II Die Restklassenringe des Rings $\mathbb{Z}$

4 Die Restklassenringe

(4.1) Definition (C. F. Gauß 1801): Es sei $m \in \mathbb{N}$, und es seien $a, b \in \mathbb{Z}$. Man nennt a kongruent zu b modulo m und schreibt

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

wenn $b - a$ durch m teilbar ist, also wenn gilt: Es ist $a \bmod m = b \bmod m$.

(4.2) Es sei $m \in \mathbb{N}$.
(1) Man sieht sogleich: Die Relation $\equiv \pmod{m}$ ist eine Äquivalenzrelation auf $\mathbb{Z}$, d.h. es gilt:
(Reflexivität:) Für jedes $a \in \mathbb{Z}$ gilt $a \equiv a \pmod{m}$.
(Symmetrie:) Sind $a, b \in \mathbb{Z}$ und gilt $a \equiv b \pmod{m}$, so gilt $b \equiv a \pmod{m}$.
(Transitivität:) Sind $a, b, c \in \mathbb{Z}$ und gilt $a \equiv b \pmod{m}$ und $b \equiv c \pmod{m}$, so gilt $a \equiv c \pmod{m}$.
(2) Für $a \in \mathbb{Z}$ heißt die Äquivalenzklasse

$$[a]_m := \{x \in \mathbb{Z} \mid x \equiv a \pmod{m}\}$$

die Restklasse von a modulo m.
Für $a, b \in \mathbb{Z}$ gilt

$$[a]_m = [b]_m \iff a \equiv b \pmod{m} \quad \text{und}$$
$$[a]_m \neq [b]_m \iff [a]_m \cap [b]_m = \varnothing \iff a \not\equiv b \pmod{m}.$$

Man setzt

$$\mathbb{Z}/m\mathbb{Z} := \{[a]_m \mid a \in \mathbb{Z}\}.$$

(3) Für jedes $a \in \mathbb{Z}$ gilt $a \equiv (a \bmod m) \pmod{m}$, also

$$[a]_m = [a \bmod m]_m \in \{[0]_m, [1]_m, \ldots, [m-1]_m\}.$$

Für $b, c \in \{0, 1, \ldots, m-1\}$ mit $b \neq c$ gilt $m \nmid c - b$, also $b \not\equiv c \pmod{m}$, also $[b]_m \neq [c]_m$. Es gilt daher

$$\mathbb{Z}/m\mathbb{Z} = \{[0]_m, [1]_m, \ldots, [m-1]_m\} \quad \text{und} \quad \#(\mathbb{Z}/m\mathbb{Z}) = m.$$

F. Schwarz, *Einführung in die Elementare Zahlentheorie*
© B.G. Teubner Stuttgart · Leipzig 1998

(4.3) Es sei m eine natürliche Zahl.
(1) Es seien a, b, a', $b' \in \mathbb{Z}$, und es gelte $[a]_m = [a']_m$ und $[b]_m = [b']_m$, also $a \equiv a' \pmod{m}$ und $b \equiv b' \pmod{m}$. Dann ist m ein Teiler von $a' - a$ und von $b' - b$ und daher auch von $(a' + b') - (a + b) = (a' - a) + (b' - b)$ und von $a'b' - ab = (a' - a)b' + a(b' - b)$. Also gilt $a + b \equiv a' + b' \pmod{m}$ und $ab \equiv a'b' \pmod{m}$, d.h. es gilt $[a + b]_m = [a' + b']_m$ und $[ab]_m = [a'b']_m$.
(2) Nach (1) erhält man wohldefinierte Verknüpfungen $+$ und $\cdot$ auf $\mathbb{Z}/m\mathbb{Z}$, indem man festsetzt: Für alle a, $b \in \mathbb{Z}$ sei

$$[a]_m + [b]_m := [a + b]_m \quad \text{und} \quad [a]_m \cdot [b]_m := [ab]_m.$$

Man sieht: Mit dieser Addition $+$ und dieser Multiplikation $\cdot$ ist $\mathbb{Z}/m\mathbb{Z}$ ein kommutativer Ring, der ein Einselement besitzt; sein Nullelement ist $[0]_m$, für jedes $a \in \mathbb{Z}$ ist $-[a]_m = [-a]_m$, und sein Einselement ist $[1]_m$. Der Ring $\mathbb{Z}/m\mathbb{Z}$ heißt der Restklassenring modulo m von $\mathbb{Z}$. (Die abelsche Gruppe $(\mathbb{Z}/m\mathbb{Z}, +)$ ist gerade die in (3.17) definierte Faktorgruppe der abelschen Gruppe $(\mathbb{Z}, +)$ nach ihrer Untergruppe $m\mathbb{Z}$).

(4.4) Bemerkung: Es sei R ein kommutativer Ring, der ein Einselement 1_R besitzt. Ein Element $a \in R$ heißt eine Einheit von R, wenn es ein $b \in R$ mit $ab = 1_R$ gibt. Die Menge $E(R)$ aller Einheiten von R ist mit der im Ring R gegebenen Multiplikation $\cdot$ als Verknüpfung eine abelsche Gruppe mit dem neutralen Element 1_R und heißt die Einheitengruppe von R. Jedes $a \in E(R)$ besitzt in der Gruppe $E(R)$ ein eindeutig bestimmtes inverses Element, das mit a^{-1} bezeichnet wird.

(4.5) Satz: *Es sei $m \in \mathbb{N}$. Es gilt*

$$\begin{aligned} E(\mathbb{Z}/m\mathbb{Z}) &= \{[a]_m \mid a \in \mathbb{Z};\ \mathrm{ggT}(a, m) = 1\} = \\ &= \{[a]_m \mid a \in \{0, 1, \ldots, m-1\};\ \mathrm{ggT}(a, m) = 1\}. \end{aligned}$$

Beweis: Für $a \in \mathbb{Z}$ gilt: $[a]_m$ ist eine Einheit im Ring $\mathbb{Z}/m\mathbb{Z}$, genau wenn es ein $b \in \mathbb{Z}$ mit $[a]_m[b]_m = [1]_m$ gibt, also genau wenn es ein $b \in \mathbb{Z}$ mit $ab \equiv 1 \pmod{m}$ gibt, also genau wenn es b, $c \in \mathbb{Z}$ mit $ab + mc = 1$ gibt, und dies ist damit äquivalent, daß a und m teilerfremd sind.

(4.6) Bemerkung: Es sei $m \in \mathbb{N}$, und es sei $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, m) = 1$. Dann ist $[a]_m$ eine Einheit im Restklassenring $\mathbb{Z}/m\mathbb{Z}$, und daher gibt es ein eindeutig bestimmtes $b \in \{0, 1, \ldots, m-1\}$ mit $[a]_m[b]_m = [1]_m$, also mit $[a]_m^{-1} = [b]_m$. Der Beweis in (4.5) zeigt, wie man b berechnet: Man ermittelt mit dem erweiterten Euklidischen Algorithmus aus (1.18) ganze Zahlen v und w mit $av + mw = 1$ und setzt $b := v \bmod m$.

MuPAD: Die Anweisung `modp(1/a,m)` liefert die Zahl $b \in \{0,1,\ldots,m-1\}$ mit $[a]_m^{-1} = [b]_m$.

(4.7) Satz: *Es sei $m \in \mathbb{N}$. Der Restklassenring $\mathbb{Z}/m\mathbb{Z}$ ist dann und nur dann ein Körper, wenn m eine Primzahl ist.*

Beweis: $\mathbb{Z}/m\mathbb{Z}$ ist ein kommutativer Ring; sein Nullelement ist $[0]_m$, und sein Einselement ist $[1]_m$.
(1) Es gelte: $\mathbb{Z}/m\mathbb{Z}$ ist ein Körper. Das Einselement eines Körpers ist stets von seinem Nullelement verschieden, also ist $m = \#(\mathbb{Z}/m\mathbb{Z}) > 1$. Für jedes $a \in \{2,3,\ldots,m-1\}$ gilt $[a]_m \neq [0]_m$, also $[a]_m \in E(\mathbb{Z}/m\mathbb{Z})$, also $\mathrm{ggT}(a,m) = 1$, also $a \nmid m$, und daher ist m eine Primzahl.
(2) Es gelte: m ist eine Primzahl. Der Ring $\mathbb{Z}/m\mathbb{Z}$ ist kommutativ, und wegen $\#(\mathbb{Z}/m\mathbb{Z}) = m > 1$ ist sein Einselement von seinem Nullelement verschieden. Für jedes $a \in \{1,2,\ldots,m-1\}$ gilt $m \nmid a$ und daher $\mathrm{ggT}(a,m) = 1$ (da m eine Primzahl ist), also $[a]_m \in E(\mathbb{Z}/m\mathbb{Z})$, und somit ist jedes Element von $\mathbb{Z}/m\mathbb{Z} \setminus \{[0]_m\}$ eine Einheit von $\mathbb{Z}/m\mathbb{Z}$. Also ist $\mathbb{Z}/m\mathbb{Z}$ ein Körper.

(4.8) Bezeichnung: Ist p eine Primzahl, so heißt der Körper

$$\mathbb{F}_p \;:=\; \mathbb{Z}/p\mathbb{Z}$$

der Restklassenkörper modulo p von $\mathbb{Z}$.

(4.9) Es sei $m \in \mathbb{N}$, und es seien $a, b \in \mathbb{Z}$.
(1) Es gibt dann und nur dann ein $x \in \mathbb{Z}$ mit $ax \equiv b \pmod m$, also mit $[a]_m \cdot [x]_m = [b]_m$, wenn b durch $d := \mathrm{ggT}(a,m)$ teilbar ist.
Beweis: Nach (1.9) existieren $v, w \in \mathbb{Z}$ mit $av + mw = d$. Gilt $d \mid b$, so gilt $x := bv/d \in \mathbb{Z}$ und

$$ax \;=\; \frac{b}{d}av \;=\; \frac{b}{d}(d - mw) \;=\; b - m\left(\frac{b}{d}w\right) \;\equiv\; b \pmod m.$$

Ist andererseits x eine ganze Zahl, für die $ax \equiv b \pmod m$ ist, so gibt es ein $y \in \mathbb{Z}$ mit $b = ax + my$, und wegen $d \mid a$ und $d \mid m$ folgt $d \mid b$.
(2) Es gelte $\mathrm{ggT}(a,m) = 1$. Dann findet man mit dem erweiterten Euklidischen Algorithmus aus (1.18) ein $v \in \{0,1,\ldots,m-1\}$ mit $av \equiv 1 \pmod m$. Für $x_0 := (bv) \bmod m \in \{0,1,\ldots,m-1\}$ gilt $ax_0 \equiv avb \equiv b \pmod m$. Für jedes $x \in \mathbb{Z}$ mit $ax \equiv b \pmod m$ gilt $x \equiv xav \equiv bv \equiv x_0 \pmod m$. Es gibt also ein eindeutig bestimmtes $x_0 \in \{0,1,\ldots,m-1\}$ mit $ax_0 \equiv b \pmod m$, und hiermit gilt

$$\{x \in \mathbb{Z} \mid ax \equiv b \pmod m\} \;=\; \{x \in \mathbb{Z} \mid x \equiv x_0 \pmod m\}.$$

Dies läßt sich auch so formulieren: Die Gleichung $[a]_m \cdot X = [b]_m$ besitzt im Ring $\mathbb{Z}/m\mathbb{Z}$ eine und nur eine Lösung, nämlich $[x_0]_m = [a]_m^{-1}[b]_m$.

(3) Es gelte $d := \mathrm{ggT}(a, m) > 1$ und $d \mid b$.
(a) Es gilt $\mathrm{ggT}(a/d, m/d) = 1$, und daher gibt es nach (2) ein eindeutig bestimmtes $x_{00} \in \{0, 1, \ldots, m/d - 1\}$ mit $(a/d)x_{00} \equiv b/d \pmod{m/d}$. Für jedes $i \in \{0, 1, \ldots, d-1\}$ gilt $x_i := x_{00} + im/d \in \{0, 1, \ldots, m-1\}$ und

$$ax_i \;=\; d\frac{a}{d}x_{00} + ia\frac{m}{d} \;=\; b + d\Big(\frac{a}{d}x_{00} - \frac{b}{d}\Big) + \frac{ia}{d}m \;\equiv\; b \pmod{m}.$$

(b) Für jedes $x \in \mathbb{Z}$ mit $ax \equiv b \pmod{m}$ gilt $(a/d)x \equiv b/d \pmod{m/d}$ und daher $x \equiv x_{00} \pmod{m/d}$, also gibt es ein $k \in \mathbb{Z}$ mit

$$x \;=\; x_{00} + k\frac{m}{d} \;\equiv\; x_{00} + (k \bmod d)\frac{m}{d} \;=\; x_{k \bmod d} \pmod{m}.$$

(c) Aus (a) und (b) folgt: In $\{0, 1, \ldots, m-1\}$ gibt es genau $d = \mathrm{ggT}(a, m)$ verschiedene Lösungen $x_0, x_1, \ldots, x_{d-1}$ der Kongruenz $ax \equiv b \pmod{m}$, und damit gilt

$$\big\{x \in \mathbb{Z} \mid ax \equiv b \pmod{m}\big\} \;=\; \bigcup_{i=0}^{d-1} \big\{x \in \mathbb{Z} \mid x \equiv x_i \pmod{m}\big\}.$$

(4.10) MuPAD: Die Anweisung `numlib::lincongruence(a,b,m)` liefert zu einer natürlichen Zahl m und zu ganzen Zahlen a und b die Ausdruckssequenz der $x \in \{0, 1, \ldots, m-1\}$ mit $ax \equiv b \pmod{m}$, falls es solche x gibt, und andernfalls die Ausgabe `FAIL`.

(4.11) Hilfssatz: *Es seien $m', m'' \in \mathbb{N}$, und es seien $a', a'' \in \mathbb{Z}$. Es gibt dann und nur dann ein $x \in \mathbb{Z}$ mit $x \equiv a' \pmod{m'}$ und $x \equiv a'' \pmod{m''}$, wenn $a'' - a'$ durch $\mathrm{ggT}(m', m'')$ teilbar ist.*

Beweis: (a) Es gelte: Es existiert ein $x \in \mathbb{Z}$, für das $x \equiv a' \pmod{m'}$ und $x \equiv a'' \pmod{m''}$ gilt. Wegen $m' \mid a' - x$ und $m'' \mid a'' - x$ gilt dann: $\mathrm{ggT}(m', m'')$ teilt $(a'' - x) - (a' - x) = a'' - a'$.
(b) Es gelte $d := \mathrm{ggT}(m', m'') \mid a'' - a'$. Der erweiterte Euklidische Algorithmus aus (1.18) liefert $v', v'' \in \mathbb{Z}$ mit $m'v' + m''v'' = d$. Für $z := v'(a'' - a')/d$ gilt

$$m'z \;\equiv\; (d - m''v'') \cdot \frac{a'' - a'}{d} \;\equiv\; a'' - a' \pmod{m''},$$

und für $x := a' + m'z$ gilt

$$x \;\equiv\; a' \pmod{m'} \quad \text{und} \quad x \;\equiv\; a' + (a'' - a') \;=\; a'' \pmod{m''}.$$

(4.12) Hilfssatz: *Es sei $k \in \mathbb{N}$ mit $k \geq 2$.*
(1) *Für alle $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{R}$ gilt*

$$\min\big(\{\max(\{\alpha_1, \alpha_2, \ldots, \alpha_{k-1}\}), \alpha_k\}\big) = \\ = \max\big(\{\min(\{\alpha_1, \alpha_k\}), \min(\{\alpha_2, \alpha_k\}), \ldots, \min(\{\alpha_{k-1}, \alpha_k\})\}\big).$$

(2) *Für alle $m_1, m_2, \ldots, m_k \in \mathbb{N}$ gilt*

$$\mathrm{ggT}\big(\mathrm{kgV}(m_1, m_2 \ldots, m_{k-1}), m_k\big) = \\ = \mathrm{kgV}\big(\mathrm{ggT}(m_1, m_k), \mathrm{ggT}(m_2, m_k), \ldots, \mathrm{ggT}(m_{k-1}, m_k)\big).$$

Beweis: (1) ist klar, und (2) folgt mit Hilfe von (1) aus (2.19)(3).

(4.13) Satz (Chinesischer Restsatz): *Es sei $n \in \mathbb{N}$; es seien $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ und $m_1, m_2, \ldots, m_n \in \mathbb{N}$. Es gibt dann und nur dann eine ganze Zahl x mit $x \equiv a_i \pmod{m_i}$ für jedes $i \in \{1, 2, \ldots, n\}$, wenn gilt: Für alle $i, j \in \{1, 2, \ldots, n\}$ mit $i \neq j$ ist $a_j - a_i$ durch $\mathrm{ggT}(m_i, m_j)$ teilbar. Ist diese Bedingung erfüllt, so gibt es ein eindeutig bestimmtes $x_0 \in \mathbb{Z}$ mit $0 \leq x_0 \leq \mathrm{kgV}(m_1, m_2, \ldots, m_n) - 1$ und mit $x_0 \equiv a_i \pmod{m_i}$ für jedes $i \in \{1, 2, \ldots, n\}$, und damit gilt*

$$\big\{x \in \mathbb{Z} \mid x \equiv a_i \pmod{m_i} \text{ für } i = 1, 2, \ldots, n\big\} = \\ = \big\{x \in \mathbb{Z} \mid x \equiv x_0 \pmod{\mathrm{kgV}(m_1, m_2, \ldots, m_n)}\big\}.$$

Beweis: (1) Es gelte: Es gibt ein $x \in \mathbb{Z}$ mit $x \equiv a_i \pmod{m_i}$ für jedes $i \in \{1, 2, \ldots, n\}$. Für alle $i, j \in \{1, 2, \ldots, n\}$ mit $i \neq j$ gilt $m_i \mid a_i - x$ und $m_j \mid a_j - x$ und daher $\mathrm{ggT}(m_i, m_j) \mid (a_j - x) - (a_i - x) = a_j - a_i$.
(2) Es gelte: Für alle $i, j \in \{1, 2, \ldots, n\}$ mit $i \neq j$ ist $a_j - a_i$ durch $\mathrm{ggT}(m_i, m_j)$ teilbar.
(a) Zu jedem $k \in \{1, 2, \ldots, n\}$ wird eine ganze Zahl y_k konstruiert, für die $y_k \equiv a_1 \pmod{m_1}$, $y_k \equiv a_2 \pmod{m_2}, \ldots, y_k \equiv a_k \pmod{m_k}$ gilt.
Dazu setzt man zuerst $y_1 := a_1 \bmod m_1$. Ist $k \in \{1, 2, \ldots, n-1\}$ und sind $y_1, y_2, \ldots, y_k$ bereits konstruiert, so findet man ein geeignetes y_{k+1} folgendermaßen: Für jedes $i \in \{1, 2, \ldots, k\}$ gilt: Es ist $y_k \equiv a_i \pmod{m_i}$, also ist $y_k - a_i$ durch m_i und daher auch durch $\mathrm{ggT}(m_i, m_{k+1})$ teilbar; nach Voraussetzung ist $a_i - a_{k+1}$ durch $\mathrm{ggT}(m_i, m_{k+1})$ teilbar, und daher ist $y_k - a_{k+1} = (y_k - a_i) + (a_i - a_{k+1})$ durch $\mathrm{ggT}(m_i, m_{k+1})$ teilbar. Also ist $y_k - a_{k+1}$ durch

$$\mathrm{kgV}\big(\mathrm{ggT}(m_1, m_{k+1}), \mathrm{ggT}(m_2, m_{k+1}), \ldots, \mathrm{ggT}(m_k, m_{k+1})\big) = \\ \overset{(4.12)(2)}{=} \mathrm{ggT}\big(\mathrm{kgV}(m_1, m_2, \ldots, m_k), m_{k+1}\big)$$

teilbar, und daher gibt es nach (4.11) ein $y_{k+1} \in \mathbb{Z}$ mit

$$y_{k+1} \equiv y_k \pmod{\mathrm{kgV}(m_1, m_2, \ldots, m_k)} \quad \text{und} \quad y_{k+1} \equiv a_{k+1} \pmod{m_{k+1}}.$$

Für jedes $i \in \{1,2,\ldots,k\}$ gilt: m_i teilt $\mathrm{kgV}(m_1,m_2,\ldots,m_k)$, und daher ist

$$y_{k+1} \equiv y_k \equiv a_i \pmod{m_i}.$$

(b) Es sei $M_n := \mathrm{kgV}(m_1,m_2,\ldots,m_n)$, und es sei $x_0 := y_n \bmod M_n$. Es ist $0 \leq x_0 \leq M_n - 1$, und für jedes $i \in \{1,2,\ldots,n\}$ ist $x_0 \equiv a_i \pmod{m_i}$. Ist x eine ganze Zahl mit $x \equiv a_i \pmod{m_i}$ für jedes $i \in \{1,2,\ldots,n\}$, so gilt $x \equiv a_i \equiv x_0 \pmod{m_i}$, also $m_i \mid x_0 - x$ für jedes $i \in \{1,2,\ldots,n\}$, und daher gilt $M_n = \mathrm{kgV}(m_1,m_2,\ldots,m_n) \mid x_0 - x$, d.h. es ist $x \equiv x_0 \pmod{M_n}$. Andererseits gilt für jedes $x \in \mathbb{Z}$ mit $x \equiv x_0 \pmod{M_n}$: Da m_i für jedes $i \in \{1,2,\ldots,n\}$ ein Teiler von M_n ist, gilt $x \equiv x_0 \equiv a_i \pmod{m_i}$. Damit ist gezeigt: Es ist

$$\{x \in \mathbb{Z} \mid x \equiv a_i \,(\mathrm{mod}\ m_i) \text{ für } i = 1,2,\ldots,n\} = \{x \in \mathbb{Z} \mid x \equiv x_0 \,(\mathrm{mod}\ M_n)\}.$$

Insbesondere folgt daraus: x_0 ist das einzige Element von $\{0,1,\ldots,M_n - 1\}$ mit $x_0 \equiv a_i \pmod{m_i}$ für jedes $i \in \{1,2,\ldots,n\}$.

(4.14) Folgerung: *Es sei $n \in \mathbb{N}$, es seien $m_1, m_2, \ldots, m_n \in \mathbb{N}$ paarweise teilerfremd, und es seien $a_1, a_2, \ldots, a_n \in \mathbb{Z}$; es sei $m := m_1 m_2 \cdots m_n$. Es gibt ein eindeutig bestimmtes $x_0 \in \{0,1,\ldots,m-1\}$ mit $x_0 \equiv a_i \pmod{m_i}$ für jedes $i \in \{1,2,\ldots,n\}$, und damit gilt*

$$\{x \in \mathbb{Z} \mid x \equiv a_i \pmod{m_i} \text{ für } i = 1,2,\ldots,n\} = \{x \in \mathbb{Z} \mid x \equiv x_0 \pmod{m}\}.$$

(4.15) Bemerkung: (1) Der vielleicht ein wenig seltsam erscheinende Name des in (4.13) bewiesenen Satzes rührt daher, daß in einem chinesischen Rechenbuch, dem Mathematischen Handbuch des Meisters Sūn, das wohl in den Jahren zwischen 280 und 473 entstanden ist, ein erstes Beispiel dazu vorkommt.
(2) Es sei $n \in \mathbb{N}$, und es seien $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ und $m_1, m_2, \ldots, m_n \in \mathbb{N}$. Der Beweis in (4.13) liefert den folgenden Algorithmus CRS, der entscheidet, ob es eine ganze Zahl x mit $x \equiv a_i \pmod{m_i}$ für jedes $i \in \{1,2,\ldots,n\}$ gibt, und der im Fall der Existenz das kleinste nichtnegative solche x berechnet:
(CRS1) Man setzt $M_1 := m_1$, $y_1 := a_1 \bmod M_1$ und $k := 1$.
(CRS2) Ist $k = n$, so gibt man y_k aus und bricht ab.
(CRS3) Man setzt $d_k := \mathrm{ggT}(M_k, m_{k+1})$. Ist $y_k - a_{k+1}$ durch d_k teilbar, so bestimmt man mit Hilfe des im Beweis von (4.11) angegebenen Verfahrens, also letztlich mit Hilfe des erweiterten Euklidischen Algorithmus, eine ganze Zahl y mit $y \equiv y_k \pmod{M_k}$ und mit $y \equiv a_{k+1} \pmod{m_{k+1}}$. Dann setzt man

$$M_{k+1} := \mathrm{kgV}(M_k, m_{k+1}), \quad y_{k+1} := y \bmod M_{k+1} \quad \text{und} \quad k := k+1$$

und geht zu (CRS2).

(CRS4) Ist $y_k - a_{k+1}$ nicht durch d_k teilbar, so gibt man die Meldung FAIL aus und bricht ab. (In diesem Fall gibt es nach (4.11) kein $y \in \mathbb{Z}$, für das $y \equiv y_k \pmod{M_k}$ und $y \equiv a_{k+1} \pmod{m_{k+1}}$ gilt, und somit gibt es auch kein $x \in \mathbb{Z}$ mit $x \equiv a_i \pmod{m_i}$ für jedes $i \in \{1, 2, \ldots, n\}$).

(3) **MuPAD:** Die MuPAD-Funktion `numlib::ichrem` verwendet den Algorithmus CRS aus (2). Ist $n \in \mathbb{N}$ und sind $a := [a_1, a_2, \ldots, a_n]$ eine Liste von ganzen und $m := [m_1, m_2, \ldots, m_n]$ eine Liste von natürlichen Zahlen, so liefert die Anweisung `numlib::ichrem(a,m)` die ganze Zahl x_0 mit $x_0 \equiv a_i \pmod{m_i}$ für jedes $i \in \{1, 2, \ldots, n\}$ und mit $0 \leq x_0 \leq \mathrm{kgV}(m_1, m_2, \cdots, m_n) - 1$, falls eine solche Zahl x_0 existiert, und andernfalls die Ausgabe `FAIL`.

(4.16) Definition: Die Funktion

$$\varphi : \mathbb{N} \to \mathbb{N} \quad \text{mit} \quad \varphi(m) := \#\big(E(\mathbb{Z}/m\mathbb{Z})\big) \quad \text{für jedes } m \in \mathbb{Z}$$

heißt die Euler-Funktion (nach L. Euler, 1707 - 1783).

(4.17) Satz: (1) *Es seien $m_1, m_2, \ldots, m_n \in \mathbb{N}$ paarweise teilerfremd. Dann gilt*

$$\varphi(m_1 m_2 \cdots m_n) \;=\; \varphi(m_1)\varphi(m_2)\cdots\varphi(m_n).$$

(2) *Es sei p eine Primzahl, und es sei $\alpha \in \mathbb{N}$. Dann gilt*

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

(3) *Es sei m eine natürliche Zahl mit der Primzerlegung $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$. Dann gilt*

$$\varphi(m) \;=\; \prod_{i=1}^{r} \varphi(p_i^{\alpha_i}) \;=\; \prod_{i=1}^{r} p_i^{\alpha_i - 1}(p_i - 1) \;=\; m \cdot \prod_{i=1}^{r} \Big(1 - \frac{1}{p_i}\Big).$$

Beweis: (1) Es sei $m := m_1 m_2 \cdots m_n$. Man sieht, daß

$$\begin{cases} \Phi : E(\mathbb{Z}/m\mathbb{Z}) \to E(\mathbb{Z}/m_1\mathbb{Z}) \times E(\mathbb{Z}/m_2\mathbb{Z}) \times \cdots \times E(\mathbb{Z}/m_n\mathbb{Z}) \quad \text{mit} \\ \Phi\big([a]_m\big) := \big([a]_{m_1}, [a]_{m_2}, \ldots, [a]_{m_n}\big) \text{ für jedes } a \in \mathbb{Z} \text{ mit } \mathrm{ggT}(a, m) = 1 \end{cases}$$

eine wohldefinierte Abbildung ist. Diese Abbildung Φ ist bijektiv.
Beweis: (a) Es sei $\alpha \in E(\mathbb{Z}/m_1\mathbb{Z}) \times E(\mathbb{Z}/m_2\mathbb{Z}) \times \cdots \times E(\mathbb{Z}/m_n\mathbb{Z})$. Es existieren $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ mit

$$\mathrm{ggT}(a_1, m_1) \;=\; \mathrm{ggT}(a_2, m_2) \;=\; \cdots \;=\; \mathrm{ggT}(a_n, m_n) \;=\; 1$$

und mit

$$\alpha \;=\; \big([a_1]_{m_1}, [a_2]_{m_2}, \ldots, [a_n]_{m_n}\big).$$

Da $m_1, m_2, \ldots, m_n$ paarweise teilerfremd sind, liefert der Chinesische Restsatz (vgl. (4.14)) eine ganze Zahl a mit: Für jedes $i \in \{1,2,\ldots,n\}$ gilt $a \equiv a_i \pmod{m_i}$, also $[a]_{m_i} = [a_i]_{m_i}$. Für jedes $i \in \{1,2,\ldots,n\}$ gilt $\mathrm{ggT}(a,m_i) = \mathrm{ggT}(a_i,m_i) = 1$ (vgl. (1.12)), und daher ist $\mathrm{ggT}(a,m) = 1$ (vgl. (1.14)(2)), also ist $[a]_m \in E(\mathbb{Z}/m\mathbb{Z})$. Es gilt

$$\Phi([a]_m) = ([a]_{m_1},[a]_{m_2},\ldots,[a]_{m_n}) = ([a_1]_{m_1},[a_2]_{m_2},\ldots,[a_n]_{m_n}) = \alpha.$$

(b) Nach (a) ist Φ surjektiv. Daß Φ injektiv ist, folgt aus der Einzigkeitsaussage in (4.14).
(2) Für $a \in \mathcal{M} := \{0,1,\ldots,p^\alpha - 1\}$ gilt $[a]_{p^\alpha} \in E(\mathbb{Z}/p^\alpha\mathbb{Z})$, genau wenn $\mathrm{ggT}(a,p^\alpha) = 1$ ist, also genau wenn a nicht durch p teilbar ist, also genau wenn $a \notin \mathcal{M}_0 := \{kp \mid 0 \le k \le p^{\alpha-1} - 1\}$ ist. Also ist

$$\varphi(p^\alpha) = \#(E(\mathbb{Z}/p^\alpha\mathbb{Z})) = \#(\mathcal{M}) - \#(\mathcal{M}_0) = p^\alpha - p^{\alpha-1}.$$

(3) folgt aus (1) und (2).

(4.18) MuPAD: Für eine natürliche Zahl m liefert `phi(m)` den Wert $\varphi(m)$ der Euler-Funktion. `phi` verwendet `ifactor`.

(4.19) Bemerkung: Es sei $m \in \mathbb{N}$. Dann ist

$$\begin{aligned} E(\mathbb{Z}/m\mathbb{Z}) &= \{[a]_m \mid a \in \mathbb{Z};\ \mathrm{ggT}(a,m) = 1\} = \\ &= \{[a]_m \mid a \in \{0,1,\ldots,m-1\};\ \mathrm{ggT}(a,m) = 1\} \end{aligned}$$

die Gruppe der Einheiten des Restklassenrings $\mathbb{Z}/m\mathbb{Z}$. Für jede ganze Zahl a mit $\mathrm{ggT}(a,m) = 1$ bedeutet $\mathrm{ord}([a]_m)$ die Ordnung des Elements $[a]_m$ in der Gruppe $E(\mathbb{Z}/m\mathbb{Z})$, d.h. es gilt

$$\begin{aligned} \mathrm{ord}([a]_m) &= \#(\langle [a]_m \rangle) = \#(\{[a]_m^j \mid j \in \mathbb{Z}\}) = \\ &= \min(\{i \in \mathbb{N} \mid [a]_m^i = [1]_m\}) = \min(\{i \in \mathbb{N} \mid a^i \equiv 1 \pmod{m}\}). \end{aligned}$$

(4.20) Satz (L. Euler 1760): *Es sei $m \in \mathbb{N}$, und es sei a eine ganze Zahl mit $\mathrm{ggT}(a,m) = 1$. Es ist $a^{\varphi(m)} \equiv 1 \pmod{m}$, und $\mathrm{ord}([a]_m)$ ist ein Teiler von $\varphi(m)$, und zwar ist*

$$\mathrm{ord}([a]_m) = \min(\{d \in \mathbb{N} \mid d \text{ teilt } \varphi(m);\ a^d \equiv 1 \pmod{m}\}).$$

Beweis: Es ist $[a]_m \in E(\mathbb{Z}/m\mathbb{Z})$. $\mathrm{ord}([a]_m)$ teilt $\#(E(\mathbb{Z}/m\mathbb{Z})) = \varphi(m)$, und es gilt $[a]_m^{\varphi(m)} = [1]_m$, also $a^{\varphi(m)} \equiv 1 \pmod{m}$ (vgl. (3.6)(2)). Aus (3.6)(2) folgt auch, daß $\mathrm{ord}([a]_m)$ der kleinste Teiler $d \in \mathbb{N}$ von $\varphi(m)$ mit $a^d \equiv 1 \pmod{m}$ ist.

(4.21) Folgerung (P. de Fermat 1640): *Es sei p eine Primzahl.*
(1) *Für jedes $a \in \mathbb{Z}$ mit $p \nmid a$ gilt $a^{p-1} \equiv 1 \pmod{p}$ und* $\operatorname{ord}([a]_p) \mid p-1$.
(2) *Für jedes $a \in \mathbb{Z}$ gilt $a^p \equiv a \pmod{p}$.*

Beweis: Es sei $a \in \mathbb{Z}$. Gilt $p \mid a$, so gilt $a^p \equiv 0 \equiv a \pmod{p}$; nach (4.20) und wegen $\varphi(p) = p-1$ gilt andernfalls $\operatorname{ord}([a]_p) \mid p-1$ und $a^{p-1} \equiv 1 \pmod{p}$, also $a^p \equiv a \pmod{p}$.

(4.22) Bemerkung: Aus dem Satz von Fermat ergibt sich ein "Nichtprimzahl-Test": Eine natürliche Zahl m, zu der es ein $a \in \mathbb{Z}$ mit $\operatorname{ggT}(a,m) = 1$ und mit $a^{m-1} \not\equiv 1 \pmod{m}$ gibt, ist keine Primzahl. Hiermit ergibt sich zum Beispiel für die sechste Fermat-Zahl

$$m := F(6) = 2^{64}+1 = 18446\,74407\,37095\,51617 :$$

Wegen $3^{m-1} \equiv 8752\,24953\,54656\,29170 \not\equiv 1 \pmod{m}$ ist m keine Primzahl. Man beachte, daß man damit festgestellt hat, daß m keine Primzahl ist, ohne einen nichttrivialen Teiler von m gefunden zu haben.

Aber auf diese Weise ergibt sich kein praktikables Verfahren, Primzahlen und Nichtprimzahlen zu unterscheiden. Es gibt nämlich Nichtprimzahlen $m \in \mathbb{N}$ mit $m > 2$ und mit $a^{m-1} \equiv 1 \pmod{m}$ für jedes $a \in \mathbb{Z}$ mit $\operatorname{ggT}(a,m) = 1$. Dies sind die sogenannten Carmichael-Zahlen (nach R. D. Carmichael, 1879 – 1967). Es gibt unendlich viele solche Zahlen, was 1992 von W. R. Alford, A. Granville und C. Pomerance bewiesen wurde (vgl. [1] und den Überblicksartikel [45] von Granville). Die drei kleinsten Carmichael-Zahlen sind 561, 1105 und 1729, und es gibt genau 105 212 Carmichael-Zahlen, die kleiner als 10^{15} sind (vgl. dazu Pinch [79]). Von einigen Eigenschaften der Carmichael-Zahlen handelt Aufgabe 7 in (5.26).

(4.23) Bemerkung: (1) Es sei $m \in \mathbb{N}$, und es sei $a \in \mathbb{Z}$. Für die Ordnung $\operatorname{ord}([a]_m)$ der Restklasse $[a]_m$ in der Gruppe $E(\mathbb{Z}/m\mathbb{Z})$ gilt nach (4.19)

$$\operatorname{ord}([a]_m) = \min(\{i \in \mathbb{N} \mid a^i \equiv 1 \pmod{m}\})$$

und nach (4.20)

$$\operatorname{ord}([a]_m) = \min(\{d \in \mathbb{N} \mid d \text{ teilt } \varphi(m);\ a^d \equiv 1 \pmod{m}\}).$$

Die MuPAD-Funktion `numlib::order` benutzt das zweite Ergebnis; sie verwendet dabei die Funktionen `phi` und `ifactor` aus dem MuPAD-Kern: Zuerst berechnet sie $\varphi(m)$, dann mit Hilfe der Funktion `numlib::divisors` (und damit letztlich mit Hilfe von `ifactor`) die Liste der nach der Größe geordneten Teiler $d \in \mathbb{N}$ von $\varphi(m)$ und sucht schließlich unter ihnen den kleinsten, für den $a^d \equiv 1 \pmod{m}$ gilt.

(2) Es sei p eine Primzahl, und es sei $a \in \mathbb{Z}$ nicht durch p teilbar. Für die Ordnung $\mathrm{ord}([\,a\,]_p)$ der Restklasse $[\,a\,]_p$ in der Multiplikativgruppe $\mathbb{F}_p^\times$ des Körpers $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ gilt .

$$\begin{aligned}\mathrm{ord}([\,a\,]_p) &= \min(\{i \in \mathbb{N} \mid a^i \equiv 1 \pmod p\}) = \\ &= \min(\{d \in \mathbb{N} \mid d \text{ teilt } p-1;\ a^d \equiv 1 \pmod p\}).\end{aligned}$$

(4.24) MuPAD: (1) Es sei $m \in \mathbb{N}$, und es seien $a \in \mathbb{Z}$ und $n \in \mathbb{N}_0$. Im Restklassenring $\mathbb{Z}/m\mathbb{Z}$ gilt $[\,a\,]_m^n = [\,a^n\,]_m = [\,(a^n) \bmod m\,]_m$, und daher kann man zur Berechnung von $[\,a\,]_m^n$ die Anweisung `modp(a^n,m)` verwenden. Dies ist aber nicht zu empfehlen, denn wenn $|\,a\,|$ und n nicht vergleichsweise klein sind, so hat MuPAD mit langen ganzen Zahlen zu rechnen, was viel Zeit kostet. Das kann man vermeiden, wenn man zur Berechnung von $(a^n) \bmod m$ die Anweisungssequenz

```
x := 1; for i from 1 to n do x := modp(a * x,m) end_for;
```

verwendet. Dieses Verfahren ist aber recht aufwendig: Es benötigt n Multiplikationen und n Reduktionen modulo m. Es gibt eine wesentlich bessere Methode zur Berechnung von $(a^n) \bmod m$.
(2) Die folgende Funktion `quickpot` berechnet zu $a \in \mathbb{Z}$, $n \in \mathbb{N}_0$ und $m \in \mathbb{N}$ die Zahl $(a^n) \bmod m$:

```
quickpot := proc(a,n,m)
begin
  if n = 0 then
    1
  elif n = 1 then
    modp(a,m)
  elif modp(n,2) = 0 then
    modp((quickpot(a,n/2,m)^2),m)
  else
    modp(a * (quickpot(a,(n-1)/2,m)^2),m)
  end_if
end_proc:
```

Eine solche rekursiv erklärte Funktion benötigt zur Laufzeit zu viel Arbeitsspeicher. Daher ist in MuPAD die Rekursionstiefe in der Standardeinstellung auf 500 beschränkt, d.h. eine Funktion wie `quickpot` kann sich nur höchstens 499-mal selbst aufrufen. (Man informiere sich in einer MuPAD-Sitzung über die Environment-Variable `MAXDEPTH`).

Der rekursiven Version von `quickpot` ist die folgende iterative Version vorzuziehen. Daß sie das Gewünschte leistet, zeigen die Kommentare.

```
quickpot := proc(a,n,m)
  local x, y, d;
begin
  if testargs() then
    if args(0) <> 3 then
      error("quickpot requires three arguments")
    elif domtype(a) <> DOM_INT then
      error("the 1st argument must be an integer")
    elif domtype(n) <> DOM_INT then
      error("the 2nd argument must be a nonnegative integer")
    elif n < 0 then
      error("the 2nd argument must be a nonnegative integer")
    elif domtype(m) <> DOM_INT then
      error("the 3rd argument must be a nonzero integer")
    elif m = 0 then
      error("the 3rd argument must be a nonzero integer")
    end_if
  end_if;
  x := 1;
  if n > 0 then
    y := modp(a,m); d := n;
    while d > 1 do
        # jetzt ist (x * y^d) mod m = a^n mod m #
      if modp(d,2) = 1 then
        x := modp(x * y,m)
      end_if;
      y := modp(y^2,m); d := d div 2
        # auch jetzt ist (x * y^d) mod m = a^n mod m #
    end_while;
        # jetzt gilt (x * y^d) mod m = a^n mod m und #
        # d = 1, also gilt (x * y) mod m = a^n mod m #
    x := modp(x * y,m)
  end_if;
  x
end_proc:
```

Diese zweite Version von `quickpot` benötigt zu einer ganzen Zahl a und natürlichen Zahlen n und m für die Berechnung von $a^n \bmod m$ höchstens $2\lfloor \log_2 n \rfloor + 1$ Multiplikationen und höchstens $2\lfloor \log_2 n \rfloor + 2$ Reduktionen modulo m, ihr Aufwand ist also, bei festen a und m, höchstens proportional zu $\log n$ (man vgl. dazu Aufgabe 3 in (4.30)).

Die MuPAD-Funktion `powermod` ist im wesentlichen diese zweite Version von `quickpot`. Sind $a \in \mathbb{Z}$, $n \in \mathbb{N}_0$ und $m \in \mathbb{N}$, so liefert die Anweisung `powermod(a,n,m)` die Zahl $(a^n) \bmod m$, falls `_mod` den Wert `modp` hat. Der folgende Ausschnitt aus dem Protokoll einer MuPAD-Sitzung zeigt, wie der Wert von `_mod` die Ausgabe von `powermod` steuert:

```
>> a := 333; n := 222; m := 1234;
                                333
                                222
                               1234
>> modp(a^n,m), mods(a^n,m);
                             1015,-219
>> powermod(a,n,m);
                                1015
>> _mod := mods;
                                mods
>> powermod(a,n,m);
                                -219
>> _mod := modp;
                                modp
>> powermod(a,n,m);
                                1015
```

Will man erzwingen, daß das Ergebnis eines Aufrufs von `powermod` innerhalb einer MuPAD-Funktion nicht davon abhängt, welchen Wert `_mod` zur Laufzeit besitzt, so wird man statt einer Anweisung `powermod(a,n,m)` die Anweisung `modp(powermod(a,n,m),m)` oder die Anweisung `mods(powermod(a,n,m),m)` verwenden, je nachdem welche innerhalb der Funktion das gewünschte Ergebnis liefert.

(4.25) Bemerkung: Der folgende Satz ist eine Art Umkehrung des Satzes von Fermat in (4.21); er zeigt, daß man bereits mit den doch recht elementaren Methoden, die in diesem Paragraphen zu Verfügung gestellt werden, manche vergleichsweise große natürliche Zahlen als Primzahlen identifizieren kann. Wenn man ihn in konkreten Fällen anwendet, so sieht man, wie wichtig eine schnelle Funktion `powermod` ist.

(4.26) Satz: *Es sei $m > 1$ eine ungerade natürliche Zahl, für die gilt: Zu jedem Primteiler q von $m-1$ gibt es ein $a_q \in \mathbb{Z}$ mit*

$$a_q^{(m-1)/q} \not\equiv 1 \pmod{m} \quad \textit{und} \quad a_q^{m-1} \equiv 1 \pmod{m}.$$

Dann ist m eine Primzahl.

Beweis: (a) Es sei q ein Primteiler von $m-1$, und es seien $\alpha := v_q(m-1)$ und $c := (m-1)/q^\alpha$. Wegen $a_q^{m-1} \equiv 1 \pmod{m}$ sind a_q und m teilerfremd, und $d := \mathrm{ord}([a_q]_m)$ teilt $m-1 = q^\alpha c$. Wegen $a_q^{(m-1)/q} \not\equiv 1 \pmod{m}$ ist d nicht Teiler von $(m-1)/q = q^{\alpha-1}c$. Also ist $d = q^\alpha c'$ mit einem Teiler $c' \in \mathbb{N}$ von c. Weil d nach dem Satz von Euler (vgl. (4.20)) ein Teiler von $\varphi(m)$ ist, folgt: q^α ist ein Teiler von $\varphi(m)$.
(b) Aus (a) folgt, daß $\varphi(m)$ durch $m-1$ teilbar ist. Wegen $\varphi(m) \leq m-1$ gilt daher $\varphi(m) = m-1$, und somit ist im Ring $\mathbb{Z}/m\mathbb{Z}$ jedes vom Nullelement verschiedene Element eine Einheit. Also ist $\mathbb{Z}/m\mathbb{Z}$ ein Körper, und daher ist m eine Primzahl.

(4.27) Bemerkung: Die Anwendung des Satzes in (4.26) auf eine ungerade natürliche Zahl $m > 1$ setzt die Kenntnis der Primzerlegung von $m-1$ voraus. Daher ist dieser Satz nur für spezielle m anwendbar, etwa auf die in Abschnitt (2.22) definierten Fermat-Zahlen. Man kann den Satz verbessern: In (4.30), Aufgabe 6, ist eine Version angegeben, in der nicht die Kenntnis der vollen Primzerlegung von $m-1$ vorausgesetzt wird.

(4.28) Beispiel: Es sei

$$m := 3^{31} - 2^{31} = 61767\,12488\,00299.$$

Die Primzerlegung von $m-1$ ist

$$m - 1 = 2 \cdot 3 \cdot 7^2 \cdot 11 \cdot 31 \cdot 53 \cdot 3203 \cdot 36293,$$

und für jeden Primteiler $q \neq 3$ von $m-1$ gilt $2^{(m-1)/q} \not\equiv 1 \pmod{m}$. Es gilt $2^{(m-1)/3} \equiv 1 \pmod{m}$, $3^{(m-1)/3} \equiv 1 \pmod{m}$, $5^{(m-1)/3} \equiv 1 \pmod{m}$, $7^{(m-1)/3} \equiv 1 \pmod{m}$, $11^{(m-1)/3} \equiv 59650\,38382\,01234 \not\equiv 1 \pmod{m}$ und $2^{m-1} \equiv 1 \pmod{m}$ und $11^{m-1} \equiv 1 \pmod{m}$. Also ist m eine Primzahl.

(4.29) Bemerkung: In (4.22) wurde gezeigt, wie man in manchen Fällen einfach und schnell zeigen kann, daß eine natürliche Zahl keine Primzahl ist. Ähnlich einfach und schnell kann man bisweilen zu einer natürlichen Zahl einen nichttrivialen Teiler finden. Es sei dazu $m \in \mathbb{N}$ keine Primzahl. Man wählt eine Zahl $a \in \mathbb{N}$ und berechnet den größten gemeinsamen Teiler d von $(a^m \bmod m) - a$ und m (in MuPAD mit Hilfe der Funktionen `powermod` und `igcd`). Ist $1 < d < m$, so hat man einen nichttrivialen Teiler von m gefunden, andernfalls kann man mit neuen a das Spiel einige Male wiederholen. Natürlich wird das Verfahren in vielen Fällen nicht zum Erfolg führen; bei Eingabe einer Carmichael-Zahl m etwa wird der größte gemeinsame Teiler d für jedes a gleich m sein. Aber bisweilen funktioniert dieser Versuch, eine natürliche Zahl zu faktorisieren, überraschend gut: Man kann etwa die Primzerlegung der beiden Zahlen n und N aus (7.6) auf die hier geschilderte Weise finden.

(4.30) Aufgaben:

Aufgabe 1: (a) Man schreibe MuPAD-Funktionen, die zu einer natürlichen Zahl m die Verknüpfungstafeln des Rings $\mathbb{Z}/m\mathbb{Z}$ berechnet.
(b) Man schreibe eine MuPAD-Funktion, die zu einer natürlichen Zahl die Gruppe $E(\mathbb{Z}/m\mathbb{Z})$ und ihre Verknüpfungstafel berechnet.

Aufgabe 2: (a) Man zeige, daß es in einer endlichen Gruppe gerader Ordnung ein Element der Ordnung zwei gibt.
(b) Man folgere aus (a), daß jede Carmichael-Zahl ungerade ist.
(c) Man schreibe eine MuPAD-Funktion, die zu zwei natürlichen Zahlen m und n mit $m < n$ alle Carmichael-Zahlen zwischen m und n berechnet. Man ermittle die Primzerlegung jeder so berechneten Carmichael-Zahl. Was kann man ablesen? Man vergleiche dazu die Aufgabe 7 in (5.26).

Aufgabe 3: Es sei $n \in \mathbb{N}$. Es gibt ein eindeutig bestimmtes $p(n) \in \mathbb{N}_0$ und eindeutig bestimmte $a_0, a_1, \ldots, a_{p(n)} \in \{0,1\}$ mit $a_{p(n)} = 1$ und mit

$$n \;=\; a_0 + a_1 \cdot 2 + a_2 \cdot 2^2 + \cdots + a_{p(n)} \cdot 2^{p(n)}$$

(vgl. (1.32), Aufgabe 4). Es seien $a \in \mathbb{Z}$ und $m \in \mathbb{Z} \setminus \{0\}$. Man zeige, daß die in (4.24)(2) definierten Funktionen `quickpot` wirklich beide die Zahl $a^n \bmod m$ berechnen. Man zeige, daß mit $q(n) := a_0 + a_1 + \cdots + a_{p(n)}$ gilt: Die iterative Version von `quickpot` benötigt zur Berechnung von $a^n \bmod m$ $p(n) + q(n)$ Multiplikationen und $p(n) + q(n) + 1$ Reduktionen modulo m, und es gilt

$$p(n) + q(n) \;\leq\; 2p(n) + 1 \;=\; 2\lfloor \log_2 n \rfloor + 1.$$

Man schreibe eine Variante der iterativen Version von `quickpot`, die auf Wunsch auch die Anzahl der durchgeführten Multiplikationen ausgibt; dabei verwende man `userinfo`.

Aufgabe 4: Die MuPAD-Funktion `numlib::order` verwendet `ifactor`. Man überlege sich, wie man für eine natürliche Zahl m Ordnungen in der Gruppe $E(\mathbb{Z}/m\mathbb{Z})$ ohne Verwendung von `ifactor` berechnen kann. Man schreibe dazu MuPAD-Funktionen und vergleiche sie untereinander und mit `numlib::order`.

Aufgabe 5: Es sei $(F_n)_{n\geq 0}$ die Folge der Fibonacci-Zahlen (vgl. (1.21)).
(a) Man beweise: Im Ring $M(2;\mathbb{Z})$ der (2,2)-Matrizen über $\mathbb{Z}$ gilt für jedes $n \in \mathbb{N}$: Es ist

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n \;=\; \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}.$$

(b) Man folgere aus (a): Für jedes $n \in \mathbb{N}$ gilt

$$F_{2n} \;=\; F_n \cdot (F_n + 2F_{n-1}) \quad \text{und} \quad F_{2n+1} \;=\; F_{n+1}^2 + F_n^2.$$

(c) Die Ergebnisse in (a) und in (b) erlauben es, Fibonacci-Zahlen sehr schnell zu berechnen, indem man im wesentlichen so vorgeht, wie man auf intelligente Weise Potenzen in einem Ring berechnet (vgl. (4.24)). Man schreibe MuPAD-Funktionen, die auf diese Weise Fibonacci-Zahlen berechnen, und zwar eine rekursive Version und eine iterative Version (wie von `quickpot` in (4.24)).

Aufgabe 6: Es sei $m > 1$ eine ungerade natürliche Zahl, es gelte $m-1 = n_0 \cdot n$ mit teilerfremden natürlichen Zahlen n_0 und n, für die $n_0 < n$ gilt, und es sei $n = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_r^{\alpha_r}$ die Primzerlegung von n; es gelte: Es gibt ein $a \in \mathbb{Z}$ mit $a^{m-1} \equiv 1 \pmod{m}$ und mit

$$\mathrm{ggT}(a^{(m-1)/q_i} - 1, m) \;=\; 1 \quad \text{für jedes } i \in \{1, 2, \ldots, r\}.$$

Man beweise, daß m eine Primzahl ist. (Man zeige dazu zuerst ähnlich wie im Beweis in (4.26), daß für den kleinsten Primteiler p von m gilt: Für jedes $i \in \{1, 2, \ldots, r\}$ ist $q_i^{\alpha_i}$ ein Teiler von $\varphi(p) = p - 1$, und daher ist $p > \sqrt{m}$).

Aufgabe 7: Man beweise den folgenden Satz von E. Proth aus [85]: Es sei $m > 1$ eine ungerade natürliche Zahl, es gelte $m - 1 = 2^{\alpha} m_0$ mit einer ungeraden natürlichen Zahl $m_0 < 2^{\alpha}$, und es gelte: Es gibt ein $a \in \mathbb{Z}$ mit

$$a^{(m-1)/2} \;\equiv\; -1 \pmod{m}.$$

Dann ist m eine Primzahl.

Aufgabe 8: Man beweise den folgenden Satz von H. C. Pocklington aus [81]: Es sei $m > 1$ eine ungerade natürliche Zahl, es sei q ein Primteiler von $m - 1$, es sei $\alpha := v_q(m-1)$, und es gelte: Es gibt ein $a \in \mathbb{Z}$ mit

$$a^{m-1} \;\equiv\; 1 \pmod{m} \quad \text{und} \quad \mathrm{ggT}\big(a^{(m-1)/q} - 1, m\big) \;=\; 1.$$

Dann gilt für jeden Primteiler p von m: Es ist

$$p \;\equiv\; 1 \pmod{q^{\alpha}}.$$

Aufgabe 9: Man schreibe eine MuPAD-Funktion, die nach dem in (4.29) beschriebenen "Verfahren" versucht, zu einer Nichtprimzahl $m > 1$ einen Teiler $d \in \mathbb{N}$ mit $1 < d < m$ zu finden. Man experimentiere damit, etwa was die Wahl der Zahlen a (vgl. (4.29)) oder was die Anzahl der durchzuführenden Iterationen betrifft. Man versuche, mit dieser Funktion einige Mersenne-Zahlen zu faktorisieren. Man berechne damit die Primzerlegungen der in (7.6) angegebenen Zahlen n und N.

(4.31) MuPAD: Die Restklassenringe von $\mathbb{Z}$ bieten eine gute Gelegenheit zu zeigen, daß man in MuPAD nicht nur einzelne mathematische Objekte wie Zahlen oder Funktionen, sondern auch ganze mathematische Strukturen erklären kann. Ist m eine natürliche Zahl, so definiert der Aufruf

```
R := Dom::IntegerMod(m)
```

den Restklassenring $\mathbb{Z}/m\mathbb{Z}$ und gibt ihm dem Namen R. Für eine ganze Zahl a wird dann das Element $[a]_m$ von $\mathbb{Z}/m\mathbb{Z}$ durch `R(a)` oder ausführlich durch `Dom::IntegerMod(m)(a)` definiert. Im folgenden wird am konkreten Fall des Restklassenrings $\mathbb{Z}/42\mathbb{Z}$ gezeigt, wie man darin Elemente erklärt und mit ihnen rechnet. Der Leser sollte eine MuPAD-Sitzung wie die in den nächsten Zeilen protokollierte wirklich am Rechner durchführen.

```
>> R := Dom::IntegerMod(42);
                        Dom::IntegerMod(42)
>> x := R(17); y := R(31); z := R(22);
                              17 mod 42
                              31 mod 42
                              22 mod 42
```

Das Element $x := [17]_{42} \in \mathbb{Z}/42\mathbb{Z}$, das durch den Aufruf `x := R(17)` definiert wird, wird also in der Form `17 mod 42` ausgegeben; man kann es aber nicht durch den Aufruf `x := 17 mod 42` definieren. Hier ist `mod` also nicht der Operator `mod` aus (1.5); daran muß man sich vielleicht ein wenig gewöhnen.

```
>> w := 17 mod 42;
                                 17
>> bool(x = w);
                               FALSE
>> domtype(x); domtype(w);
                        Dom::IntegerMod(42)
                               DOM_INT
```

Mit den Elementen von $\mathbb{Z}/42\mathbb{Z}$ kann man in MuPAD in gewohnter Weise rechnen:

```
>> x + y + z;
                              28 mod 42
>> x - y*z;
                               7 mod 42
>> x^1001;
                               5 mod 42
>> y/x;
                              29 mod 42
>> 1/z;
                                 FAIL
```

Die Ausgabe von FAIL bedeutet hier, daß $[22]_{42}$ keine Einheit im Ring $\mathbb{Z}/42\mathbb{Z}$ ist.

Man kann sich in $\mathbb{Z}/42\mathbb{Z}$ die Aussagen einiger Sätze aus diesem Paragraphen illustrieren lassen:

```
>> Liste := [$ 0..41];
   [0, 1, 2, 3, 4, 5, 6, 7, 8, 9,10,11,12,13,14,
           15,16,17,18,19,20,21,22,23,24,25,26,27,28,
                    29,30,31,32,33,34,35,36,37,38,39,40,41]
>> f := func(bool(igcd(x,42) = 1),x);
                func(bool(igcd(x, 42) = 1), x)
                     # eine Funktion -- siehe das MuPAD-Manual #
>> L := select(Liste,f);
              [1,5,11,13,17,19,23,25,29,31,37,41]
>> Einheitengruppe := map(L,R);
   [1 mod 42, 5 mod 42,11 mod 42,13 mod 42,17 mod 42,
            19 mod 42,23 mod 42,25 mod 42,29 mod 42,
                    31 mod 42,37 mod 42,41 mod 42]
>> n := nops(Einheitengruppe);
                      # die Ordnung der Einheitengruppe von R #
                              12
>> bool(n = phi(42));
                            TRUE
>> {Einheitengruppe[i]^n $ hold(i) = 1..n};
                                          # der Satz von Euler #
                          {1 mod 42}
>> ordnungen := map(L,numlib::order,42);
                  [1,6,6,2,6,6,6,3,2,6,3,2]
>> lambda := max(op(ordnungen));
                     # der Exponent der Einheitengruppe von R #
                              6
>> {Einheitengruppe[i]^lambda $ hold(i) = 1..n};
                                           # vergleiche (3.13) #
                          {1 mod 42}
```

Auch die Ausgabe der Elemente eines Restklassenrings von $\mathbb{Z}$ wird übrigens von dem Wert des Operators mod gesteuert. Eine Fortsetzung der oben protokollierten MuPAD-Sitzung könnte so aussehen:

```
>> _mod := mods;
                            mods
```

```
>> L := select(Liste,f);
              [1,5,11,13,17,19,23,25,29,31,37,41]
>> Einheitengruppe := map(L,R);
   [1 mod 42,  5 mod 42, 11 mod 42, 13 mod 42, 17 mod 42,
              19 mod 42,-19 mod 42,-17 mod 42,-13 mod 42,
                        -11 mod 42, -5 mod 42, -1 mod 42]
```

Für die Elementare Zahlentheorie, wie sie in diesem Buch behandelt wird, mag die Fähigkeit von MuPAD, die Restklassenringe von $\mathbb{Z}$ als algebraische Strukturen zu definieren, nicht von wesentlicher Bedeutung sein. MuPAD erlaubt es aber auch, etwa über einem Restklassenkörper $\mathbb{F}$ von $\mathbb{Z}$ den Ring $M(n;\mathbb{F})$ der quadratischen Matrizen einer bestimmten Zeilenzahl n zu erklären, und weiß dann, wie man darin rechnet, und auch, wie man den Rang, die Determinante oder das charakteristische Polynom einer Matrix aus $M(n;\mathbb{F})$ oder die Lösungsmenge eines linearen Gleichungssystems über dem Körper $\mathbb{F}$ berechnet. Darüber informiert die Dokumentation für die MuPAD-Library `linalg`.

5 Primitivwurzeln

(5.1) In diesem Paragraphen werden die natürlichen Zahlen m charakterisiert, für die die Einheitengruppe $E(\mathbb{Z}/m\mathbb{Z})$ des Restklassenrings $\mathbb{Z}/m\mathbb{Z}$ zyklisch ist. Außerdem wird für jedes $m \in \mathbb{N}$ die maximale Elementordnung in der Gruppe $E(\mathbb{Z}/m\mathbb{Z})$ berechnet.

(5.2) Bemerkung: Es sei p eine Primzahl. Der Restklassenring $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ ist ein Körper mit p Elementen, und seine Multiplikativgruppe

$$\mathbb{F}_p^\times \;=\; E(\mathbb{Z}/p\mathbb{Z}) \;=\; \big\{[\,1\,]_p, [\,2\,]_p, \ldots, [\,p-1\,]_p\big\}$$

ist eine zyklische Gruppe (vgl. (3.14)). Also gibt es ein $g \in \{1, 2, \ldots, p-1\}$ mit $\mathbb{F}_p^\times = \langle\, [\,g\,]_p \,\rangle$.

(5.3) Definition: Es sei p eine Primzahl. $g \in \mathbb{Z}$ heißt eine Primitivwurzel modulo p, wenn g nicht durch p teilbar ist und $\mathbb{F}_p^\times = \langle\, [\,g\,]_p \,\rangle$ gilt.

(5.4) Bemerkung: (1) Die Primitivwurzeln modulo 2 sind die ungeraden ganzen Zahlen.
(2) Es sei p eine ungerade Primzahl; es sei $g \in \mathbb{Z}$ mit $p \nmid g$. Die folgenden Aussagen sind äquivalent:

(a) g ist eine Primitivwurzel modulo p.
(b) Es ist $\operatorname{ord}([\,g\,]_p) = p - 1$.
(c) Es ist $\min(\{i \in \mathbb{N} \mid g^i \equiv 1 \pmod p\}) = p - 1$.
(d) Für jeden Primteiler q von $p-1$ gilt $g^{(p-1)/q} \not\equiv 1 \pmod p$.