5 Grundlagen der Zahlentheorie

1. Primfaktorzerlegung

Seien$m, n \in \mathbb{N}_+ := \{k \in \mathbb{N} \mid k > 0\}$. Man schreibt

$$n \mid n\,, \text{ gesprochen „}m \text{ teilt } n\text{“ oder „}m \text{ ist ein Teiler von } n\text{“},$$

wenn es eine positive natürliche Zahl k gibt mit $mk = n$.

Definition 1.1. *Eine natürliche Zahl p heißt **Primzahl** (oder **prim**), wenn $p \geq 2$ ist und 1 und p die einzigen Teiler von p sind.*

Ist n eine natürliche Zahl ≥ 2, so ist die kleinste natürliche Zahl $p \geq 2$, die n teilt, eine Primzahl (denn aus $a \mid b$ und $a \neq b$ folgt $a < b$). Eine solche Zahl, die gleichzeitig Teiler von n und eine Primzahl ist, nennt man dann einen Primteiler von n. Es gilt also insbesondere: Jede natürliche Zahl ≥ 2 hat (wenigstens) einen Primteiler.

Als einfache Folgerung ergibt sich der berühmte Satz, den Euklid schon vor über 2000 Jahren bewies:

Satz 1.2 (Euklid)**.** *Es gibt unendlich viele Primzahlen.*

Beweis. Es gibt sehr viele Beweise für diesen Satz; einer ist der folgende. Angenommen es gäbe nur endlich viele Primzahlen $p_1, \ldots, p_n$. Dann ist $p_1 \cdots p_n + 1$ eine natürliche Zahl ≥ 2, die einen Primteiler p besitzt, wie oben schon gesehen. Dieses p ist von den Primzahlen $p_1, \ldots, p_n$ verschieden, denn sonst wäre p auch ein Teiler von 1. □

Die Reihe der Primzahlen beginnt mit

$$2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots$$

die größte bekannte Primzahl (Sommer 2009) ist

$$2^{43112609} - 1\,,$$

eine Zahl mit ca. 13 Millionen Stellen.

Eine einfache Methode, alle Primzahlen zu finden, die kleiner oder gleich einer vorgegebenen Zahl n sind, ist das sogenannte *Sieb des Eratosthenes*: man schreibe eine Liste aller (ungeraden) Zahlen $\leq n$ und streiche alle Vielfachen aller Primzahlen $\leq \sqrt{n}$. Will man umgekehrt eine bestimmte Zahl m darauf testen, ob sie prim ist, reicht es, sie auf Teilbarkeit durch alle Primzahlen $\leq \sqrt{m}$ zu prüfen.

Zahlen der Form $M_p = 2^p - 1$ für eine Primzahl p nennt man Mersenne[1]-Zahlen. Alle sehr großen bekannten Primzahlen sind Mersenne-Zahlen, denn für sie gibt es einen einfachen Primzahltest, den sogenannten Lucas-Test: Man bilde rekursiv die Folge $(r_k)_{k\geq 1}$ mit $r_1 = 4$ und

$$r_{k+1} = \text{ der kleinste nichtnegative Rest bei der Division von } r_k^2 - 2 \text{ durch } M_p.$$

Ist $p \geq 3$, so gilt: M_p ist genau dann prim, wenn $r_{p-1} = 0$ ist.

[1] Marin Mersenne, 1588–1648, französischer Priester und Mathematiker.

Beispiel. $M_7 = 127$ ist prim:

$$\begin{aligned} r_1^2 - 2 &= 14 = 0 \cdot 127 + 14 && \Rightarrow r_2 = 14 \\ r_2^2 - 2 &= 194 = 127 + 67 && \Rightarrow r_3 = 67 \\ r_3^2 - 2 &= 4487 = 35 \cdot 127 + 42 && \Rightarrow r_4 = 42 \\ r_4^2 - 2 &= 1762 = 13 \cdot 127 + 111 && \Rightarrow r_5 = 111 \\ r_5^2 - 2 &= 12319 = 97 \cdot 127 && \Rightarrow r_6 = 0 \end{aligned}$$

In diesem Beispiel ist der Lucas-Test natürlich nicht sehr effizient, aber das ändert sich schnell bei größeren p.

Satz 1.3. *Jede positive natürliche Zahl ist Produkt von Primzahlen.*

Beweis. Die Zahl 1 ist das leere Produkt. Sei nun $n \geq 2$, und per Induktion sei angenommen, dass die Behauptung für alle kleineren natürlichen Zahlen gilt. n besitzt einen Primteiler p, und es ist $n = pm$ mit $m \in \mathbb{N}_+$. Ist $m = 1$, so ist $n = p$ prim, ansonsten ist $m > 1$ und daher $m < n$. Nach Induktionsvoraussetzung lässt sich also m als Produkt

$$m = p_1 \cdots p_k$$

mit Primzahlen $p_1, \ldots, p_k$ schreiben. Folglich ist

$$n = p \cdot p = p \cdot_1 \cdots p_n$$

ebenfalls Produkt von Primzahlen. □

Ziel dieses Abschnittes ist es zu zeigen, dass diese Produktdarstellung bis auf die Reihenfolge der Faktoren eindeutig ist. Dazu sei als Hilfsmittel zunächst der Divisionsalgorithmus beschrieben.

Satz 1.4 (Division mit Rest)**.** *Seien $n, m \in \mathbb{Z}$ mit $m > 0$. Dann gibt es eindeutig bestimmte ganze Zahlen q und r mit*

$$n = q \cdot m + r \quad \textit{und} \quad 0 \leq r < m\,.$$

Beweis. Sei zunächst $n \geq 0$. Die Behauptung wird durch Induktion über n gezeigt. Ist $0 \leq n < m$, so ist

$$n = 0 \cdot m + n$$

eine Darstellung in der gewünschten Form. Sei also $n > m$ und die Behauptung wahr für alle natürlichen Zahlen, die kleiner als n sind. Dann gilt sie auch für n: es ist $n - m < n$, also gibt es nach Induktionsvoraussetzung ganze Zahlen q' und r mit

$$n - m = q' \cdot m + r \quad \text{mit } 0 \leq r < m,$$

und wegen

$$n = m + q' \cdot m + r = (q' + 1) \cdot m + r$$

folgt die Behauptung mit $q = q' + 1$.
Ist $n < 0$, so gibt es nach dem gerade Gezeigten ganze Zahlen $\tilde{q}$ und $\tilde{r}$, so dass

$$-n = \tilde{q} \cdot m + \tilde{r} \quad \text{mit } 0 \leq \tilde{r} < m,$$

und die gewünschte Darstellung ist

$$n = \begin{cases} (-\tilde{q} - 1) \cdot m + (m - \tilde{r}) & \text{falls } \tilde{r} \neq 0, \\ -\tilde{q} \cdot m & \text{falls } \tilde{r} = 0. \end{cases}$$

Zu zeigen ist noch die Eindeutigkeit der Darstellung: Sei

$$n = q_1 \cdot m + r_1 = q_2 \cdot m + r_2 \quad \text{mit } 0 \leq r_1, r_2 < m.$$

Dann ist

$$0 = n - n = (q_1 - q_2) \cdot m + (r_1 - r_2)\,,$$

also ist m ein Teiler von $r_1 - r_2$, was wegen $|r_1 - r_2| < m$ dann $r_1 = r_2$ impliziert, woraus wiederum $q_1 = q_2$ folgt. □

Die Zahl r in Satz 1.4 ist der (kleinste nichtnegative) **Rest** von n bei Division durch m, und q ist der **ganze Anteil** der rationalen Zahl $\frac{n}{m}$, geschrieben als die *Gauß-Klammer* $\left[\frac{n}{m}\right]$ (oder manchmal auch $\left\lfloor\frac{n}{m}\right\rfloor$).

Folgerung: Sei ℓ eine natürliche Zahl ≥ 2. Dann gibt es zu jeder natürlichen Zahl $n \geq 1$ eindeutig bestimmte natürliche Zahlen r und $n_0, n_1, \ldots, n_r$ mit $0 \leq r_i < \ell$ für $0 \leq i \leq r$ und $n_r \neq 0$, so dass

$$n = n_0 + n_1 \cdot \ell + n_2 \cdot \ell^2 + \cdots + n_r \cdot \ell^r = \sum_{i=0}^{r} n_i \cdot \ell^i \,.$$

Diese Schreibweise von n nennt man die **ℓ-adische Entwicklung** von n.
Die Ziffern $n_0, \ldots, n_r$ gewinnt man rekursiv durch Division mit Rest nach dem Schema

$$\begin{aligned} n = q_0 &= q_1 \cdot \ell + n_0 && 0 \leq n_0 < \ell \\ q_1 &= q_2 \cdot \ell + n_1 && 0 \leq n_1 < \ell \\ q_2 &= q_3 \cdot \ell + n_2 && 0 \leq n_2 < \ell \\ &\vdots \\ q_{r-1} &= q_r \cdot \ell + n_{r-1} && 0 \leq n_{r-1} < \ell \\ q_r &= n_r && 0 < n_r < \ell \end{aligned}$$

Diese Prozedur muss abbrechen, da die Zahlen q_i immer kleiner werden: es gilt

$$q_i - q_{i+1} = q_{i+1}\ell + n_i - q_{i+1} = q_{i+1} \cdot (\ell - 1) + n_i \geq 0 \,,$$

denn es ist $\ell - 1 \geq 1$ und $q_i, n_i \geq 0$.
Für $\ell = 10$ ist dies die wohlbekannte Dezimalschreibweise, bei der man allerdings die Ziffern n_i von rechts nach links schreibt.

Beispiel. Sei $\ell = 5$ und $n = 167$:

$$\begin{aligned} 167 &= 33 \cdot 5 + 2 && n_0 = 2\,, \quad q_1 = 33 \\ 33 &= 6 \cdot 5 + 3 && n_1 = 3\,, \quad q_2 = 6 \\ 6 &= 1 \cdot 5 + 1 && n_2 = 1\,, \quad q_3 = 1 \\ 1 &= 1 \end{aligned}$$

Daraus liest man ab:

$$167 = 2 + 3 \cdot 5 + 1 \cdot 5^2 + 1 \cdot 5^3 \,.$$

Im 5er-System schriebe sich die Zahl 167 also als 1132 (wobei die Ziffern wie im Dezimalsystem auch wieder von rechts nach links geschrieben seien).

Definition 1.5. *Für $m, n \in \mathbb{N}_+$ heißt $d \in \mathbb{N}_+$ der **größte gemeinsame Teiler** von m und n, geschrieben (m, n), wenn d ein Teiler von m und von n ist und wenn für jeden Teiler d' von m und von n gilt: $d' \mid d$.*

Ist $(m, n) = 1$, so nennt man m und n **teilerfremd**. Ist $d = (m, n)$, so sind offenbar $\frac{n}{d}$ und $\frac{m}{d}$ teilerfremd.

Zur Berechnung des größten gemeinsamen Teilers zweier Zahlen gibt es ein Verfahren, das man den **Euklidischen Algorithmus** nennt. Dieser funktionert folgendermaßen: Setze $r_0 = n$ und $r_1 = m$, und definiere dann rekursiv

$$\begin{aligned} r_0 &= q_1 \cdot r_1 + r_2 && 0 < r_2 < r_1 \\ r_1 &= q_2 \cdot r_2 + r_3 && 0 < r_3 < r_2 \\ &\vdots \\ r_{k-1} &= q_k \cdot r_k + r_{k+1} && 0 < r_{k+1} < r_k \\ r_k &= q_k \cdot r_{k+1} \end{aligned}$$

Das Verfahren endet, falls r_{k+1} ein Teiler von r_k ist. Da die Reste r_i sukzessive kleiner werden, muss das Verfahren abbrechen.

Satz 1.6. $(n, m) = r_{k+1}$.

Beweis. Da r_{k+1} ein Teiler von r_k ist, gilt $r_{k+1} = (r_k, r_{k+1})$. Es genügt also zu zeigen, dass für jedes i mit $1 \leq i \leq k$ gilt: Existiert (r_i, r_{i+1}), so existiert auch (r_{i-1}, r_i), und diese beiden Zahlen sind gleich. Hat man diese Behauptung nämlich gezeigt, folgt durch (absteigende) Induktion auch $r_{k+1} = (r_0, r_1) = (n, m)$. Aus der Gleichung

$$r_{i-1} = q_i \cdot r_i + r_{i+1}$$

folgt aber, dass die gemeinsamen Teiler von r_{i-1} und r_i dieselben sind wie die gemeinsamen Teiler von r_i und r_{i+1}. □

Beispiel. Sei $n = 1513$ und $m = 1037$.

$$\begin{aligned} 1513 &= 1 \cdot 1037 + 476 \\ 1037 &= 2 \cdot 476 + 85 \\ 476 &= 5 \cdot 85 + 51 \\ 85 &= 1 \cdot 51 + 34 \\ 51 &= 1 \cdot 34 + 17 \\ 34 &= 2 \cdot 17 \end{aligned}$$

Es ist also $(1513, 1037) = 17$.

Die Reste r_i, die im Euklidischen Algorithmus auftauchen, kann man in der Form

$$r_i = s_i \cdot n + t_i \cdot m \ , \quad s_i, t_i \in \mathbb{Z}$$

schreiben. Dazu setzt man $s_0 = 1$, $t_0 = 0$ und $s_1 = 0$, $t_1 = 1$, und aus der Rekursionsformel des Algorithmus erhält man rekursiv die weiteren Werte:

$$\begin{aligned} r_{i+1} &= r_{i-1} - q_i \cdot r_i = s_{i-1} \cdot n + t_{i-1} \cdot m - q_i \cdot s_i \cdot n - q_i \cdot t_i \cdot m \\ &= \underbrace{(s_{i-1} - q_i \cdot s_i)}_{=:s_{i+1}} \cdot n + \underbrace{(t_{i-1} - q_i \cdot t_i)}_{=:t_{i+1}} \cdot m \end{aligned}$$

d.h. mit

$$s_{i+1} = s_{i-1} - q_i \cdot s_i \quad \text{und} \quad t_{i+1} = t_{i-1} - q_i \cdot t_i$$

hat man die gewünschte Darstellung auch für den nächsten Rest. Dies setzt man fort bis zum letzten Rest, dem größten gemeinsamen Teiler. Damit ist gezeigt:

Korollar 1.7. *Sind $n, m \in \mathbb{N}_+$, so gibt es ganze Zahlen s, t mit $(n, m) = s \cdot n + t \cdot n$.* □

Beispiel (Fortsetzung des obigen Beispiels)**.**

$$\begin{aligned} 17 &= 51 - 1 \cdot 34 \\ &= 51 - (85 - 1 \cdot 51) \\ &= 2 \cdot 51 - 1 \cdot 85 \\ &= 2 \cdot (476 - 5 \cdot 85) - 1 \cdot 85 \\ &= 2 \cdot 476 - 11 \cdot 85 \\ &= 2 \cdot 476 - 11 \cdot (1037 - 2 \cdot 476) \\ &= 24 \cdot 476 - 11 \cdot 1037 \\ &= 24 \cdot (1513 - 1 \cdot 1037) - 11 \cdot 1037 \\ &= 24 \cdot 1513 - 35 \cdot 1037 \end{aligned}$$

Man erhält also die Darstellung

$$(1513, 1037) = 24 \cdot 1513 - 35 \cdot 1037 \, .$$

Sind insbesondere n und m teilerfremd, so gibt es ganze Zahlen s, t mit $1 = s \cdot n + t \cdot m$. Hier gilt auch die Umkehrung: wenn es solche s, t gibt, so ist $(n, m) = 1$, denn ist d ein gemeinsamer Teiler von n und m, so teilt d auch $s \cdot n + t \cdot m = 1$, und es folgt $d = 1$.

Satz 1.8 (Lemma von Euklid)**.** *Teilt eine Primzahl p ein Produkt $n_1 \cdots n_k$ positiver natürlicher Zahlen, so teilt p wenigstens einen Faktor n_i.*

Beweis. Es reicht, die Aussage für $k = 2$ zu beweisen (Induktion über k). Nach Voraussetzung gibt es ein $m \in \mathbb{N}_+$ mit $pm = n_1 n_2$. Falls p kein Teiler von n_1 ist, so ist, da p prim ist, $(p, n_1) = 1$. Also gibt es $s, t \in \mathbb{Z}$ mit $1 = s \cdot p + t \cdot n_1$, und es folgt

$$n_2 = n_2 \cdot 1 = s \cdot p \cdot n_1 + t \cdot n_1 \cdot n_2 = s \cdot p \cdot n_1 + t \cdot m \cdot p = p \cdot (sn_1 + mt)\,,$$

d.h. p teilt n_2. □

Nun ist alles beisammen, um den Satz von der eindeutigen Primfaktorzerlegung beweisen zu können, der wegen seiner Bedeutung auch als der Hauptsatz des elementaren Zahlentheorie bezeichnet wird.

Satz 1.9 (Hauptsatz der elementaren Zahlentheorie)**.** *Jede positive natürliche Zahl lässt sich bis auf die Reihenfolge der Faktoren eindeutig als Produkt von Primzahlen darstellen.*

Beweis. Wegen Satz 1.3 ist nur noch Eindeutigkeit zu zeigen. Seien also

$$n = p_1 \cdots p_k = q_1 \cdots q_\ell$$

zwei Darstellungen. Per Induktion über n soll gezeigt werden, dass $k = l$ gilt, sowie $p_i = q_i$ $(1 \le i \le k)$ nach Umnumerieren. Für $n = 1$ ist nichts zu zeigen (das leere Produkt ist eindeutig). Sei also $k \ge 1$. Dann teilt p_1 das Produkt $q_1 \cdots q_\ell$, wegen des Lemmas von Euklid also einen der Faktoren q_i. Nach Umnumerierung kann man $p_1 \mid q_1$ annehmen. Da q_1 prim ist, folgt $p_1 = q_1$, also

$$p_2 \cdots p_k = q_2 \cdots q_\ell =: m\,.$$

Dann ist $m < n$, und die Behauptung folgt aus der Induktionsannahme. □

Fasst man identische Primfaktoren zusammen, erhält man die sogenannte *kanonische* Zerlegung einer Zahl n:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} = \prod_{i=1}^{r} p_i^{\alpha_i}\,,$$

wobei $p_1, \ldots, p_r$ paarweise verschieden sind. Dabei nennt man α_i die Vielfachheit von p_i (sie kann auch Null sein). Sind nun n und m zwei positive natürliche Zahlen und ist $\{p_1, p_2, \ldots, p_r\}$ die Menge der Primfaktoren von n oder m, so kann man n und m schreiben als

$$n = \prod_{i=1}^{r} p_i^{\alpha_i}\,, \quad m = \prod_{i=1}^{r} p_i^{\beta_i}$$

mit Vielfachheiten $\alpha_i, \beta_i \ge 0$ für $1 \le i \le r$. Dann ist n ein Teiler von m, wenn alle $\alpha_i \le \beta_i$ sind, und es gilt

$$(n, m) = \prod_{i=1}^{r} p_i^{\min\{\alpha_i, \beta_i\}}\,.$$

Die Zahl

$$\mathrm{kgV}(n, m) = \prod_{i=1}^{r} p_i^{\max\{\alpha_i, \beta_i\}}$$

nennt man aus naheliegenden Gründen das kleinste gemeinsame Vielfache von n und m.

Bisher wurde nur von positiven Zahlen gesprochen. Ist nun $n \in \mathbb{Z}$ und $n \neq 0$, so kann man n ebenso zerlegen als

$$n = \varepsilon \prod_{i=1}^{r} p_i^{\alpha_i} \quad \text{mit } \varepsilon \in \{-1, +1\},$$

wobei ε das Vorzeichen von n ist, also $+1$, falls $n > 0$ und -1 für $n < 0$.

2. Restklassenringe: Das Rechnen mit Restklassen modulo m

Sei m eine natürliche Zahl, $m \geq 2$. Betrachte die Äquivalenzrelation auf $\mathbb{Z}$, die durch

$$a \sim b \ :\Leftrightarrow \ m \mid a - b$$

definiert ist. Statt $a \sim b$ schreibt man dann auch

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

gesprochen als „a kongruent b modulo m“, und nennt dies eine **Kongruenz**.
Die Äquivalenzklassen dieser Relation nennt man die **Restklassen** bei Division durch m. Die Restklasse einer Zahl a schreibt man der Tradition folgend nicht mit eckigen Klammern, sondern als $\overline{a}$, d.h.

$$\overline{a} = \{n \in \mathbb{Z} \mid m \text{ teilt } n - a\}\,.$$

Beispiel. Sei $m = 7$. Dann sind also zwei Zahlen genau dann äquivalent, wenn ihre Differenz durch 7 teilbar ist. Damit gibt es 7 Äquivalenzklassen, die genau den möglichen Resten bei Division durch 7 entsprechen und daher auch so bezeichnet werden:

$$\begin{aligned}
\overline{0} &= \{n \in \mathbb{Z} \mid \ 7 \mid n\} = \{\ldots, -14, -7, 0, 7, 14, 21, \ldots\} \\
\overline{1} &= \{n \in \mathbb{Z} \mid \ 7 \mid n - 1\} = \{\ldots, -13, -6, 1, 8, 15, 22, \ldots\} \\
&\vdots \\
\overline{6} &= \{n \in \mathbb{Z} \mid \ 7 \mid n - 6\} = \{-15, -8, -1, 6, 13, 20, \ldots\}
\end{aligned}$$

Statt dieser Repräsentanten hätte man natürlich auch andere nehmen können; es ist $\overline{0} = \overline{7}$ usw.

Sei c eine ganze Zahl. Aus $a \equiv b \bmod m$ folgt offenbar

$$\begin{aligned}
a + c &\equiv b + c \bmod m \\
ac &\equiv bc \bmod m
\end{aligned}$$

Weiterhin gilt:

Lemma 2.1. *Ist $a \equiv a' \bmod m$, so gilt für jedes b*

$$a + b \equiv a' + b \bmod m \quad \textit{und} \quad ab \equiv a'b \bmod m.$$

Beweis. Nach Voraussetzung gibt es ein $k \in \mathbb{Z}$ mit $a - a' = km$. Aber dann gilt auch

$$(a + b) - (a' + b) = a - a' = km \quad \text{und} \quad ab - a'b = (a - a')b = kbm\,,$$

d.h. $(a + b) - (a' + b)$ sowie $ab - a'b$ sind durch m teilbar wie behauptet. □

Da Addition und Multiplikation kommutativ sind, hätte man auch b durch ein äquivalentes b' ersetzen können, ohne die Restklassen von Summe und Produkt zu ändern. Das heißt aber, dass die Restklasse von Summe und Produkt zweier Zahlen nur von den Restklassen der Summanden bzw. Faktoren abhängen. Folglich kann man die Addition und Multiplikation von Restklassen durch die entsprechenden Operationen auf beliebigen Repräsentanten definieren:

$$\overline{a} + \overline{b} := \overline{a + b}$$

und

$$\overline{a} \cdot \overline{b} := \overline{a \cdot b}$$

Dann ist auch klar: Die Null, also das neutrale Element für die Addition, ist die Klasse $\overline{0}$, und die Eins, d.h. das neutrale Element der Multiplikation, ist die Klasse $\overline{1}$.

Die Rechenreglen für ganze Zahlen implizieren nun auch, dass die gleichen Regeln für das Rechnen mit Restklassen gilt. Die eben definierte Addition und Multiplikation von Restklassen erfüllen also die Assoziativ- und Kommutativgesetze sowie das Distributivgesetz.

Definition 2.2. *$\mathbb{Z}/m\mathbb{Z}$ sei die Menge der Restklassen der Division durch m.*

Die eben dargelegten Eigenschaften der arithmetischen Operationen auf $\mathbb{Z}/m\mathbb{Z}$ zeigen also:

Satz 2.3. *$(\mathbb{Z}/m\mathbb{Z}, +, \cdot, \overline{0}, \overline{1})$ ist ein kommutativer Ring.* □

Beispiele. 1. Sei $m = 6$. Die Multiplikationstafel für $\mathbb{Z}/6\mathbb{Z}$ hat die Gestalt:

	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

(Die Multiplikation mit $\overline{0}$ wurde ausgespart, denn sie ergibt immer $\overline{0}$, was schon aus den Ringaxiomen folgt.) Dabei fällt auf, dass es Elmente $\neq \overline{0}$ gibt, deren Produkt Null ist.

2. Sei $m = 7$. Diesmal erhält man die Multiplikationstafel

	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{1}$	$\overline{3}$	$\overline{6}$
$\overline{3}$	$\overline{3}$	$\overline{6}$	$\overline{2}$	$\overline{5}$	$\overline{1}$	$\overline{4}$
$\overline{4}$	$\overline{4}$	$\overline{1}$	$\overline{5}$	$\overline{2}$	$\overline{6}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{3}$	$\overline{1}$	$\overline{6}$	$\overline{4}$	$\overline{2}$
$\overline{6}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Hier kommt jede der Restklassen $\neq \overline{0}$ in jeder Zeile und in jeder Spalte genau einmal vor. Das bedeutet aber, dass $(\mathbb{Z}/7\mathbb{Z} - \{0\}, \cdot, \overline{1})$ eine abelsche Gruppe ist und folglich $\mathbb{Z}/7\mathbb{Z}$ ein Körper.

Warnung: Kürzen darf man in Kongruenzen im allgemeinen nicht! Zum Beispiel ist

$$15 \equiv 3 \bmod 6\,,$$

aber

$$5 \not\equiv 1 \bmod 6\,.$$

Definition 2.4. *Sei $(R, +, \cdot, 0, 1)$ ein kommutativer Ring.*

(a) *Ein Element $a \neq 0$ von R heißt **Nullteiler**, wenn es ein $x \in R$ gibt, $x \neq 0$, mit $ax = 0$.*
(b) *Ein Element $a \in R$ heißt eine **Einheit**, wenn es ein $x \in R$ gibt mit $ax = 1$.*

Bemerkung. Ein kommutativer Ring ist also genau dann ein Körper, wenn jedes Element $a \neq 0$ eine Einheit ist.

Beispiele. 1. Der Ring $\mathbb{Z}$ hat keine Nullteiler („ist nullteilerfrei“). Die einzigen Einheiten sind 1 und -1.

2. Die Einheiten im Ring $\mathbb{Z}/6\mathbb{Z}$ sind $\overline{1}$ und $\overline{5}$, die übrigen Elemente $\neq \overline{0}$ sind Nullteiler.

3. Jedes Element $\neq \overline{0}$ in $\mathbb{Z}/7\mathbb{Z}$ ist eine Einheit.

Nach diesen Beispielen soll nun der allgemeine Fall untersucht werden. Dazu ist folgende Sprachregelung nützlich:

Definition 2.5. *Sei $m \in \mathbb{N}$, $m \geq 2$. Eine Restklasse $\overline{a} \in \mathbb{Z}/m\mathbb{Z}$ heißt **prime Restklasse**, wenn $(a, m) = 1$ ist.*

Da die Eigenschaft einer Restklasse, prim zu sein, über einen Vertreter dieser Restklasse definiert wurde, muss noch nachgewiesen werden, dass das eine vernünftige Definition ist. Zu zeigen ist

also: ist $(a,m)=1$ und $b\equiv a \bmod m$, so gilt auch $(b,m)=1$. Aber das ist klar: Sei $b-a=k\cdot m$, dann folgt aus $1=s\cdot a+t\cdot m$ auch

$$s\cdot b+(t-sk)\cdot m=s\cdot(b-km)+t\cdot m=s\cdot a+t\cdot m=1\,,$$

also $(b,m)=1$.

Satz 2.6. *Sei m eine natürliche Zahl, $m\geq 2$. Die Einheiten in $\mathbb{Z}/m\mathbb{Z}$ sind gerade die primen Restklassen.*

Beweis. Ist $\overline{a}$ eine prime Restklasse, so gibt es $s,t\in\mathbb{Z}$ mit $1=s\cdot a+t\cdot m$, d.h. es ist $\overline{s}\cdot\overline{a}=\overline{1}$. Ist umgekehrt $\overline{a}$ eine Einheit, so gibt es eine Restklasse $\overline{s}$ mit $\overline{1}=\overline{s}\cdot\overline{a}=\overline{s\cdot a}$, d.h. es gibt ein $t\in\mathbb{Z}$ mit $1-s\cdot a=t\cdot m$ bzw. $1=s\cdot a+t\cdot m$; es folgt $(a,m)=1$. □

Beispiel. Sei $m=427$ $(=7\cdot 61)$ und $a=21$. Dann ist $\overline{a}$ keine Einheit, denn $(21,427)=7\neq 1$. Andererseits ist $(12,427)=1$, also ist $\overline{12}$ eine Einheit. Um das Inverse zu finden, muss man wieder den Euklidischen Algorithmus anwerfen, mit $r_0=427$ und $r_1=12$:

$$\begin{aligned}427&=35\cdot 12+7\\12&=1\cdot 7+5\\7&=1\cdot 5+2\\5&=2\cdot 2+1\\2&=2\cdot 1\end{aligned}$$

Dies zeigt noch einmal $(427,12)=1$, und um die Zahlen s,t zu finden, das Ganze rückwärts:

$$\begin{aligned}1&=&5&-&2\cdot 2\\&=&5&-&2\cdot(7-5)\\&=&3\cdot 5&-&2\cdot 7\\&=&3\cdot(12-7)&-&2\cdot 7\\&=&3\cdot 12&-&5\cdot 7\\&=&3\cdot 12&-&5\cdot(427-35\cdot 12)\\&=&178\cdot 12&-&5\cdot 427\end{aligned}$$

woraus man abliest: $(\overline{12})^{-1}=\overline{178}$.

Aus dem letzten Satz folgt aber auch eine Charakterisierung derjenigen Zahlen m, für die $\mathbb{Z}/m\mathbb{Z}$ ein Körper ist:

Satz 2.7. *Sei m eine natürliche Zahl, $m\geq 2$. Dann gilt: $\mathbb{Z}/m\mathbb{Z}$ ist genau dann ein Körper, wenn m eine Primzahl ist.*

Beweis. Ist m eine Primzahl, so gilt $(m,a)=1$ für jedes a, das kein Vielfaches von m ist. Folglich hat jedes $\overline{a}\neq\overline{0}$ ein multiplikatives Inverses. Ist m keine Primzahl, so hat m einen Primteiler p, etwa $m=pa$ mit $a>1$. Dann gilt $\overline{p}\cdot\overline{a}=\overline{0}$ und $\overline{a}$ kann kein Inverses haben: wenn nämlich doch, etwa $\overline{a}\cdot\overline{b}=\overline{1}$, so folgte

$$\overline{p}=\overline{p}\cdot\overline{a}\cdot\overline{b}=\overline{0}\cdot\overline{b}=\overline{0}$$

im Widerspruch zur Annahme. □

Zum Abschluss noch ein klassisches Resultat der elementaren Zahlentheorie.

Satz 2.8 (Kleiner Fermat)**.** *Sei p eine Primzahl und $n\in n$. Dann gilt $n^p\equiv n$ mod p.*

Zum Beweis benötigt man ein kleines Lemma:

Lemma 2.9. *Sei p eine Primzahl und $i\in\mathbb{N}$ mit $0<i<p$. Dann gilt $p\mid\binom{p}{i}$.*

Beweis. Es ist $i!\binom{p}{i}=p(p-1)\cdots(p-i+1)$. Da der Primfaktor p rechts vorkommt, muss er auch im Produkt auf der linken Seite vorkommen. Andererseits kann p wegen $0<i<p$ kein Teiler von $i!$ sein. □

Beweis des Satzes. Durch Induktion über n. Der Fall $n = 1$ ist klar. Nimmt man die Behauptung für n an, folgt aus dem Binomischen Lehrsatz und dem Lemma

$$\begin{aligned}(n+1)^p &= \sum_{i=0}^{p} \binom{p}{i} n^i \\ &= 1 + \sum_{i=1}^{p-1} \binom{p}{i} n^i + \binom{p}{p} n^p \\ &\equiv n^p + 1 \bmod p \\ &\equiv n + 1 \bmod p\end{aligned}$$

wobei im letzten Schritt die Induktionsannahme benutzt wurde. □