equiv 1^{p^{k-1}} \equiv x^{sp^{k-1}} \equiv g^{sp^{2k-2}}(1+p)^{sp^{k-1}} \equiv g^{sp^{2k-2}} \mod p^k,$$

also

$$g^{sp^{2k-2}} \equiv 1 \mod p,$$

woraus $p-1 = \mathrm{ord}_p\, g \mid sp^{2k-2}$ und damit $p-1 \mid s$ folgt.

Daher gilt $\varphi(p^k) = p^{k-1}(p-1) = \mathrm{kgV}(p-1, p^{k-1}) \mid s$, was zu zeigen war. □

Weiters ist noch der Beweis von Lemma 5.3.6 zu erbringen.

Beweis von Lemma 5.3.6. Wir zeigen zunächst (5.3.1) durch vollständige Induktion nach α.

Die Induktionsbasis für $\alpha = 3$ ergibt sich aus

$a \mod 8$	1	3	5	7
$a^2 \mod 8$	1	1	1	1

.

Wir nehmen an, dass $a^{2^{\alpha-2}} \equiv 1 \pmod{2^\alpha}$ gilt, es also eine ganze Zahl b mit $a^{2^{\alpha-2}} = 2^\alpha b + 1$ gibt. Somit gilt

$$a^{2^{\alpha-1}} = \left(a^{2^{\alpha-2}}\right)^2 = (1+2^\alpha b)^2 = 1 + 2^{\alpha+1}b + 2^{2\alpha}b^2 \equiv 1 + 0 \cdot b + 0 \cdot b^2 = 1 \pmod{2^{\alpha+1}},$$

weil für $\alpha \geq 3$ auch $2\alpha \geq \alpha + 1$ gilt. Somit ist (5.3.1) bewiesen.

Schließlich beweisen wir (5.3.2). Dazu beweisen wir zunächst durch Induktion nach α, dass

$$v_2(3^{2^{\alpha-2}} - 1) = \alpha \tag{5.4.3}$$

für $\alpha \geq 3$ gilt. Für $\alpha = 3$ gilt wie behauptet $v_2(3^2 - 1) = v_2(8) = 3$. Es gelte nun (5.4.3) für ein bestimmtes α. Dann gilt

$$\begin{aligned} v_2(3^{2^{\alpha-1}} - 1) &= v_2\big((3^{2^{\alpha-2}} - 1) \cdot (3^{2^{\alpha-2}} + 1)\big) \\ &= v_2(3^{2^{\alpha-2}} - 1) + v_2(3^{2^{\alpha-2}} + 1) = \alpha + v_2(3^{2^{\alpha-2}} + 1). \end{aligned}$$

Da $3^{2^{\alpha-2}} + 1 = 3^{2^{\alpha-2}} - 1 + 2$ und $v_2(3^{2^{\alpha-2}} - 1) = \alpha \geq 3$, muss $v_2(3^{2^{\alpha-2}} + 1) = 1$ gelten, und wir erhalten wie gefordert

$$v_2(3^{2^{\alpha-1}} - 1) = \alpha + 1,$$

womit der Beweis von (5.4.3) erbracht ist.

Um jetzt (5.3.2) aus (5.4.3) herzuleiten, bemerken wir, dass (5.4.3) offensichtlich zu $3^{2^{\alpha-2}} \equiv 1 \pmod{2^\alpha}$ umgeschrieben werden kann. Daraus und aus Satz 5.1 folgt, dass $\mathrm{ord}_{2^\alpha}(3)$ ein Teiler von $2^{\alpha-2}$ sein muss, also $\mathrm{ord}_{2^\alpha}(3) = 2^k$ für ein $k \leq \alpha - 2$. Laut (5.4.3) gilt aber $3^{2^{\alpha-3}} \not\equiv 1 \pmod{2^\alpha}$ (das stimmt auch für $\alpha = 3$), weshalb $k > \alpha - 3$. Wir folgern, dass $k = \alpha - 2$, wie gefordert. □

5.5 Quadratische Reste

Definition 5.5.1. Seien $m \geq 2$ und a ganze Zahlen. a heißt *quadratischer Rest* modulo m, wenn es eine ganze Zahl x gibt, sodass

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

Andernfalls heißt a *quadratischer Nichtrest.*

Beispiel 5.5.2.

m	Quadratische Reste modulo m
3	$0, 1$
4	$0, 1$
8	$0, 1, 4$

Das sieht man einfach durch Quadrieren von $0, \ldots, m-1$.

Aufgabe 5.5.3. Zu jeder nichtnegativen ganzen Zahl k ermittle man alle nichtnegativen ganzen Zahlen x, y, z, für die

$$x^2 + y^2 + z^2 = 8^k \tag{5.5.1}$$

gilt. *(Deutschland 1998, Aufgabe 3)*

Lösung. Wir nehmen an, dass (x, y, z) eine Lösung für ein ganzzahliges $k \geq 0$ ist. Daraus folgt offensichtlich $(x, y, z) \neq (0, 0, 0)$.

Wir nehmen ohne Beschränkung der Allgemeinheit an, dass $v_2(x) \leq v_2(y) \leq v_2(z)$, wobei wir $v_2(0) = \infty$ setzen. Wir schreiben kurz $\alpha := v_2(x)$ und definieren $X = x/2^\alpha$, $Y = y/2^\alpha$, $Z = z/2^\alpha$. Nach Konstruktion sind X, Y, Z nichtnegative ganze Zahlen, und X ist ungerade. Dividiert man (5.5.1) durch $2^{2\alpha}$, so erhält man daher

$$X^2 + Y^2 + Z^2 = 2^{3k-2\alpha}. \tag{5.5.2}$$

Da die linke Seite ganzzahlig ist, gilt auch $3k - 2\alpha \geq 0$.

Wir nehmen zunächst an, dass $3k - 2\alpha \geq 2$. Betrachtet man nun (5.5.2) modulo 4, so erhält man

$$1 + Y^2 + Z^2 \equiv 0 \pmod{4}, \tag{5.5.3}$$

weil X ungerade ist. Da Y^2 und Z^2 jeweils kongruent zu 0 oder 1 modulo 4 sind, kann (5.5.3) nie gelten.

Es gibt daher nur die Möglichkeiten $3k - 2\alpha \in \{0, 1\}$. Im Fall $3k - 2\alpha = 0$ folgt aus (5.5.2), dass

$$1 = 1 + 0 + 0 \leq X^2 + Y^2 + Z^2 = 1,$$

also kann nur $(X, Y, Z) = (1, 0, 0)$ gelten. Wegen $2\alpha = 3k$ ist k gerade und wir erhalten die Lösung $(8^{k/2}, 0, 0)$.

Im anderen Fall $3k - 2\alpha = 1$ erhält man aus (5.5.2) als einzige Möglichkeit $(X, Y, Z) = (1, 1, 0)$. Wegen $3k - 2\alpha = 1$ ist k ungerade, man erhält daher $(2 \cdot 8^{(k-1)/2}, 2 \cdot 8^{(k-1)/2}, 0)$ für ungerades k.

Insgesamt erhält man daher für gerades k die Lösungen

$$(x, y, z) \in \{(8^{k/2}, 0, 0), (0, 8^{k/2}, 0), (0, 0, 8^{k/2})\},$$

für ungerades k die Lösungen

$$(x, y, z) \in \{(2 \cdot 8^{(k-1)/2}, 2 \cdot 8^{(k-1)/2}, 0), (2 \cdot 8^{(k-1)/2}, 0, 2 \cdot 8^{(k-1)/2}), (0, 2 \cdot 8^{(k-1)/2}, 2 \cdot 8^{(k-1)/2})\}.$$

□

Natürlich kann die Untersuchung quadratischer Reste bezüglich beliebiger Moduln über den chinesischen Restsatz auf die Untersuchung modulo Primzahlpotenzen zurückgeführt werden:

Satz 5.9. *Sei $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ die Primfaktorzerlegung von m und $a \in \mathbb{Z}$. Dann ist a genau dann ein quadratischer Rest modulo m, wenn a ein quadratischer Rest modulo $p_j^{\alpha_j}$ für $1 \leq j \leq r$ ist.*

Beweis. Sei a quadratischer Rest modulo m, es gebe also ein $x \in \mathbb{Z}$ mit $x^2 \equiv a \pmod{m}$. Dann gilt auch $x^2 \equiv a \pmod{p_j^{\alpha_j}}$ für jedes j, somit ist a auch quadratischer Rest modulo $p_j^{\alpha_j}$ für jedes $1 \leq j \leq r$.

Sei nun umgekehrt a ein quadratischer Rest modulo $p_j^{\alpha_j}$ für alle $1 \leq j \leq r$. Das heißt, dass es ganze Zahlen $x_1, \ldots, x_r$ gibt, sodass $x_j^2 \equiv a \pmod{p_j^{\alpha_j}}$ gilt. Wir können nach dem chinesischen Restsatz ein $x \in \mathbb{Z}$ finden, für das $x \equiv x_j \pmod{p_j^{\alpha_j}}$ für $1 \leq j \leq r$ gilt. Für dieses x gilt

$$x^2 \equiv x_j^2 \equiv a \pmod{p_j^{\alpha_j}},$$

also folgt auch $x^2 \equiv a \pmod{m}$. Somit haben wir gezeigt, dass auch a ein quadratischer Rest modulo m ist.

□

Der folgende Satz zeigt, dass man die Frage modulo $p_i^{\alpha_i}$ sogar auf die Frage modulo p_i (falls p_i ungerade) bzw. auf die Frage modulo 8 (falls $8 \mid m$) zurückführen kann.

Satz 5.10. *Sei a eine ganze Zahl.*

1. *Es gelte $2 \nmid a$. a ist genau dann ein quadratischer Rest modulo 2^ℓ für $\ell \geq 3$, wenn a quadratischer Rest modulo 8 ist.*
2. *Es gelte $p \nmid a$. a ist genau dann ein quadratischer Rest modulo p^ℓ (p eine ungerade Primzahl und $\ell \geq 1$), wenn a ein quadratischer Rest modulo p ist.*

Beweis. Wenn a ein quadratischer Rest modulo p^ℓ ist (p eine Primzahl), so gibt es ein $x \in \mathbb{Z}$, sodass $x^2 \equiv a \pmod{p^\ell}$ und damit auch $x^2 \equiv a \pmod{p^k}$ für $k \leq \ell$. Zu zeigen ist also lediglich, dass ein quadratischer Rest modulo p bzw. 8 auf höhere Potenzen des Moduls „hochgezogen“ werden kann.

1. Sei a ein quadratischer Rest modulo 2^ℓ mit $\ell \geq 3$. Dann gibt es eine ganze Zahl x, sodass $x^2 = a + b2^\ell$ für ein passendes $b \in \mathbb{Z}$. Falls b gerade ist, so folgt $x^2 \equiv a \pmod{2^{\ell+1}}$ und a ist tatsächlich ein quadratischer Rest modulo $2^{\ell+1}$. Andernfalls betrachten wir

   $$(x + 2^{\ell-1})^2 = x^2 + 2x2^{\ell-1} + 2^{2\ell-2} \equiv a + 2^\ell(x + b) \equiv a \pmod{2^{\ell+1}},$$

   weil $2\ell - 2 \geq \ell + 1$ und weil sowohl b als auch x ungerade sind. Damit ist a auch quadratischer Rest modulo $2^{\ell+1}$.

2. Sei a ein quadratischer Rest modulo p^ℓ für eine ungerade Primzahl p und ein $\ell \geq 1$. Dann gibt es ganze Zahlen x und b, sodass $x^2 = a + b \cdot p^\ell$. Da $p \nmid 2x$, gibt es (nach Satz 3.1) ein ganzes y, sodass $2xy \equiv -b \pmod{p}$. Also gilt

$$(x + yp^\ell)^2 = x^2 + 2xyp^\ell + y^2p^{2\ell} = a + p^\ell(2xy + b) + y^2p^{2\ell} \equiv a \pmod{p^{\ell+1}},$$

weil $2\ell \geq \ell + 1$ und nach Konstruktion $p \mid (2xy + b)$. Damit ist a auch ein quadratischer Rest modulo $p^{\ell+1}$.

□

Es sollen noch einfache Kriterien für quadratische Reste modulo Primzahlen studiert werden.

Satz 5.11. *Sei $p \geq 3$ eine Primzahl. Dann gibt es genau $(p+1)/2$ quadratische Reste $0 \leq a < p$ modulo p und $(p-1)/2$ quadratische Nichtreste $0 \leq a < p$ modulo p.*

Beweis. 0 ist quadratischer Rest. Ist $1 \leq a < p$ ein quadratischer Rest, so gibt es genau zwei Lösungen von $x^2 \equiv a \pmod{p}$: Wenn $x^2 \equiv a \pmod{p}$, so gilt auch $(-x)^2 \equiv a \pmod{p}$, also gibt es mindestens zwei Lösungen; gilt $x^2 \equiv y^2 \pmod{p}$, so folgt $p \mid (x^2 - y^2) = (x - y)(x + y)$, also $x \equiv y \pmod{p}$ oder $x \equiv -y \pmod{p}$, also gibt es genau zwei Lösungen. Somit ist jeder zu p relativ prime quadratische Rest das Quadrat von genau zwei $1 \leq x \leq p - 1$, also gibt es genau $(p - 1)/2$ relativ prime quadratische Reste. Zusammen mit dem quadratischen Rest 0 erhält man die Anzahl von $(p + 1)/2$ quadratischen Resten. Alle übrigen Restklassen entsprechen quadratischen Nichtresten, das sind noch $p - (p + 1)/2 = (p - 1)/2$ Stück. □

Satz 5.12. *Sei $p \geq 3$ eine Primzahl und a eine zu p teilerfremde ganze Zahl. Dann ist a genau dann quadratischer Rest, wenn*

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

Weiters ist a genau dann quadratischer Nichtrest, wenn

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

Beweis. Sei a quadratischer Rest, also $a \equiv b^2 \pmod{p}$ für ein passendes b. Dann gilt

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

nach dem Satz von Fermat 5.3.

Da die Kongruenz $x^{(p-1)/2} \equiv 1 \pmod{p}$ laut Lemma 5.4.1 höchstens $(p - 1)/2$ Lösungen modulo p besitzt und wir bereits so viele Lösungen (nämlich genau die quadratischen Reste modulo p) gefunden haben, gilt für jeden quadratischen Nichtrest a, dass $a^{(p-1)/2} \not\equiv 1 \pmod{p}$. Da $x^2 - 1 \pmod{p}$ genau zwei Lösungen, nämlich 1 und -1, besitzt, und $(a^{(p-1)/2})^2 \equiv 1 \pmod{p}$ nach dem kleinen Satz von Fermat gilt, muss für einen quadratischen Nichtrest a modulo p gelten, dass $a^{(p-1)/2} \equiv -1 \pmod{p}$.

□

Korollar 5.5.4. *Sei $p \geq 3$ eine Primzahl und a, b zu p teilerfremde ganze Zahlen. Dann ist $a \cdot b$ genau dann ein Quadratischer Rest modulo p, wenn a und b beide quadratische Reste oder beide quadratische Nichtreste sind.*

Beweis. Da $a \cdot b$ genau dann ein quadratischer Rest ist, falls

$$1 \equiv (a \cdot b)^{(p-1)/2} = a^{(p-1)/2} b^{(p-1)/2} \pmod{p}$$

und die beiden Faktoren auf der rechten Seite jeweils kongruent zu entweder $+1$ oder -1 sind, folgt die Aussage aus Satz 5.12. □

Aufgabe 5.5.5. Zeigen Sie, dass es für jede Primzahl $p > 3$ ganze Zahlen x, y, k gibt, sodass folgende Bedingungen gelten:

$$0 < 2k < p,$$
$$kp + 3 = x^2 + y^2.$$

(Polen, 2. Runde, 2003)

Lösung. Wir zeigen zunächst, dass es ganzzahlige x und y gibt, sodass $x^2 + y^2 \equiv 3 \pmod{p}$. Falls 3 ein quadratischer Rest ist, so kann man $y = 0$ wählen, ist 2 ein quadratischer Rest, so kann man $y = 1$ wählen, ist -1 ein quadratischer Rest, so kann man $y = 2$ wählen, und ist schließlich -6 ein quadratischer Rest, so kann man $y = 3$ wählen. Daher können wir nun annehmen, dass die Zahlen -6, -1,2, 3 quadratische Nichtreste sind. Daher sind laut dem Korollar $6 = (-6) \cdot (-1)$ und $-3 = 3 \cdot (-1)$ quadratische Reste, also können ganzzahlige x und y gewählt werden, sodass $x^2 \equiv 6$ und $y^2 \equiv -3 \pmod{p}$, also $x^2 + y^2 \equiv 3 \pmod{p}$.

Weiters können wir x und y modulo p reduzieren und gegebenenfalls x durch $-x$ und y durch $-y$ ersetzen, sodass es ganze Zahlen x, y mit $|x| \leq (p-1)/2$ und $|y| \leq (p-1)/2$ und $x^2 + y^2 \equiv 3 \pmod{p}$ gibt. Es gibt also eine positive ganze Zahl k mit $x^2 + y^2 - 3 = pk$. Es gilt

$$k = \frac{x^2 + y^2 - 3}{p} \leq \frac{(p-1)^2 + (p-1)^2 - 12}{4p} = \frac{2p^2 - 4p - 10}{4p} < \frac{p}{2},$$

also $2k < p$, wie gefordert. □

Die Theorie der quadratischen Reste und Nichtreste gibt unter anderem mit dem Quadratischen Reziprozitätsgesetz (und seinen Hilfssätzen) eine einfache Methode an, auch für große a und m festzustellen, ob a ein quadratischer Rest modulo m ist, wenn man alle auftretenden Zahlen in vernünftiger Zeit faktorisieren kann.

Definition 5.5.6 (Legendre-Symbol)**.** Seien a eine ganze Zahl und p eine Primzahl. Dann setze

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & a \equiv 0 \pmod{p}, \\ 1, & a \text{ ist quadratischer Rest modulo } p \text{ und } a \not\equiv 0 \pmod{p}, \\ -1, & a \text{ ist quadratischer Nichtrest modulo } p. \end{cases}$$

Wir können Satz 5.12 und Korollar 5.5.4 direkt mit dem Legendre-Symbol ausdrücken:

Korollar 5.5.7. *Sei p eine Primzahl und a eine ganze Zahl. Dann gilt*

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

Korollar 5.5.8. *Seien a, b, p ganze Zahlen und p eine Primzahl. Dann gilt*

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

Um $\left(\frac{a}{p}\right)$ zu bestimmen, reduziert man zunächst a modulo p (dabei ändert sich das Legendre-Symbol nicht) und bestimmt anschließend die Primfaktorzerlegung von a mod p. Nach Korollar 5.5.8 reicht es dann, $\left(\frac{q}{p}\right)$ für verschiedene Primzahlen p und q sowie $\left(\frac{-1}{p}\right)$ bestimmen zu können. Dies ermöglicht das quadratische Reziprozitätsgesetz:

Satz 5.13 (Quadratisches Reziprozitätsgesetz)**.** *1. Seien p und q zwei verschiedene ungerade Primzahlen. Dann gilt*

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

2. Sei $p \geq 3$ eine Primzahl. Dann gilt

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}, \qquad \left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

Zum Beweis vergleiche zum Beispiel Ireland und Rosen [4].

Aufgabe 5.5.9. Man bestimme alle positiven ganzen Zahlen k mit der folgenden Eigenschaft: Es gibt eine ganze Zahl a, sodass $(a+k)^3 - a^3$ ein Vielfaches von 2007 ist. *(MEMO 2007, Aufgabe 3.)*

Lösung. Wir suchen alle positiven ganzen Zahlen k, sodass die Kongruenz

$$0 \equiv (a+k)^3 - a^3 = 3a^2k + 3ak^2 + k^3 \pmod{2007} \tag{5.5.4}$$

lösbar ist. Da $2007 = 3^2 \cdot 223$, ist (5.5.4) nach dem chinesischen Restsatz zu

$$0 \equiv 3a^2k + 3ak^2 + k^3 \pmod{9}, \tag{5.5.5}$$
$$0 \equiv 3a^2k + 3ak^2 + k^3 \pmod{223} \tag{5.5.6}$$

äquivalent.

Wenn $a \in \mathbb{Z}$ eine Lösung von (5.5.4) ist, dann folgt aus (5.5.5), dass $0 \equiv k^3 \pmod 3$ gilt. Daher muss k durch 3 teilbar sein.

Wenn umgekehrt k durch 3 teilbar ist, dann ist jeder Summand von $3a^2k + 3ak^2 + k^3$ durch 9 teilbar und jedes $a \in \mathbb{Z}$ ist Lösung von (5.5.5).

Wir müssen nun die Lösbarkeit von (5.5.6) untersuchen. Wenn k durch 223 teilbar ist, so ist jedes $a \in \mathbb{Z}$ eine Lösung von (5.5.6). Wir nehmen daher an, dass k kein Vielfaches von 223 ist, also zu 223 teilerfremd ist. Daher können wir $a = kx$ substituieren und erhalten nach Division durch k^3 und Multiplikation mit 12, dass (5.5.6) äquivalent zu

$$(6x+3)^2 + 3 \equiv 36x^2 + 36x + 12 \equiv 0 \pmod{223}$$

ist. Daher ist (5.5.6) genau dann lösbar, wenn -3 ein quadratischer Rest modulo 223 ist. Wir bestimmen $\left(\frac{-3}{223}\right)$: Es gilt

$$\left(\frac{-3}{223}\right) = \left(\frac{-1}{223}\right)\left(\frac{3}{223}\right) = (-1)^{111}\left(\frac{223}{3}\right)(-1)^{1\cdot 111} = \left(\frac{223}{3}\right) = \left(\frac{1}{3}\right) = 1.$$

Daher ist (5.5.6) für alle k lösbar.

Insgesamt ist somit (5.5.4) genau dann lösbar, wenn $3 \mid k$.

Anmerkung: Es gibt auch (kürzere) Lösungen, die direkt die kubische Kongruenz betrachten (also kubische statt quadratische Reste betrachten). □

6 Diophantische Gleichungen

6.1 Lineare diophantische Gleichungen

Seien $a_1, \ldots, a_k$ und b ganze Zahlen. Wir suchen alle ganzzahligen Lösungen $x_1, \ldots, x_k$ von

$$a_1x_1 + \cdots + a_kx_k = b. \tag{6.1.1}$$

Nach Diophantus von Alexandrien nennt man eine Gleichung eine *diophantische Gleichung*, wenn man nur an ihren ganzzahligen Lösungen interessiert ist.

Satz 6.1. *Die lineare diophantische Gleichung* (6.1.1) *besitzt genau dann eine ganzzahlige Lösung* $(x_1, \ldots, x_k)$*, wenn*

$$\mathrm{ggT}(a_1, \ldots, a_k) \mid b.$$

Beweis. Sei $d := \mathrm{ggT}(a_1, \ldots, a_k)$. Falls es eine Lösung von (6.1.1) gibt, so gilt $d \mid b$.

Die umgekehrte Richtung beweisen wir durch Induktion nach k. Der Fall $k = 1$ ist trivial.

Schluss von $k-1$ auf k: Sei $d' := \mathrm{ggT}(a_1, \ldots, a_{k-1})$ und $d := \mathrm{ggT}(a_1, \ldots, a_k)$. Da d ein gemeinsamer Teiler von $a_1, \ldots, a_k$ ist, teilt d sowohl d' als auch a_k, also $d \mid \mathrm{ggT}(d', a_k)$. Teilt andererseits ein d'' sowohl d' als auch a_k, so teilt es auch $a_1, \ldots, a_{k-1}$, also gilt $d'' \mid \mathrm{ggT}(a_1, \ldots, a_k)$. Aus dieser Überlegung folgt $d = \mathrm{ggT}(d', a_k)$.

Nach Induktionsannahme besitzt die Gleichung

$$d' = a_1x_1' + \cdots + a_{k-1}x_{k-1}'$$

eine ganzzahlige Lösung $(x_1', \ldots, x_{k-1}')$. Nach dem Euklidschen Algorithmus (Satz 1.4) gibt es ganze Zahlen x und y, sodass

$$d = xd' + ya_k.$$

Setzt man $(x_1, \ldots, x_{k-1}, x_k) = (xx_1'b', \ldots, xx_{k-1}'b', y \cdot b')$, wobei $b' = b/d$, so erhält man eine Lösung von (6.1.1). □

6.2 Quadratische diophantische Gleichungen in zwei Unbekannten

Rückführung auf Normalform

Wir betrachten eine quadratische diophantische Gleichung in zwei Unbekannten

$$ax^2 + bxy + cy^2 + dx + ey + f = 0 \tag{6.2.1}$$

mit bekannten ganzzahligen $a, \ldots, f$ und Unbekannten x und y.

Man führt nun eine Reihe von Transformationen durch, um auf gewisse „Normalformen“ zu kommen. Im Wesentlichen handelt es sich dabei um das Zusammenfassen zu vollständigen Quadraten. Wir gehen hier der Einfachheit halber davon aus, dass einige auftretende Konstanten ungleich 0 sind, andernfalls vertauscht man entweder x und y oder man gelangt sogar zu einfacheren Gleichungen.

Wir nehmen $a \neq 0$ an. Multiplikation mit $4a$ ergibt

$$\begin{aligned} 0 &= 4a^2x^2 + 4abxy + 4a(cy^2 + dx + ey + f) \\ &= (2ax + by)^2 + (4ac - b^2)y^2 + 2d(2ax + by) + (4ae - 2db)y + 4af. \end{aligned}$$

Setzt man $x_1 = 2ax + by$ und $y_1 = y$, so erhält man die Gleichung

$$0 = {x_1}^2 + c_1{y_1}^2 + d_1x_1 + e_1y_1 + f_1,$$

wobei $c_1 = (4ac - b^2)$, $d_1 = 2d$, $e_1 = (4ae - 2db)$ und $f_1 = 4af$. Wir nehmen $c_1 \neq 0$ an.

Wir multiplizieren jetzt mit $4c_1$ und erhalten

$$0 = c_1(4{x_1}^2 + 4d_1x_1) + (4(c_1y_1)^2 + 4(c_1y_1)e_1) + f_1$$

und durch quadratisches Ergänzen

$$0 = c_1(2x_1 + d_1)^2 + (2c_1y_1 + e_1)^2 + (f_1 - c_1{d_1}^2 - {e_1}^2),$$

also durch die Substitutionen $y_2 = 2x_1 + d_1$, $x_2 = 2c_1y_1 + e_1$, $c_2 = c_1$, $f_2 = -(f_1 - c_1{d_1}^2 - {e_1}^2)$ die Gleichung

$${x_2}^2 + c_2{y_2}^2 = f_2.$$

Sei jetzt $c_2 = c_3^2 \cdot C$ für ein quadratfreies C (d.h. $v_p(C) \in \{0, 1\}$ für alle Primzahlen p). Wir setzen $X = x_2$, $Y = c_3y_2$ und $F = f_2$ und erhalten

$$X^2 + CY^2 = F \tag{6.2.2}$$

für ein quadratfreies C. Wir bemerken, dass alle Transformationen derart waren, dass C und F ganze Zahlen sind. Falls (x, y) eine ganzzahlige Lösung von (6.2.1) ist, so ist (X, Y) eine ganzzahlige Lösung von (6.2.2). Um daher alle Lösungen von (6.2.1) zu finden, muss man alle Lösungen von (6.2.2) finden und anhand der Transformationen entsprechende Lösungen (x, y) der ursprünglichen Gleichung (6.2.1) ausrechnen. Dabei kann es sein, dass (x, y) nicht ganzzahlig sind, in diesem Fall geht man eben zur nächsten Lösung (X, Y) von (6.2.2) über. Dieser Prozess erfordert also lediglich viel Geduld.

Interessant ist jetzt noch die Lösung von (6.2.2). Wir betrachten zunächst den Fall $C > 0$. Falls $F < 0$, kann es offensichtlich keine Lösung geben, weil die linke Seite sicher nichtnegativ ist. Falls $F > 0$, kann es höchstens endlich viele Lösungen geben, weil sowohl X^2 als auch CY^2 positiv sind. Man kann also (zumindest theoretisch) alle $1 \leq X \leq \sqrt{F}$ durchprobieren, ob $(F - X^2)/C$ ein Quadrat ist. In der Praxis sollte man mit einfachen Kongruenzbedingungen die Suche weiter einengen. Für den Fall $C = 1$ vergleiche Abschnitt 6.4.

Es verbleibt damit der Fall $C < 0$. Wir schreiben $D := -C > 0$. Damit schreibt sich Gleichung (6.2.2) als $X^2 - DY^2 = F$ mit einem positiven D, das kein Quadrat ist.

Pellsche Gleichung

Wir betrachten zunächst den Fall $F = 1$, also

$$X^2 - DY^2 = 1.$$

In diesem Fall nennt man die Gleichung *Pellsche Gleichung.* Es gibt natürlich die *trivialen Lösungen* $(\pm 1, 0)$.

Satz 6.2. *Sei D eine positive ganze Zahl, die kein Quadrat ist. Dann besitzt die Pellsche Gleichung*

$$X^2 - DY^2 = 1 \tag{6.2.3}$$

eine Lösung (X, Y) mit $Y > 0$.
Die Lösung mit minimalem positivem Y und positivem X wird als Fundamentallösung (X_1, Y_1) bezeichnet. Alle Lösungen von (6.2.3) *sind dann durch $(\pm X_k, \pm Y_k)$, $k \geq 0$, gegeben, wobei*

$$X_k + \sqrt{D}Y_k = (X_1 + \sqrt{D}Y_1)^k \tag{6.2.4}$$

für $k \geq 0$.

Wir verschieben den Beweis der Existenz einer Fundamentallösung auf den nächsten Abschnitt. Die fundamentale Idee ist die Faktorisierung von (6.2.3) als

$$1 = X^2 - DY^2 = (X - \sqrt{D}Y)(X + \sqrt{D}Y). \tag{6.2.5}$$

Wir beweisen zunächst einige Hilfsaussagen, die bereits viel von der Lösungsstruktur beschreiben.

Lemma 6.2.1. *Sei D eine positive ganze Zahl, die kein Quadrat ist. Weiters seien (x_1, y_1) und (x_2, y_2) Lösungen von* (6.2.3) *mit x_1, $x_2 > 0$ und y_1, $y_2 \geq 0$.*

1. *Es gilt*
$$x_1 < x_2 \iff y_1 < y_2 \iff x_1 + \sqrt{D}y_1 < x_2 + \sqrt{D}y_2$$
und
$$x_1 = x_2 \iff y_1 = y_2 \iff x_1 + \sqrt{D}y_1 = x_2 + \sqrt{D}y_2.$$

2. *Seien x_3 und y_3 die eindeutigen ganzen Zahlen, die durch*
$$x_3 + \sqrt{D}y_3 = (x_1 + \sqrt{D}y_1)(x_2 + \sqrt{D}y_2)$$
definiert sind (also $x_3 = x_1x_2 + Dy_1y_2$ und $y_3 = x_1y_2 + x_2y_1$). Dann ist auch (x_3, y_3) eine Lösung von (6.2.3) *mit $x_3 > 0$ und $y_3 \geq 0$.*

3. *Es gelte $x_1 \leq x_2$ und seien x_4, y_4 die eindeutigen ganzen Zahlen, die durch*
$$x_4 + \sqrt{D}y_4 = \frac{x_1 + \sqrt{D}y_1}{x_2 + \sqrt{D}y_2} = (x_1 + \sqrt{D}y_1)(x_2 - \sqrt{D}y_2) \tag{6.2.6}$$
definiert sind. Dann ist auch (x_4, y_4) eine Lösung von (6.2.3) *mit $x_4 > 0$ und $y_4 \geq 0$.*

Der erste Punkt zeigt, dass es sinnvoll ist, die positiven Lösungen der Pellschen Gleichung „der Größe nach“ zu ordnen, wobei es egal ist, ob man dazu x, y oder $x + \sqrt{D}y$ heranzieht. In den weiteren Punkten wird beschrieben, wie man aus Lösungen weitere Lösungen gewinnen kann. Die zweite Gleichheit in (6.2.6) ist eine unmittelbare Konsequenz aus $(x_2 + \sqrt{D}y_2)(x_2 - \sqrt{D}y_2) = x_2^2 - Dy_2^2 = 1$; man kann das auch als „Rationalmachen“ des Nenners sehen.

Beweis. 1. Wegen $x_1^2 = Dy_1^2 + 1$ und $x_2^2 = Dy_2^2 + 1$ und der Nicht-Negativität aller beteiligten Größen folgt

(a) aus $y_1 < y_2$, dass $x_1 < x_2$ und damit $x_1 + \sqrt{D}y_1 < x_2 + \sqrt{D}y_2$,

(b) aus $y_1 = y_2$, dass $x_1 = x_2$ und damit $x_1 + \sqrt{D}y_1 = x_2 + \sqrt{D}y_2$,

(c) aus $y_1 > y_2$, dass $x_1 > x_2$ und damit $x_1 + \sqrt{D}y_1 > x_2 + \sqrt{D}y_2$.

Daraus folgen die angegebenen Äquivalenzen.

2. Nach Konstruktion gilt $x_3 > 0$ und $y_3 \geq 0$. Weiters gilt

$$x_3 - \sqrt{D}y_3 = (x_1 - \sqrt{D}y_1)(x_2 - \sqrt{D}y_2).$$

Daher erhalten wir

$$\begin{aligned} x_3^2 - Dy_3^2 &= (x_3 + \sqrt{D}y_3)(x_3 - \sqrt{D}y_3) \\ &= (x_1 + \sqrt{D}y_1)(x_2 + \sqrt{D}y_2)(x_1 - \sqrt{D}y_1)(x_2 - \sqrt{D}y_2) \\ &= (x_1^2 - Dy_1^2)(x_2^2 - Dy_2^2) = 1 \cdot 1 = 1, \end{aligned}$$

somit ist (x_3, y_3) wieder Lösung.

3. Zunächst gilt wieder

$$x_4 - \sqrt{D}y_4 = (x_1 - \sqrt{D}y_1)(x_2 + \sqrt{D}y_2)$$

und daher wieder

$$\begin{aligned} x_4^2 - Dy_4^2 &= (x_4 + \sqrt{D}y_4)(x_4 - \sqrt{D}y_4) \\ &= (x_1 + \sqrt{D}y_1)(x_2 - \sqrt{D}y_2)(x_1 - \sqrt{D}y_1)(x_2 + \sqrt{D}y_2) \\ &= (x_1^2 - Dy_1^2)(x_2^2 - Dy_2^2) = 1 \cdot 1 = 1. \end{aligned}$$

Weiters sind x_4 und y_4 offensichtlich ganze Zahlen und nach Konstruktion ist $x_4 + \sqrt{D}y_4 \geq 1$. Wegen $x_4 - \sqrt{D}y_4 = 1/(x_4 + \sqrt{D}y_4)$ gilt $1 \geq x_4 - \sqrt{D}y_4 > 0$. Addition dieser beiden Ungleichungen ergibt $x_4 > 0$. Wegen $x_4 + \sqrt{D}y_4 > 1 > x_4 - \sqrt{D}y_4$ folgt dann auch $y_4 \geq 0$. □

Wir sind nun in der Lage, den zweiten Teil von Satz (6.2.3) über die Darstellung aller Lösungen zu beweisen.

Beweis von Satz 6.2, 2. Teil (Darstellung aller Lösungen). Sei (X_1, Y_1) jene Lösung von (6.2.3) mit $X_1 > 0$, $Y_1 > 0$, die $X_1 + \sqrt{D}Y_1$ über alle solchen Lösungen minimiert.

Nach Lemma 6.2.1 (2) (und Induktion nach k) sind die durch (6.2.4) gegebenen (X_k, Y_k) tatsächlich Lösungen der Pellschen Gleichung (6.2.3).

Wir müssen lediglich zeigen, dass damit alle Lösungen beschrieben werden. Dazu sei jetzt (X, Y) mit $X > 0$ und $Y > 0$ eine beliebige Lösung von (6.2.3). Wir wählen $k \geq 0$ so, dass

$$(X_1 + \sqrt{D}Y_1)^k \leq X + \sqrt{D}Y < (X_1 + \sqrt{D}Y_1)^{k+1}. \tag{6.2.7}$$

Wir definieren (X', Y') durch

$$X' + \sqrt{D}Y' = \frac{X + \sqrt{D}Y}{(X_1 + \sqrt{D}Y_1)^k}.$$

Aus dem Lemma 6.2.1 (3) folgt, dass (X', Y') eine Lösung der Pellschen Gleichung (6.2.3) mit $X' > 0$ und $Y' \geq 0$ ist. Dividiert man (6.2.7) durch $(X_1 + \sqrt{D}Y_1)^k$, so erhält man

$$1 \leq X' + \sqrt{D}Y' < X_1 + \sqrt{D}Y_1.$$

Aufgrund der Minimalität der Fundamentallösung erhalten wir $X' + \sqrt{D}Y' = 1$, also $X + \sqrt{D}Y = (X_1 + \sqrt{D}Y_1)^k$ und nach Lemma 6.2.1 (1), dass $(X, Y) = (X_k, Y_k)$. □

Jetzt soll noch eine Rekursionsformel für die Lösungen der Pellschen Gleichung bewiesen werden.

Satz 6.3. *Sei D kein Quadrat und (X_1, Y_1) die Fundamentallösung mit $X_1 \geq 1$, $Y_1 \geq 1$ der Pellschen Gleichung*

$$X^2 - DY^2 = 1.$$

Dann erfüllen alle positiven Lösungen die Rekursion

$$X_{k+2} = 2X_1 \cdot X_{k+1} - X_k, \qquad Y_{k+2} = 2X_1 \cdot Y_{k+1} - Y_k$$

für $k \geq 0$.

Beweis. Nach Satz 6.2 gilt

$$X_k + \sqrt{D}Y_k = (X_1 + \sqrt{D}Y_1)^k$$

und damit auch

$$X_k - \sqrt{D}Y_k = (X_1 - \sqrt{D}Y_1)^k.$$

Addiert bzw. subtrahiert man diese beiden Gleichungen, so erhält man

$$X_k = c_1\alpha^k + c_2\beta^k$$
$$Y_k = d_1\alpha^k + d_2\beta^k$$

für $\alpha = (X_1 + \sqrt{D}Y_1)$, $\beta = (X_1 - \sqrt{D}Y_1)$ und gewisse (reelle) Konstanten c_1, c_2, d_1, d_2. Das heißt, dass sowohl X_k als auch Y_k eine lineare Rekursion zweiter Ordnung mit charakteristischem Polynom $(q - \alpha)(q - \beta) = q^2 - (\alpha + \beta)q + \alpha\beta = 0$ erfüllen. Da $\alpha + \beta = 2X_1$ und $\alpha\beta = 1$, folgt die angegebene Rekursion. □

Aufgabe 6.2.2. Zeigen Sie, dass es unendlich viele nicht-kongruente Dreiecke T gibt, sodass die Längen der Seiten von T aufeinanderfolgende ganze Zahlen sind und der Flächeninhalt von T eine ganze Zahl ist. *(Nordic 1995)*

Lösung. Wir bezeichnen die Seitenlängen des gesuchten Dreiecks mit $x - 1$, x, $x + 1$ und den Flächeninhalt mit A. Dann gilt für den halben Umfang $s = 3x/2$ und nach der Heronschen Flächenformel gilt

$$A^2 = s(s - (x - 1))(s - x)(s - (x + 1)) = \frac{1}{16}3x(x + 2)x(x - 2).$$

Damit A^2 ganzzahlig ist, muss x gerade sein; wir setzen $x = 2z$. Weiters muss $A^2/z^2 = 3(z^2 - 1)$ eine durch 3 teilbare ganze Zahl sein, wir setzen $A/z = 3y$ und erhalten schließlich

$$1 = z^2 - 3y^2.$$

Das ist eine Pellsche Gleichung, sie besitzt daher laut Satz 6.2 unendlich viele Lösungen (z, y). Jeder dieser Lösungen führt über $x = 2z$ und $A = 3yz$ zu einer Lösung der ursprünglichen Aufgabe.

Wollte man die Lösungen tatsächlich bestimmen, so stellt man fest, dass $(z, y) = (2, 1)$ offensichtlich eine Lösung ist, deren y offensichtlich minimal ist. Somit ergeben sich sämtliche positiven Lösungen durch

$$(z_n + \sqrt{3}y_n) = (2 + \sqrt{3})^n.$$

□

Existenz einer nichttrivialen Lösung der Pellschen Gleichung

Um die Existenz einer Lösung zu zeigen, benötigt man den Dirichletschen Approximationssatz.

Satz 6.4 (Dirichlet). *Sei $\alpha \in \mathbb{R} \setminus \mathbb{Q}$. Dann gibt es unendlich viele $p/q \in \mathbb{Q}$, sodass*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}. \tag{6.2.8}$$

Beweis. Zunächst wird gezeigt, dass es für alle ganzen $Q > 0$ ein p und ein $0 < q \leq Q$ gibt, sodass

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{Qq} \leq \frac{1}{q^2}.$$

Man betrachtet dazu die $Q + 1$ Zahlen $\{j\alpha\}, j = 0, \ldots, Q$, die in den Q Intervallen $\left[\frac{k}{Q}, \frac{k+1}{Q}\right)$, $k = 0, \ldots, Q - 1$ liegen — für $x \in \mathbb{R}$ sei $\{x\} := x - \lfloor x \rfloor$ der gebrochene Anteil von x. Dann gibt es nach dem Schubfachschluss $j_1 < j_2$, sodass

$$|\{j_2\alpha\} - \{j_1\alpha\}| = |(j_2 - j_1)\alpha - (\lfloor j_2\alpha \rfloor - \lfloor j_1\alpha \rfloor)| < \frac{1}{Q},$$

man hat daher mit $q := (j_2 - j_1)$ und $p := \lfloor j_2\alpha \rfloor - \lfloor j_1\alpha \rfloor$ Zahlen mit der gewünschten Eigenschaft gefunden. Gibt es nur endlich viele p/q, die (6.2.8) erfüllen, also

$$\frac{p_1}{q_1}, \ldots, \frac{p_k}{q_k},$$

so gibt es eine positive ganze Zahl Q, für das für $s = 1, \ldots, k$

$$\left|\frac{p_s}{q_s} - \alpha\right| > \frac{1}{Q}$$

gilt. Dann gibt es nach dem ersten Punkt ein p/q, das einerseits die geforderte Approximationseigenschaft hat, andererseits wegen

$$\left|\frac{p}{q} - \alpha\right| < \frac{1}{qQ} \leq \frac{1}{Q}$$

nicht in den p_s/q_s enthalten ist. □

Folgendes Lemma hilft einerseits beim Beweis der Existenz einer Lösung von (6.2.3), ist aber andererseits auch bei allgemeinen rechten Seiten nützlich.

Lemma 6.2.3. *Sei $F \neq 0$ eine ganze Zahl und seien (p_1, q_1) und (p_2, q_2) verschiedene Paare positiver ganzer Zahlen, die die verallgemeinerte Pellsche Gleichung*

$$p_j^2 - Dq_j^2 = F, \qquad j \in \{1, 2\}$$

lösen und für die

$$p_1 \equiv p_2 \pmod{F}, \qquad q_1 \equiv q_2 \pmod{F} \tag{6.2.9}$$

gilt.

Dann gibt es eine nichttriviale Lösung (x, y) von (6.2.3) mit

$$p_1 + \sqrt{D}q_1 = (p_2 + \sqrt{D}q_2)(x + \sqrt{D}y).$$

Beweis. Wir bestimmen (x, y) durch

$$x + \sqrt{D}y := \frac{p_1 + \sqrt{D}q_1}{p_2 + \sqrt{D}q_2} = \frac{p_1p_2 - Dq_1q_2}{F} + \frac{q_1p_2 - p_1q_2}{F}\sqrt{D}.$$

Aufgrund der Kongruenzbedingungen (6.2.9) sind x und y ganze Zahlen. Weiters gilt

$$x^2 - Dy^2 = (x + \sqrt{D}y)(x - \sqrt{D}y) = \frac{p_1 + \sqrt{D}q_1}{p_2 + \sqrt{D}q_2} \cdot \frac{p_1 - \sqrt{D}q_1}{p_2 - \sqrt{D}q_2} = \frac{F}{F} = 1,$$

somit ist (x, y) eine Lösung von (6.2.3). Schließlich kann nicht $y = 0$ gelten, weil das zu $(p_1, q_1) = (p_2, q_2)$ führen würde. □

Wir können nun zeigen, dass (6.2.3) tatsächlich immer eine Lösung besitzt.

Beweis von Satz 6.2, 1. Teil (Existenz). Betrachte ein $p/q \in \mathbb{Q}$, das (6.2.8) erfüllt. Dann gilt

$$|p^2 - Dq^2| = |p - \sqrt{D}q| \cdot |p + \sqrt{D}q| < \frac{1}{q} \cdot (|p - \sqrt{D}q| + 2\sqrt{D}q) < (2\sqrt{D} + 1). \tag{6.2.10}$$

Da es nach dem Satz von Dirichlet 6.4 unendlich viele Paare (p, q) gibt, die (6.2.10) erfüllen, gibt es nach Schubfachschluss ein $m \in \mathbb{Z}$, sodass

$$p^2 - Dq^2 = m \tag{6.2.11}$$

für unendlich viele Paare p, q gilt. Dieses m kann nicht 0 sein, weil sonst D eine Quadratzahl wäre.

Da es unendlich viele Paare (p, q) gibt, die (6.2.11) erfüllen, gibt es nach Schubfachschluss eine Lösung (p_0, q_0) von (6.2.11), sodass es unendlich viele Paare (p, q) gibt, sodass

$$p \equiv p_0 \pmod{m}, \qquad q \equiv q_0 \pmod{m}, \qquad p^2 - Dq^2 = m. \tag{6.2.12}$$

Dann existiert laut Lemma 6.2.3 eine nicht-triviale Lösung von (6.2.3). □

Verallgemeinerte Pellsche Gleichung

Für $F \neq 1$ hat die Gleichung $X^2 - DY^2 = F$ nicht immer eine Lösung, wie das Beispiel

$$X^2 - 3Y^2 = -1$$

zeigt: Hier gibt es nicht einmal modulo 3 eine Lösung.

Wenn allerdings eine Lösung (u_1, v_1) von

$$u^2 - Dv^2 = F \tag{6.2.13}$$

existiert und (X_1, Y_1) die Fundamentallösung von $X^2 - DY^2 = 1$ ist, so erhält man durch

$$u_k + \sqrt{D}v_k = (u + \sqrt{D}v)(X_1 + \sqrt{D}Y_1)^k$$

wieder unendlich viele Lösungen von (6.2.13). Wenn $F = -1$ und $v_1 > 0$ minimal war, so erhält man nach Lemma 6.2.3 wieder alle Lösungen; für allgemeines F muss das nicht der Fall sein.
Beispiel 6.2.4. Wir betrachten die Pellsche Gleichung

$$u^2 - 2v^2 = 7.$$

Die Fundamentallösung von $X^2 - 2Y^2 = 1$ ist $(3, 2)$. Weiters sind $(3, 1)$ und $(5, 3)$ Lösungen von $u^2 - 2v^2 = 7$, allerdings gilt

$$\frac{5 + 3\sqrt{2}}{3 + \sqrt{2}} = \frac{9}{7} + \frac{4}{7}\sqrt{2},$$

damit unterscheiden sie sich nicht nur um Potenzen der Fundamentallösung der Pellschen Gleichung. Wir erhalten damit Lösungen

$$(3 + 1\sqrt{2})(3 + 2\sqrt{2})^k \text{ und } (5 + 3\sqrt{2})(3 + 2\sqrt{2})^k.$$

Man kann zeigen, dass das alle Lösungen mit positiven Komponenten ergibt.

6.3 Pythagoräische Tripel, Indische Formeln

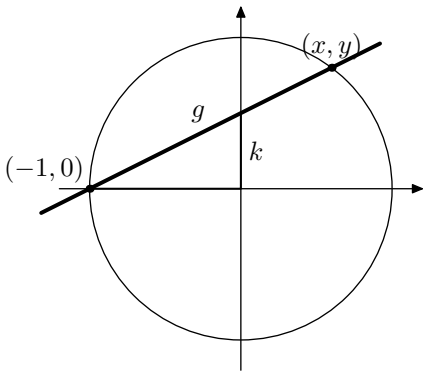
Hier soll noch eine spezielle quadratische diophantische Gleichung in drei Unbekannten behandelt werden:

$$X^2 + Y^2 = Z^2, \tag{6.3.1}$$

wobei in diesem Fall nur positive Lösungen interessant sind. Man spricht von einem *pythagoräischen Tripel*, weil die Lösungen dieser Gleichung Seitenlängen eines rechtwinkeligen Dreiecks sind. Das wohl bekannteste Beispiel ist das Tripel $(X, Y, Z) = (3, 4, 5)$.

Wir wollen nun sämtliche pythagoräischen Tripel finden. Dies soll hier geometrisch argumentiert werden. Da mit jedem pythagoräischen Tripel (X, Y, Z) auch (tX, tY, tZ) mit positivem ganzem t ein pythagoräisches Tripel ist (und umgekehrt), reicht es, nur pythagoräische Tripel (X, Y, Z) mit $\mathrm{ggT}(X, Y, Z) = 1$ zu finden.

Sei (X, Y, Z) ein solches pythagoräisches Tripel. Wenn X und Y beide ungerade sind, so gilt $Z^2 = X^2 + Y^2 \equiv 2 \pmod 4$, ein Widerspruch. Wenn X und Y beide gerade sind, so ist auch Z gerade, was ebenfalls ein Widerspruch ist. Wir nehmen ohne Beschränkung der Allgemeinheit an, dass Y gerade und X ungerade ist.



Wir dividieren (6.3.1) durch Z^2 und erhalten mit $x = X/Z$ und $y = Y/Z$ die Gleichung

$$x^2 + y^2 = 1 \tag{6.3.2}$$

mit rationalen x und y. Der Punkt (x, y) ist also ein rationaler Punkt am Einheitskreis. Wir legen eine Gerade g durch (x, y) und den speziellen Punkt $(-1, 0)$. Sie hat offensichtlich eine rationale Steigung

$$k = \frac{y - 0}{x + 1}. \tag{6.3.3}$$

Die Steigung ist positiv, weil $x > 0$ und $y > 0$. Wir drücken y aus (6.3.3) aus und setzen in (6.3.2) ein und erhalten

$$x^2 + k^2(x + 1)^2 = 1,$$

was zu $(x^2 - 1) + k^2(x + 1)^2 = 0$ und nach Kürzen von $x + 1 > 1$ zu $(x - 1) + k^2(x + 1) = 0$ äquivalent ist. Wir erhalten damit

$$x = \frac{1 - k^2}{1 + k^2}.$$

Es entspricht jedem pythagoräischen Tripel genau eine positive rationale Steigung $0 < k < 1$ und umgekehrt. Wir schreiben $k = v/u$ für positive ganze teilerfremde Zahlen u und v. Es ergibt sich

$$x = \frac{u^2 - v^2}{u^2 + v^2}, \qquad y = \frac{v}{u}\left(1 + \frac{u^2 - v^2}{u^2 + v^2}\right) = \frac{2uv}{u^2 + v^2}. \tag{6.3.4}$$

Offensichtlich muss $u > v$ gelten, damit $x > 0$. Nehmen wir an, dass $u \equiv v \equiv 1 \pmod 2$. In diesem Fall ist $u^2 - v^2 \equiv 1 - 1 \equiv 0 \pmod 4$ und $u^2 + v^2 \equiv 1 + 1 \equiv 2 \pmod 4$. Da $x = X/Z = (u^2 - v^2)/(u^2 + v^2)$, folgt daraus, dass X gerade ist, ein Widerspruch. Da u und v teilerfremd sind, folgt daraus $u \not\equiv v \pmod 2$ und damit $u^2 + v^2 \equiv 1 \pmod 2$. Daher gilt $\mathrm{ggT}(2uv, u^2 + v^2) = \mathrm{ggT}(uv, u^2 + v^2) = 1$, weil $\mathrm{ggT}(u, v) = 1$. Ebenso gilt $\mathrm{ggT}(u^2 - v^2, u^2 + v^2) = \mathrm{ggT}(u^2 + v^2, -2v^2) = \mathrm{ggT}(u^2 + v^2, v^2) = \mathrm{ggT}(u^2, v^2) = 1$. Damit sind die Darstellungen von x und y in (6.3.4) bereits gekürzt. Wir lesen die so genannten indischen Formeln für X, Y und Z ab:

$$\begin{aligned} X &= u^2 - v^2, \\ Y &= 2uv, \\ Z &= u^2 + v^2. \end{aligned} \tag{6.3.5}$$

Wenn umgekehrt u und v relativ prime Zahlen mit $u > v$ und $u \not\equiv v \pmod 2$ sind, so rechnet man leicht nach, dass die in (6.3.5) gegebenen (X, Y, Z) ein pythagoräisches Tripel bilden, wobei $\mathrm{ggT}(X, Y, Z) = 1$ und Y gerade.

Damit haben wir folgenden Satz bewiesen:

Satz 6.5. *Die drei positiven ganzen Zahlen (X, Y, Z) bilden genau dann ein pythagoräisches Tripel mit $2 \mid Y$ und $\mathrm{ggT}(X, Y, Z) = 1$, wenn es relativ prime ganze Zahlen u und v mit $u > v$ und $u \not\equiv v \pmod 2$ gibt, sodass die* indischen Formeln (6.3.5) *gelten.*

6.4 Darstellung von Zahlen als Summe von Quadraten

In diesem Abschnitt soll die Frage geklärt werden, welche positiven ganzen Zahlen n eine Darstellung der Form

$$n = x^2 + y^2 \text{ oder } n = x_1^2 + x_2^2 + x_3^2 + x_4^2$$

mit ganzen x, y, x_1, …, x_4 haben.

Satz 6.6. *Sei n eine positive ganze Zahl. Dann besitzt n genau dann eine Darstellung*

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

mit ganzen x und y, wenn für alle Primteiler $p \mid n$ mit $p \equiv 3 \pmod 4$ gilt, dass $v_p(n)$ gerade ist.

Beweis. 1. Wir beweisen zunächst die Aussage für den Fall, dass eine n eine Primzahl p ist, die kongruent 1 modulo 4 ist.

Aus Satz 5.12 folgt, dass -1 ein quadratischer Rest modulo p ist, weil $(p-1)/2$ gerade ist und damit $(-1)^{(p-1)/2} = 1$ gilt.

Wir wählen jetzt die positive ganze Zahl r so, dass $r^2 < p < (r+1)^2$ gilt. Weiters sei $s := \lfloor p/r \rfloor$. Für $0 \le i \le s$ sei y_i durch $y_i \equiv i \cdot z \pmod p$ mit $0 \le y_i \le p-1$ definiert. Wenn für alle $0 \le i < j \le s$ gilt, dass $|y_j - y_i| \ge r+1$, so gilt für das größte y_i, dass

$$p - 1 \ge y_i \ge (r+1)s > (r+1) \cdot \left(\frac{p}{r} - 1\right) \ge p + \frac{p}{r} - (r+1) > p - 1,$$

ein Widerspruch. Daher muss es ein Paar $0 \le i < j \le s$ mit $|y_j - y_i| \le r$ geben. Wir setzen $x := j - i$ und $y := y_j - y_i$ und erhalten

$$x^2 + y^2 \le s^2 + r^2.$$

Falls $p < r(r+1)$, so ist $s \le r < \sqrt{p}$, also $0 < x^2 + y^2 < 2p$. Andernfalls gilt $p > r(r+1)$ (weil p eine Primzahl ist) und $p \le (r+1)^2 - 1 = r(r+2)$ und damit $p < r(r+2)$ (wiederum weil p eine Primzahl ist). Daher gilt $s = r+1$ und damit $x^2 + y^2 \le (r+1)^2 + r^2 = 2r(r+1) + 1 \le 2(p-1) + 1 = 2p - 1 < 2p$. Wir haben daher in allen Fällen

$$0 < x^2 + y^2 < 2p$$

bewiesen. Nach Konstruktion gilt $x^2 + y^2 \equiv x^2(1 + z^2) \equiv 0 \pmod p$, weshalb nur $p = x^2 + y^2$ gelten kann.

2. Wir bemerken, dass auch die Primzahl 2 als Summe $2 = 1^2 + 1^2$ dargestellt werden kann.

3. Jede Quadratzahl a^2 kann als $a^2 = a^2 + 0^2$ geschrieben werden.

4. Wir zeigen, dass mit zwei Zahlen auch das Produkt als Summe zweier Quadrate geschrieben werden kann. Sei nämlich $m = a^2 + b^2$ und $n = c^2 + d^2$. Dann gilt

$$mn = (a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2.$$

Es wurde also eine Darstellung der gesuchten Form gefunden.

5. Aus dem bisher Gezeigten folgt, dass jede Zahl der im Satz angegebenen Form als Summe zweier Quadrate geschrieben werden kann.

6. Sei p eine Primzahl mit $p \equiv 3 \pmod 4$, die n teilt, und sei $n = x^2 + y^2$. Sei $\alpha := \min(v_p(x), v_p(y))$. Dann teilt $p^{2\alpha}$ offensichtlich n, und wir erhalten $n_1 = x_1^2 + y_1^2$ mit $x_1 := x/p^\alpha$, $y_1 := y/p^\alpha$ und $n_1 := n/p^{2\alpha}$. Durch die Wahl von α ist nun x_1 oder y_1 nicht durch p teilbar.

Wir nehmen an, dass $p \mid n_1$. Da dann $x_1^2 \equiv -y_1^2 \pmod{p}$, sind sowohl x_1 als auch y_1 nicht durch p teilbar. Daher gilt nach Satz 5.3

$$1 \equiv \left(x_1^2\right)^{(p-1)/2} \equiv (-y_1^2)^{(p-1)/2} \equiv (-1)^{(p-1)/2} \cdot 1 \equiv -1 \pmod{p},$$

weil $(p-1)/2$ ungerade ist. Das ist ein Widerspruch, also kann p kein Teiler von n_1 mehr sein, d.h. $v_p(n) = 2\alpha$ war gerade. Somit ist die Bedingung an die Primfaktorzerlegung auch notwendig.

□

Wenn man hingegen 4 Quadrate zulässt, so lässt sich jede Zahl darstellen:

Satz 6.7 (Lagrange)**.** *Sei n eine positive ganze Zahl. Dann gibt es ganze x_1, x_2, x_3, x_4, sodass*

$$n = x_1^2 + x_2^2 + x_3^2 + x_4^2.$$

Auch dieses Resultat lässt sich durch eine Art Schubfachschluss beweisen, vergleiche zum Beispiel Ireland und Rosen [4, Abschnitt 17.7].

7 Primzahlverteilung

In diesem Abschnitt sollen einige Resultate über die Verteilung der Primzahlen bewiesen werden. Das klassischste Resultat soll auf Euklid zurückgehen:

Satz 7.1. *Es gibt unendlich viele Primzahlen.*

Beweis. Wir führen einen indirekten Beweis: Wir nehmen an, dass es *endlich viele* Primzahlen gäbe und bezeichnen diese mit $p_1, \ldots, p_N$. Wir betrachten die Zahl

$$x = p_1 \cdot p_2 \cdots p_N + 1.$$

Offensichtlich gilt für alle Primzahlen p_i, dass $x \equiv 1 \pmod{p_i}$ und dass daher p_i kein Teiler von x ist. Nach dem Satz über die eindeutige Primfaktordarstellung muss es aber eine Primzahl p geben, die x teilt. Somit war die Liste $p_1, \ldots, p_N$ — im Widerspruch zur Annahme — nicht die vollständige Liste aller Primzahlen. □

Ein wenig präziser ist bereits der

Satz 7.2 (Bertrandsches Postulat)**.** *Für jede positive ganze Zahl n gibt es eine Primzahl p, sodass*

$$n < p \leq 2n.$$

Ein (elementarer) Beweis stützt sich auf eine genaue Abschätzung des Binomialkoeffizienten $\binom{2n}{n}$ und auf Satz 4.8, vgl. [1].

Das vermutlich berühmteste Ergebnis über die Verteilung der Primzahlen ist der Primzahlsatz. Er besagt, dass der Anteil der Primzahlen bis zu einer (großen) ganzen Zahl n näherungsweise $1/\ln n$ beträgt; präziser:

Satz 7.3 (Primzahlsatz)**.** *Für eine positive ganze Zahl n bezeichne $\pi(n)$ die Anzahl der Primzahlen $\leq n$. Dann gilt*

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

Der Beweis wurde das erste Mal von Hadamard und de la Vallée-Poussin im Jahr 1896 geführt; üblicherweise verwendet man Techniken der komplexen Analysis. Es gibt allerdings einen „elementaren“ (d.h., ohne Verwendung der komplexen Analysis) Beweis von Selberg und Erdős, der allerdings ziemlich lang und kompliziert ist.

Es gibt nicht nur unendlich viele Primzahlen, sondern auch unendlich viele Primzahlen in jeder arithmetischen Folge $x_n = an + b$, falls $\mathrm{ggT}(a, b) = 1$:

Satz 7.4 (Dirichlet)**.** *Seien a und b relativ prime ganze Zahlen mit $a > 0$. Dann gibt es unendlich viele Primzahlen p mit*

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

Der Beweis wird analytisch geführt, er verwendet die Theorie der L-Reihen.

8 Kongruenzen für Fakultäten und Binomialkoeffizienten

8.1 Satz von Wilson

Satz 8.1 (Wilson)**.** *Sei $n \geq 2$ eine ganze Zahl. Dann ist n genau dann eine Primzahl, wenn*

$$(n-1)! \equiv -1 \pmod{n} \tag{8.1.1}$$

gilt.

Beweis. Wir nehmen zunächst an, dass (8.1.1) gilt. Sei p eine Primzahl, die n teilt, aber ungleich n ist. Dann ist offensichtlich $p < n$, also $p \mid (n-1)!$, womit aber nach (8.1.1) auch $p \mid -1$ folgt. Daher kann es eine solche Primzahl nicht geben, also ist n selbst schon prim.

Sei jetzt umgekehrt n eine Primzahl. Dann gibt es nach Satz 3.1 zu jedem $1 \leq x \leq n-1$ ein $1 \leq f(x) \leq n-1$, sodass $xf(x) \equiv 1 \pmod{n}$, das heißt, dass die Faktoren von $(n-1)!$ in Paare (x, y) eingeteilt werden können, sodass $xy \equiv 1 \pmod{n}$. Dabei ist lediglich auf den Fall Rücksicht zu nehmen, dass $x = y$. In diesem Fall gilt aber $x^2 \equiv 1 \pmod{n}$, was äquivalent zu $p \mid (x-1)(x+1)$ ist, also folgt $x \in \{1, n-1\}$. Damit kürzen sich alle Faktoren in $(n-1)!$ bis auf 1 und $n-1$ weg, und wir erhalten $(n-1)! \equiv 1 \cdot (-1) \equiv -1 \pmod{n}$. □

Aufgabe 8.1.1. Für jede positive ganze Zahl n sei $f(n)$ der größte gemeinsame Teiler von $n! + 1$ und $(n+1)!$. Finden Sie (mit Beweis) eine Formel für $f(n)$ für alle n. ($n! = 1 \cdot 2 \cdots (n-1) \cdot n$) *(Irland 1996)*

Lösung. Sei p ein Primteiler von $f(n)$. Wegen $p \mid (n! + 1)$, ist p teilerfremd zu 1, 2, …, n. Aus $p \mid (n+1)!$ kann man daher $p|(n+1)$ folgern. Allerdings kann p kein echter Teiler von $(n+1)$ sein, weil p ja zu den Zahlen $\leq n$ teilerfremd ist, also gilt $p = n+1$. Falls also $n+1$ keine Primzahl ist, so ist $f(n) = 1$. Falls $n+1 = p$ eine Primzahl ist, so ist $f(n) = p^\alpha$ für ein $\alpha \geq 0$. Da in $(n+1)! = p!$ die Primzahl p offensichtlich genau einmal vorkommt, kommt nur mehr $\alpha \in \{0, 1\}$ in Frage. Da laut dem Satz von Wilson $n! \equiv -1 \pmod{p}$, ist p tatsächlich ein gemeinsamer Teiler von $(n!+1)$ und $(n+1)! = p!$, also $f(n) = p = n+1$.

Zusammenfassend gilt

$$f(n) = \begin{cases} n+1, & \text{falls } n+1 \text{ eine Primzahl ist,} \\ 1, & \text{sonst.} \end{cases}$$

□

8.2 Reste von Binomialkoeffizienten

In diesem Abschnitt soll untersucht werden, welche Reste der Binomialkoeffizient $\binom{n}{k}$ bei Division durch eine Primzahl lässt.

Wir zeigen zunächst ein einfaches, aber immer wieder nützliches Lemma.

Lemma 8.2.1. *Sei p eine Primzahl und $1 \leq k \leq p-1$. Dann teilt p den Binomialkoeffizienten $\binom{p}{k}$.*

Beweis. Es gilt

$$\binom{p}{k} = \frac{p(p-1)\cdots(p-k+1)}{k!}. \tag{8.2.1}$$

Wegen $1 \leq k \leq p-1$ ist keine der Zahlen $p-1, \ldots, p-k+1$ sowie $k, k-1, \ldots, 1$ durch p teilbar. Somit kommt der Primfaktor p in der rechten Seite von (8.2.1) im Zähler genau einmal und im Nenner überhaupt nicht vor. Somit ist $\binom{p}{k}$ durch p teilbar. □

Wir bemerken sofort, dass die Aussage des Lemmas für $k = 0$ oder für $k = p$ sicherlich falsch ist, weil bekanntlich $\binom{p}{0} = \binom{p}{p} = 1$ gilt.

Wir betrachten nun die Restklasse eines Binomialkoeffizienten modulo p in Abhängigkeit von der Ziffernentwicklung zur Basis p:

Satz 8.2 (Lucas)**.** *Sei p eine Primzahl und seien n und k in der Zifferndarstellung zur Basis p als*

$$n = n_\ell p^\ell + n_{\ell-1} p^{\ell-1} + \cdots + n_1 p^1 + n_0,$$
$$k = k_\ell p^\ell + k_{\ell-1} p^{\ell-1} + \cdots + k_1 p^1 + k_0$$

gegeben. Dann gilt

$$\binom{n}{k} \equiv \binom{n_\ell}{k_\ell}\binom{n_{\ell-1}}{k_{\ell-1}}\cdots\binom{n_1}{k_1}\binom{n_0}{k_0} \pmod{p}, \tag{8.2.2}$$

wobei (wie üblich) per Definition $\binom{a}{b} = 0$ für $b > a$ gilt.

Beweis. Wir berechnen den Koeffizienten von x^k im Polynom $(1+x)^n$ auf zweierlei Arten. Einerseits ist dieser Koeffizient laut binomischem Lehrsatz gleich $\binom{n}{k}$. Andererseits gilt

$$(1+x)^n = (1+x)^{\sum_{j=0}^{\ell} n_j p^j} = \prod_{j=0}^{\ell} (1+x)^{n_j p^j} = \prod_{j=0}^{\ell} \left((1+x)^{p^j}\right)^{n_j}.$$

Aus Lemma 8.2.1 und durch Induktion nach j erhalten wir

$$(1+x)^{p^j} \equiv 1 + x^{p^j} \pmod{p},$$

weil ja

$$(1+x)^p = \sum_{i=0}^{p} \binom{p}{i} x^i \equiv 1 + x^p \pmod{p}.$$

Wir erhalten also

$$(1+x)^n \equiv \prod_{j=0}^{\ell} (1+x^{p^j})^{n_j} = \prod_{j=0}^{\ell} \left(\sum_{a_j=0}^{n_j} \binom{n_j}{a_j} x^{a_j p^j} \right) = \prod_{j=0}^{\ell} \left(\sum_{a_j=0}^{p-1} \binom{n_j}{a_j} x^{a_j p^j} \right) \pmod{p}.$$

Im letzten Schritt wurde verwendet, dass $\binom{n_j}{a_j} = 0$ für $a_j > n_j$. Ausmultiplizieren des Produkts ergibt

$$\begin{aligned}(1+x)^n &\equiv \sum_{0 \le a_\ell, a_{\ell-1}, \ldots, a_1, a_0 \le p-1} \prod_{j=0}^{\ell} \binom{n_j}{a_j} x^{a_j p^j} \\ &= \sum_{0 \le a_\ell, a_{\ell-1}, \ldots, a_1, a_0 \le p-1} \left(\prod_{j=0}^{\ell} \binom{n_j}{a_j} \right) x^{\sum_{j=0}^{\ell} a_j p^j} \pmod{p}.\end{aligned}$$

Die Exponenten von x sind also offensichtlich durch ihre Zifferndarstellung zur Basis p gegeben. Um den Koeffizienten von x^k abzulesen, müssen wir daher den Summanden $(a_\ell, \ldots, a_0) = (k_\ell, \ldots, k_0)$ heranziehen und erhalten (8.2.2). □

8.3 Satz von Wolstenholme

Satz 8.3. *Sei $p > 3$ eine Primzahl. Dann ist der Zähler von*

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1} \tag{8.3.1}$$

durch p^2 teilbar. Weiters ist der Zähler von

$$1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{(p-1)^2} \tag{8.3.2}$$

durch p teilbar.

Vor dem Beweis geben wir folgendes Korollar an:

Korollar 8.3.1. *Sei $p > 3$ eine Primzahl. Dann gilt*

$$\binom{2p}{p} \equiv 2 \pmod{p^3}$$

und

$$\binom{2p-1}{p-1} \equiv 1 \pmod{p^3}. \tag{8.3.3}$$

Beweis von Satz 8.3. Für $1 \le k \le p-1$ bezeichnen wir den inversen Rest von k modulo p mit $\frac{1}{k}$.

Wir beweisen zunächst (8.3.2). Da die Abbildung $x \mapsto \frac{1}{x}$ die Reste $1, \ldots, p-1$ permutiert, gilt

$$\sum_{k=1}^{p-1} \frac{1}{k^2} \equiv \sum_{k=1}^{p-1} k^2 \equiv \frac{(p-1)p(2p-1)}{6} \equiv 0 \pmod{p}, \tag{8.3.4}$$

und (8.3.2) ist bewiesen.

Wir betrachten das Polynom

$$Q(x) = (x-1)(x-2)\dots(x-(p-1)).$$

Ausmultiplizieren ergibt

$$Q(x) = (p-1)! - x(p-1)!\sum_{k=1}^{p-1}\frac{1}{k} + x^2(p-1)!\left(\sum_{1\le i<j\le p-1}\frac{1}{ij}\right) + \cdots .$$

Da $p-1$ gerade ist, gilt $Q(0) = Q(p) = (p-1)!$. Daher gilt

$$0 = Q(p) - Q(0) \equiv -p(p-1)!\sum_{k=1}^{p-1}\frac{1}{k} + p^2(p-1)!\left(\sum_{1\le i<j\le p-1}\frac{1}{ij}\right) \pmod{p^3}. \tag{8.3.5}$$

Betrachtet man diese Kongruenz nur modulo p^2, sieht man, dass

$$\sum_{k=1}^{p-1}\frac{1}{k} \equiv 0 \pmod{p} \tag{8.3.6}$$

gilt. Dies hätte man auch durch ein Argument wie in (8.3.4) gesehen. Unsere Aufgabe ist es allerdings, dieselbe Kongruenz modulo p^2 zu zeigen.

Es gilt

$$\begin{aligned}\sum_{1\le i<j\le p-1}\frac{1}{ij} &= \frac{1}{2}\left(\sum_{1\le i,j\le p-1}\frac{1}{ij} - \sum_{1\le i\le p-1}\frac{1}{i^2}\right) = \frac{1}{2}\left(\sum_{1\le i\le p-1}\frac{1}{i}\sum_{1\le j\le p-1}\frac{1}{j} - \sum_{1\le i\le p-1}\frac{1}{i^2}\right) \\ &\equiv \frac{1}{2}\left(0\cdot 0 + 0\right) \pmod{p},\end{aligned} \tag{8.3.7}$$

wobei im letzten Schritt (8.3.6) und (8.3.2) verwendet wurden.

Damit ergibt sich aus (8.3.5), dass

$$0 \equiv -p(p-1)!\sum_{k=1}^{p-1}\frac{1}{k} \pmod{p^3},$$

woraus nach Kürzen von p unter Berücksichtigung von $\mathrm{ggT}(p,(p-1)!) = 1$

$$0 \equiv \sum_{k=1}^{p-1}\frac{1}{k} \pmod{p^2}.$$

folgt. □

Beweis von Korollar 8.3.1. Zunächst bemerken wir, dass

$$\binom{2p}{p} = \frac{2p(2p-1)\dots(p+1)}{p(p-1)\dots 1} = 2\frac{(2p-1)\dots(p+1)}{(p-1)\dots 1} = 2\binom{2p-1}{p-1}$$

gilt, es reicht also, (8.3.3) zu beweisen.

Es gilt

$$\begin{aligned}\binom{2p-1}{p-1} &= \frac{(2p-1)\dots(p+1)}{(p-1)\dots 1} = \frac{(p+p-1)\dots(p+1)}{(p-1)\dots 1} = \left(1+\frac{p}{1}\right)\left(1+\frac{p}{2}\right)\dots\left(1+\frac{p}{p-1}\right) \\ &\equiv 1 + p\sum_{i=1}^{p-1}\frac{1}{i} + p^2\sum_{1\le i<j\le p-1}\frac{1}{ij} \equiv 1 \pmod{p^3},\end{aligned}$$

wobei im letzten Schritt der Satz von Wolstenholme und (8.3.7) verwendet wurden.

□

Literatur

[1] M. Aigner and G. M. Ziegler, *Proofs from The Book*, second ed., Springer-Verlag, Berlin, 2001.

[2] P. Bundschuh, *Einführung in die Zahlentheorie*, Springer, Berlin *etc.*, 1996.

[3] E. Hlawka and J. Schoißengeier, *Zahlentheorie. Eine Einführung*, Manzsche Verlags- und Universitätsbuchhandlung, Wien, 1979.

[4] K. Ireland and M. Rosen, *A classical introduction to modern number theory*, Graduate Texts in Mathematics, vol. 84, Springer, 1993.

Clemens Heuberger, Institut für Mathematik, Alpen-Adria-Universität, Universitätsstraße 65–67, 9020 Klagenfurt am Wörthersee, `clemens.heuberger@aau.at`