Kapitel 2

Ganze Zahlen

In diesem Kapitel setzen wir voraus, dass die Menge $\mathbb{Z}$ der ganzen Zahlen, ihre Ordnung und die Eigenschaften der Addition und Multiplikation ganzer Zahlen dem Leser vertraut sind. Wir werden später sehen, dass die Menge mit diesen beiden Operationen der Prototyp eines *Ringes* ist. In Aufgabe 2.2.9 erfolgt die algebraische Konstruktion dieses Ringes mit Hilfe der Struktur $(\mathbb{N}_0, +, \cdot)$. Ebenso bilden die Restklassen modulo n einen Ring und insbesondere eine abelsche Gruppe bzgl. der in 2.6 vorgestellten Operationen auf der Menge $\mathbb{Z}_n$ der Restklassen. So erhalten wir Standardbeispiele für sog. Faktorstrukturen und können die später behandelten abstrakten Faktorgruppen und Faktorringe am konkreten Beispiel studieren. Analoges gilt für Teilbarkeit und Idealtheorie. Die Abschnitte über diophantische Gleichungen, über Kongruenzen und über die Eulersche φ-Funktion stellen eine Verbindung zur Zahlentheorie her und gehören zum mathematischen Grundwissen. Schließlich wird im letzten Abschnitt eine Anwendung aus der Codierungstheorie vorgestellt, die Verschlüsselung von Nachrichten durch das Produkt zweier großer Primzahlen.

2.1 Teilbarkeit

Bekanntlich heißt eine ganze Zahl a ein **Teiler** der ganzen Zahl b, geschrieben als $a \mid b$ (lies: a teilt b), wenn es ein $c \in \mathbb{Z}$ gibt mit $ac = b$; b heißt dann **Vielfaches** von a.

Ein einfaches, aber sehr wichtiges Lemma über Teilbarkeit ist das Lemma über die Division mit Rest, auch Lemma von Euklid genannt. Durch Iteration gewinnt man aus ihm den Euklidischen Algorithmus zur Berechnung des größten gemeinsamen Teilers zweier ganzer Zahlen.

Lemma von Euklid (Division mit Rest)

Zu $a, b \in \mathbb{Z}$ mit $b \neq 0$ gibt es eindeutig bestimmte Zahlen q (der **Quotient**) und r (der **Rest**) mit

$$a = qb + r \quad \text{und} \quad 0 \leq r < |b|.$$

Primzahlen

Eine natürliche Zahl p heißt eine **Primzahl**, wenn sie verschieden von 1 ist und außer 1 und sich selbst keine natürlichen Zahlen als Teiler hat. Mit $\mathbb{P}$ bezeichnen wir die Menge der Primzahlen.

Für jede Primzahl p gilt: Aus $p \mid mn$ folgt $p \mid m$ oder $p \mid n$.

Es gibt unendlich viele Primzahlen.

Hauptsatz der elementaren Zahlentheorie:
Jede natürliche Zahl $n \geq 2$ ist als Produkt von Primzahlen darstellbar. Diese Darstellung ist, bis auf die Reihenfolge der Faktoren, eindeutig bestimmt.

$d \in \mathbb{Z}$ heißt ein **gemeinsamer Teiler** von a und b, wenn d sowohl ein Teiler von a als auch von b ist, also beide Zahlen teilt. Sind a und b nicht beide 0, so heißt $d \in \mathbb{N}$ ein **größter gemeinsamer Teiler** oder auch **ggT** von a und b, geschrieben als $d = \mathrm{ggT}(a, b)$, wenn d ein gemeinsamer Teiler von a und b ist und jeder gemeinsame Teiler von a und b ein Teiler von d ist. a und b heißen **teilerfremd**, falls $\mathrm{ggT}(a, b) = 1$. Sind a und b nicht beide 0, so existiert $\mathrm{ggT}(a, b)$, siehe Aufgabe 6, und ist durch diese Bedingungen eindeutig bestimmt[1]. Ferner setzen wir $\mathrm{ggT}(0, 0) := 0$. Für mehr als zwei Zahlen $a_1, \ldots, a_n$, die nicht alle 0 sind, wird die Zahl $\mathrm{ggT}(a_1, \ldots, a_n)$ völlig analog definiert. Ihre Existenz lässt sich auch mit Idealen beweisen – diese werden im nächsten Abschnitt behandelt.

Entsprechend definieren wir das **kleinste gemeinsame Vielfache** oder auch **kgV** zweier ganzer Zahlen a und b als diejenige Zahl $e > 0$, die ein gemeinsames Vielfaches von a und b ist und jedes weitere gemeinsame Vielfache von a und b teilt.

[1] Man beachte zunächst, dass 0 jede Zahl als Teiler hat. Ist d' ein weiterer ggT von a und b, so folgt aus der zweiten Bedingung $d \mid d'$ und $d' \mid d$. Also ist $d = cd'$, $d' = c'd$ für gewisse $c, c' \in \mathbb{Z}$. Es folgt $d = cc'd$, $d(1 - cc') = 0$, $cc' = 1$ und daher, wegen $d > 0$, $d' > 0$, $c = c' = 1$, also $d = d'$.

ggT und kgV

$\mathrm{ggT}(0,0) := 0 =: \mathrm{kgV}(0,0)$. Sind $a, b \in \mathbb{Z}$ nicht beide 0, so gilt

$$d = \mathrm{ggT}(a,b) \iff d > 0 \wedge d \mid a \wedge d \mid b \wedge \forall c \in \mathbb{Z}(c \mid a \wedge c \mid b \Longrightarrow c \mid d).$$

$$e = \mathrm{kgV}(a,b) \iff e > 0 \wedge a \mid e \wedge b \mid e \wedge \forall c \in \mathbb{Z}(a \mid c \wedge b \mid c \Longrightarrow e \mid c).$$

Für $a, b \in \mathbb{N}$ gilt $ab = \mathrm{ggT}(a,b) \cdot \mathrm{kgV}(a,b)$.

Man berechnet $\mathrm{ggT}(a,b)$ mit dem **Euklidischen Algorithmus**: Iterierte Anwendung des Lemmas von Euklid liefert das folgende Verfahren, das abbrechen muss, da die Folge $r_1, r_2, \ldots$ der Reste eine absteigende Folge natürlicher Zahlen ist. Der kleinste Rest $r_n \neq 0$ ist der ggT von a und b. O.B.d.A. seien $a, b \in \mathbb{N}$.

$$\begin{array}{lll}
(1) & a = q_0 b + r_1 & 0 < r_1 < b \\
(2) & b = q_1 r_1 + r_2 & 0 < r_2 < r_1 \\
(3) & r_1 = q_2 r_2 + r_3 & 0 < r_3 < r_2 \\
\vdots & \vdots & \\
(n) & r_{n-2} = q_{n-1} r_{n-1} + r_n & 0 < r_n < r_{n-1} \\
(n+1) & r_{n-1} = q_n r_n + 0 &
\end{array}$$

Rechnet man, beginnend mit Gleichung (n) in der Form $r_n = r_{n-2} - r_{n-1} q_{n-1}$, „rückwärts“ und eliminiert den Rest r_{n-1} mit Gleichung $(n-1)$, dann den Rest r_{n-2} mit Gleichung $(n-2)$ usf., so erhält man ganze Zahlen x und y mit

$$\mathrm{ggT}(a,b) = ax + by.$$

Insbesondere gilt (**Lemma von Bézout**):

$$a \text{ und } b \text{ sind teilerfremd} \iff \exists x, y \in \mathbb{Z}(1 = ax + by).$$

$\mathrm{ggT}(a,b) = 1 \wedge a \mid bc \Longrightarrow a \mid c$.
$\mathrm{ggT}(a,b) = 1 \wedge \mathrm{ggT}(a,c) = 1 \iff \mathrm{ggT}(a,bc) = 1$.

Dieser Algorithmus lässt sich völlig analog für **Polynome** über einem Körper K durchführen, auch mit der Darstellung des ggT, siehe das Lemma über die Division mit Rest in 4.2. Man muss nur die Aussagen $0 < r_1 < b$ bzw. $0 < r_j < r_{j-1}$ ersetzen durch $\mathrm{grad}(r_1) < \mathrm{grad}(b)$ bzw. $\mathrm{grad}(r_j) < \mathrm{grad}(r_{j-1})$.

Aufgaben

2.1.1 *Man berechne jeweils den größten gemeinsamen Teiler d der Zahlen $a, b \in \mathbb{Z}$ und bestimme ganze Zahlen x und y mit $ax + by = d$:*
a) $a = 61$, $b = 24$. b) $a = 2331$, $b = 6825$.

Zu a): Mit Hilfe des Euklidischen Algorithmus kann man den ggT von a und b bestimmen und als ganzzahlige Linearkombination von a und b darstellen. Wir gehen nach dem obigen Schema vor: $61 = 2 \cdot 24 + 13$, $24 = 1 \cdot 13 + 11$, $13 = 1 \cdot 11 + 2$, $11 = 5 \cdot 2 + 1$, und damit ist $\mathrm{ggT}(61, 24) = 1$. Rückwärts Einsetzen liefert $1 = 11 - 5 \cdot 2 = 11 - 5(13 - 11) = 6 \cdot 11 - 5 \cdot 13 = 6(24 - 13) - 5 \cdot 13 = 6 \cdot 24 - 11 \cdot 13 = 6 \cdot 24 - 11(61 - 2 \cdot 24) = 28 \cdot 24 - 11 \cdot 61$.

Zu b): Wir gehen vor wie in Teil a). Es ist $6825 = 2 \cdot 2331 + 2163$, $2331 = 1 \cdot 2163 + 168$, $2163 = 12 \cdot 168 + 147$, $168 = 1 \cdot 147 + 21$, $147 = 7 \cdot 21 + 0$, also ist $\mathrm{ggT}(6825, 2331) = 21$. Rückwärts Einsetzen liefert wie oben $21 = (-14) \cdot 6825 + 41 \cdot 2331$ (und damit die spezielle Lösung $(-14, 41)$ der sog. diophantischen Gleichung $6825x + 2331y = 21$, siehe 2.4).

2.1.2 Wichtig! *Seien $a, b \in \mathbb{Z}$ teilerfremd und sei a ein Teiler von bc. Man zeige: a ist ein Teiler von c.*
Insbesondere gilt für Primzahlen p: Aus $p \mid bc$ folgt $p \mid b$ oder $p \mid c$.

Da a und b teilerfremd sind, gibt es nach dem Lemma von Bézout Zahlen $\lambda, \mu \in \mathbb{Z}$ mit $1 = \mathrm{ggT}(a, b) = \lambda a + \mu b$. Also ist $c = \lambda ac + \mu bc$. Nach Voraussetzung teilt a die Zahl bc und damit auch die rechte Seite der Gleichung. Somit ist a ein Teiler der linken Seite, d. h. von c.

Ist p eine Primzahl mit $p \mid bc$, und ist p kein Teiler von b, so ist $\mathrm{ggT}(b, p) = 1$. Daher folgt $p \mid c$.

2.1.3 *Sei p eine Primzahl und $n \in \mathbb{N}$ mit $1 \leq n < p$. Man zeige, dass der Binomialkoeffizient $\binom{p}{n}$ durch p teilbar ist.*

Bekanntlich ist $k := \binom{p}{n}$ für $n < p$ eine natürliche Zahl mit dem Nenner $n!$ und dem Zähler $z := \prod_{j=0}^{n-1}(p - j)$. Da $p > n$ vorausgesetzt ist, ist p größer als jede Primzahl, die $n!$ teilt. Wegen $k \cdot n! = z$, $p \mid z$ und $\mathrm{ggT}(p, n!) = 1$ folgt $p \mid k = \binom{p}{n}$.

2.1.4 *Seien $a, b, c \in \mathbb{Z}$ mit $\mathrm{ggT}(a, b) = 1$ und $c \neq 0$. Man zeige: Es gibt $m \in \mathbb{N}$ mit $\mathrm{ggT}(a + mb, c) = 1$.*

Sei m das Produkt aller Primteiler von c, die keine Teiler von a sind. Sei p ein Primteiler von c. Dann gilt $p \mid a$ oder $p \nmid a$. Falls $p \mid a$, folgt $p \nmid a+mb$ wegen $p \nmid mb$, da $\mathrm{ggT}(a, mb) = 1$. Falls $p \nmid a$, folgt $p \mid mb$ nach Wahl von m, also $p \nmid a+mb$, da sonst $p \mid a$ folgen würde. Daher ist $\mathrm{ggT}(a+mb, c) = 1$.

2.1.5 *Sei $f = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$ ein Polynom vom Grad n mit dem Leitkoeffizienten $a_n \neq 0$ und $a_0 = f(0)$; sei $\alpha \in \mathbb{Q}$ eine Nullstelle von f. Man zeige: Ist $a_n = 1$, so ist $\alpha \in \mathbb{Z}$ und ein Teiler von a_0. Ist f nicht normiert und $\alpha = \frac{s}{t}$ mit $s, t \in \mathbb{Z}$ und $\mathrm{ggT}(s,t) = 1$, so ist t ein Teiler von a_n und s ein Teiler von a_0.*

Der erste Teil der Aufgabe wird sehr oft in unseren Beispielen angewandt! Sei $f = \sum_{j=0}^{n} a_j x^j$, $a_n = 1$ und $\alpha = \frac{s}{t}$ mit $s, t \in \mathbb{Z}$ und $\mathrm{ggT}(s,t) = 1$. Einsetzen liefert $0 = \sum_{j=0}^{n} a_j \frac{s^j}{t^j}$, also $0 \overset{(*)}{=} \sum_{j=0}^{n} a_j s^j t^{n-j}$. Damit ist $a_n s^n = s^n = -\sum_{j=0}^{n-1} a_j s^j t^{n-j} = -t \sum_{j=0}^{n-1} a_j s^j t^{n-j-1}$. Es folgt $t \mid s^n$. Da $1 = \mathrm{ggT}(s,t) = \mathrm{ggT}(s^n, t)$, ist $t \in \{1, -1\}$ und folglich $\alpha \in \mathbb{Z}$. Falls $a_n \neq 1$, folgt $t \mid a_n s^n$ und, wegen $\mathrm{ggT}(s,t) = 1$, $t \mid a_n$.

Löst man $(*)$ nach $a_0 t^n$ auf, so ergibt sich $a_0 t^n = -\sum_{j=1}^{n} a_j s^j t^{n-j} = -s \sum_{j=1}^{n} a_j s^{j-1} t^{n-j}$. Somit folgt $s \mid a_0 t^n$. Da $\mathrm{ggT}(s,t) = 1$, ergibt sich $s \mid a_0$. Im Fall $a_n = 1$ ist damit $\alpha = \pm s$ ein Teiler von a_0, wie gewünscht.

2.1.6 *Seien a und b natürliche Zahlen, $a = \prod_{j=1}^{k} p_j^{l_j}$ und $b = \prod_{j=1}^{k} p_j^{m_j}$ seien ihre Darstellungen als Produkt von Primzahlen, wobei $l_j, m_j \in \mathbb{N}_0$ sind (wir können wegen $p_j^0 = 1$ für beide Zahlen dieselben Primzahlen in der Darstellung wählen). Es sei $r_j := \min(l_j, m_j)$ und $s_j := \max(l_j, m_j)$. Man zeige:*

$$\mathrm{ggT}(a,b) = \prod_{j=1}^{k} p_j^{r_j} \quad \text{und} \quad \mathrm{kgV}(a,b) = \prod_{j=1}^{k} p_j^{s_j}.$$

Hiermit löse man Aufgabe 1 noch einmal (für große Zahlen ist diese Methode ungeeignet, da die Zerlegung in Primzahlen praktisch undurchführbar sein kann).

Sei $d := \prod_{j=1}^{k} p_j^{r_j}$. Dann ist d ein gemeinsamer Teiler von a und b, da, für alle j, $p_j^{r_j}$ ein Teiler von $p_j^{l_j}$ und von $p_j^{m_j}$ ist. Ist c ein beliebiger gemeinsamer

Teiler von a und b und p ein Primteiler von c, so folgt aus $c \cdot a' = a$ für ein a', dass $p = p_t$ für ein t gelten muss, und dass die Anzahl des Auftretens von p in der Darstellung von c als Produkt von Primzahlen höchstens l_t ist. Macht man die gleiche Überlegung mit $c \mid b$, so ist diese Anzahl höchstens m_t. Also ist sie höchstens $\min(l_t, m_t)$, und das ist r_t. Folglich ist c ein Teiler von d, und es folgt $d = \mathrm{ggT}(a, b)$. Beim kgV von a und b argumentiert man analog.

Es ergibt sich für $a = 61 \in \mathbb{P}$ und $b = 24 = 2^3 \cdot 3$: $\mathrm{ggT}(a, b) = 1$, $\mathrm{kgV}(a, b) = 61 \cdot 24$; für $a = 2331 = 3^2 \cdot 7 \cdot 37$ und $b = 6825 = 3 \cdot 5^2 \cdot 7 \cdot 13$: $\mathrm{ggT}(a, b) = 3 \cdot 7 = 21$, $\mathrm{kgV}(a, b) = 3^2 \cdot 5^2 \cdot 7 \cdot 13 \cdot 37 = 757575 = \frac{ab}{\mathrm{ggT}(a,b)}$.

2.1.7 *Sei g eine natürliche Zahl mit $g > 1$. Nach Aufgabe 1.3.4 lässt sich jede natürliche Zahl n in der Form $n = c_0 + c_1 g + \ldots + c_k g^k$ für gewisse $c_0, \ldots, c_k \in \mathbb{N}_0$ mit $0 \leq c_j < g$ für $j = 0, \ldots, k$ eindeutig darstellen. Dies ist die sog.* **g-adische Darstellung** *von n – man schreibt auch, in Anlehnung an die übliche Dezimaldarstellung für $g = 10$, $n = (c_k c_{k-1} \ldots c_0)_g$. Man entwickle ein Verfahren zur Berechnung der Koeffizienten $c_0, \ldots, c_k$. Ferner berechne man die g-adische Darstellung von 6825 für $g = 2$ und $g = 5$.*

Zur Erinnerung: Nach dem Lemma von Euklid gibt es $q, r \in \mathbb{Z}$ mit $n = qg + r$ und $0 \leq r < g$. Sicherlich ist dann $q \in \mathbb{N}_0$. Wähle $c_0 := r$. Ist $q = 0$, so haben wir eine gewünschte Darstellung bereits gefunden. Anderenfalls ist $0 < q < n$, da $g > 1$, und die Induktionsvoraussetzung liefert Zahlen $c_1, \ldots, c_k$ mit $0 \leq c_j < g$ für $j = 1, \ldots, k$ und $q = c_1 + c_2 g + \ldots + c_k g^{k-1}$. Einsetzen liefert die Existenzaussage für n. Da q und r eindeutig bestimmt sind, folgt auch die Eindeutigkeitsaussage durch vollständige Induktion.

Der Beweis ergibt auch ein **Verfahren**.
1. Schritt: Dividiere n mit Rest durch g, $n = q_1 g + c_0$. Ist $q_1 = 0$, so bricht das Verfahren ab. 2. Schritt: Dividiere q_1 mit Rest durch g, $q_1 = q_2 g + c_1$. Ist $q_2 = 0$, so bricht das Verfahren ab. 3. Schritt: Dividiere q_2 mit Rest durch g usf. Da die Folge der Quotienten $q_1, q_2 \ldots$ streng monoton fällt, muss das Verfahren abbrechen mit $q_{k+1} = 0$, $q_k \neq 0$. Dann ist $(c_k c_{k-1} \ldots c_1 c_0)_g$ die g-adische Darstellung von n.

Sei nun $n = 6825$ und $g = 2$. Dann gilt: $6825 = 3412 \cdot 2 + 1, 3412 = 1706 \cdot 2 + 0, 1706 = 853 \cdot 2, 853 = 426 \cdot 2 + 1, 426 = 213 \cdot 2, 213 = 106 \cdot 2 + 1, 106 = 53 \cdot 2, 53 = 26 \cdot 2 + 1, 26 = 13 \cdot 2, 13 = 6 \cdot 2 + 1, 6 = 3 \cdot 2, 3 = 1 \cdot 2 + 1, 1 = 0 \cdot 2 + 1$.

Folglich ist $6825 = (1101010101001)_2$. Probe: $2^{12}+2^{11}+2^9+2^7+2^5+2^3+1 = 4096+2048+512+128+32+8+1 = 6825$.

Sei $n = 6825$ und $g = 5$. Es ist $6825 = 1365 \cdot 5, 1365 = 273 \cdot 5, 273 = 54 \cdot 5 + 3, 54 = 10 \cdot 5 + 4, 10 = 2 \cdot 5, 2 = 0 \cdot 5 + 2$. Also ist $6825 = (204300)_5$. Probe: $2 \cdot 5^5 + 4 \cdot 5^3 + 3 \cdot 5^2 = 2 \cdot 3125 + 4 \cdot 125 + 3 \cdot 25 = 6250 + 500 + 75 = 6825$.

2.1.8 a) *Man zeige durch einen indirekten Beweis, dass es unendlich viele Primzahlen gibt.*

b) *Sei $p_0, p_1, \ldots$ eine Aufzählung der Primzahlen in der natürlichen Reihenfolge. Man bestimme das kleinste n, für das $(p_0 \cdot \ldots \cdot p_n) + 1$ keine Primzahl ist. Warum kann man aber auf diese Art eine Folge paarweise teilerfremder Zahlen definieren? Aus deren Existenz schließe man noch einmal auf die Existenz unendlich vieler Primzahlen.*

Zu a): Angenommen, die Menge $\mathbb{P}$ der Primzahlen ist endlich. Dann gibt es ein $n \in \mathbb{N}$ mit $\mathbb{P} = \{p_1, \ldots, , p_n\}$. Sei $m := 1 + \prod_{j=1}^{n} p_j$. Dann ist $m \in \mathbb{N}$ und $m \geq 2$, und m besitzt eine Primzahl als Teiler (siehe Aufgabe 1.3.1), die ja nach Annahme eine Zahl p_k sein muss für ein $k \in \{1, \ldots, n\}$. Also teilt p_k auch die Differenz $m - \prod_{j=1}^{n} p_j$ (Ausklammern!) und damit die Zahl 1, ein Widerspruch.

Zu b): Sei $(p_0 \cdot \ldots \cdot p_n) + 1 =: a_n$. Dann ist $a_0 = 3, a_1 = 7, a_2 = 31, a_3 = 211, a_4 = 2311$. Dies sind Primzahlen. Aber schon $a_5 = 30031 = 59 \cdot 509$ ist keine Primzahl.

Durch vollständige Induktion erhalten wir jedoch die Folge $b_0 := 2$, $b_n = b_0 \cdot \ldots \cdot b_{n-1} + 1$. Sicherlich ist b_k teilerfremd zu b_l, $l < k$, denn ein gemeinsamer Teiler würde 1 teilen. Jedes b_n ist ≥ 2 und hat eine Primzahl q_n als Teiler. Da $\mathrm{ggT}(b_k, b_l) = 1$ für $k \neq l$, sind die q_n, $n \in \mathbb{N}_0$, paarweise verschieden. Folglich gibt es unendlich viele Primzahlen.

2.1.9 *Man zeige:* a) *Es gibt beliebig große Intervalle von $\mathbb{N}$, in denen keine Primzahl liegt. D. h. für alle $n \in \mathbb{N}$ gibt es $b \in \mathbb{N}$, so dass die Zahlen $b, b+1, \ldots, b+n-1$ keine Primzahlen sind.*

b) *Im Intervall $]n, n!+1]$ liegt immer eine Primzahl.*

Zu a): Offensichtlich sind $(n+1)!+2, \ldots, (n+1)!+n+1$ keine Primzahlen. Wähle also $b = (n+1)!+2$.

Zu b): Sei $n \in \mathbb{N}$. Nach Aufgabe 8 gibt es die kleinste Primzahl p, die größer als n ist. Wir zeigen $p \leq n!+1$. Annahme: $p > n!+1$. Dann sind alle Zahlen

$n+1, \ldots, n!+1$ nicht prim. Sei q ein Primteiler von $n!+1$. Nach Annahme ist $q \leq n$. Aber dann gilt $q \mid n!$ und damit $q \mid 1$, ein Widerspruch.

2.1.10 *Man zeige: Es gibt unendlich viele Primzahlen der Form* $4k+3$. *Hinweis: Indirekter Beweis. Sind* $p_1, \ldots, p_n$ *all diese Primzahlen, so hat jeder Primteiler von* $a := 4(p_1 \cdot \ldots \cdot p_n) - 1$ *die Form* $4k+1$.

Zunächst liefert die Definition einer Primzahl, dass höchstens $4k+1$ und $4k+3$ Primzahlen sind, denn die Zahlen $4k$ und $4k+2$ sind durch 2 teilbar, und jede natürliche Zahl hat eine der Darstellungen $4k$, $4k+1$, $4k+2$, $4k+3$, da wir sie mit Rest durch 4 dividieren können. Nun kommt eine Argumentation ähnlich zum Beweis der Existenz unendlich vieler Primzahlen. Annahme: $p_1, \ldots, p_n$ sind alle Primzahlen der Form $4k+3$. Setze $a := 4(p_1 \cdot \ldots \cdot p_n) - 1$. Sei q ein beliebiger Primteiler von a. Wäre q von der Form $q = 4r+3$, so wäre $q = p_j$ für ein $j \in \{1, \ldots, n\}$, also wäre q wegen $q \mid a$ und $q \mid 4(p_1 \cdot \ldots \cdot p_n)$ ein Teiler von 1, ein Widerspruch. Folglich hat jeder Primteiler von a die Form $4k+1$. Wegen $(4k_1+1)(4k_2+1) = 16k_1k_2 + 4k_1 + 4k_2 + 1 =: 4k_3 + 1$ hat aber a als Produkt solcher Zahlen ebenfalls die Form $4s+1$. Setzt man dies für a ein, so ergibt sich $4(p_1 \cdot \ldots \cdot p_n - s) = 2$, und $4 \mid 2$ liefert einen Widerspruch.

2.1.11 *Primzahlen der Form* $2^n + 1$ *heißen* **Fermatsche Primzahlen**. *Wir werden ihnen bei der Konstruktion regelmäßiger n-Ecke wieder begegnen.*

a) *Man zeige: Ist* $2^n + 1$ *eine Primzahl, so ist n eine Zweierpotenz. Hinweis: Für ungerades k gilt* $x+1 \mid x^k + 1$ *nach 1.3.3.*

b) *Sei* $a_n = 2^{2^n} + 1$. *Man beweise: Für* $n \neq m$ *ist* $\mathrm{ggT}(a_n, a_m) = 1$. *(Zeige: Für* $m < n$ *gilt* $a_m \mid a_n - 2$.*)*

Zu a): Sei $n \in \mathbb{N}$ und $2^n + 1$ eine Primzahl. Annahme: $n = k \cdot 2^m$ mit ungeradem k und $1 < k < n$. Für ungerades k folgt mit 1.3.3: $x^k + 1 = 1 - (-x)^k = (1+x)(x^{k-1} - x^{k-2} + - \ldots + 1)$. Setze $s := 2^m$. Dann ist $s < n$, und es folgt für $x = 2^s$: $2^n + 1 = (2^s)^k + 1 = (2^s + 1)(2^{s(k-1)} - 2^{s(k-2)} + - \ldots + 1)$ im Widerspruch dazu, dass $2^n + 1$ eine Primzahl ist.

Zu b): Sei $m < n$, $r := n - m$, $a := a_m - 1 = 2^{2^m}$. Dann ist $2^{2^n} - 1 = (2^{2^m})^{2^r} - 1 = (a-1)(1 + a + a^2 + \ldots + a^{2^r - 1})$. Da die Anzahl der Summanden in der letzten Summe gerade ist, können wir je zwei zusammenfassen und $(1+a)$ ausklammern. Es folgt $2^{2^n} - 1 = (a-1)(1+a)(1 + a^2 + \ldots + a^{2^r - 2})$. Folglich ist $a + 1 = a_m$ ein Teiler von $a_n - 2$. Dies liefert $\mathrm{ggT}(a_m, a_n) = 1$.

2.2 Ideale im Ring $\mathbb{Z}$

Der Begriff der Teilbarkeit, den wir im letzten Abschnitt für ganze Zahlen behandelt haben, spielt eine bedeutende Rolle in sog. Ringen. Wichtigstes Element der Ringtheorie sind die Ideale, gewisse Teilmengen der Ringe. Mit ihnen lassen sich neue Ringe konstruieren, die Struktur von Ringen lässt sich charakterisieren. $(\mathbb{Z}, +, \cdot)$, auch oft nur kurz $\mathbb{Z}$ genannt, ist der Prototyp eines Ringes – seine Ideale haben eine besonders einfache Form, sie sind alle sog. Hauptideale, d. h. Teilmengen von $\mathbb{Z}$, die genau die Vielfachen einer ganzen Zahl als Elemente haben. Im Hinblick auf Kapitel 4 definieren wir die Begriffe bereits hier für beliebige Ringe.

Ringe und Ideale

Eine algebraische Struktur $(R, +, \cdot)$ heißt ein **Ring**, falls gilt:

(R1) $(R, +)$ ist eine abelsche Gruppe (wie üblich bezeichnet 0 das neutrale Element bzgl. $+$).

(R2) $(R, \cdot)$ ist eine Halbgruppe, d. h. $\cdot$ ist eine zweistellige Verknüpfung auf R, die das Assoziativgesetz erfüllt.
Statt $a \cdot b$ schreibt man meist ab.

(R3) Es gelten die **Distributivgesetze**: Für alle $a, b, c \in R$ ist
$a \cdot (b + c) = a \cdot b + a \cdot c$ und $(a + b) \cdot c = a \cdot c + b \cdot c$.

Ein Ring heißt **kommutativ**, falls die Verknüpfung $\cdot$ kommutativ ist.
$e \in R$ heißt ein **Einselement** von R, falls e das neutrale Element bzgl. $\cdot$ ist, falls also $a \cdot e = e \cdot a = a$ für alle $a \in R$ gilt; falls es existiert, ist es eindeutig bestimmt und wird meist mit 1 bezeichnet, und R heißt dann ein **Ring mit Einselement** oder auch **Ring mit Eins**.
Eine Teilmenge I eines kommutativen[2] Ringes R heißt ein **Ideal** von R (in R), wenn gilt:

(I1) $0 \in I$ (oder, mit (I3), auch äquivalent: $I \neq \emptyset$).

(I2) Für alle $a, b \in I$ ist $a - b \in I$.

(I3) Für alle $r \in R$ und alle $a \in I$ ist $ra \in I$.

[2]Bis auf Matrizen- bzw. Abbildungsringe werden wir nur kommutative Ringe kennenlernen. Wir verzichten auf die Idealdefinition für beliebige Ringe, bei der man zwischen Links- und Rechtsideal unter-

Jeder Durchschnitt von Idealen in R ist wieder ein Ideal in R. Ist also A eine nichtleere Teilmenge eines kommutativen Ringes R, so existiert ein (bzgl. $\subseteq$) kleinstes Ideal, das A als Teilmenge hat (das ist definitionsgemäß dasjenige Ideal, das A als Teilmenge hat und in jedem Ideal, das A als Teilmenge hat, enthalten ist und heißt das von A erzeugte Ideal), nämlich der Durchschnitt über alle Ideale in R, die Obermenge von A sind. Da R ein Ideal ist, das Obermenge von A ist, bilden wir den Durchschnitt über eine nichtleere Menge von Idealen.

Von Teilmengen erzeugte Ideale

Sei A eine nichtleere Teilmenge eines kommutativen Ringes R.
(A) bezeichnet das **von A erzeugte Ideal**, also das bzgl. $\subseteq$ kleinste Ideal, das Obermenge von A ist.
Es gilt: $(A) = \bigcap\{I : I \text{ ist ein Ideal in } R \text{ und } A \subseteq I\}$, und für Ringe mit Eins

$$(A) = \{r_1a_1 + \ldots + r_ma_m : \ m \in \mathbb{N}; a_1, \ldots, a_m \in A; r_1, \ldots, r_m \in R\}.$$

Ist A endlich, $A = \{a_1, \ldots, a_n\}$, und R ein Ring mit Einselement, so ist

$$(A) =: (a_1, \ldots, a_n) = \{r_1a_1 + \ldots + r_na_n : r_1, \ldots, r_n \in R\}.$$

Ein Ideal I von R heißt **endlich erzeugt**, wenn es diese Form hat, wenn es also eine endliche Teilmenge A von R gibt mit $I = (A)$. Hat dann A genau ein Element a, so schreiben wir $I = (a)$ und nennen I ein **Hauptideal**. Also

I ist ein Hauptideal $\iff$ Es gibt ein $a \in R$ mit $I = (a) = \{ra : r \in R\}$.

R heißt ein **Hauptidealring**, wenn jedes Ideal von R ein Hauptideal ist.[3]

Ein Ideal $I \neq R$ eines kommutativen Ringes R mit Eins heißt ein **Primideal**, wenn für alle $a, b \in R$ aus $ab \in I$ stets $a \in I$ oder $b \in I$ folgt.
I heißt **maximal**, wenn I ein maximales Element bzgl. $\subseteq$ in der Menge der von R verschiedenen Ideale ist; d. h. ist J ein Ideal mit $I \subseteq J$ und $J \neq R$, so folgt $I = J$.

scheiden muss. Der Leser sei auf die Literatur verwiesen.

[3]Manche Autoren verstehen unter einem Hauptidealring einen Integritätsring mit der genannten Eigenschaft, d. h. einen Ring ohne Nullteiler, siehe den Abschnitt über Ringtheorie.

Ideale in $\mathbb{Z}$

$\mathbb{Z}$ ist ein Hauptidealring, d. h. jedes Ideal in $\mathbb{Z}$ ist ein Hauptideal.

Die Ideale I von $\mathbb{Z}$ haben die Form $I = (n)$ für ein $n \in \mathbb{N}_0$.
Es gilt $(a) \subseteq (b) \iff b \mid a$.

(n) ist ein Primideal $\iff n = 0$ oder n ist eine Primzahl.

(n) ist ein maximales Ideal $\iff n$ ist eine Primzahl.

Die maximalen Ideale von $\mathbb{Z}$ sind also genau die Primideale $\neq (0)$ und damit die von Primzahlen erzeugten Ideale.

Das von $\{a, b\}$ erzeugte Ideal (a, b) wird durch $d := \mathrm{ggT}(a, b)$ erzeugt; es gilt also $(a, b) = \{ra + sb : r, s \in \mathbb{Z}\} = (d) = \{zd : z \in \mathbb{Z}\}$.

Analog gilt für das Ideal $(a_1, \ldots, a_n)$, dass es von $\mathrm{ggT}(a_1, \ldots, a_n)$ erzeugt wird. Insbesondere ist der ggT von $a_1, \ldots, a_n$ darstellbar als Linearkombination von $a_1, \ldots, a_n$:
Zu $a_1, \ldots, a_n \in \mathbb{Z}$ gibt es $z_1, \ldots, z_n \in \mathbb{Z}$ mit

$$\mathrm{ggT}(a_1, \ldots, a_n) = z_1 a_1 + \ldots + z_n a_n.$$

Man berechnet $z_1, \ldots, z_n$ mit dem Euklidischen Algorithmus, siehe Aufgabe 4.

Es gilt: $(a) \cap (b) = (\mathrm{kgV}(a, b))$ und $((a) \cup (b)) = (\mathrm{ggT}(a, b))$.

Aufgaben

2.2.1 *Man berechne $d_1, d_2 \in \mathbb{Z}$ mit $I_j = (d_j)$, wobei $I_1 = (63, 24)$ und $I_2 = (2331, 6825)$.*

Nach dem Vorspann ist $I_1 = \{63a + 24b : a, b \in \mathbb{Z}\} = (\mathrm{ggT}(24, 63))$. Da $24 = 3 \cdot 8$ und $63 = 7 \cdot 9$, ist $\mathrm{ggT}(24, 63) = 3$ und $I_1 = (3) = \{3c : c \in \mathbb{Z}\}$. In Aufgabe 2.1.1 wurde $\mathrm{ggT}(2331, 6825) = 21$ berechnet. Daher ist $I_2 = (21) = \{21c : c \in \mathbb{Z}\}$.

2.2.2 *Man gebe Ideale I und J in $\mathbb{Z}$ an, so daß $I \cup J$ kein Ideal in $\mathbb{Z}$ ist.*

Sei $I := (2)$ und $J := (3)$. Dann ist $2 \in I$ und $3 \in J$, also $2, 3 \in I \cup J$. Aber $1 = 3 - 2$ ist kein Element von $I \cup J$, denn 1 ist kein Vielfaches von 2 und kein Vielfaches von 3. Damit ist die Idealeigenschaft (I2) verletzt. (I1) und (I3) sind für Vereinigungen von Idealen stets erfüllt.

2.2.3 *Man gebe eine ganze Zahl b an, die das von der Menge*

$$A := (30) \cup (135) \cup (1015)$$

erzeugte Ideal (A) erzeugt. Wie lässt sich das Ergebnis verallgemeinern?

Wie in Aufgabe 2 sieht man, dass A kein Ideal ist. Sei I das von A erzeugte Ideal. Nach dem Vorspann hat I die Form $I = (b)$ für ein $b \in \mathbb{N}_0$. Wegen $A \subseteq I$ müssen 30, 135 und 1015 Vielfache von b sein, d. h. b muss ein gemeinsamer Teiler dieser Zahlen sein. Ist andererseits c ein gemeinsamer Teiler dieser Zahlen, so gilt $(30) \subseteq (c)$, $(135) \subseteq (c)$ und $(1015) \subseteq (c)$, also $A \subseteq (c)$. Da (b) das kleinste Ideal ist, das A enthält, folgt $(b) \subseteq (c)$, also c teilt b. Wir haben gezeigt: $b = \mathrm{ggT}(30, 135, 1015)$. Nun ist die Lösung leicht, jedenfalls bei den gegebenen Zahlen; $b = 5$ erzeugt das Ideal (A).

Die Argumente ergeben, dass man $((a_1) \cup \ldots \cup (a_n)) = (\mathrm{ggT}(a_1, \ldots, a_n))$ völlig analog beweisen kann.

2.2.4 *Man stelle den ggT von* $36, 204, 117$ *als Linearkombination dieser Zahlen dar.*

Sei $d = \mathrm{ggT}(36, 204)$. Der Euklidische Algorithmus liefert Zahlen a', b' mit $d = 36a' + 204b'$. Zu d und 117 liefert er x und y mit $\mathrm{ggT}(d, 117) = dx + 117y$. Da die Definition des ggT sofort $\mathrm{ggT}(d, 117) = \mathrm{ggT}(\mathrm{ggT}(36, 204), 117) = \mathrm{ggT}(36, 204, 117)$ ergibt, erhalten wir durch Einsetzen der Darstellung von d in die rechte Seite der Gleichung $\mathrm{ggT}(d, 117) = dx + 117y$ die gewünschte Linearkombination. Wie im Abschnitt über Teilbarkeit erhält man $204 = 5 \cdot 36 + 24, 36 = 1 \cdot 24 + 12, 24 = 2 \cdot 12 + 0$ also $12 = \mathrm{ggT}(36, 204) = 36 - 24 = 36 - (204 - 5 \cdot 36) = 6 \cdot 36 - 204$. Ferner ist $117 = 9 \cdot 12 + 9, 12 = 1 \cdot 9 + 3, 9 = 3 \cdot 3 + 0$, also $3 = \mathrm{ggT}(12, 117) = 10 \cdot 12 - 117$. Einsetzen ergibt $3 = \mathrm{ggT}(36, 204, 117) = 10 \cdot (6 \cdot 36 - 204) - 117 = 60 \cdot 36 - 10 \cdot 204 - 117$.

2.2.5 *Man zeige für $a, b \in \mathbb{Z}$: $(a) \cap (b) = (\mathrm{kgV}(a, b))$. Welches $c \in \mathbb{N}$ hat also die Eigenschaft $(c) = (12) \cap (14) \cap (16) \cap (18)$?*

Der Durchschnitt von Idealen in $\mathbb{Z}$ ist wieder ein Ideal in $\mathbb{Z}$ und wird nach dem Vorspann von einem Element $c \in \mathbb{N}_0$ erzeugt, $(c) = (a) \cap (b)$. c ist als Element des Durchschnitts ein gemeinsames Vielfaches von a und b. Ist d ein weiteres gemeinsames Vielfaches von a und b, so ist $d \in (a) \cap (b)$, also $d \in (c)$, c teilt d. Somit haben wir gezeigt, dass c das kleinste gemeinsame Vielfache von a und b ist.

Diese Überlegungen lassen sich fast wörtlich übertragen auf das Ideal $(a_1) \cap \ldots \cap (a_n)$. Das kgV von $12, 14, 16, 18$ erhält man (für kleine Zahlen), indem man alle in den Primzahlzerlegungen auftauchenden Primzahlen, jeweils mit dem höchsten auftauchenden Exponenten versehen, miteinander multipliziert (siehe Aufgabe 2.1.6). Also ist $c = 2^4 \cdot 3^2 \cdot 7 = 1008$.

2.2.6 *Man zeige für $A \neq \emptyset$: Ist $(I_a : a \in A)$ eine Familie von Idealen in $\mathbb{Z}$, so ist auch $J := \bigcap_{a \in A} I_a$ ein Ideal in $\mathbb{Z}$.*

Man kann sich leicht davon überzeugen, dass die Eigenschaften eines Ideals erfüllt sind, da sie für die Ideale der Familie erfüllt sind. So ist $0 \in J$, da $0 \in I_a$ für jedes $a \in A$; mit $b, c \in J$ ist $b, c \in I_a$ für alle $a \in A$, also $b - c \in I_a$ für alle $a \in A$, da I_a ein Ideal ist, und folglich $b - c \in J$ nach Definition des Durchschnitts. Analog folgt für $b \in \mathbb{Z}$ und $c \in J$ auch $bc \in J$.

2.2.7 *Man zeige mit Hilfe der Division mit Rest, dass $\mathbb{Z}$ ein Hauptidealring ist.*

Sei I ein beliebiges Ideal des Ringes $\mathbb{Z}$. Ist $I = \{0\}$, so ist I das von 0 erzeugte Ideal, $I = (0)$. Sei also $I \neq (0)$. Die dritte Idealeigenschaft impliziert, dass mit $a \in I$ auch $-a = (-1) \cdot a \in I$ ist. I enthält daher eine positive Zahl und folglich auch eine kleinste positive Zahl b. Wir zeigen, dass b das Ideal erzeugt, dass also $I = \{\lambda b : \lambda \in \mathbb{Z}\}$ gilt. Eine Inklusion ist klar, denn mit $b \in I$ ist auch $\lambda b \in I$ für jedes $\lambda \in \mathbb{Z}$.

Sei $a \in I$ beliebig gewählt. Dann ist $a = qb + r$ mit $0 \leq r < b$ für gewisse $q, r \in \mathbb{Z}$. Da $b \in I$, ist auch $qb \in I$, und damit folgt auch $a - qb = r \in I$. Da wir b als kleinstes positives Element von I gewählt hatten, muss folglich $r = 0$ sein, und daher ist $a = qb$, was zu zeigen blieb.

2.2.8 *Man zeige mit der vorangehenden Aufgabe ohne Berufung auf den Euklidischen Algorithmus, dass beliebige ganze Zahlen $a_1, \ldots, a_n$ einen ggT besitzen.*