Inhaltsverzeichnis

Vorbemerkungen und Konventionen:

(i) $(\mathbb{Z}, +, *)$ ist ein kommutativer Ring mit 1. (Aber: $(\mathbb{Z}, +, *)$ ist kein Körper, da nur 1 und -1 ein multipikatives Inverses in $\mathbb{Z}$ besitzen.)

(ii) $\mathbb{Z}$ ist nullteilerfrei, d. h. ein Integritätsbereich (d. h. $ab = 0 \Rightarrow a = 0 \vee b = 0$).
Es folgt: Ist $ax = bx$ und $x \neq 0$, so ist $a = b$ (da $(a - b)x = ax - bx = 0 \Rightarrow a - b = 0$)

(iii) Auf $\mathbb{Z}$ ist durch $\leq$ eine totale Ordnung gegeben, die mit $+$ und $*$ verträglich ist.

(iv) Ist $A \subseteq \mathbb{Z}, A \neq \emptyset$ und A ist nach oben (bzw. unten) beschränkt, so besitzt A ein größtes (bzw. kleinstes) Element.

(v) $\mathbb{N} := \{a \in \mathbb{Z} \mid a > 0\} = \{1, 2, 3, \ldots\}$.

Kapitel 1

Teiler und ggT

Definition „Teiler und Komplimentärteiler“
Seien $m, n \in \mathbb{Z}$. Man sagt m ist Teiler von n, oder kurz m teilt n, wenn

$$\exists d \in \mathbb{Z} : n = m \cdot d,$$

wobei d der Komplimentärteiler von m zu n genannt wird.

Notation: Wenn m Teiler von n ist schreibt man $m \mid n$. Wenn m kein Teiler von n ist schreibt man $m \nmid n$.

Satz 1
Seien $m, n, m_i, n_i, l, l_i \in \mathbb{Z}$.

(i) $\forall n$ gilt $1 \mid n,\ n \mid n$ und $n \mid 0$. Wenn $0 \mid n \Rightarrow n = 0$.

(ii) $m \mid n \Rightarrow (-m) \mid n$ und $m \mid (-n)$.

(iii) $m \mid n$ und $n \neq 0 \Rightarrow |m| \leq |n|$.

(iv) $n \mid 1 \Rightarrow n \in \{-1, 1\}$.

(v) $m \mid n$ und $n \mid m \Rightarrow (n = m$ oder $n = -m) \Leftrightarrow |m| = |n|$.

(vi) $l \mid n$ und $m \mid n \Rightarrow l \mid n$.

(vii) $l \mid n \Rightarrow (lm) \mid (ln),\ \forall l$.

(viii) $(lm) \mid (ln) \Rightarrow m \mid n,\ \forall l \setminus \{0\}$.

(ix) $m \mid n_i\ (1 \leq i \leq k) \Rightarrow m \mid (l_1 n_1 +_l 2_n 2 + ... + l_k n_k),\ \forall l_i$.

(x) $m_i \mid n_i\ (1 \leq i \leq k) \Rightarrow (m_1 \cdot m_2 \cdot ... \cdot m_k) \mid (n_1 \cdot n_2 \cdot ... \cdot n_k)$.

Beweis. (i) $n = 1n$, $0 = 0n$, $\exists d \in \mathbb{Z} : n = 0d \Rightarrow n = 0$

(ii) $\exists d \in \mathbb{Z} : n = md \Rightarrow n = (-m)(-d)$ und $-n = m(-d)$

(iii) $\exists d \in \mathbb{Z},\ d \neq 0 : n = md \Rightarrow |n| = |m| \underbrace{|d|}_{\geq 1} \geq |m|$

(iv) Wegen (iii) ist $|n| \leq 1 \Rightarrow n \in \{-1, 0, 1\}$. Da $n = 0$ unmöglich ist, folgt $n \in \{-1, 1\}$.

(v) Stimmt für $m = n = 0$.
Falls $m \neq 0 \Rightarrow n \neq 0$ (Wegen $n \mid m$). Ebenfalls gilt $n \neq 0 \Rightarrow m \neq 0$ (Wegen $m \mid n$)
Wegen (iii) gilt daher $|m| = |n|$ d. h. $n \in \{-m, m\}$

(vi) $\exists d_1 \in \mathbb{Z} : m = d_1 l, \exists d_2 \in \mathbb{Z} : n = d_2 m \Rightarrow n = d_1 d_2 l \Rightarrow l \mid n$

(vii) $\exists d \in \mathbb{Z} : n = md \Rightarrow ln = (lm)d \Rightarrow (lm) \mid (ln)$

(viii) $\exists d \in \mathbb{Z} : ln = lmd = (lm)d = l(md) \Rightarrow n = md \Rightarrow m \mid n$

(ix) $\forall i \in \{1, \ldots, k\} : \exists d_i \in \mathbb{Z} : n_i = md_i \Rightarrow \sum_{i=1}^{k} l_i n_i = \sum_{i=1}^{k} l_i (md_i) = m \sum_{i=1}^{k} l_i d_i$

(x) $\forall i \in \{1, \ldots, k\} : \exists d_i \in \mathbb{Z} : n_i = m_i d_i \Rightarrow \prod_{i=1}^{k} n_i = \prod_{i=1}^{k} (m_i d_i) = (\prod_{i=1}^{k} d_i)(\prod_{i=1}^{k} m_i)$

□

Bemerkung

1. Jedes n besitzt die folgenden Teiler: $1, -1, n, -n$. Ist $d \mid n$
und $d \notin \{1, -1, n, -n\}$, so heißt d echter Teiler von n.
2. Ist $n \neq 0$ und $m \mid n$, so ist $m \in \{-|n|, -|n| + 1, \ldots, |n| - 1, |n|\}$. Es folgt: Jedes $n \neq 0$ besitzt nur endlich viele Teiler.
3. Ist $n \in \mathbb{N}$ und man hat alle Teiler $m > 0$ von n mit $1 \leq m \leq \sqrt{n}$ gefunden, so sind die restlichen positiven Teiler von n gerade die Komplementärteiler.
(Ist $d \mid n$ und $d > \sqrt{n}$, so ist $n = m \cdot d \Leftrightarrow m = \frac{n}{d}$ und $m = \frac{n}{d} < \frac{n}{\sqrt{n}} = \sqrt{n}$).

Beispiel
Sei $n = 60$. Teiler von 60 mit $m \leq \sqrt{60} = 7.74$ (d. h. $m \leq 7$) sind: $1, 2, 3, 4, 5, 6 \Rightarrow$ die restlichen positiven Teiler von 60 sind: $60, 30, 20, 15, 12, 10$.

Definition „Gaußklammer“
Für $x \in \mathbb{R}$ sei die Gaußklammer definiert als

$$\lfloor x \rfloor := \max\{k \in \mathbb{Z} : k \leq x\}.$$

Bemerkung

1. Die Gaußklammer definiert also die größte ganze Zahl kleiner als x.
2. Offenbar gilt $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1 \; \forall x \in \mathbb{R}$
3. Beachte: Es gilt $\lfloor \frac{5}{2} \rfloor = \lfloor 2, 5 \rfloor = 2$, aber $\lfloor -\frac{5}{2} \rfloor = \lfloor -2, 5 \rfloor = -3$

Satz 2 „Division mit Rest“
Seien $m, n \in \mathbb{Z}$, $n > 0$. Dann gibt es eindeutig bestimmte $q, r \in \mathbb{Z}$ mit

$$m = q \cdot n + r, \; 0 \leq r < n.$$

Beweis.

- Existenz. Sei $q := [\frac{m}{n}]$. Dann $q \leq \frac{m}{n} < q+1$
  $\Rightarrow qn \leq m < qn + n \Rightarrow 0 \leq m - qn < n$. Setze $r := m - qn$.
  Dann $m = qn + r$ und $0 \leq r < n$.

- Eindeutigkeit. Sei $m = qn + r = \overline{q}n + \overline{r}$ mit $0 \leq r, \overline{r} < n$.
  Dann ist $(q - \overline{q})n = \overline{r} - r \Rightarrow q - \overline{q} = \frac{\overline{r}-r}{n}$.
  Wegen $-n < \overline{r} - r < n \Rightarrow -1 < \underbrace{\frac{\overline{r} - r}{n}}_{\in\mathbb{Z}} < 1 \Rightarrow \frac{\overline{r}-r}{n} = 0$
  $\Rightarrow \overline{r} = r \Rightarrow qn = \overline{q}n \Rightarrow q = \overline{q}$.

□

Definition „gemeinsamer Teiler“
Sind $n_1, \ldots, n_k, m \in \mathbb{Z}$, dann heißt m gemeinsamer Teiler von $n_1, \ldots, n_k$, wenn gilt

$$m \mid n_i,\ 1 \leq i \leq k.$$

Bemerkung Die Menge der gemeinsamen Teiler ist stets $\neq \emptyset$, da sie 1 enthält.
Sind $n_1, \ldots, n_k$ nicht alle 0, so ist die Menge der gemeinsamen Teiler nach oben beschränkt (z. B. durch $\min\{|n_i| \mid 1 \leq i \leq k,\ n_i \neq 0\}$). Man kann daher einen größten gemeinsamen Teiler definieren.

Definition „größter gemeinsamer Teiler“
Seien $n_1, \ldots, n_k \in \mathbb{Z}$ nicht alle Null, dann wird der größte gemeinsame Teiler definiert durch

$$\text{ggT}(n_1, ..., n_k) := \max\{m \in \mathbb{Z} : m \mid n_i,\ 1 \leq i \leq k.\}$$

Bemerkung

1. Da 1 stets gemeinsamer Teiler ist, kann man sich bei den Bestimmungen des ggT auf positive gemeinsame Teiler beschränken.
2. Es gilt $\text{ggT}(n_1, \ldots, n_k) = \text{ggT}(|n_1|, \ldots, |n_k|),\ \forall n_1, \ldots, n_k \in \mathbb{Z}$ (nicht alle 0).

Beispiel
Bestimme $\text{ggT}(12, -8)$. Positive Teiler von 12 (bzw. -8) sind $1, 2, 3, 4, 6, 12$ (beziehungsweise $1, 2, 4, 8$). Gemeinsame Teiler sind $1, 2, 4 \Rightarrow \text{ggT}(12, -8) = 4$

Satz 3 „Euklidischer Algorithmus“
Sind $a, b \in \mathbb{N}$ und $b \leq a$, so führe wiederholt Division mit Rest durch.

$$\begin{aligned}
a &= b \cdot q_0 + r_1, & 0 \leq r_1 < b \\
b &= r_1 \cdot q_1 + r_2, & 0 \leq r_2 < r_1 \\
r_1 &= r_2 \cdot q_2 + r_3, & 0 \leq r_3 < r_2 \\
&\vdots & \vdots \\
r_{m-1} &= r_m \cdot q_m + r_{m+1}, & 0 \leq r_{m+1} < r_m
\end{aligned}$$

Wegen $r_1 > r_2 > r_3 > \ldots > r_m > r_{m+1} > \ldots \geq 0$ gibt es ein kleinstes n mit $r_{n+1} = 0$. Es gilt dann $r_n = \text{ggT}(a, b)$.

Beweis. 1. Zeige, dass r_n gemeinsamer Teiler von a, b ist:
Wegen $r_{n-1} = r_n q_n$ gilt $r_n \mid r_{n-1}$.
Wegen $r_{n-2} = r_{n-1}q_{n-1} + r_n$ (und Satz 1(ix)) folgt, dass $r_n \mid r_{n-2}$.
Verfahre weiter so. Ist $r_n \mid r_{m+1}$ und $r_n \mid r_m$ bereits gezeigt, so folgt $r_n \mid r_{m-1}$ wegen $r_{m-1} = r_m q_m + r_{m+1}$.
Schließlich folgt $r_n \mid b$ wegen $b = r_1 q_1 + r_2$ und $r_n \mid a$ wegen $a = bq_0 + r_1$.

2. Zeige, dass r_n größter gemeinsamer Teiler von a, b ist:
Sei d ein beliebiger positiver gemeinsamer Teiler von a, b.
Wegen $r_1 = a - bq_0$ folgt $d \mid r_1$.
Wegen $r_2 = b - r_1 q_1$ folgt $d \mid r_2$.
Verfahre weiter so. Ist $d \mid r_{m-1}$ und $d \mid r_m$ bereits gezeigt, so folgt $d \mid r_{m+1}$ wegen $r_{m+1} = r_{m-1} - r_m q_m$.
Es folgt $d \mid r_n \overset{\text{Satz 1(iii)}}{\Rightarrow} d \leq r_n$.

□

Beispiel
Bestimme $\text{ggT}\,(97, -44) = \text{ggT}\,(97, |-44|) = \text{ggT}\,(97, 44)$.

$$\begin{aligned} 97 &= 2 \cdot 44 + 9 \\ 44 &= 4 \cdot 9 + 8 \\ 9 &= 1 \cdot 8 + 1 \\ 8 &= 8 \cdot 1 + 0 \end{aligned}$$

$$\Rightarrow \text{ggT}\,(97, 44) = 1$$

Satz 4 „kleinste positive Linearkombination ist ggT“
Seien $n_1, \ldots, n_k \in \mathbb{Z}$ nicht alle Null, dann ist

$$\text{ggT}(n_1, ..., n_k) = \min \left\{ x_1, ..., x_k \in \mathbb{Z} : \sum_{i=1}^{k} x_i \cdot n_i > 0 \right\}.$$

Beweis. Sei $L := \{x_1, \ldots, x_n \in \mathbb{Z}, \sum_{i=1}^{k} x_i n_i > 0\}$.
Setzt man $x_i = n_i$, dann erhält man $\sum_{i=1}^{k} n_i^2 > 0 \Rightarrow L \neq \emptyset$ und wird nach unten durch 0 beschränkt $\Rightarrow \exists d' := \min(L)$. Sei $d := \text{ggT}\,(n_1, \ldots, n_k)$. (Zu zeigen: $d = d'$)

- Zeige $d \leq d'$: $\exists y_1, \ldots, y_k \in \mathbb{Z} : d' = \sum_{i=1}^{k} y_i n_i \overset{\text{Satz 1(ix)}}{\Rightarrow} d \mid d' \overset{\text{Satz 1(iii)}}{\Rightarrow} d \leq d'$.

- Zeige $d' \leq d$: Wende Satz 2 auf n_j, d' an (für $1 \leq j \leq k$).
  $\forall j \in \{1, \ldots, k\} : \exists q_j, r_j \in \mathbb{Z}$ mit $n_j = q_j d' + r_j$ und $0 \leq r_j < d' \Rightarrow$ für $1 \leq j \leq k$ gilt:

$$r_j = n_j - q_j d' = n_j - q_j \sum_{i=1}^{k} y_i n_i = \underbrace{(1 - q_j y_j)}_{=:z_{jj}} n_j + \sum_{\substack{1 \leq i \leq k \\ i \neq j}} \underbrace{(-q_i y_i)}_{=:z_{ij}} n_i.$$

Würde ein j mit $1 \leq j \leq k$ existieren, derart dass $r_j > 0$, so wäre $r_j = \sum_{i=1}^{k} z_{ij} n_i \in L$ und $r_j < d'$. Widerspruch!
Also gilt $d' \mid n_j$ für $1 \leq j \leq k \Rightarrow d' \leq d$. □

Bemerkung

1. Satz 4 beinhaltet: Sind $n_1, \ldots, n_k \in \mathbb{Z}$ (nicht alle 0) und $d = \text{ggT}(n_1, \ldots, n_k)$, so $\exists x_1, \ldots, x_k \in \mathbb{Z} : d = x_1 n_1 + \ldots + x_k n_k$.
2. Für $k = 2$ liefert der Euklidische Algorithmus Satz 3 eine Methode x_1, x_2 mit $d = x_1 n_1 + x_2 n_2$ zu finden.

Beispiel
Wir hatten: $\text{ggT}(97, -44) = 1 = 9 - 8 = 9 - (44 - 4 \cdot 9) = 5 \cdot 9 - 44 = 5 \cdot (97 - 2 \cdot 44) - 44 = 5 \cdot 97 - 11 \cdot 44 = 5 \cdot 97 + 11(-44)$.

Satz 5
Seien $n_1, \ldots, n_k \in \mathbb{Z}$ nicht alle Null und $d > 0 \in \mathbb{Z}$, dann sind äquivalent

(i) $d = \text{ggT}(n_1, ..., n_k)$,

(ii) $d \mid n_i,\ 1 \leq i \leq k$ und wenn $d' \mid n_i,\ 1 \leq i \leq k \Rightarrow d' \mid d$.

Beweis. (i) $\Rightarrow$ (ii): Ist $d = \text{ggT}(n_1, \ldots, n_k)$, so gilt: $d \mid n_i$ für $1 \leq i \leq k$. Nach Satz 4 $\exists x_1, \ldots, x_k \in \mathbb{Z} : d = \sum_{i=1}^{k} x_i n_i$. Gilt $d' \mid n_i$ für $1 \leq i \leq k$, so folgt $d' \mid d$ (wegen Satz 1(ix)).
(ii) $\Rightarrow$ (i): d ist gemeinsamer Teiler von $n_1, \ldots, n_k$. Ist d' ebenfalls gemeinsamer Teiler von $n_1, \ldots, n_k$, so $d' \mid d \overset{\text{Satz 1(iii)}}{\Rightarrow} d' \leq |d'| \leq d$. □

Bemerkung Satz 5 charakterisiert den ggT ohne Verwendung der Ordnungsrelation und ist darum für Verallgemeinerungen geeignet.

Satz 6
Seien $n_1, \ldots, n_k \in \mathbb{Z}$ nicht alle Null und $d = ggt(n_1, \ldots, n_k)$.

(i) Für jede Permutation $\sigma \in S_k$ ist $\text{ggT}(n_{\sigma(1)}, \ldots, n_{\sigma(k)}) = d$.

(ii) Ist $k \geq 2$ und $n_k = 0$, so ist $d = \text{ggT}(n_1, \ldots, n_{k-1})$.

(iii) Ist $k \geq 2$ und $n_{k-1} = n_k$, so ist $d = \text{ggT}(n_1, \ldots, n_{k-1})$

(iv) Für alle $x_1, \ldots, x_{k-1} \in \mathbb{Z} : \text{ggT}(n_1, \ldots, n_{k-1}, n_k + \sum_{i=1}^{k-1} x_i n_i) = d$

(v) $\forall l \in \mathbb{Z} \setminus \{0\} : \text{ggT}(ln_1, \ldots, ln_k) = |l| d$

(vi) Es gilt: $\text{ggT}(\frac{n_1}{d}, \ldots, \frac{n_k}{d}) = 1$

(vii) Ist $k \geq 2$ und $n_1, \ldots, n_{k-1}$ nicht alle 0, so gilt: $d = \text{ggT}(\text{ggT}(n_1, \ldots, n_{k-1}), n_k)$.

Beweis. (i)-(iii) Gelten, da die Mengen der positiven gemeinsamen Teiler auf beiden seiten jeweils gleich sind (Linke und rechte Seite haben stets dieselben gemeinsamen Teiler) und besagen, dass es nicht auf die Reihenfolge der Zahlen $n_1, \ldots, n_k$ ankommt und dass man Nullen und sich wiederholende Zahlen weglassen kann.

(iv) : Wegen Satz 1(ix) haben $n_1, \ldots, n_{k-1}, n_k$ und $n_1, \ldots, n_{k-1}, n_k + \sum_{i=1}^{k-1} x_i n_i$ dieselben gemeinsamen Teiler und daher denselben ggT.

(v) Sei $e := \text{ggT}\,(ln_1, \ldots, ln_k)$. Wir wollen zeigen, dass $e = l \cdot d$ ist, denn wenn sie sich gegenseitig teilen sind sie gleich.

1. Zeige $l \mid e$: Wegen $d \mid n_i \ (1 \leq i \leq k) \Rightarrow (ld) \mid (ln_i) \ (1 \leq i \leq k)$ $\overset{\text{Satz 5}}{\Rightarrow} (ld) \mid e$. Insbesondere gilt $\frac{e}{l} \in \mathbb{Z}$.
2. Zeige $ld \mid e$: Wegen $e \mid (ln_i) \ (1 \leq i \leq k) \Rightarrow \exists m_1, \ldots, m_k \in \mathbb{Z} : ln_i = m_i e \ (1 \leq i \leq k)$ $\Rightarrow n_i = \frac{e}{l} m_i \ (1 \leq i \leq k) \Rightarrow \frac{e}{l} \mid n_i \ (1 \leq i \leq k) \overset{\text{Satz 5}}{\Rightarrow} \frac{e}{l} \mid d \Rightarrow \exists m \in \mathbb{Z} : d = \frac{e}{l} m$ $\Rightarrow ld = em \Rightarrow e \mid (ld)$.

Wegen Satz 1(v) folgt $e = |e| = |ld| = |l||d| = |l|d$.

(vi) Wegen $d \mid n_i \ (1 \leq i \leq k)$ gilt $\frac{n_i}{d} \in \mathbb{Z} \ (1 \leq i \leq k)$ nicht alle 0.

Sei $f := \text{ggT}\,(\frac{n_1}{d}, \ldots, \frac{n_k}{d})$. Dann gilt: $d = \text{ggT}\,(n_1, \ldots, n_k) = \text{ggT}\,(d\frac{n_1}{d}, \ldots, d\frac{n_k}{d}) \overset{\text{(v)}}{=} d \cdot \text{ggT}\,(\frac{n_1}{d}, \ldots, \frac{n_k}{d}) = df \Rightarrow f = 1$.

(vii)
1. Sei $d' := \text{ggT}\,(\text{ggT}\,(n_1, \ldots, n_{k-1}), n_k)$ und $e := \text{ggT}\,(n_1, \ldots, n_{k-1}) \Rightarrow d' = \text{ggT}(e, n_k)$. Wegen $d' \mid e$ und $d' \mid n_k \Rightarrow d' \mid n_i \ (1 \leq i \leq k) \overset{\text{Satz 5}}{\Rightarrow} d' \mid d$.
2. Ebenso folgt aus $d \mid n_i \ (1 \leq i \leq k-1)$, dass $d \mid e$ und aus $d \mid e$ und $d \mid n_k$ folgt $d \mid d'$.

Und damit aus $d' \mid d \ \wedge \ d \mid d' \Rightarrow d = d'$.

□

Bemerkung Man kann $\text{ggT}\,(n_1, \ldots, n_k)$ folgendermaßen berechnen (o.B.d.A. kann man $n_i > 0$ für $1 \leq i \leq k$ voraussetzen, sowie dass $n_1, \ldots, n_k$ paarweise verschieden sind.) O.B.d.A. sei $n_1 = \min\{n_1, \ldots, n_k\}$. Führe Division mit Rest durch: $n_i = q_i n_1 + r_i$ mit $0 \leq r_i < n_1$ für $2 \leq i \leq k$. Wegen Satz 6(i) und (iv) gilt:

$$\text{ggT}\,(n_1, \ldots, n_k) = \text{ggT}\,(n_1, r_2, \ldots, r_k).$$

Wiederhole das, bis der Wert des ggT offensichtlich ist.

Beispiel
Bestimme $\text{ggT}\,(721, 613, 114)$:

$$\begin{aligned}
&\text{ggT}\,(721, 613, 114) = \text{ggT}\,(6 \cdot 114 + 37, 5 \cdot 114 + 43, 114) \\
&= \text{ggT}\,(37, 43, 114) = \text{ggT}\,(37, 1 \cdot 37 + 6, 3 \cdot 37 + 3) \\
&\quad = \text{ggT}\,(37, 3, 6) = \text{ggT}\,(12 \cdot 3 + 1, 2 \cdot 3, 3) \\
&\quad\quad = \text{ggT}\,(1, 0, 3) = 1
\end{aligned}$$

Bemerkung Satz 6(vii) ermöglicht es, durch wiederholte Anwendung von Satz 3 $x_1, \ldots, x_k \in \mathbb{Z}$ zu finden, sodass $x_1 n_1 + \ldots + x_k n_k = \text{ggT}(n_1, \ldots, n_k)$.

Beispiel
Zeige: $\text{ggT}(6, 10, 15) = 1$ und finde $x, y, z \in \mathbb{Z}$, sodass $6x + 10y + 15z = 1$.

- Rekursiv: Bestimme zuerst $\text{ggT}(6, 10)$:

$$\begin{aligned} 10 &= 1 \cdot 6 + 4 \\ 6 &= 1 \cdot 4 + 2 \\ 4 &= 2 \cdot 2 + 0 \\ \Rightarrow \text{ggT}(6, 10) = 2 &= 6 - 4 = 6 - (10 - 6) = 2 \cdot 6 - 10. \end{aligned}$$

- Bestimme $\text{ggT}(6, 10, 15) = \text{ggT}(\text{ggT}(6, 10), 15) = \text{ggT}(2, 15)$:
  $15 = 7 \cdot 2 + 1$, $2 = 2 \cdot 1 + 0 \Rightarrow 1 = 15 - 7 \cdot 2$
  $\Rightarrow 15 - 7 \cdot (2 \cdot 6 - 10) = \underbrace{(-14)}_{=x} \cdot 6 + \underbrace{7}_{=y} \cdot 10 + \underbrace{1}_{=z} \cdot 15.$
  Auch diese Lösung ist nicht eindeutig, da auch z. B.: $1 \cdot 6 + 1 \cdot 10 - 1 \cdot 15 = 1$ ist.

Definition „relativ prim oder teilerfremd“
$n_1, \ldots, n_k \in \mathbb{Z}$ heißen relativ prim (oder teilerfremd), wenn $\text{ggT}(n_1, \ldots, n_k) = 1$.

Definition „paarweise relativ prim“
$n_1, \ldots, n_k \in \mathbb{Z}$ heißen paarweise relativ prim (oder paarweise teilerfremd), wenn $\text{ggT}(n_i, n_j) = 1$ für $1 \leq i, j \leq k$, $i \neq j$.

Bemerkung Sind $n_1, \ldots, n_k$ paarweise relativ prim, so sind sie auch relativ prim, die Umkehrung gilt nicht!

Beispiel
Es sind $6, 10, 15$ relativ prim (d. h. $\text{ggT}(6, 10, 15) = 1$), aber
$\text{ggT}(6, 10) = 2$, $\text{ggT}(6, 15) = 3$, $\text{ggT}(10, 15) = 5$, d. h. $6, 10, 15$ sind nicht paarweise relativ prim.

Satz 7
Seien $m, m_1, m_2, n, n_1, n_2 \in \mathbb{Z}$ und $m, m_1, m_2 \neq 0$. Dann gilt

(i) Wenn $m \mid (n_1 n_2)$ und $\text{ggT}(m, n_1) = 1$, dann $m \mid n_2$.

(ii) Wenn $\text{ggT}(m_1, m_2) = 1$ und $m_1 \mid n$ und $m_2 \mid n$, dann $(m_1 \cdot m_2) \mid n$.

(iii) Wenn $\text{ggT}(m, n_1, n_2) = 1$, dann gilt $\text{ggT}(n_1, m) \cdot \text{ggT}(n_2, m) = \text{ggT}(n_1 \cdot n_2, m)$.

(iv) Wenn $\text{ggT}(m, n_1) = \text{ggT}(m, n_2) = 1$, dann $\text{ggT}(m, n_1 \cdot n_2) = 1$.

Beweis. (i) $\text{ggT}(m, n_1) = 1 \overset{\text{Satz 4}}{\Rightarrow} \exists x, y \in \mathbb{Z} : mx + n_1 y = 1 \Rightarrow mn_2 x + n_1 n_2 y = n_2$. Wegen $m \mid (n_1 n_2) \Rightarrow m \mid (mn_2 x + n_1 n_2 y)$, d. h. $m \mid n_2$.

(ii) $m_2 \mid n \Rightarrow m_2 \mid (m_1 \frac{n}{m_1})$. Da $\mathrm{ggT}\,(m_1, m_2) = 1 \overset{\text{(i)}}{\Rightarrow} m_2 \mid \frac{n}{m_1} \Rightarrow (m_1 m_2) \mid n$.

(iii) Setze $d_1 := \mathrm{ggT}\,(m, n_1)$, $d_2 := \mathrm{ggT}\,(m, n_2)$, $d := \mathrm{ggT}\,(n_1 n_2, m)$
$\overset{\text{Satz 4}}{\Rightarrow} \exists x_1, x_2, y_1, y_2 \in \mathbb{Z} : d_1 = x_1 n_1 + y_1 m, d_2 = x_2 n_2 + y_2 m$
$\Rightarrow d_1 d_2 = (x_1 n_1 + y_1 m)(x_2 n_2 + y_2 m) = (n_1 n_2)(x_1 x_2) + m(x_1 y_2 n_1 + x_2 y_1 n_2 + y_1 y_2 m)$
$\Rightarrow d \mid (d_1 d_2)$.
Zeige: $\mathrm{ggT}\,(d_1, d_2) = 1$. Setze $d' := \mathrm{ggT}\,(d_1, d_2) \Rightarrow d' \mid m$, $d' \mid n_1$, $d' \mid n_2 \Rightarrow$
$d' \mid \mathrm{ggT}\,(m, n_1, n_2) \Rightarrow d' = 1$.
Es gilt: $d_1 \mid d$, $d_2 \mid d$, da $\mathrm{ggT}\,(m, n_1, n_2) = 1 \overset{(ii)}{\Rightarrow} (d_1 d_2) \mid d$

(iv) $\mathrm{ggT}\,(m, n_1) = \mathrm{ggT}\,(m, n_2) = 1 \Rightarrow \mathrm{ggT}\,(m, n_1, n_2) = 1 \overset{(iii)}{\Rightarrow}$ Behauptung.

□

Kapitel 2

Primzahlen und kgV

Definition „Primzahl“
Sei $p \in \mathbb{Z}$, $p > 1$. Wenn p nur die Teiler $1, -1, p, -p$ besitzt, dann heißt p Primzahl.

Bemerkung Beachte, dass 1 keine Primzahl ist. 1 besitzt ein multiplikatives Inverses in $\mathbb{Z}$.

Lemma 8
Sei p Primzahl und $n \in \mathbb{Z}$. Dann sind äquivalent:

(i) $\text{ggT}(p, n) = 1$

(ii) $p \nmid n$.

Beweis. (i) $\Rightarrow$ (ii): $p \mid n \Rightarrow \text{ggT}(p, n) = p > 1$
(ii) $\Rightarrow$ (i): $ggT(p, n) > 1 \Rightarrow \exists d \in \mathbb{Z},\ d > 1 : d \mid p$ und $d \mid n \Rightarrow d = p$ und $p \mid n$. □

Satz 9
Es sei $p \in \mathbb{Z}$, $p > 1$. Dann sind äquivalent:

(i) p ist Primzahl

(ii) p ist prim: $\forall a, b \in \mathbb{Z} : p \mid (ab) \Rightarrow p \mid a$ oder $p \mid b$.

(iii) p ist irreduzibel: Wenn $p = xy$ (mit $x, y \in \mathbb{Z}$), dann gilt: $x \in \{1, -1\}$ oder $y \in \{1, -1\}$.

Beweis. (i) $\Rightarrow$ (ii): Wenn $p \mid a$, dann ist die Behauptung bewiesen.
Sei also $p \nmid a \overset{\text{Lemma 8}}{\Rightarrow} \text{ggT}(p, a) = 1 \overset{\text{Satz 7(i)}}{\Rightarrow} p \mid b$.
(ii) $\Rightarrow$ (iii): $p \mid (xy) \overset{\text{(ii)}}{\Rightarrow} p \mid x$ oder $p \mid y$. Falls $p \mid x \Rightarrow p \leq |x|$, andererseits gilt, sei $p = xy \Rightarrow p = |x||y| \geq |x| \Rightarrow p = |x| \Rightarrow x \in \{-p, p\}$ und $y \in \{-1, 1\}$, der andere Fall analog.
(iii) $\Rightarrow$ (i): Angenommen $m \mid p \Rightarrow \exists n \in \mathbb{Z} : p = mn \Rightarrow$ entweder $m \in \{-1, 1\}$ und daher $n \in \{-p, p\}$ oder $n \in \{-1, 1\}$ und $m \in \{-p, p\}$. Insbesondere ist $m \in \{-1, 1, -p, p\}$, also p Primzahl. □

Bemerkung

1. Bedingung (ii) und (iii) eignen sich gut zur Verallgemeinerung (Ringtheorie).
2. Aus (ii) folgt mit Induktion nach n: Ist p eine Primzahl, so gilt:
   $\forall a_1, \ldots, a_n \in \mathbb{Z} : p \mid (a_1 \cdots a_n) \Rightarrow \exists i \in \{1, \ldots, n\} : p \mid a_i$.

Lemma 10
Sei $n \in \mathbb{Z}$, $|n| \geq 2$, dann gibt es eine Primzahl, die n teilt.

Beweis. Betrachte die Menge $T_n = \{m \in \mathbb{Z} : m > 1, m \mid n\}$. Diese Menge $T_n \neq \emptyset$, da zumindest $|n| \in T_n$ und ebenfalls ist diese Menge nach Definition nach unten beschränkt $\Rightarrow \exists p := \min\{T_n\}$. Diese Zahl p ist nach Konstruktion eine Primzahl $p \in \mathbb{Z}, p > 1$, denn wäre p keine Primzahl, so würde ein $\exists d \in \mathbb{Z}, 1 < d < p$ mit $d \mid p \Rightarrow d \mid n$ und $d < p$, was ein Widerspruch zur Minimalität von p wäre. Schließlich gilt ebenfalls nach Konstruktion, dass $p \mid n$. □

Satz 11
Es gibt unendlich viele Primzahlen $\Leftrightarrow$ Es gibt keine größte Primzahl.

Beweis. Wir zeigen mit Induktion $\forall k \in \mathbb{N} : \exists k$ Primzahlen:
Induktionsanfang, k=1: 2 ist Primzahl, denn nur $\{-2, -1, 1, 2\}$ sind Teiler und weiter kann es nach Satz 1(iii) nicht geben.
Induktionsannahme: Wir haben schon k Primzahlen gefunden.
Induktionsschritt: Nach Lemma 10 gibt es eine Primzahl p mit der Eigenschaft $p \mid (p_1 \cdot \ldots \cdot p_k + 1) \Rightarrow p \notin \{p_1, \ldots, p_k\}$. Denn wäre $p \in \{p_1, \ldots, p_k\}$, so würde aus $p \mid (p_1 \cdot \ldots \cdot p_k + 1)$ und $p \in (p_1 \cdot \ldots \cdot p_k)$ folgen, dass $p \mid [(p_1 \cdot \ldots \cdot p_k + 1) - (p_1 \cdot \ldots \cdot p_k)]$, also $p \mid 1$. Dies ist aber ein Widerspruch zur Konstruktion von p in Lemma 10 $\Rightarrow p$ ist die $(k+1)$te Primzahl. □

Bemerkung Achtung bei diesem Beweis muss $(p_1 \cdot \ldots \cdot p_k + 1)$ keine Primzahl sein, z. B.: $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509$.

Satz 12 „Primfaktorzerlegung“
Sei $n \in \mathbb{Z}$, $n \geq 2$, dann lässt sich n als Produkt von (nicht notwendigerweise verschiedenen) Primzahlen darstellen, d. h. es gibt Primzahlen $p_1, \ldots, p_k$, sodass $n = p_1 \cdots p_k$. Diese Darstellung ist bis auf die Reihenfolge eindeutig, d. h. sind $n = p_1 \cdots p_k = q_1 \cdots q_l$ zwei Darstellungen von n als Produkt von Primzahlen, so ist $k = l$ und es gibt eine Permutation $\sigma \in S_k$, sodass $q_i = p_{\sigma(i)}$ für $1 \leq i \leq k$.

Beweis.
- *Existenz.* Wir zeigen mit Induktion nach n:
  Induktionsanfang, n=2: ist Primzahl, denn nur $\{-2, -1, 1, 2\}$ sind Teiler und weiter kann es nach Satz 1(iii) nicht geben.
  Sei nun $n > 2$. Falls n Primzahl ist, ist die Behauptung gezeigt.
  Induktionsannahme: n lässt sich als Produkt von Primzahlen darstellen.
  Angenommen, n ist keine Primzahl. Nach dem Beweis von Satz 11 ist $p_0 := \min\{T_n\}$ Primzahl und $p_0 \mid n$, d. h. $\exists m \in \mathbb{N} : n = p_0 m$. Induktionsschritt: Da $m < n$, gibt es nach Induktionsvoraussetzung Primzahlen $p_1, \ldots, p_r$, sodass $m = p_1 \cdot \ldots \cdot p_r \Rightarrow n = p_0 \cdot p_1 \cdot \ldots \cdot p_r$.

- *Eindeutigkeit.* Angenommen, es gibt ganze Zahlen größer gleich 2 mit zwei verschiedenen Darstellungen. Sei n die kleinste solche Zahl und $n = p_1 \cdots p_r = q_1 \cdots q_s$ die zwei Darstellungen. Dann teilt p_r die rechte Seite $\Rightarrow \exists i \in \{1, \ldots, s\} : p_r \mid q_i$. O.B.d.A. sei $i = s$, d. h. $p_r \mid q_s \Rightarrow p_r = q_s$ (beide sind ja Primzahlen) $\Rightarrow \frac{n}{p_r} = p_1 \cdots p_{r-1} = q_1 \cdots q_{s-1} < n$, d. h. $\frac{n}{p_r}$ würde ebenfalls zwei verschiedene Produktdarstellungen besitzen, was ein Widerspruch zur Minimalität von n ist.

□

Bemerkung 1. Die Folge der Primzahlen beginnt mit $2, 3, 5, 7, 11, 13, 17, 19, \ldots$. Wir schreiben daher oft p_n für die n-te Primzahl, d. h. $p_1 = 2$, $p_2 = 3$, $p_3 = 5, \ldots$

2. Für die Primfaktorzerlegung einer natürlichen Zahl n schreiben wir:

$$n = \prod_p p^{\alpha_p}$$

(p ist Index vor α). Dabei läuft p über alle Primzahlen, $\alpha_p \in \mathbb{Z}, \alpha_p \geq 0 \, \forall p$ Primzahlen und $\alpha_p = 0$ für alle bis auf endlich viele Primzahlen p.
Manchmal ist es bequemer, $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ zu schreiben mit $p_1, \ldots, p_k$ paarweise verschiedene Primzahlen und $\alpha_1, \ldots, \alpha_k \in \mathbb{Z}$ mit $\alpha_1, \ldots, \alpha_k > 0$ (oder $\alpha_1, \ldots, \alpha_k \geq 0$).

Bemerkung 1. Die Frage, wieviele Primzahlen es zwischen 1 und $x > 1$ gibt, beantwortet in erster Näherung der *„Primzahlsatz“* (bewiesen unabhängig voneinander 1896 von Hadamard und De la Vallee Poussin).
Für $x > 0$ sei $\pi(x) = |\{n \in \mathbb{N} | \, n \leq x, \, n \text{ ist Primzahl}\}|$. Dann gilt:

$$\pi(x) \sim \frac{x}{logx} \text{ für } x \to \infty \qquad \text{d. h.} \qquad \lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{logx}} = \lim_{x\to\infty} \frac{\pi(x) \cdot logx}{x} = 1.$$

Warnung: $x^2 + x \sim x^2$ für $x \to \infty$ (da $\lim_{x\to\infty} \frac{x^2+x}{x^2} = 1$), aber $(x^2 + x) - x^2 \to \infty$ für $x \to \infty$.
Äquivalent dazu gilt: $p_n \sim n \cdot logn$ für $n \to \infty$ d. h. $\lim_{n\to\infty} \frac{p_n}{n \cdot logn} = 1$.

2. Um die Primzahlen bis zu einer gegebenen Schranke zu finden, kann man das Sieb des Eratosthenes anwenden: Streiche nach Finden einer Primzahl p alle Vielfachen $2p, 3p, 4p, \ldots$. Um alle Primzahlen p bis $x > 1$ zu finden, reicht es, die Vielfachen von Primzahlen $< \sqrt{x}$ zu streichen.

Satz 13
Die Folge der Primzahlen enthält beliebig große Lücken, d. h.

$$\limsup_{n\to\infty} (p_{n+1} - p_n) = +\infty$$

Beweis. Für $k \in \mathbb{N}$, $k \geq 2$ betrachte die $k - 1$ Zahlen $k! + 2, k! + 3, \ldots, k! + k$.
Für $2 \leq d \leq k$ gilt: $d \mid (k! + d)$ und $1 < d < k! + d$, d. h. $k! + d$ ist keine Primzahl.
Ist p_n die größte Primzahl p mit $p < k! + 2$, so gilt: $p_{n+1} > k! + k$,
d. h. $p_{n+1} - p_n \geq (k! + k + 1) - (k! + 1) = k$. □

Bemerkung 1. Zwei Zahlen p, $p+2$, die beide Primzahlen sind, heißen Primzahlzwillinge. Die ersten Primzahlzwillinge sind: $(3,5),(5,7),(11,13),(17,19),\ldots$
Es ist eine unbewiesene Vermutung, dass es unendlich viele Primzahlzwillinge gibt, d. h.

$$\liminf_{n\to\infty}(p_{n+1}-p_n)=2.$$

2. Ebenfalls unbewiesen ist die GOLDBACHsche Vermutung: Jede gerade Zahl ≥ 4 lässt sich als Summe zweier Primzahlen darstellen $(4=2+2, 6=3+3, 8=5+3, 10=5+5,\ldots)$

Satz 14
Es gibt unendlich viele Primzahlen der Gestalt $4k+3$ $(k\in\mathbb{Z},\ k\geq 0)$.

Beweis. Vorbemerkung: Das Produkt zweier Zahlen der Gestalt $4l+1$ bzw. $4l+3$ ist von der Gestalt $4k+1$:

$$(4l+1)(4m+1)=16lm+4l+4m+1=4(4lm+l+m)+1$$
$$(4l+3)(4m+3)=16lm+12l+12m+9=4(4lm+3l+3m+2)+1$$

Angenommen, es gäbe nur endlich viele Primzahlen $p_1,\ldots,p_s$ der Gestalt $4k+3$. Betrachte $N:=p_1^2\cdots p_s^2+2$. Nach der Vorbemerkung hat N die Gestalt $4k+3$. Sei $N=q_1\cdots q_r$ die Primfaktorzerlegung von N. Hätten $q_1,\ldots,q_r$ alle die Gestalt $4k+1$, so würde das auch für N gelten, Widerspruch! Also $\exists j\in\{1,\ldots,r\}: q_j$ hat eine andere Gestalt. Da $q_j=4k$ und $q_j=4k+2$ als Primzahlen unmöglich sind, muss q_j die Gestalt $4k+3$ haben.
$\Rightarrow \exists i\in\{1,\ldots,s\}$ mit $q_j=p_i \Rightarrow q_j \mid N$ und $q_j \mid (p_1^2\cdot\ldots\cdot p_s^2) \Rightarrow q_j \mid (N-p_1^2\cdot\ldots\cdot p_s^2)$, also $q_j \mid 2$, Widerspruch! □

Bemerkung Seien $a,d\in\mathbb{N}$. Wenn die arithmetische Progression $a+d, 2a+d, 3a+d,\ldots$ unendlich viele Primzahlen enthält, muss offenbar $\mathrm{ggT}\,(a,d)=1$ gelten.
Allgemein gilt der DIRICHLETsche Primzahlsatz (1837):
Wenn $\mathrm{ggT}\,(a,d)=1$, dann gibt es unendlich viele Primzahlen der Gestalt $ak+d$ (mit $k\in\mathbb{N}$).
Für viele Spezialfälle (spezielle Werte von a und d) kann man elementare Beweise wie oben bei Satz 14 angeben. Die allgemeine Aussage beweist man mit Methoden der analytischen Zahlentheorie.

Satz 15
Seien $k,n\in\mathbb{Z}$.

(i) Wenn die Zahl 2^k+1 (mit $k\geq 1$) eine Primzahl ist, dann muss k die Gestalt $k=2^n$ (mit $n\geq 0$) haben.

(ii) Wenn die Zahl 2^k-1 (mit $k\geq 2$) eine Primzahl ist, muss k Primzahl sein.

Beweis. (i) Angenommen, $k=ab$ mit $a,b\in\mathbb{N}$ und $a>1$ ungerade (alle anderen Primzahlen außer 2 sind ungerade!). Dann gilt:

$$2^k+1=2^{ab}+1=(2^b+1)(2^{(a-1)b}-2^{(a-2)b}+2^{(a-3)b}-+\ldots-2^b+1)$$
$$=(2^b+1)\sum_{i=1}^{a}(-1)^{i+1}2^{(a-i)b}$$

d. h. $2^k + 1$ ist keine Primzahl (Primzahlen sind irreduzibel), da $(2^b + 1) \mid (2^k + 1)$ und $1 < 2^b + 1 < 2^k + 1$.

(ii) Angenommen, $k = ab$ für $a, b \in \mathbb{N}$ mit $1 < a, b < k$. Dann gilt:

$$\begin{aligned} 2^k - 1 = 2^{ab} - 1 &= (2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + \ldots + 2^a + 1) \\ &= (2^a - 1) \sum_{i=0}^{b-1} 2^{ia}, \end{aligned}$$

d. h. $2^k - 1$ ist keine Primzahl, da $(2^a - 1) \mid (2^k - 1)$ und $1 < 2^a - 1 < 2^k - 1$.

□

Bemerkung 1. Eine Primzahl der Gestalt $2^{2^n} + 1$ heißt FERMATsche Primzahl. $2^{2^n} + 1$ ist Primzahl für $0 \leq n \leq 4$ (man erhält so die Primzahlen $3, 5, 17, 25$ und 65537) aber $2^{2^5} + 1 = 614 \cdot 6700417$ ist keine Primzahl. Es ist unbekannt, ob es unendlich viele Fermatsche Primazhlen gibt.

2. Eine Primzahl der Gestalt $2^p - 1$ heißt MERSENNEsche Primzahl. $2^p - 1$ ist Primzahl für $p \in \{2, 3, 5, 7\}$ (man erhält so die Primzahlen $3, 7, 31, 127$) aber $2^{11} - 1 = 2047 = 23 \cdot 89$. Es ist unbekannt, ob es unendlich viele Mersennesche Primzahlen gibt. Für Zahlen der Gestalt $2^p - 1$ existiert aber ein besonders einfacher Primzahltest. Darum ist die größte bekannte Primzahl oft eine Mersennesche Primzahl.

Lemma 16
Haben $a, b \in \mathbb{N}$ die Primfaktorzerlegungen $a = \prod_p p^{\alpha_p}$, $b = \prod_p p^{\beta_p}$, so sind äquivalent:

(i) $a \mid b$

(ii) $\alpha_p \leq \beta_p \; \forall p$ Primzahlen.

Beweis. $a \mid b \Leftrightarrow \exists c \in \mathbb{N} : b = ac$. Sei $c = \prod_p p^{\gamma_p}$ Primfaktorzerlegung, dann gilt:
$b = ac \Leftrightarrow \beta_p = \alpha_p + \gamma_p \; \forall p \Leftrightarrow \alpha_p \leq \beta_p \; \forall p$ □

Satz 17
Haben $a_1, \ldots, a_n \in \mathbb{N}$ die Primfaktorzerlgung $a_i = \prod_p p^{\alpha_{ip}}$ (für $1 \leq i \leq n$), so besitzt $\mathrm{ggT}(a_1, \ldots, a_n)$ die Primfaktorzerlegung

$$\mathrm{ggT}(a_1, \ldots, a_n) = \prod_p p^{\min\{\alpha_{1p}, \ldots, \alpha_{np}\}}$$

Beweis. Sei $d := \prod_p p^{\min\{\alpha_{1p}, \ldots, \alpha_{np}\}}$.

1. d ist gemeinsamer Teiler ($d \mid a_i$): Da $\min\{\alpha_{1p}, \ldots, \alpha_{np}\} \leq \alpha_{ip} \; \forall i \in \{1, \ldots, n\} \; \forall p$ gilt $d \mid a_i$ $(1 \leq i \leq n)$.

2. d ist größter gemeinsamer Teiler ($b \mid d$): Wenn $b \mid a_i$ $(1 \leq i \leq n)$ für ein $b \in \mathbb{N}$, $b = \prod_p p^{\beta_p}$, dann gilt:
$\beta_p \leq \alpha_{ip} \; \forall i \in \{1, \ldots, n\} \; \forall p \Rightarrow \beta_p \leq \min\{\alpha_{1p}, \ldots, \alpha_{np}\} \; \forall p$
$\Rightarrow b \mid d \overset{\text{Satz } 5}{\Rightarrow} d = \mathrm{ggT}(a_1, \ldots, a_n)$.

□

Bemerkung Wichtigster Spezialfall: Wenn $a = \prod_p p^{\alpha_p}$ und $b = \prod_p p^{\beta_p}$, dann ist

$$\text{ggT}\,(a,b) = \prod_p p^{\min\{\alpha_p,\beta_p\}}$$

Beispiel
$a = 8100 = 2^2 3^4 5^2, b = 24696 = 2^3 3^2 7^3 \Rightarrow \text{ggT}\,(a,b) = 2^2 3^2 5^0 7^0 = 36.$

Definition „kleinstes gemeinsames Vielfaches“
Sind $n_1, \ldots, n_k \in \mathbb{Z}$, dann heißt $m \in \mathbb{Z}$ gemeinsames Vielfaches von $n_1, \ldots, n_k$ wenn $n_i \mid m$ für $i = 1, \ldots, k$. Sind $n_1, \ldots, n_k \neq 0$, dann ist die Menge der positiven gemeinsamen Vielfachen $\neq \emptyset$ (da sie $|n_1 \cdots n_k| = |n_1| \cdots |n_k|$ enthält) und nach unten beschränkt. Man definiert daher (für $n_1, \ldots, n_k \neq 0$):

$$\text{kgV}(n_1, \ldots, n_k) = \min\{m \in \mathbb{N} : n_i \mid m,\ 1 \leq i \leq k\}$$

Satz 18
Seien $n_1, \ldots, n_k \in \mathbb{Z} \setminus \{0\}$ und $m \in \mathbb{Z} \setminus \{0\}$, $m > 0$. Dann sind äquivalent:

(i) $m = \text{kgV}\,(n_1, \ldots, n_k)$

(ii) $n_i \mid m$ für $1 \leq i \leq k$ und $n_i \mid m'$ für $1 \leq i \leq k$. Dann $m \mid m'$.

Beweis. (i) $\Rightarrow$ (ii): Wenn $m = \text{kgV}\,(n_1, \ldots, n_k)$, dann $n_i \mid m$ für $1 \leq i \leq k$. Es gelte $n_i \mid m'$ für $1 \leq i \leq k$. Nach Satz 2 $\exists q, r \in \mathbb{Z} : m' = qm + r$, $0 \leq r < m$. Wegen $n_i \mid m$ und $n_i \mid m'$ folgt $n_i \mid r$ für $1 \leq i \leq k$. Nach Definition von m folgt $r = 0$, d. h. $m \mid m'$.
(ii) $\Rightarrow$ (i): m ist ein gemeinsames Vielfaches von $n_1, \ldots, n_k$. Wenn $m' \in \mathbb{N}$ und $n_i \mid m'$ für $1 \leq i \leq k$, dann $m \mid m'$ und daher $m \leq m'$. □

Satz 19
Sind $a_1, \ldots, a_n \in \mathbb{N}$ mit Primfaktorzerlegungen $a_i = \prod_p p^{\alpha_{ip}}$ $(1 \leq i \leq k)$, so besitzt $\text{kgV}\,(a_1, \ldots, a_n)$ die Primfaktorzerlegung

$$\text{kgV}\,(a_1, \ldots, a_n) = \prod_p p^{\max\{\alpha_{1p}, \ldots, \alpha_{np}\}}$$

Beweis. Sei $k = \prod_p p^{\max\{\alpha_{1p}, \ldots, \alpha_{np}\}}$. Da $\alpha_{ip} \leq \max\{\alpha_{1p}, \ldots, \alpha_{np}\}$ $\forall i \in \{1, \ldots, n\}$ $\forall p$ Primzahl gilt: $a_i \mid k$ $(1 \leq i \leq n)$. Wenn $a_i \mid m$ $(1 \leq i \leq n)$ für ein $m \in \mathbb{N}$, $m = \prod_p p^{\mu_p}$, dann $\alpha_{ip} \leq \mu_{ip}$ $\forall i \in \{1, \ldots, n\}$ $\forall p \Rightarrow \max\{\alpha_{1p}, \ldots, \alpha_{np}\} \leq \mu_p$ $\forall p \Rightarrow k \mid m \overset{\text{Satz } 18}{\Rightarrow} k = \text{kgV}\,(a_1, \ldots, a_n)$. □

Satz 20
Es seien $n_1, \ldots, n_k$, $m_1, \ldots, m_k \in \mathbb{N}$ mit der Eigenschaft $n_i m_i = a$ für $1 \leq i \leq k$. Dann gilt:

$$\text{kgV}\,(n_1, \ldots, n_k)\,\text{ggT}\,(m_1, \ldots, m_k) = a$$

Beweis. $n_i = \prod_p p^{\nu_{ip}}$, $m_i = \prod_p p^{\mu_{ip}}$ $(1 \leq i \leq k)$ und $a = \prod_p p^{\alpha_p}$ seien Primfaktorzerlegungen.
Da $m_i n_i = a \Rightarrow \nu_{ip} + \mu_{ip} = \alpha_p \; \forall i \in \{1, \ldots, k\} \; \forall p \Rightarrow \mu_{ip} = \alpha_p - \nu_{ip} \; \forall i \in \{1, \ldots, k\} \; \forall p$.
Wir betrachten jetzt

$$\begin{aligned}
&\max\{\nu_{1p}, \ldots, \nu_{kp}\} + \min\{\mu_{1p}, \ldots, \mu_{kp}\} \\
&= \max\{\nu_{1p}, \ldots, \nu_{kp}\} + \min\{\alpha_p - \nu_{1p}, \ldots, \alpha_p - \nu_{kp}\} \\
&= \max\{\nu_{1p}, \ldots, \nu_{kp}\} + \alpha_p - \max\{\nu_{1p}, \ldots, \nu_{kp}\} = \alpha_p \; \forall p \text{ Primzahl} \\
&\Rightarrow \operatorname{kgV}(n_1, \ldots, n_k) \operatorname{ggT}(m_1, \ldots, m_k) = \prod_p p^{\max\{\nu_{1p}, \ldots, \nu_{kp}\}} \prod_p p^{\min\{\mu_{1p}, \ldots, \mu_{kp}\}} = \prod_p p^{\alpha_p} = a
\end{aligned}$$

□

Korollar 21
Seien $n_1, \ldots, n_k \in \mathbb{N}$ und $N_i := \frac{n_1 \cdots n_k}{n_i}$ für $1 \leq i \leq k$. Dann gilt:

(i) $\operatorname{kgV}(n_1, \ldots, n_k) \operatorname{ggT}(N_1, \ldots, N_k) = n_1 \cdots n_k$.

(ii) Sind $n_1, n_2 \in \mathbb{N}$, so gilt:

$$\operatorname{kgV}(n_1, n_2) \operatorname{ggT}(n_1, n_2) = n_1 n_2$$

Beweis. (i) Folgt aus Satz 20 wegen $n_i N_i = n_1 \cdots n_k$ für $1 \leq i \leq k$

(ii) Folgt aus (i) als Spezialfall $k = 2$ (da $n_1 = N_2$, $n_2 = N_1$).

□

Korollar 22
Sei $k \geq 2$ und $n_1, \ldots, n_k \in \mathbb{N}$. Dann sind äquivalent:

(i) $n_1, \ldots, n_k$ sind paarweise relativ prim

(ii) $\operatorname{kgV}(n_1, \ldots, n_k) = n_1 \cdots n_k$

Beweis. Es gilt: $n_1, \ldots, n_k$ sind paarweise relativ prim $\Leftrightarrow \operatorname{ggT}(N_1, \ldots, N_k) = 1$.
Angenommen $n_1, \ldots, n_k$ sind nicht paarweise relativ prim $\Leftrightarrow$
$\exists p$ Primzahl $\exists i, j \in \{1, \ldots, k\}$, $i \neq j : p \mid n_i \wedge p \mid n_j \overset{(*)}{\Leftrightarrow} \exists p$ Primzahl, $p \mid N_1, \ldots, p \mid N_k \Leftrightarrow$ $\operatorname{ggT}(N_1, \ldots, N_k) > 1$.
Die Implikation $(\Rightarrow)$ in (*) ist klar.
Es gelte $p \mid N_1, \ldots, p \mid N_k$. Da $p \mid N_1 \Rightarrow p \mid (n_2 \cdots n_k) \Rightarrow \exists i \in \{2, \ldots, k\} : p \mid n_i$. Wegen $p \mid N_i \Rightarrow p \mid (n_1 \cdots n_{i-1} n_{i+1} \cdots n_k) \Rightarrow \exists j \in \{1, \ldots, k\}$, $j \neq i : p \mid n_j \Rightarrow \operatorname{ggT}(n_i, n_j) > 1$.
Die Behauptung folgt aus Korollar 21(i). □

Kapitel 3

Kongruenzen

Definition „kongruent modulo m“
Es seien $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$. Man sagt, a und b seien kongruent modulo m, wenn $m \mid (a-b)$. Man schreibt dafür $a \equiv b \mod m$ oder kurz $a \equiv b\,(m)$. Die Zahl m heißt dabei Modul. Falls $m \nmid (a-b)$, so schreibt man a nicht kongruent $b \mod m$ und sagt, a und b seien inkongruent modulo m.

Beispiel
$6 \equiv 24 \mod 9$, da $9 \mid (6-24)$, also $9 \mid (-18)$.
$14 \equiv -1 \mod 5$, da $5 \mid (14-(-1))$, also $5 \mid 15$.

Lemma 23
Seien $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$. Äquivalent sind:

(i) $a \equiv b \mod m$

(ii) Bei Division durch m haben a und b denselben Rest.

Beweis. Seien $a = qm + r$, $b = \overline{q}m + \overline{r}$ mit $0 \leq r, \overline{r} < m$.
(i) $\Rightarrow$ (ii): $a - b = (q-\overline{q})m + r - \overline{r}$. Da $m \mid (a-b) \Rightarrow m \mid (r-\overline{r})$. Wegen $-m < r - \overline{r} < m$ folgt $r - \overline{r} = 0$, d. h. $r = \overline{r}$.
(ii) $\Rightarrow$ (i): Nach Voraussetzung ist $r = \overline{r} \Rightarrow a - b = (q-\overline{q})m \Rightarrow m \mid (a-b)$. □

Lemma 24
Kongruent modulo $m \in \mathbb{N}$ zu sein ist eine Äquivalenzrelation, d. h. sie ist

(i) <u>reflexiv:</u> $a \equiv a \mod m \; \forall a \in \mathbb{Z}$,

(ii) <u>symmetrisch:</u> $a \equiv b \mod m \Rightarrow b \equiv a \pmod m \; \forall a, b \in \mathbb{Z}$ und

(iii) <u>transitiv:</u> $a \equiv b \mod m$, $b \equiv c \pmod m \Rightarrow a \equiv c \pmod m \; \forall a, b, c \in \mathbb{Z}$

Beweis. (i) Folgt aus $m \mid 0$

(ii) $m \mid (a-b) \Rightarrow m \mid (-1)(a-b)$, d. h. $m \mid (b-a)$

(iii) $m \mid (a-b),\ m \mid (b-c) \Rightarrow m \mid ((a-b)+(b-c))$, d. h. $m \mid (a-c)$

□

Bemerkung Die Äquivalenzklassen der in Lemma 24 behandelten Äquivalenzrelation heißen Restklassen modulo m.

Satz 25 „Rechenregeln für die Restklassen modulo m“
Es seien $a, b, c, d, k \in \mathbb{Z}$, $k \neq 0$ und $m, n \in \mathbb{N}$. Dann gelten:

(i) $a \equiv b \mod m$ und $c \equiv d \pmod m \Rightarrow a + c \equiv b + d \pmod m$.

(ii) $a \equiv b \mod m$ und $c \equiv d \pmod m \Rightarrow ac \equiv bd \pmod m$

(iii) $a \equiv b \mod m$ und $k \mid m \Rightarrow a \equiv b \pmod{|k|}$

(iv) $a \equiv b \mod m \Rightarrow ka \equiv kb \pmod{(|k|m)}$

(v) $ka \equiv kb \mod m \Rightarrow a \equiv b \pmod{\frac{m}{\mathrm{ggT}\,(k,m)}}$

(vi) $a \equiv b \mod m$ und $a \equiv b \pmod n \Rightarrow a \equiv b \pmod{\mathrm{kgV}\,(m,n)}$

Beweis. (i) $m \mid (a-b)$ und $m \mid (c-d) \Rightarrow m \mid ((a-b)+(c-d))$, d. h. $m \mid ((a+c)-(b+d))$

(ii) $m \mid (a-b)$ und $m \mid (c-d) \Rightarrow m \mid ((a-b)c+(c-d)b)$, d. h. $m \mid (ac-bd)$

(iii) $m \mid (a-b)$ und $k \mid m \Rightarrow k \mid (a-b) \Rightarrow |k| \mid (a-b)$

(iv) $m \mid (a-b) \Rightarrow |k|m \mid k(a-b)$, d. h. $|k|m \mid (ka-kb)$

(v) Sei $d = \mathrm{ggT}\,(k,m)$, $m \mid (ka-kb) \Rightarrow \exists l \in \mathbb{Z} : k(a-b) = lm \Rightarrow \frac{k}{d}(a-b) = l\frac{m}{d}$. Nach Satz 6(vi) ist: $\mathrm{ggT}\,(\frac{k}{d}, \frac{m}{d}) = 1$. Aus $\frac{m}{d} \mid \frac{k}{d}(a-b)$ folgt wegen Satz 7(i), dass $\frac{m}{d} \mid (a-b)$.

(vi) $m \mid (a-b)$ und $n \mid (a-b) \overset{\text{Satz } 18}{\Rightarrow} \mathrm{kgV}\,(m,n) \mid (a-b)$

□

Korollar 26
Seien $m, n \in \mathbb{N}$. Dann gelten:

(i) $\forall a, b, c \in \mathbb{Z} : a \equiv b \mod m \Rightarrow a + c \equiv b + c \mod m$ und $ac \equiv bc \mod m$

(ii) $\forall a_1, \ldots, a_k, b_1, \ldots, b_k \in \mathbb{Z}$: Wenn $a_i \equiv b_i \mod m$ für $1 \leq i \leq k$, dann

$$\sum_{i=1}^{k} a_i \equiv \sum_{i=1}^{k} b_i \mod m \qquad \text{und} \qquad \prod_{i=1}^{k} a_i \equiv \prod_{i=1}^{k} b_i \mod m$$

Insbesondere gilt $\forall a, b \in \mathbb{Z}$, $\forall k \in \mathbb{N}$: Wenn $a \equiv b \mod m$, dann $a^k \equiv b^k \mod m$

(iii) $\forall a, b \in \mathbb{Z} : \forall f \in \mathbb{Z}[X] :$ Wenn $a \equiv b \mod m$, dann $f(a) \equiv f(b) \mod m$

(iv) $\forall a, b \in \mathbb{Z} : \forall k \in \mathbb{N} :$ Wenn $ka \equiv kb \mod m$ und $\mathrm{ggT}\,(k,m) = 1$, dann $a \equiv b \mod m$

(v) $\forall a, b \in \mathbb{Z}$: Wenn $a \equiv b \mod m$, $a \equiv b \mod n$ und $\mathrm{ggT}\,(m,n) = 1$, dann $a \equiv b \mod mn$

Beweis. (i) Folgt aus Satz 25(i) bzw. (ii), da $c \equiv c \mod m$.

(ii) Folgt aus Satz 25(i) bzw. (ii) mit Induktion nach k.

(iii) Folgt aus Satz 25(i) bzw. (ii).

(iv) Folgt aus Satz 25(v).

(v) Da $\text{ggT}(m,n) = 1$ ist, folgt $\text{kgV}\,(m,n) = mn$ (wegen Korollar 22 und $a \equiv b \mod mn$ nach Satz 25(vi)).

□

Korollar 27
Sei $m \in \mathbb{N}$ mit Primfaktorzerlegung $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ ($p_1, \ldots, p_k$ paarweise verschieden, $\alpha_1, \ldots, \alpha_k \in \mathbb{N}$). Für $a, b \in \mathbb{Z}$ sind äquivalent:

(i) $a \equiv b \mod m$

(ii) $a \equiv b \mod p_i^{\alpha_i}$ für $1 \leq i \leq k$

Beweis. (i) $\Rightarrow$ (ii): Aus $m \mid (a-b)$ und $p_i^{\alpha_i} \mid m$ folgt $p_i^{\alpha_i} \mid (a-b)$ für $1 \leq i \leq k$.
(ii) $\Rightarrow$ (i): Wegen $\text{ggT}\,(p_i, p_j) = 1$ für $1 \leq i, j \leq k$, $i \neq j$, folgt: $\text{ggT}\,(p_1^{\alpha_1} \cdots p_{i-1}^{\alpha_{i-1}}, p_i^{\alpha_i}) = 1$ für $2 \leq i \leq k$. Die Behauptung folgt aus Korollar 26(v) mit Induktion. □

Satz 28 „über die dekadischen Kongruenzen“
Die Zahl $n \in \mathbb{N}$ habe die Darstellung

$$n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_1 \cdot 10 + a_0$$

(mit Ziffern $a_k, a_{k-1}, \ldots, a_1, a_0 \in \{0, 1, 2, \ldots, 9\}$) im dekadischen System (wofür man $n = a_k a_{k-1} \cdots a_1 a_0$ schreibt). Dann gelten:

(i) $n \equiv a_0 \mod 2$

(ii) $n \equiv a_0 + a_1 + \ldots + a_k \mod 3$

(iii) $n \equiv a_0 + 10a_1 \mod 4$

(iv) $n \equiv a_0 \mod 5$

(v) $n \equiv a_0 + 10a_1 + 10^2 a_2 \mod 8$

(vi) $n \equiv a_0 + a_1 + \ldots + a_k \mod 9$

(vii) $n \equiv a_0 - a_1 + a_2 - \ldots + \ldots + (-1)^k a_k \mod 11$

Beweis. (i) $10 \equiv 0 \mod 2 \Rightarrow 10^i \equiv 0^i \mod 2$ für $1 \leq i \leq k \Rightarrow$
$n = a_0 + 10a_1 + \ldots + 10^k a_k \equiv a_0 + 0a_1 + \ldots + 0a_k = a_0 \mod 2$

(ii) $10 \equiv 1 \mod 3 \Rightarrow 10^i \equiv 1^i = 1 \mod 3$ für $1 \leq i \leq k \Rightarrow$
$n = a_0 + 10a_1 + \ldots + 10^k a_k \equiv a_0 + 1a_1 + \ldots + 1a_k = a_0 + a_1 + \ldots + a_k \mod 3$

(iii) $10^2 \equiv 0 \mod 4 \Rightarrow 10^i = 10^{i-2}10^2 \equiv 10^{i-2}0 \equiv 0 \mod 4$ für $2 \leq i \leq k \Rightarrow$
$n = a_0 + 10a_1 + \ldots + 10^k a_k \equiv a_0 + 10a_1 + 0a_2 + \ldots + 0a_k = a_0 + 10a_1 \mod 4$

(iv) $10 \equiv 0 \mod 5$ und weiter analog zu (i)

(v) $10^3 \equiv 0 \mod 8 \Rightarrow 10^i \equiv 0 \mod 8$ für $3 \leq i \leq k$ und weiter analog wie (iii)

(vi) $10 \equiv 1 \mod 9 \Rightarrow 10^i \equiv 1 \mod 9$ für $1 \leq i \leq k$ und weiter analog wie (ii)

(vii) $10 \equiv -1 \mod 11 \Rightarrow 10^i \equiv (-1)^i \mod 11$ für $1 \leq i \leq k \Rightarrow$
$n = a_0 + 10a_1 + 10^2 a_2 + \ldots + 10^k a_k \equiv a_0 - a_1 + a_2 - \ldots + \ldots + (-1)^k a_k \mod 11$

□

Korollar 29 „Teilbarkeitsregeln“
$n \in \mathbb{N}$ habe die Darstellung $n = a_k 10^k + a_{k-1}10^{k-1} + \ldots + 10a_1 + a_0$ (mit $a_k, \ldots, a_0 \in \{0, \ldots, 9\}$) im dekadischen System. Dann gelten:

(i) $2 \mid n \Leftrightarrow 2 \mid a_0 \ (\Leftrightarrow a_0 \in \{0, 2, 4, 6, 8\})$

(ii) $3 \mid n \Leftrightarrow 3 \mid (a_0 + a_1 + \ldots + a_k)$

(iii) $4 \mid n \Leftrightarrow 4 \mid (a_0 + 10a_1)$

(iv) $5 \mid n \Leftrightarrow 5 \mid a_0 \ (\Leftrightarrow a_0 \in \{0, 5\})$

(v) $8 \mid n \Leftrightarrow 8 \mid (a_0 + 10a_1 + 10^2 a_2)$

(vi) $9 \mid n \Leftrightarrow 9 \mid (a_0 + a_1 + \ldots + a_k)$

(vii) $11 \mid n \Leftrightarrow 11 \mid (a_0 - a_1 + a_2 - \ldots + \ldots + (-1)^k a_k)$

Beweis. $n = (n - a_0) + a_0$. Nach Satz 28(i) gilt $2 \mid (n - a_0)$, woraus die Behauptung folgt. (ii)-(vii) folgen analog aus Satz 28(ii)-(vii). □

Bemerkung Teilbarkeit bezüglich zusammengesetzter Teiler kann man auf Teilbarkeit bezüglich Teiler zurückführen, die paarweise relativ prim sind.

Beispiel
$6 \mid n \Leftrightarrow 2 \mid n$ und $3 \mid n \Leftrightarrow 2 \mid a_0$ und $3 \mid (a_0 + a_1 + \ldots + a_k)$.
Sei $n = 9723438$. $2 \mid n$ (da $2 \mid 8$), $3 \mid n$ (da $3 \mid 36$), $4 \nmid n$ (da $4 \nmid 38$), $5 \nmid n$ (da $5 \nmid 8$), $6 \mid n$ (da $2 \mid n$ und $3 \mid n$), $8 \nmid n$ (da $4 \nmid n$), $9 \mid n$ (da $9 \mid 36$), $11 \nmid n$ (da $11 \nmid 10$).

Definition „lineare diophantische Gleichung“
Es seien $a_1, \ldots, a_k, c \in \mathbb{Z}$. Eine Gleichung der Form $a_1x_1 + \ldots + a_kx_k = c$, für die man Lösungen $(x_1, \ldots, x_k) \in \mathbb{Z}^k$ sucht, heißt lineare diophantische Gleichung.

Bemerkung Allgemein versteht man unter einer diophantischen Gleichung eine polynomiale Gleichung mit ganzzahligen Koeffizienten, für die ganzzahlige Lösungen gesucht werden.

Lemma 30
Es seien $a, b \in \mathbb{Z}$ und $a, b \neq 0$. Dann sind äquivalent:

(i) Die lineare diophantische Gleichung $ax + by = c$ ist lösbar.

(ii) $\text{ggT}(a, b) \mid c$.

Beweis. Es sei $d = \text{ggT}(a, b)$.
(i) $\Rightarrow$ (ii) Es sei $(x_0, y_0) \in \mathbb{Z}^2$ Lösung, d. h. $ax_0 + by_0 = c$. Wegen $d \mid a$ und $d \mid b$ folgt $d \mid c$.
(ii) $\Rightarrow$ (i) Nach Satz 4 $\exists \overline{x}, \overline{y} \in \mathbb{Z} : a\overline{x} + b\overline{y} = d \Rightarrow a(\frac{c}{d}\overline{x}) + b(\frac{c}{d}\overline{y}) = \frac{c}{d}d = c$, d. h. $(\frac{c}{d}\overline{x}, \frac{c}{d}\overline{y}) \in \mathbb{Z}^2$ ist Lösung von $ax + by = c$. □

Definition „Lineare Kongruenz“
Sei $m \in \mathbb{N}$ und $a, b \in \mathbb{Z}$. Man bezeichnet $ax \equiv b \mod m$ als lineare Kongruenz. Gesucht sind dabei $x \in \mathbb{Z}$, die dieser Kongruenz genügen. Ist x_0 eine Lösung (d. h. $ax_0 \equiv b \mod m$) und $x_1 \equiv x_0 \mod m$, so ist x_1 ebenfalls Lösung (da $ax_1 \equiv ax_0 \mod m$), weshalb man sich für modulo m inkongruente Lösungen interessiert.

Satz 31
Seien $m \in \mathbb{N}$ und $a, b \in \mathbb{Z}$. Die lineare Kongruenz $ax \equiv b \mod m$ ist genau dann lösbar, wenn $\text{ggT}(a, m) \mid b$. Gilt $\text{ggT}(a, m) \mid b$, so gibt es genau $\text{ggT}(a, m)$ modulo m inkongruente Lösungen.

Beweis. Falls $a = 0$, so ist $ax \equiv b \mod m$ lösbar $\Leftrightarrow b \equiv 0 \mod m \Leftrightarrow m \mid b \Leftrightarrow \text{ggT}(a, m) \mid b$.
Sei nun $a \neq 0$. Dann gilt: $ax \equiv b \mod m$ lösbar $\Leftrightarrow \exists x_0 \in \mathbb{Z} : ax_0 \equiv b \mod m \Leftrightarrow$
$\exists x_0 \in \mathbb{Z} : m \mid (ax_0 - b) \Leftrightarrow \exists x_0, y_0 \in \mathbb{Z} : ax_0 - b = my_0 \Leftrightarrow \exists x_0, y_0 \in \mathbb{Z} : ax_0 - my_0 = b \Leftrightarrow$
die lineare diophantische Gleichung $ax + my = b$ ist lösbar $\overset{\text{Lemma 30}}{\Leftrightarrow} \text{ggT}(a, m) \mid b$.

Sei nun $ax \equiv b \mod m$ lösbar (d. h. $\text{ggT}(a, m) \mid b$) und x_0 eine Lösung. Es bezeichne $d := \text{ggT}(a, m)$.
Behauptung: Dann sind $x_0 + k\frac{m}{d}$ mit $0 \leq k \leq d - 1$, d. h.

$$x_0,\ x_0 + \frac{m}{d},\ x_0 + 2\frac{m}{d}, \ldots,\ x_0 + (d-1)\frac{m}{d}$$

modulo m paarweise inkongruente Lösungen von $ax \equiv b \mod m$. Wegen

$$a(x_0 + k\frac{m}{d}) = ax_0 + \underbrace{\frac{a}{d}km}_{\equiv 0 \mod m} \equiv ax_0 \equiv b \mod m \quad \text{für} \quad 0 \leq k \leq d-1$$

ist $x_0 + k\frac{m}{d}$ ebenfalls Lösung.

Zeige: Diese sind paarweise inkongruent. Seien $0 \leq k, l \leq d - 1$ und $x_0 + k\frac{m}{d} \equiv x_0 + l\frac{m}{d} \mod m \Rightarrow k\frac{m}{d} \equiv l\frac{m}{d} \mod m$. Wegen $\text{ggT}(\frac{m}{d}, m) = \frac{m}{d}$ und Satz 25(v) folgt: $k \equiv l \mod d$ (da $\frac{\frac{m}{d}}{\frac{m}{d}} = d$) $\Rightarrow k = l$, d. h. diese Lösungen sind paarweise inkongruent modulo m.
Sei nun $x_1 \in \mathbb{Z}$ Lösung, d. h. $ax_1 \equiv b \mod m \Rightarrow ax_1 \equiv ax_0 \mod m \overset{\text{Satz 25(v)}}{\Rightarrow} x_1 \equiv x_0 \mod \frac{m}{d} \Rightarrow \exists t \in \mathbb{Z} : x_1 = x_0 + t\frac{m}{d}$. Sei $t = qd + r$ mit $0 \leq r \leq d - 1$. Dann folgt $x_1 = x_0 + (qd + r)\frac{m}{d} = x_0 + \underbrace{qm}_{\equiv 0 \mod m} + r\frac{m}{d} \equiv x_0 + r\frac{m}{d} \mod m$, d. h. jede Lösung ist zu einer solchen Lösung kongruent. □

Bemerkung Aus Satz 31 erhält man sofort den folgenden wichtigen Spezialfall:
Ist $a \in \mathbb{Z}$, $m \in \mathbb{N}$ und $\text{ggT}(a, m) = 1$, so gibt es ein modulo m eindeutig bestimmtes $x \in \mathbb{Z}$, sodass $ax \equiv 1 \mod m$.

Beispiel
Löse $4x \equiv 6 \mod 14$. Da $\text{ggT}(4, 14) = 2$ und $2 \mid 6 \Rightarrow$ lösbar.
1. Lösungsweg: Verwende den euklidischen Algorithmus, um $x_0, y_0 \in \mathbb{Z}$ zu finden, die $4x_0 + 14y_0 = 2$ erfüllen.

$$14 = 3 \cdot 4 + 2 \Rightarrow 2 = 14 + (-3) \cdot 4 \Rightarrow 6 = 3 \cdot 14 + (-9) \cdot 4$$

und daher auch 5, da $-9 \equiv 5 \mod 14$. Wähle $x_0 = 5$. Nach Satz 31 erhält man die zweite modulo 14 inkongruente Lösung durch: $5 + 1 \cdot \frac{14}{2} = 5 + 7 = 12$. (Ebenso ist $5 + 14k$, $12 + 14l$ mit $k, l \in \mathbb{Z}$ beliebig, ein Paar inkongruenter Lösungen.) D. h. die Lösungen sind $x \equiv 5 \mod 14$ und $x \equiv 12 \mod 14$
2. Lösungsweg:

$$4x \equiv 6 \mod 14 \overset{\text{Satz } 25}{\Rightarrow} 4 \cdot 2x \equiv 4 \cdot 3 \mod 7 \Rightarrow x \equiv 8x \equiv 12 \equiv 5 \mod 7$$
$$\Rightarrow x \equiv 5 \mod 14 \text{ oder } x \equiv 12 \mod 14$$

Bemerkung Man kann lineare Kongruenzen verwenden, um lineare diophantische Gleichungen zu lösen.

Beispiel
Gesucht sind alle $(x, y) \in \mathbb{Z}^2$, die $3x + 5y = 2$ erfüllen.

$$\begin{aligned} 3x + 5y = 2 &\Rightarrow 3x \equiv 2 \mod 5 \Rightarrow 6x \equiv 4 \mod 5 \Rightarrow x \equiv 4 \mod 5 \\ &\Rightarrow: x = 4 + 5t \ (t \in \mathbb{Z}) \Rightarrow 3(4 + 5t) + 5y = 2 \Rightarrow 12 + 15t + 5y = 2 \\ &\Rightarrow 10 + 15t = -5y \Rightarrow -2 - 3t = y \ \forall t \in \mathbb{Z} \end{aligned}$$

D. h. $\{(x, y) \in \mathbb{Z}^2 \mid 3x + 5y = 2\} = \{(4 + 5t, -2 - 3t) \mid t \in \mathbb{Z}\}$.

Definition „Simultane lineare Kongruenz“
Seien $m_1, \ldots, m_k \in \mathbb{N}$ und $a_1, \ldots, a_k \in \mathbb{Z}$. Als simultane (lineare) Kongruenz bezeichnet man ein System

$$x \equiv a_1 \mod m_1,\ x \equiv a_2 \mod m_2, \ldots,\ x \equiv a_k \mod m_k$$

Gesucht sind alle $x \in \mathbb{Z}$, die alle k Kongruenzen erfüllen.

Bemerkung

1. Es ist möglich, dass ein System simultaner Kongruenzen unlösbar ist. Z. B. $x \equiv 1 \mod 8$, $x \equiv 3 \mod 4$ sind unlösbar. (Denn: $x \equiv 3 \mod 4 \Rightarrow$ $x \equiv 3 \mod 8$ oder $x \equiv 7 \mod 8$). Solche einander widersprechenden Kongruenzen können nicht auftreten, wenn man voraussetzt, dass $m_1, \ldots, m_k$ paarweise relativ prim sind.

2. Betrachte das allgemeinere System:

$$a_1 x \equiv b_1 \mod m_1, \ldots, a_k x \equiv b_k \mod m_k \tag{3.1}$$

Falls $\operatorname{ggT}(a_i, m_i) \nmid b_i$ für ein $i \in \{1, \ldots, k\}$, dann ist es unlösbar. Nehmen wir darum an, dass $\operatorname{ggT}(a_i, m_i) \mid b_i$ für $1 \leq i \leq k$. Sei $d_i := \operatorname{ggT}(a_i, m_i)$. Dann ist (1) äquivalent zu dem System:

$$\frac{a_1}{d_1} x \equiv \frac{b_1}{d_1} \mod \frac{m_1}{d_1}, \ldots, \frac{a_k}{d_k} x \equiv \frac{b_k}{d_k} \mod \frac{m_k}{d_k} \tag{3.2}$$

Nach Satz 6(vi) ist $\operatorname{ggT}(\frac{a_i}{d_i}, \frac{m_i}{d_i}) = 1$ für $1 \leq i \leq k$ und daher gibt es $c_1, \ldots, c_k \in \mathbb{Z}$, sodass $\frac{a_i}{d_i} c_i \equiv 1 \mod \frac{m_i}{d_i}$ für $1 \leq i \leq k$ und (2) ist äquivalent zu:

$$x \equiv \frac{b_1}{d_1} c_1 \mod \frac{m_1}{d_1}, \ldots, x \equiv \frac{b_k}{d_k} c_k \mod \frac{m_k}{d_k} \tag{3.3}$$

d. h. zu einem System, das dieselbe Gestalt hat wie in der Definition.

3. Ist x_0 Lösung (d. h. $x_0 \equiv a_i \mod m_i$ für $1 \leq i \leq k$) und $x_1 \equiv x_0 \mod \operatorname{kgV}(m_1, \ldots, m_k)$, so ist x_1 ebenfalls Lösung.
Man interessiert sich darum nur für modulo $\operatorname{kgV}(m_1, \ldots, m_k)$ inkongruente Lösungen. (Ist $m = \operatorname{kgV}(m_1, \ldots, m_k)$, so folgt aus $m \mid (x_1 - x_0)$ und $m_i \mid m$ für $1 \leq i \leq k$, dass $m_i \mid (x_1 - x_0) \Rightarrow x_1 \equiv x_0 \equiv a_i \mod m_i$)

Lemma 32
Seien $m_1, \ldots, m_k \in \mathbb{N}$ und $a_1, \ldots, a_k \in \mathbb{Z}$. Wenn das System linearer Kongruenzen

$$x \equiv a_1 \mod m_1, \ldots, x \equiv a_k \mod m_k$$

lösbar ist, so ist die Lösung modulo $\operatorname{kgV}(m_1, \ldots, m_k)$ eindeutig bestimmt.

Beweis. Seien x_0, x_1 zwei Lösungen $\Rightarrow x_0 \equiv a_i \mod m_i$, $x_1 \equiv a_i \mod m_i$ $(1 \leq i \leq k)$
$\Rightarrow x_0 \equiv x_1 \mod m_i$ für $1 \leq i \leq k \Rightarrow m_i \mid (x_0 - x_1)$ für $1 \leq i \leq k$
$\overset{\text{Satz 18}}{\Rightarrow} \operatorname{kgV}(m_1, \ldots, m_k) \mid (x_1 - x_0) \Rightarrow x_1 \equiv x_0 \mod \operatorname{kgV}(m_1, \ldots, m_k)$. □

Satz 33 „Chinesischer Restsatz“
Seien $m_1, \ldots, m_k \in \mathbb{N}$ und $a_1, \ldots, a_k \in \mathbb{Z}$. Wenn $m_1, \ldots, m_k$ paarweise relativ prim sind, so besitzen die simultanen Kongruenzen

$$x \equiv a_1 \mod m_1, \ldots, x \equiv a_k \mod m_k$$

genau eine modulo $m_1 \cdots m_k$ inkongruente Lösung.

Beweis. Für $1 \leq i \leq k$ sei $M_i := \frac{m_1 \cdots m_k}{m_i}$. Dann ist $\text{ggT}(m_i, M_i) = 1$.
(Angenommen, $\text{ggT}(m_i, M_i) > 1 \Rightarrow \exists p$ Primzahl $: p \mid m_i$ und $p \mid (m_i \cdots m_{i-1} m_{i+1} \cdots m_k) \Rightarrow$
$\exists j \in \{1, \ldots, k\}$, $i \neq j : p \mid m_j$, Widerspruch!)
Aus Satz 31 folgt: $\forall j \in \{1, \ldots k\} : \exists y_j \in \mathbb{Z} : M_j y_j \equiv 1 \mod m_j$.
Behauptung: $x_0 = \sum_{i=1}^{k} a_i M_i y_i$ ist eine Lösung des Systems.
Für $1 \leq i \leq k$, $i \neq j$ ist $a_i M_i y_i \equiv 0 \mod m_j$, da $m_j \mid M_i$

$$\Rightarrow x_0 = a_1 M_1 y_1 + \ldots + a_k M_k y_k \equiv a_j \underbrace{M_j y_j}_{\substack{\equiv 1 \\ \mod m_j}} \equiv a_j \mod m_j \quad \text{für} \quad 1 \leq i \leq k$$

Nach Lemma 32 ist die Lösung modulo kgV $(m_1, \ldots, m_k)$ eindeutig bestimmt und nach Korollar 22 gilt: $\text{kgV}(m_1, \ldots, m_k) = m_1 \cdots m_k$. □

Beispiel
Zu lösen ist die simultane Kongruenz $x \equiv 2 \mod 3$, $x \equiv 3 \mod 5$, $x \equiv 2 \mod 7$.
1. Lösungsweg: Verwende den Beweis von Satz 33: $m_1 = 3$, $m_2 = 5$, $m_3 = 7$
$\Rightarrow M_1 = 35$, $M_2 = 21$, $M_3 = 15$. Löse:

$$\begin{aligned} 35x &\equiv 1 \mod 3 \\ 2x &\equiv 1 \mod 3 \\ 2x &\equiv 4 \mod 3 \\ x &\equiv 2 \mod 3 \\ y_1 &= 2 \end{aligned} \qquad \begin{aligned} 21x &\equiv 1 \mod 5 \\ x &\equiv 1 \mod 5 \\ y_2 &= 1 \end{aligned} \qquad \begin{aligned} 15x &\equiv 1 \mod 7 \\ x &\equiv 1 \mod 7 \\ y_3 &= 1 \end{aligned}$$

$$\Rightarrow x_0 = a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233$$

Die Lösung ist $x \equiv 23 \mod 105$.

2. Lösungsweg: Sukzessives Einsetzen. $x \equiv 2 \mod 3 \Rightarrow x = 2 + 3 \cdot t$ $(t \in \mathbb{Z})$,

$x \equiv 3 \mod 5 \Rightarrow 2 + 3t \equiv 3 \mod 5 \Rightarrow 3t \equiv 1 \mod 5 \Rightarrow 6t \equiv 2 \mod 5 \Rightarrow t \equiv 2 \mod 5$
$\Rightarrow t = 2 + 5s$ $(s \in \mathbb{Z}) \Rightarrow x = 2 + 3t = 2 + 3(2 + 5s) = 8 + 15s$

$x \equiv 2 \mod 7 \Rightarrow 8 + 15s \equiv 2 \mod 7 \Rightarrow 15s \equiv -6 \mod 7 \Rightarrow 15s \equiv 1 \mod 7 \Rightarrow$
$s \equiv 1 \mod 7 \Rightarrow s = 1 + 7u$ $(u \in \mathbb{Z}) \Rightarrow x = 8 + 15s = 8 + 15(1 + 7u) = 23 + 105u$,

d. h. $x \equiv 23 \mod 105$.

Bemerkung Mit dem im 2. Lösungsweg beschriebenen Verfahren kann man allgemeinere simultane Kongruenzen lösen (sofern alle Kongruenzen einzeln lösbar sind und die Moduln relativ prim).

Beispiel
Zu lösen ist die simultane Kongruenz $4x \equiv 12 \mod 8$, $3x \equiv 5 \mod 7$

$4x \equiv 12 \mod 8 \Rightarrow x \equiv 3 \mod 2 \Rightarrow x \equiv 1 \mod 2 \Rightarrow x = 1 + 2t \ (t \in \mathbb{Z})$

$3x \equiv 5 \mod 5 \Rightarrow 3(1 + 2t) \equiv 5 \mod 7 \Rightarrow 6t + 3 \equiv 5 \mod 7 \Rightarrow -6t \equiv -2 \mod 7$
$\Rightarrow t \equiv -2 \equiv 5 \mod 7 \Rightarrow t = 5 + 7s \ (s \in \mathbb{Z})$

$\Rightarrow x = 1 + 2t = 1 + 2(5 + 7s) = 11 + 14s$
$\Rightarrow$ modulo 56 ($= \text{kgV}(8, 7)$) inkongruente Lösungen sind $11, 25, 39, 53$ (was man leicht durch Einsetzen überprüft).

Kapitel 4

Der Restklassenring $\mathbb{Z}_m$

Nach Lemma 24 ist Kongruenz modulo $m\,(\in \mathbb{N})$ eine Äquivalenzrelation auf $\mathbb{Z}$. Die Äquivalenzklasse $\overline{a}$ von $a \in \mathbb{Z}$ ist daher

$$\begin{aligned}\overline{a} &= \{x \in \mathbb{Z} \mid x \equiv a \mod m\} = \{x \in \mathbb{Z} \mid m \mid (x-a)\} = \{x \in \mathbb{Z} \mid \exists k \in \mathbb{Z} : x - a = km\} \\ &= \{x \in \mathbb{Z} \mid \exists k \in \mathbb{Z} : x = a + km\} = \{a + km \mid k \in \mathbb{Z}\} = a + m\mathbb{Z}\end{aligned}$$

$(= \{a\} \cup \{a+m,\ a+2m,\ a+3m, \dots\} \cup \{a-m,\ a-2m,\ a-3m, \dots\})$
Die Äquivalenzklassen mod m bilden eine Partition von $\mathbb{Z}$, d. h. es gelten:

1. $\overline{a} \neq \emptyset\ \forall a \in \mathbb{Z}$
2. $\overline{a} \cap \overline{b} = \emptyset$ oder $\overline{a} = \overline{b}$
3. $\bigcup_{a \in \mathbb{Z}} \overline{a} = \mathbb{Z}$

Beispiel
Ist $m = 2$ so sind die Äquivalenzklassen die geraden Zahlen (d. h. $2\mathbb{Z}$) und die ungeraden Zahlen (d. h. $1 + 2\mathbb{Z}$).

Definition „Restklasse modulo m“
Ist $m \in \mathbb{N}$ so wird jede Äquivalenzklasse $\overline{a}$ modulo m als Restklasse modulo m bezeichnet. Jedes $x \in \overline{a}$ wird als Repräsentant von $\overline{a}$ bezeichnet. Für die Menge der Restklassen modulo m schreibt man $\mathbb{Z}_m$ (oder $\mathbb{Z}/m\mathbb{Z}$), d. h.,
$\mathbb{Z}_m = \{\overline{a} \mid a \in \mathbb{Z}\}$ (bzw. $\mathbb{Z}/m\mathbb{Z} = \{a + m\mathbb{Z} \mid a \in \mathbb{Z}\}$)

Lemma 34
$\forall m \in \mathbb{N} : |\mathbb{Z}_m| = m$, genauer gilt $\mathbb{Z}_m = \{\overline{0}, \dots, \overline{m-1}\}$.

Beweis. Sei $a \in \mathbb{Z}$ mit $a = q \cdot m + r$, $0 \leq r \leq m-1$. Dann ist $a \equiv r \mod m \Rightarrow \overline{a} = \overline{r}$, d. h., es gibt höchstens die Restklassen $\overline{0}, \dots, \overline{m-1}$.
Da r nicht kongruent $s \mod m\ \forall r, s \in \{0, 1, \dots, m-1\}$, $r \neq s$ sind diese verschieden. □

Beispiel
$\mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$, wobei z. B. $\overline{2} = 2 + 5\mathbb{Z} = \{2\} \cup \{7, 12, 17, \dots\} \cup \{-3, -8, -13, \dots\}$, d. h., $\overline{2} = \overline{-3} = \overline{12} = \dots$

Definition „Vollständiges Restsystem“
Sei $m \in \mathbb{N}$. Eine m-elementige Teilmenge von $\mathbb{Z}$ heißt vollständiges Restsystem modulo m, wenn sie aus jeder Restklasse genau ein Element enthält.

Bemerkung Offenbar gilt: $\{r_1, \ldots, r_m\}$ ist ein vollständiges Restsystem modulo m
$\Leftrightarrow r_i \neq r_j \mod m \ \ \forall i, j \in \{1, \ldots m\}, \ i \neq j$

Beispiel
Vollständige Restsysteme modulo 4 sind z. B.: $\{0, 1, 2, 3\}$, $\{4, -3, -2, 3\}$ oder $\{97, 98, 99, 100\}$

Satz 35 (i) Sei $m \in \mathbb{N}, \{r_1, \ldots, r_m\}$ vollständiges Restsystem modulo m, $a, b \in \mathbb{Z}$ mit $\text{ggT}(a, m) = 1$. Dann ist $\{ar_1 + b, \ldots, ar_m + b\}$ ebenfalls ein vollständiges Restsystem modulo m.

(ii) Seien $m, n \in \mathbb{N}, \{r_1, \ldots, r_m\}$ vollständiges Restsytem modulo m, $\{s_1, \ldots, s_n\}$ vollständiges Restsytem modulo n und $\text{ggT}(m, n) = 1$. Dann ist $\{nr_i + ms_j \mid 1 \leq i \leq m, 1 \leq j \leq n\}$ ein vollständiges Restsystem modulo mn.

Beweis. (i) $ar_i + b \equiv ar_j + b \mod m \Rightarrow ar_i \equiv ar_j \mod m \overset{\text{Satz 25(v)}}{\Rightarrow} r_i \equiv r_j \mod m \Rightarrow i = j$

(ii) $nr_i + ms_k \equiv nr_j + ms_l \mod mn \Rightarrow nr_i + ms_k \equiv nr_j + ms_l \mod m$
$\Rightarrow nr_i \equiv nr_j \mod m \overset{\text{Satz 25 (v)}}{\Rightarrow} r_i \equiv r_j \mod m \Rightarrow i = j \Rightarrow ms_k = ms_l \mod mn$
$\Rightarrow ms_k = ms_l \mod n \overset{\text{Satz 25(v)}}{\Rightarrow} s_k \equiv s_l \mod n \Rightarrow k = l$ □

Definition „Addition und Multiplikation auf $\mathbb{Z}_m$“
Auf $\mathbb{Z}_m$ definieren wir $\overline{a} + \overline{b} := \overline{a + b}$ und $\overline{a} \cdot \overline{b} := \overline{ab}$ (bzw. in der anderen Formulierung $(a + m\mathbb{Z}) + (b + m\mathbb{Z}) := (a + b) + m\mathbb{Z}$ und $(a + m\mathbb{Z}) \cdot (b + m\mathbb{Z}) := (ab) + m\mathbb{Z}$).

Beispiel
Additions- und Multiplikationstafel für $m = 4$:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Beachte: $\overline{2} \cdot \overline{2} = \overline{0}$ (d. h. $\overline{2}$ ist Nullteiler)

Satz 36
$(\mathbb{Z}_m, +, \cdot)$ ist kommutativer Ring mit 1.

Beweis. Zeige: Addition und Multiplikation sind *wohldefiniert*. Sei $\overline{a} = \overline{c}$, $\overline{b} = \overline{d}$

$\Rightarrow a \equiv c \mod m, \ b \equiv d \mod m \overset{\text{Satz 25}}{\Rightarrow} a + b \equiv c + d \mod m$ und $ab \equiv cd \mod m$
$\Rightarrow \overline{a + b} = \overline{c + d}, \ \overline{ab} = \overline{cd} \Rightarrow \overline{a} + \overline{b} = \overline{c} + \overline{d}, \ \overline{a} \cdot \overline{b} = \overline{c} \cdot \overline{d}$

Assoziativität: $\forall \overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_m$:

$$(\overline{a}+\overline{b})+\overline{c} = \overline{a+b}+\overline{c} = \overline{(a+b)+c} = \overline{a+(b+c)} = \overline{a}+\overline{b+c} = \overline{a}+(\overline{b}+\overline{c})$$

Neutrales Element der Addition (bzw. Multiplikation) ist $\overline{0}$ (bzw. $\overline{1}$)
Inverses Element der Addition zu $\overline{a}$ ist $\overline{-a} = \overline{m-a}$
Die übrigen Rechenregeln können analog zum Assoziativgesetz der Addition bewiesen werden. □

Definition „Nullteiler und Einheiten“
Sei $(R, +, \cdot)$ ein kommutativer Ring mit 1 (in dem $0 \neq 1$ gilt).

1. Ein Element $a \in R$ heißt Nullteiler, wenn es ein $b \in R$, $b \neq 0$ gibt mit $ab = 0$.
2. Gibt es außer 0 keine Nullteiler in R, so wird R Integritätsbereich (oder Integritätsring) genannt.
3. Ein $a \in R$ heißt Einheit in R, wenn es ein $b \in R$ mit $ab = 1$ gibt. (In diesem Fall heißt b Inverses zu a. Da es eindeutig bestimmt ist, schreibt man dafür a^{-1}.)
4. Die Menge aller Einheiten von R wird mit R^* bezeichnet.

Lemma 37
Sei $(R, +, \cdot)$ ein kommutativer Ring mit 1 (in dem $0 \neq 1$ gilt).

(i) R^* enthält keine Nullteiler.

(ii) $(R^*, \cdot)$ ist eine abelsche Gruppe.

(iii) $(R, +, \cdot)$ ist genau dann ein Körper, wenn $R^* = R \setminus \{0\}$.

Beweis. (i) Angenommen $a \in R^*$ ist Nullteiler $\Rightarrow \exists b \in R$, $b \neq 0$ mit $ab = 0$ und $\exists c \in R$ mit $ac = 1 \Rightarrow 0 = 0c = (ab)c = acb = 1b = b$, Widerspruch!

(ii) Angenommen seien $a, b \in R^* \Rightarrow \exists c, d \in R : ac = bd = 1 \Rightarrow (ab)(cd) = (ac)(bd) = 1 \cdot 1 = 1 \Rightarrow ab \in R^*$.
Ist $a \in R^*$, so ist auch sein Inverses $a' \in R^*$, da a Inverses von a' ist.
Außerdem ist $1 \in R$, da $1 \cdot 1 = 1$.

(iii) trivial □

Beispiel 1. $\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$, Nullteiler $(\neq \overline{0})$ sind $\overline{2}, \overline{3}$ (da $\overline{2} \cdot \overline{3} = \overline{6} = \overline{0}$) und $\overline{4}$ (da $\overline{4} \cdot \overline{3} = \overline{12} = \overline{0}$). $\mathbb{Z}_6^* = \{\overline{1}, \overline{5}\}$ (da $\overline{1} \cdot \overline{1} = \overline{1}$, $\overline{5} \cdot \overline{5} = \overline{25} = \overline{1}$ beziehungsweise $\overline{5} \cdot \overline{5} = \overline{-1} \cdot \overline{-1} = \overline{1}$).

2. $\mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$ enthält keine Nullteiler $\neq \overline{0}$, $\mathbb{Z}_5^* = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$, da $\overline{1} \cdot \overline{1} = \overline{2} \cdot \overline{3} = \overline{4} \cdot \overline{4} = \overline{1}$, also ist $(\mathbb{Z}_5, +, \cdot)$ ein Körper.

Definition „Prime Restklasse“
Sei $m \in \mathbb{N}$ und $a \in \mathbb{Z}$. Die Restklasse $\overline{a} \in \mathbb{Z}_m$ heißt prim, wenn $\operatorname{ggT}(a, m) = 1$

Bemerkung Der Begriff der primen Restklasse ist wohldefiniert: Sei $\overline{a} = \overline{b}$, d. h. $a \equiv b \mod m$. Angenommen, $\text{ggT}(b, m) > 1 \Rightarrow \exists p$ Primzahl mit $p \mid b$ und $p \mid m \Rightarrow p \mid a \Rightarrow \text{ggT}(a, m) > 1$, Widerspruch!

Satz 38
Sei $m \in \mathbb{N}$ $(m \neq 1)$. Dann sind äquivalent:

(i) $\overline{a} \in \mathbb{Z}_m^*$ (ii) $\overline{a}$ ist prime Restklasse.

Beweis. $\overline{a} \in \mathbb{Z}_m^* \Leftrightarrow \exists \overline{x} \in \mathbb{Z}_m : \overline{ax} = \overline{1} \Leftrightarrow \exists x \in \mathbb{Z} : ax \equiv 1 \mod m \overset{\text{Satz 31}}{\Leftrightarrow} \text{ggT}(a, m) \mid 1 \Leftrightarrow \text{ggT}(a, m) = 1$ □

Korollar 39
Sei $m \in \mathbb{N}$, $m \neq 1$. Dann sind äquivalent:

(i) $(\mathbb{Z}_m, +, \cdot)$ ist ein Körper (ii) m ist eine Primzahl

Beweis. (ii) $\Rightarrow$ (i): Sei m eine Primzahl $\Rightarrow \text{ggT}(1, m) = \text{ggT}(2, m) = \ldots = \text{ggT}(m-1, m) = 1 \Rightarrow \overline{1}, \overline{2}, \ldots, \overline{m-1}$ sind prime Restklassen $\Rightarrow \overline{1}, \overline{2}, \ldots, \overline{m-1} \in \mathbb{Z}_m^* \Rightarrow (\mathbb{Z}_m, +, \cdot)$ ist ein Körper.
(i) $\Rightarrow$ (ii): Sei m keine Primzahl $\Rightarrow \exists a, b \in \mathbb{Z}$ mit $1 < a, b < m$ und $ab = m \Rightarrow \overline{a}\overline{b} = \overline{m} = \overline{0} \Rightarrow \overline{a} \in \mathbb{Z}_m \setminus \{\overline{0}\}$ ist Nullteiler $\overset{\text{Lemma 37(i)}}{\Rightarrow} \overline{a} \notin \mathbb{Z}_m^* \Rightarrow (\mathbb{Z}_m, +, \cdot)$ ist kein Körper. □

Definition „Prime Restklassengruppe“
Die abelsche Gruppe $(\mathbb{Z}_m^*, \cdot)$ heißt prime Restklassengruppe modulo m.

Satz 40 „Satz von Wilson“
Sei $p \in \mathbb{N}$, $p > 1$, dann sind äquivalent:

(i) p ist Primzahl (ii) $(p-1)! \equiv -1 \mod p$

Beweis. (i) $\Rightarrow$ (ii): Die Behauptung ist für $p \in \{2, 3\}$ erfüllt
(da $1! \equiv -1 \mod 2$ und $2! \equiv -1 \mod 3$).
Sei also $p \geq 5$. Da $\mathbb{Z}_p$ ein Körper ist, besitzen die Restklassen $\overline{1}, \overline{2}, \ldots, \overline{p-1}$ alle ein multiplikatives Inverses. Dabei gilt: $\overline{a}^{-1} = \overline{a} \Leftrightarrow \overline{a} \in \{\overline{1}, \overline{p-1}\} = \{\overline{1}, \overline{-1}\}$
„$\Rightarrow$“: $\overline{a}^{-1} = \overline{a} \Rightarrow \overline{a}^2 = \overline{1} \Rightarrow a^2 \equiv 1 \mod p \Rightarrow p \mid (a^2 - 1) \Rightarrow p \mid (a-1)(a+1) \Rightarrow p \mid (a-1) \vee p \mid (a+1) \Rightarrow a \equiv 1 \mod p \vee a \equiv -1 \mod p \Rightarrow \overline{a} = \overline{1} \vee \overline{a} = \overline{-1}$
„$\Leftarrow$“ ist trivial.
Außerdem gilt: $\overline{a} = \overline{b} \Leftrightarrow \overline{a}^{-1} = \overline{b}^{-1}$ $\forall \overline{a}, \overline{b} \in \mathbb{Z}_p^*$. Daher enthält $\{\overline{2}, \overline{3}, \ldots, \overline{p-2}\}$ insgesamt $\frac{p-3}{2}$ Paare jeweils zueinander multiplikativ inverser Restklassen $\Rightarrow \overline{2} \cdot \overline{3} \cdot \cdots \cdot \overline{p-2} = \overline{1} \Rightarrow 2 \cdot 3 \cdot \cdots \cdot (p-2) \equiv 1 \mod p \Rightarrow 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p-2)(p-1) \equiv (p-1)! \equiv -1 \mod p$
(ii) $\Rightarrow$ (i): Sei umgekehrt $(p-1)! \equiv -1 \mod p$. Angenommen, p wäre keine Primzahl $\Rightarrow \exists a \in \mathbb{Z}$, $2 \leq a \leq p-1$ mit $a \mid p$. Dann gilt $a \mid (p-1)! \Rightarrow (p-1)! \equiv 0 \mod a$ und $(p-1)! \equiv -1 \mod a \Rightarrow 0 \equiv -1 \mod a$, Widerspruch! □

Definition „Ordnung einer Gruppe“
Sei $(G, \cdot)$ eine abelsche Gruppe. Die Anzahl $|G|$ der Elemente von G wird als die Ordnung von G bezeichnet.

Definition „Eulersche φ-Funktion“
Für $m \in \mathbb{N}$ wird die Eulersche φ-Funktion defininert durch

$$\varphi(m) = |\{k \in \mathbb{Z} \mid 0 \leq k \leq m-1,\ \mathrm{ggT}\,(k,m) = 1\}|$$

Aus Satz 38 folgt: $\forall m \in \mathbb{N},\ m \neq 1$ ist $\varphi(m) = |\mathbb{Z}_m^*|$, also die Ordnung von $\mathbb{Z}_m^*$ ($\varphi(1) = 1$).

Lemma 41
Sei p eine Primzahl. Dann ist $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1)\ \forall \alpha \in \mathbb{N}$.

Beweis. Unter den Zahlen $1, 2, \ldots, p^\alpha$ sind diejenigen kp mit $1 \leq k \leq p^{\alpha-1}$ nicht relativ prim zu p^α. □

Definition „Primes Restsystem modulo m“
Sei $m \in \mathbb{N}$. Eine $\varphi(m)$-elementige Teilmenge von $\mathbb{Z}$ heißt primes Restsystem modulo m, wenn sie aus jeder primen Restklasse genau ein Element enthält.

Bemerkung Offenbar gilt: $\{r_1, \ldots, r_{\varphi(m)}\}$ ist primes Restklassensystem modulo m
$\Leftrightarrow r_i \not\equiv r_j \mod m\, \forall i, j \in \{1, \ldots, \varphi(m)\},\ i \neq j$ und $\mathrm{ggT}\,(r_i, m) = 1$ für $1 \leq i \leq \varphi(m)$.

Satz 42 (i) Sei $m \in \mathbb{N}$, $\{r_1, \ldots, r_{\varphi(m)}\}$ primes Restsystem modulo m, $a \in \mathbb{Z}$, $\mathrm{ggT}\,(a, m) = 1$. Dann ist $\{ar_1, \ldots, ar_{\varphi(m)}\}$ ebenfalls primes Restsystem modulo m.

(ii) Seien $m, n \in \mathbb{N}$, $\{r_1, \ldots, r_{\varphi(m)}\}$ primes Restsystem modulo m, $\{s_1, \ldots, s_{\varphi(n)}\}$ primes Restsystem modulo n und $\mathrm{ggT}\,(m, n) = 1$.
Dann ist $\{nr_i + ms_j \mid 1 \leq i \leq \varphi(m), 1 \leq j \leq \varphi(n)\}$ primes Restsystem modulo mn.

Beweis. (i) Aus Satz 35(i) folgt: ar_i nicht kongruent $ar_j \mod m$ für $1 \leq i, j \leq \varphi(m)$, $i \neq j$.
Da $\mathrm{ggT}\,(r_i, m) = \mathrm{ggT}\,(a, m) = 1 \overset{\text{Satz 7(iv)}}{\Rightarrow} \mathrm{ggT}\,(ar_i, m) = 1$ für $1 \leq i \leq \varphi(m)$.

(ii) Aus Satz 35(ii) folgt, dass die Elemente von $\{nr_i + ms_j \mid 1 \leq i \leq \varphi(m), 1 \leq j \leq \varphi(n)\}$ modulo mn relativ prim sind.
Zeige $\mathrm{ggT}\,(nr_i + ms_j, mn) = 1$ für $1 \leq i \leq \varphi(m)$, $1 \leq j \leq \varphi(n)$:
Angenommen, $\exists p$ Primzahl mit $p \mid (nr_i + ms_j)$ und $p \mid (mn)$. Dann folgt, dass $p \mid m \vee p \mid n$, o.B.d.A. $p \mid n \Rightarrow p \mid (ms_j)$. Da $\mathrm{ggT}\,(m, n) = 1$ ist $p \mid m$ unmöglich, also $p \mid s_j \Rightarrow \mathrm{ggT}\,(n, s_j) \geq p$, Widerspruch!
Ergänze nun die primen Restsysteme $\{r_1, \ldots, r_{\varphi(m)}\}$ und $\{s_1, \ldots, s_{\varphi(n)}\}$ zu vollständigen Restsystemen $\{r_1, \ldots, r_{\varphi(m)}, \ldots, r_m\}$ und $\{s_1, \ldots, s_{\varphi(n)}, \ldots, s_n\}$
(d. h. $\mathrm{ggT}\,(r_i, m) > 1$ für $\varphi(m) < i \leq m$ und $\mathrm{ggT}\,(s_j, n) > 1$ für $\varphi(n) < j \leq n$).
Nach Satz 35(ii) ist $\{nr_i + ms_j \mid 1 \leq i \leq m,\ 1 \leq j \leq n\}$ vollständiges Restsystem modulo mn. Gilt $\mathrm{ggT}\,(nr_i + ms_j, mn) = 1$, so folgt $\mathrm{ggT}\,(r_i, m) = \mathrm{ggT}\,(s_j, n) = 1$ für $1 \leq i \leq m, 1 \leq j \leq n$, d. h. $1 \leq i \leq \varphi(m),\ 1 \leq j \leq \varphi(n)$.
Daher ist $\{nr_i + ms_j \mid 1 \leq i \leq \varphi(m),\ 1 \leq j \leq \varphi(n)\}$ tatsächlich primes Restsystem modulo mn. □

Beispiel 1. Sei $m = 3$, $\{1, 2\}$ primes Restsystem modulo 3, $n = 4$, $\{1, 3\}$ primes Restsystem modulo 4, $mn = 12$. $\{1, 5, 7, 11\}$ ist primes Restsystem modulo 12. Nach Satz 42(ii) ist

$$\{\underbrace{4 \cdot 1 + 3 \cdot 1}_{=7}, \underbrace{4 \cdot 1 + 3 \cdot 3}_{=13 \equiv 1 \mod 12}, \underbrace{4 \cdot 2 + 3 \cdot 1}_{=11}, \underbrace{4 \cdot 2 + 3 \cdot 3}_{=17 \equiv 5 \mod 12}\}$$

2. $\varphi(3) = 2 = \varphi(3^1) = 3^1 - 3^0$, $\varphi(4) = 3 = \varphi(2^2) = 2^2 - 2^1$, $\varphi(12) = 4 = \varphi(2^2 3) = \varphi(2^2)\varphi(3) = (2^2 - 2^1)(3^1 - 3^0)$.

3. Sei $m = 9$. Vollständiges Restsystem ist $\{0, 1, 2, 3, 4, 5, 6, 7, 8\}$, primes Restsystem ist $\{1, 2, 4, 5, 7, 8\}$.

Korollar 43
Wenn $m, n \in \mathbb{N}$ und ggT $(m, n) = 1$, dann gilt $\varphi(mn) = \varphi(m)\varphi(n)$.

Beweis. Folgt sofort aus Satz 42(ii). □

Korollar 44
Besitzt $m \in \mathbb{N}$ die Primfaktorzerlegung $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, so gilt:

$$\begin{aligned}\varphi(m) &= (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \cdots (p_k^{\alpha_k} - p_k^{\alpha_k - 1}) \\ &= p_1^{\alpha_1 - 1} \cdots p_k^{\alpha_k - 1}(p_1 - 1) \cdots (p_k - 1)\end{aligned}$$

Bemerkung Man kann Korollar 44 auch so formulieren:

$$\varphi(m) = m \prod_{p|m} \left(1 - \frac{1}{p}\right)$$

(wobei p über alle Primzahlen läuft, die m teilen.) Dann

$$\varphi(m) = \prod_{i=1}^{k} p_i^{\alpha_i - 1}(p_i - 1) = \underbrace{\prod_{i=1}^{k} p_i^{\alpha_i}}_{=m} \prod_{i=1}^{k} (1 - \frac{1}{p_i}) = m \prod_{p|m} \left(1 - \frac{1}{p}\right)$$

Beweis. Aus Korollar 43 folgt mit Induktion nach k, dass $\varphi(m) = \varphi(p_1^{\alpha_1}) \cdots \varphi(p_k^{\alpha_k})$. Nach Lemma 41 ist $\varphi(p_i^{\alpha_i}) = p_i^{\alpha_i} - p_i^{\alpha_i - 1} = p_i^{\alpha_i - 1}(p_i - 1)$ für $1 \leq i \leq k$. □

Satz 45
Sei $(G, \cdot)$ eine endliche abelsche Gruppe der Ordnung $|G|$ mit neutralem Element e. Dann gilt $a^{|G|} = e \; \forall a \in G$.

Beweis. Sei $a \in G$. Die Abbildung $\varphi : G \to G$, $\varphi(x) = ax$ ist bijektiv (denn angenommen $\varphi(x) = \varphi(y) \Rightarrow ax = ay \Rightarrow x = a^{-1}(ax) = a^{-1}(ay) = y$, d. h. φ ist injektiv.
Weiters gilt $\varphi(a^{-1}x) = a(a^{-1}x) = x \; \forall x \in G$, d. h. φ ist surjektiv) $\Rightarrow G = \{ax \mid x \in G\} \Rightarrow \prod_{x \in G} x = \prod_{x \in G} ax = a^{|G|} \prod_{x \in G} x \Rightarrow a^{|G|} = e$ □

Korollar 46 „Euler“
Sei $m \in \mathbb{N}$, $a \in \mathbb{Z}$ und $\text{ggT}(a, m) = 1$.
Dann gilt $a^{\varphi(m)} \equiv 1 \mod m$.

Beweis. Folgt sofort durch die Anwendung von Satz 45 auf die Gruppe $(\mathbb{Z}_m^*, \cdot)$:
$\overline{a}^{|\mathbb{Z}_m^*|} = \overline{a}^{\varphi(m)} = \overline{1}\ \forall \overline{a} \in \mathbb{Z}_m^* \Rightarrow a^{\varphi(m)} \equiv 1 \mod m\ \forall a \in \mathbb{Z}$ mit $\text{ggT}(a, m) = 1$. □

Korollar 47 „Kleiner Fermatscher Satz“
Sei p eine Primzahl:

(i) Ist $a \in \mathbb{Z}$ und $p \nmid a$, so gilt $a^{p-1} \equiv 1 \mod p$.

(ii) $\forall a \in \mathbb{Z} : a^p \equiv a \mod p$.

Beweis. (i) Folgt sofort aus Korollar 46 und $\varphi(p) = p - 1$.

(ii) Für $p \nmid a$ folgt dies aus Teil (i). Für $p \mid a$ gilt $a^p \equiv 0 \equiv a \mod p$.

□

Bemerkung

1. Ist $\text{ggT}(a, m) = 1$, so kann man eine Lösung der linearen Kongruenz $ax \equiv b \mod m$ mit Hilfe von Korollar 46 explizit angeben: $x \equiv ba^{\varphi(m)-1}(m)$
   $(\Rightarrow ax \equiv ba^{\varphi(m)} \equiv b \mod m)$
2. Man kann zeigen, dass $m \in \mathbb{N}$ keine Primzahl ist, indem man ein $a \in \mathbb{Z}$ findet, für das $a^m \not\equiv a \mod m$ gilt (oft reicht es, zu überprüfen, ob $2^m \equiv 2 \mod m$ gilt).
3. Es gibt allerdings sogenannte Pseudoprimzahlen m, bei denen dieser Test versagt, d. h. m ist zusammengesetzt und $a^m \equiv a \mod m\ \forall a \in \mathbb{Z}$, z. B. $561 = 3 \cdot 11 \cdot 17$

Kapitel 5

Das quadratische Reziprozitätsgesetz

Vorbemerkung: In diesem Abschnitt werden wir die Lösbarkeit von quadratischen Kongruenzen $ax^2 + bx + c \equiv 0 \mod m$ studieren. Zunächst werden wir sie in mehreren Reduktionsschritten auf die spezielle Gestalt $x^2 \equiv a \mod p$ zurückführen:

1. Die Kongruenz $ax^2 + bx + c \equiv 0 \mod m$ ist genau dann lösbar, wenn die Kongruenz $(2ax + b)^2 \equiv b^2 - 4ac \mod 4am$ lösbar ist.
   (Es ist $ax^2 + bx + c \equiv 0 \mod m \Leftrightarrow m \mid (ax^2 + bx + c) \Leftrightarrow (4am) \mid (4a^2x^2 + 4abx + 4ac)$ und $4a^2x^2 + 4abx + 4ac = (2ax + b)^2 + 4ac - b^2$). D. h. es reicht, die Lösbarkeit von Kongruenzen der Gestalt $x^2 \equiv a \mod m$ zu untersuchen.

2. Wenn m die Primfaktorzerlegung $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ besitzt, gilt $x^2 \equiv a \mod m$ ist lösbar $\Leftrightarrow x^2 \equiv a \mod p_i^{\alpha_i}$ ist lösbar für $1 \leq i \leq k$:
   „$\Rightarrow$“ ist trivial
   „$\Leftarrow$“ Seien $x_1, \ldots, x_k \in \mathbb{Z}$ derart, dass $x_i^2 \equiv a \mod p_i^{\alpha_i}$ für $1 \leq i \leq k$. Nach dem chinesischen Restsatz (Satz 33) $\exists x_0 \in \mathbb{Z} : x_0 \equiv x_i \mod p_i^{\alpha_i}$ für $1 \leq i \leq k \Rightarrow x_0^2 \equiv x_i^2 \equiv a \mod p_i^{\alpha_i}$ für $1 \leq i \leq k \Rightarrow p_i^{\alpha_i} \mid (x_0^2 - a)$ für $1 \leq i \leq k \overset{\text{Satz } 17}{\Rightarrow} m \mid (x_0^2 - a)$ (da $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k} = \text{kgV}\,(p_1^{\alpha_1}, \ldots, p_k^{\alpha_k})$ nach Korollar 22) $\Rightarrow x_0^2 \equiv a \mod m$
   Es reicht also, die Lösbarkeit von Kongruenzen der Gestalt $x^2 \equiv a \mod p^\alpha$ zu untersuchen.

3. Es sei p eine Primzahl, $\alpha \in \mathbb{N}$ und $a \in \mathbb{Z} \setminus \{0\}$ habe die Darstellung $a = p^\beta b$ mit $\beta \in \mathbb{N} \cup \{0\}$, $b \in \mathbb{Z}$ und $p \nmid b$.
   Ist $\beta \geq \alpha$, so ist die Kongruenz $x^2 \equiv a = p^\beta b \equiv 0 \mod p^\alpha$ trivialerweise lösbar. Ist $\beta < \alpha$, so ist $x^2 \equiv a \mod p^\alpha$ genau dann lösbar, wenn $2 \mid \beta$ und die Kongruenz $y^2 \equiv b \mod p^{\alpha-\beta}$ lösbar ist.
   („$\Rightarrow$“: Sei $x_0 \in \mathbb{Z}$ derart, dass $x_0^2 \equiv p^\beta b \mod p^\alpha$ und $x_0^2 = p^\gamma y_0^2$ mit $\gamma \in \mathbb{N} \cup \{0\}$ gerade und $p \nmid y_0^2$. Offenbar gilt $2 \mid \gamma$. Zeige $\gamma = \beta$: Wegen $p^\beta \mid p^\alpha$ und $p^\alpha \mid (x_0^2 - p^\beta b)$ folgt, dass $p^\beta \mid x_0^2 \Rightarrow \beta \leq \gamma$. Wäre $\gamma > \beta$, so würde gelten: $p^{\beta+1} \mid p^\alpha \Rightarrow p^{\beta+1} \mid (x_0^2 - p^\beta b)$ und $p^{\beta+1} \mid p^\gamma \Rightarrow p^{\beta+1} \mid x_0^2 \Rightarrow p^{\beta+1} \mid p^\beta b$, Widerspruch!
   Also gilt $\gamma = \beta$ und $2 \mid \beta$. Schließlich gilt $p^\alpha \mid (x_0^2 - a) \Rightarrow p^\alpha \mid (p^\beta y_0^2 - p^\beta b)$
   $\Rightarrow p^{\alpha-\beta} \mid (y_0^2 - b) \Rightarrow y_0^2 \equiv b \mod p^{\alpha-\beta}$).
   „$\Leftarrow$“: Ist $2 \mid \beta$ und erfüllt $\gamma_0 \in \mathbb{Z}$ die Kongruenz $y^2 \equiv b(p^{\alpha-\beta})$, so gilt: $(p^{\frac{\beta}{2}} y_0)^2 = p^\beta y_0^2 \equiv$

$p^\beta b \equiv a \mod p^\alpha$)
Also kann man sich darauf beschränken, die Lösbarkeit von Kongruenzen der Gestalt $x^2 \equiv a \mod p^\alpha$ mit $p \nmid a$ zu untersuchen.

4. Ist die Kongruenz $x^2 \equiv a \mod p^\alpha$ mit p Primzahl, $\alpha \in \mathbb{N}$ lösbar, so ist trivialerweise auch die Kongruenz $x^2 \equiv a \mod p$ lösbar. Wenn $p \neq 2$ und $p \nmid a$, gilt auch die Umkehrung, d. h. aus der Lösbarkeit von $x^2 \equiv a \mod p$ folgt bereits die Lösbarkeit von $x^2 \equiv a \mod p^\alpha \ \forall \alpha \in \mathbb{N}$.
Angenommen, $x_0 \in \mathbb{Z}$ erfülle nun die Kongruenz $x_0^2 \equiv a \mod p^\alpha$. Dann gilt dies auch für $x_0 + tp^\alpha \ \forall t \in \mathbb{Z}$, da $(x_0 + tp^\alpha)^2 = x_0^2 + 2x_0tp^\alpha + t^2p^{2\alpha} \equiv x_0^2 \equiv a \mod p^\alpha$. Wir wollen nun zeigen, dass es ein $t_0 \in \mathbb{Z}$ mit der Eigenschaft $(x_0 + tp^\alpha)^2 \equiv a \mod p^{\alpha+1}$ gibt. Wegen

$$\begin{aligned}(x_0 + tp^\alpha)^2 - a = x_0^2 + 2x_0tp^\alpha + t^2p^{2\alpha} - a &\equiv x_0^2 - a + 2x_0tp^\alpha \\ &= p^\alpha \left(\frac{x_0^2 - a}{p^\alpha} + 2x_0t \right) \mod p^{\alpha+1}\end{aligned}$$

reicht es, als t_0 eine Lösung der Kongruenz

$$2x_0t \equiv \frac{a - x_0^2}{p^\alpha} \mod p \qquad (*)$$

zu wählen. Da $p \neq 2$ und $p \nmid a$ (also $p \nmid x_0$), gilt: $\mathrm{ggT}\,(2x_0, p) = 1$ und (*) ist nach Satz 31 lösbar.

Für $p \neq 2$ kann man sich also darauf beschränken, Kongruenzen der Gestalt $x^2 \equiv a \mod p$ mit $p \nmid a$ zu untersuchen. Der Fall $p = 2$ unterscheidet sich vom (schwierigeren und interessanteren) Fall $p \neq 2$ und wird zuerst behandelt:

Satz 48
Sei $2 \nmid a$, dann gelten:

(i) Die Kongruenz $x^2 \equiv a \mod 2$ ist immer lösbar.

(ii) Die Kongruenz $x^2 \equiv a \mod 4$ ist lösbar $\Leftrightarrow a \equiv 1 \mod 4$

(iii) Sei $\alpha \in \mathbb{N}, \alpha \geq 3$. Dann gilt: Die Kongruenz $x^2 \equiv a \mod 2^\alpha$ ist lösbar $\Leftrightarrow a \equiv 1 \mod 8$

Beweis. (i) Es muss $a \equiv 1 \mod 2$ gelten, d. h. $x = 1$ ist Lösung.

(ii) Ist x Lösung von $x^2 \equiv a \mod 4$, so muss $2 \nmid x$ gelten. Für $x \equiv \pm 1 \mod 4$ gilt: $x^2 \equiv 1 \mod 4$, d. h. es muss $a \equiv 1 \mod 4$ gelten. Umgekehrt sind ± 1 zwei modulo 4 inkongruente Lösungen, wenn $a \equiv 1 \mod 4$.

(iii) Angenommen, $x^2 \equiv a \mod 8$ sei lösbar. Es muss wieder $2 \nmid x$ gelten. Sowohl für $x \equiv \pm 1 \mod 8$ als auch für $x \equiv \pm 3 \mod 8$ gilt $x^2 \equiv 1 \mod 8$. Also muss $a \equiv 1 \mod 8$ gelten.
Ist $x^2 \equiv a \mod 2^\alpha$ für $\alpha \geq 3$ lösbar $\Rightarrow x^2 \equiv a \mod 8$ lösbar $\Rightarrow a \equiv 1 \mod 8$.
Ist umgekehrt $a \equiv 1 \mod 8$, so sind ± 1 und ± 3 vier inkongruente Lösungen modulo 8 von $x^2 \equiv a \mod 8$. Wir zeigen nun: Ist $x^2 \equiv a \mod 8$ lösbar, so ist $x^2 \equiv a \mod 2^\alpha$ mit

$\alpha \geq 3$ lösbar. Angenommen, $x_0^2 \equiv a \mod 2^\alpha$, $\alpha \geq 3$: Dann ist auch $x_0 + 2^{\alpha-1}t$ Lösung für alle $t \in \mathbb{Z}$:

$$(x_0 + 2^{\alpha-1}t)^2 = x_0^2 + 2^\alpha t x_0 + 2^{2\alpha-2}t^2 \equiv x_0^2 \equiv a \mod 2^\alpha$$

Wir wollen nun zeigen: $\exists t_0 \in \mathbb{Z}$, sodass $(x_0 + 2^{\alpha-1}t_0)^2 \equiv a \mod 2^{\alpha+1}$. Da $\alpha \geq 3 \Leftrightarrow 2\alpha - 2 \geq \alpha + 1$, gilt

$$\begin{aligned}(x_0 + 2^{\alpha-1}t)^2 - a &= x_0^2 + 2^\alpha x_0 t + \underbrace{2^{2\alpha-2}t^2}_{\equiv 0 \mod 2^{\alpha+1}} - a \\ &\equiv x_0^2 - a + 2^\alpha x_0 t \\ &= 2^\alpha \left(\frac{x_0^2 - a}{2^\alpha} + x_0 t\right) \mod 2^{\alpha+1}\end{aligned}$$

und man kann t_0 eine Lösung der Kongruenz $x_0 t \equiv \frac{a - x_0^2}{2^\alpha} \mod 2$ wählen (diese existiert nach Satz 31, da $2 \nmid a \Rightarrow 2 \nmid x_0 \Rightarrow \text{ggT}(x_0, 2) = 1$). □

Definition „Quadratische Reste und Nichtreste“
Es sei $p \neq 2$ eine Primzahl und $a \in \mathbb{Z}$ mit $p \nmid a$. Man sagt, a sei quadratischer Rest modulo p, wenn die Kongruenz $x^2 \equiv a \mod p$ lösbar ist. Ist diese Kongruenz nicht lösbar, wird a quadratischer Nichtrest modulo p genannt.

Bemerkung Aufgrund der vorangegangenen Reduktionsschritte können wir uns darauf beschränken, den Fall zu untersuchen, dass $m \neq 2$ eine Primzahl ist und $m \nmid a$ gilt.

Lemma 49
Sei $p \neq 2$ Primzahl und $a \in \mathbb{Z}$ mit $p \nmid a$. Ist a quadratischer Rest modulo p, so gibt es genau zwei modulo p inkongruente Lösungen der Kongruenz $x^2 \equiv a \mod p$.

Beweis. Ist $x_0^2 \equiv a \mod p$ so gilt natürlich auch $(p - x_0)^2 \equiv x_0^2 \equiv a \mod p$. Es ist $x_0 \not\equiv -x_0 \mod p$ (denn: $x_0 \equiv -x_0 \mod p \Rightarrow 2x_0 \equiv 0 \mod p \Rightarrow p \mid (2x_0)$, Widerspruch, da $p \neq 2$ und $p \nmid a \Rightarrow p \nmid x_0$), d. h., es gibt mindestens zwei inkongruente Lösungen.
Gilt $x_0^2 \equiv a \mod p$ und $x_1^2 \equiv a \mod p$

$$\begin{aligned}&\Rightarrow x_0^2 \equiv x_1^2 \mod p \Rightarrow p \mid (x_0^2 - x_1^2) \Rightarrow p \mid (x_0 - x_1)(x_0 + x_1) \Rightarrow p \mid (x_0 - x_1) \vee p \mid (x_0 + x_1) \\ &\Rightarrow x_1 \equiv x_0 \mod p \vee x_1 \equiv -x_0 \mod p\end{aligned}$$

d. h. es gibt keine weiteren Lösungen. □

Lemma 50
Sei $p \neq 2$ Primzahl. Von den $p-1$ primen Restklassen modulo p ist genau die Hälfte $\left(\text{d. h. } \frac{p-1}{2}\right)$ quadratischer Rest, nämlich $1^2, \ldots, \left(\frac{p-1}{2}\right)^2$.

Beweis. Die Restklassen $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$ sind offenbar quadratischer Rest. Sie sind alle verschieden, denn wenn $k, l \in \{1, \ldots, \frac{p-1}{2}\}$ und $k^2 \equiv l^2 \mod p \Rightarrow k \equiv l \mod p \vee k \equiv -l \mod p$. Aus $k \equiv l \mod p$ folgt $k = l$ und $k \equiv -l \mod p$ ist unmöglich ($k \equiv -l \mod p \Rightarrow p \mid$

$(k+l)$, was wegen $1 \leq k+l \leq p-1$ unmöglich ist.)
Also gibt es mindestens $\frac{p-1}{2}$ modulo p paarweise inkongruente quadratische Reste.
Zeige: Es gibt keine weiteren. Ist a quadratischer Rest, so $\exists x_0 \in \{1, \ldots, p-1\} : x_0^2 \equiv a \mod p$.
Man erhält durch $\left(\frac{p+1}{2}\right)^2, \left(\frac{p+3}{2}\right)^2, \ldots, (p-1)^2$ aber keine zusätzlichen quadratischen Reste, da

$$\left(\frac{p+1}{2}\right)^2 \equiv \left(\frac{p-1}{2}\right)^2 \mod p, \ldots, (p-1)^2 \equiv 1^2 \mod p$$

□

Definition „Legendre-Symbol“
Sei $p \neq 2$ Primzahl und $a \in \mathbb{Z},\ p \nmid a$.
Das LEGENDRE-Symbol $\left(\frac{a}{p}\right)$ ist definiert durch

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{wenn a quadratischer Rest modulo } p \text{ ist} \\ -1 & \text{wenn a quadratischer Nichtrest modulo } p \text{ ist} \end{cases}$$

Bemerkung

1. Offenbar gilt: Wenn $a \equiv b \mod p$ dann ist $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.
2. Oft wird ergänzend $\left(\frac{a}{p}\right) = 0$ gesetzt, wenn $p \mid a$.
3. Man spricht „a nach p“ für $\left(\frac{a}{p}\right)$.

Satz 51
Sei $p \neq 2$ Primzahl und $a \in \mathbb{Z}$ mit $p \nmid a$. Dann ist $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \mod p$

Beweis. Sei zunächst a quadratischer Rest mod p. Dann $\exists x_0 \in \mathbb{Z} : x_0^2 \equiv a \mod p$, wobei $p \nmid x_0$ gelten muss. Daher $a^{\frac{p-1}{2}} \equiv (x_0^2)^{\frac{p-1}{2}} = x_0^{p-1} \overset{\text{Korollar 47}}{\equiv} 1 = \left(\frac{a}{p}\right) \mod p$.
Sei jetzt a quadratischer Nichtrest modulo p. Wähle $x \in \{1, 2, \ldots, p-1\}$. Nach Satz 31 gibt es genau ein $y \in \{1, 2, \ldots, p-1\}$ derart, dass $xy \equiv a \mod p$. Da a quadratischer Nichtrest ist, ist es unmöglich, dass $x = y$. Sind $x, x' \in \{1, 2, \ldots, p-1\}$ verschieden, so sind auch $y, y' \in \{1, 2, \ldots, p-1\}$ mit $xy \equiv x'y' \equiv a \mod p$ verschieden (denn $y = y' \Rightarrow xy \equiv x'y \equiv a \mod p \Rightarrow p \mid ((x-x')y) \Rightarrow p \mid (x-x') \Rightarrow x \equiv x' \mod p \Rightarrow x = x'$). D. h. die Menge $\{1, 2, \ldots, p-1\}$ zerfällt in $\frac{p-1}{2}$ Paare x, y mit der Eigenschaft $xy \equiv a \mod p \Rightarrow a^{\frac{p-1}{2}} \equiv (p-1)! \overset{\text{Satz 40}}{\equiv} \left(\frac{a}{p}\right) \mod p$ □

Korollar 52 „Eulersches Kriterium“
Sei $p \neq 2$ Primzahl und $a \in \mathbb{Z}$. Dann sind äquivalent:

(i) a ist quadratischer Rest mod p

(ii) $a^{\frac{p-1}{2}} \equiv 1 \mod p$

Beweis. Folgt aus Satz 51 □

Korollar 53
Sei $p \neq 2$ Primzahl und $a, b \in \mathbb{Z}$ mit $p \nmid a,\ p \nmid b$. Dann gilt:

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

Beweis.

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \mod p \Rightarrow \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

□

Bemerkung
1. Man kann Korollar 53 so formulieren: Das Legendre-Symbol $\left(\frac{\cdot}{p}\right)$ ist ein Gruppenhomomorphismus $(\mathbb{Z}_p^*, \cdot) \to (\{1, -1\}, \cdot)$, dessen Kern genau die quadratischen Reste sind. Insbesondere bilden die quadratischen Reste (also die Quadrate in $\mathbb{Z}_p^*$) eine Untergruppe von $(\mathbb{Z}_p^*, \cdot)$.
2. Mit Induktion folgt sofort: Gilt $p \nmid a_i$ (für $1 \leq i \leq k$), so ist $\left(\frac{a_1 \ldots a_k}{p}\right) = \prod_{i=1}^{k} \left(\frac{a_i}{p}\right)$
3. Weiters folgt $\left(\frac{a^2}{p}\right) = \left(\frac{a}{p}\right)^2 = 1\ \forall a \in \mathbb{Z},\ p \nmid a$ und daher $\left(\frac{a^2 b}{p}\right) = \left(\frac{b}{p}\right)\ \forall a, b \in \mathbb{Z},\ p \nmid a,\ p \nmid b$.
   Z. B. ist $\left(\frac{12}{5}\right) = \left(\frac{2^2 \cdot 3}{5}\right) = \left(\frac{2}{5}\right)^2 \left(\frac{3}{5}\right) = \left(\frac{3}{5}\right)$.

Korollar 54 „Erster Ergänzungssatz“
Sei $p \neq 2$ Primzahl. Dann

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

D. h. -1 ist quadratischer Rest mod p wenn $p \equiv 1 \mod 4$ und quadratischer Nichtrest wenn $p \equiv 3 \mod 4$.

Beweis.

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \mod p \Rightarrow \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

□

Korollar 55
Es gibt unendlich viele Primzahlen $\equiv 1 \mod 4$.

Beweis. Angenommen, $p_1, \ldots, p_s$ wären alle Primzahlen $\equiv 1 \mod 4$.
Setze $N := (2p_1 \cdot \cdots \cdot p_s)^2 + 1$. Sei p Primzahl mit $p \mid N$. Dann $p \notin \{2, p_1, \ldots, p_s\}$
$\Rightarrow p \equiv 3 \mod 4$. Andererseits gilt $(2p_1 \ldots p_s)^2 \equiv -1 \mod p \Rightarrow \left(\frac{-1}{p}\right) = 1$
$\Rightarrow p \equiv 1 \mod 4$, Widerspruch! □

Satz 56 „Gausssches Lemma“
Sei $p \neq 2$ Primzahl und $a \in \mathbb{Z},\ p \nmid a$.
Für $ja \in \{a, 2a, \ldots, \frac{p-1}{2}a\}$ (d. h. $1 \leq j \leq \frac{p-1}{2}$) sei $r_j \in \mathbb{Z}$ durch $ja \equiv r_j \mod p$ und $-\frac{p-1}{2} \leq r_j \leq \frac{p-1}{2}$ eindeutig festgelegt. Schließlich bezeichne $\gamma_p(a)$ die Anzahl der $j \in \{1, 2, \ldots, \frac{p-1}{2}\}$ für die $r_j < 0$ gilt. Dann ist

$$\left(\frac{a}{p}\right) = (-1)^{\gamma_p(a)}$$

Beweis. Zeige zunächst $\{|r_1|, \ldots, |r_{\frac{p-1}{2}}|\} = \{1, \ldots, \frac{p-1}{2}\}$. Es ist klar, dass $1 \leq |r_j| \leq \frac{p-1}{2}$ für $1 \leq j \leq \frac{p-1}{2}$. Es reicht zu zeigen, dass $|r_i| \neq |r_j|$ für $1 \leq i, j \leq \frac{p-1}{2},\ i \neq j$. Wäre $|r_i| = |r_j|$, so $ia \equiv ja \mod p \vee ia \equiv -ja \mod p \overset{p \nmid a}{\Longrightarrow} i \equiv j \mod p \vee i \equiv -j \mod p \Rightarrow p \mid (i-j)$ (und daher $i = j$) oder $p \mid (i+j)$ (was unmöglich ist). Also $i = j$

$$\Rightarrow \left(\frac{p-1}{2}\right)!\, a^{\frac{p-1}{2}} = a\,(2a)\cdots\left(\frac{p-1}{2}a\right) \equiv r_1 r_2 \cdots r_{\frac{p-1}{2}} = (-1)^{\gamma_p(a)}|r_1||r_2|\cdots\left|r_{\frac{p-1}{2}}\right|$$
$$= (-1)^{\gamma_p(a)}\left(\frac{p-1}{2}\right)!(p)$$
$$\text{Da } p \nmid \left(\frac{p-1}{2}\right)! \Rightarrow (-1)^{\gamma_p(a)} \overset{\text{Satz 51}}{\equiv} a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \mod p \Rightarrow \left(\frac{a}{p}\right) = (-1)^{\gamma_p(a)}$$

□

Korollar 57 „Zweiter Ergänzungssatz“
Sei $p \neq 2$ Primzahl. Dann ist:

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

D. h. 2 ist quadratischer Rest mod p wenn p $\equiv \pm 1 \mod 8$ und quadratischer Nichtrest wenn $p \equiv \pm 3 \mod 8$.

Beweis. Nach Satz 56 müssen wir bestimmen, wieviele Elemente der Menge $\{2, 4, \ldots, p-1\}$ größer $\frac{p-1}{2}$ sind, d. h., ist $m \in \{1, 2, \ldots, \frac{p-1}{2}\}$ derart, dass $2m \leq \frac{p-1}{2} < 2(m+1)$, so ist

$\gamma_p(2) = \frac{p-1}{2} - m$.

1. Fall: $p = 8k+1 \Rightarrow \dfrac{p-1}{2} = 4k \Rightarrow 2m = 4k \Rightarrow m = 2k \Rightarrow \gamma_p(2) = 4k - 2k = 2k$

$\Rightarrow \left(\dfrac{2}{p}\right) = (-1)^{2k} = 1$

2. Fall: $p = 8k+7 \Rightarrow \dfrac{p-1}{2} = 4k+3 \Rightarrow 2m = 4k+2 \Rightarrow m = 2k+1$

$\Rightarrow \gamma_p(2) = 4k+3-(2k+1) = 2k+2 \Rightarrow \left(\dfrac{2}{p}\right) = (-1)^{2k+2} = 1$

3. Fall: $p = 8k+3 \Rightarrow \dfrac{p-1}{2} = 4k+1 \Rightarrow 2m = 4k \Rightarrow m = 2k \Rightarrow \gamma_p(2) = 4k+1-2k$

$= 2k+1 \Rightarrow \left(\dfrac{2}{p}\right) = (-1)^{2k+1} = -1$

4. Fall: $p = 8k+5 \Rightarrow \dfrac{p-1}{2} = 4k+2 \Rightarrow 2m = 4k+2 \Rightarrow m = 2k+1$

$\Rightarrow \gamma_p(2) = 4k+2-2k+1 = 2k+1 \Rightarrow \left(\dfrac{2}{p}\right) = (-1)^{2k+1} = -1$

Schließlich gilt $p = 8k \pm 1 \Rightarrow p^2 = 64k^2 \pm 16k + 1 \Rightarrow \frac{p^2-1}{8} = 8k^2 + 2k \equiv 0 \mod 2$ und $p = 8k \pm 3 \Rightarrow p^2 = 64k^2 \pm 48k + 9 \Rightarrow \frac{p^2-1}{8} = 8k^2 \pm 6k + 1 \equiv 1 \mod 2$.
Bemerkung: Sei $ja = qp + r$ mit $0 \leq r \leq p-1$. Falls $0 \leq r \leq \frac{p-1}{2}$, so $r_j = r$. Falls $\frac{p+1}{2} \leq r \leq p-1$, so ist $r_j = r - p$, denn $-\frac{p-1}{2} = \frac{p+1}{2} - p \leq r - p \leq -1$. □

Korollar 58
Sei $p \neq 2$ Primzahl und $a \in \mathbb{Z}$ mit $p \nmid a$. Dann gelten:

(i) $\left(\frac{a}{p}\right) = \prod_{i=1}^{\frac{p-1}{2}} (-1)^{\left[\frac{2ai}{p}\right]}$

(ii) Gilt zusätzlich $2 \nmid a$, so $\left(\frac{a}{p}\right) = \prod_{i=1}^{\frac{p-1}{2}} (-1)^{\left[\frac{ai}{p}\right]}$

Beweis. (i) Sei r_i (für $1 \leq i \leq \frac{p-1}{2}$) wie in Satz 56. Wir zeigen

$$r_i < 0 \Leftrightarrow \left[\frac{2ai}{p}\right] \equiv 1 \mod 2$$

Sei $r_i > 0$. Dann gilt:

$$r_i = ai - \left[\frac{ai}{p}\right] p \leq \frac{p-1}{2} < \frac{p}{2} \Rightarrow 0 < \frac{2ai}{p} - 2\left[\frac{ai}{p}\right] < 1 \Rightarrow \left[\frac{2ai}{p}\right] = 2\left[\frac{ai}{p}\right] \equiv 0 \mod 2$$

Sei $r_i < 0$. Dann gilt:

$$0 < r_i + p = ai - \left[\frac{ai}{p}\right] p < p$$

$$\text{Da} \qquad r_i + p \geq -\frac{p-1}{2} + p = \frac{p+1}{2} > \frac{p}{2} \qquad \text{folgt:}$$

$$\frac{p}{2} < ai - \left[\frac{ai}{p}\right] p < p \Rightarrow 1 < \frac{2ai}{p} - 2\left[\frac{ai}{p}\right] < 2 \Rightarrow 0 < \frac{2ai}{p} - 2\left[\frac{ai}{p}\right] - 1 < 1$$
$$\Rightarrow \left[\frac{2ai}{p}\right] = 2\left[\frac{ai}{p}\right] + 1 \equiv 1 \mod 2$$

(ii)

$$\left(\frac{a}{p}\right) = \left(\frac{a+p}{p}\right) = \left(\frac{2^{\frac{a+p}{2}}}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{\frac{a+p}{2}}{p}\right) \overset{\text{(i)}}{=} \left(\frac{2}{p}\right) \prod_{i=1}^{\frac{p-1}{2}} (-1)^{\left[\frac{(a+p)i}{p}\right]} = \left(\frac{2}{p}\right) \prod_{i=1}^{\frac{p-1}{2}} (-1)^{\left[\frac{ai}{p}+i\right]} =$$
$$= \left(\frac{2}{p}\right) \prod_{i=1}^{\frac{p-1}{2}} (-1)^{\left[\frac{ai}{p}\right]+i} = \left(\frac{2}{p}\right) \prod_{i=1}^{\frac{p-1}{2}} (-1)^{\left[\frac{ai}{p}\right]} \prod_{i=1}^{\frac{p-1}{2}} (-1)^{i} = \left(\frac{2}{p}\right) \prod_{i=1}^{\frac{p-1}{2}} (-1)^{\left[\frac{ai}{p}\right]} (-1)^{\frac{1}{2}\frac{p-1}{2}\frac{p+1}{2}} =$$
$$= \left(\frac{2}{p}\right) \prod_{i=1}^{\frac{p-1}{2}} (-1)^{\left[\frac{ai}{p}\right]} (-1)^{\frac{p^2-1}{8}} = \prod_{i=1}^{\frac{p-1}{2}} (-1)^{\left[\frac{ai}{p}\right]}$$

□

Satz 59 „Quadratisches Reziprozitätsgesetz für das Legendre-Symbol“
Es seien p und q zwei verschiedene ungerade Primzahlen. Dann gilt:

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

Beweis. Betrachte ein Rechteck mit den Eckpunkten $(0,0)$, $(\frac{p}{2},0)$, $(0,\frac{q}{2})$ und $(\frac{p}{2},\frac{q}{2})$.
Es enthält $\frac{p-1}{2}\frac{q-1}{2}$ Gitterpunkte (d. h. Punkte mit Koordinaten in $\mathbb{N}$) in seinem Inneren. Davon liegt keiner auf der Diagonalen $y = \frac{q}{p}x$ (denn $y \in \mathbb{N} \Rightarrow \frac{qx}{p} \in \mathbb{N} \Rightarrow p \mid (qx) \Rightarrow p \mid x$, Widerspruch zu $0 < x < \frac{p-1}{2}$).
Unterhalb der Diagonale liegen $\sum_{i=1}^{\frac{p-1}{2}} \left[\frac{q_i}{p}\right]$ Gitterpunkte und oberhalb der Diagonale liegen $\sum_{i=1}^{\frac{q-1}{2}} \left[\frac{p_j}{p}\right]$ Gitterpunkte. Daher folgt: $\sum_{i=1}^{\frac{p-1}{2}} \left[\frac{q_i}{p}\right] + \sum_{i=1}^{\frac{q-1}{2}} \left[\frac{p_j}{p}\right] = \frac{p-1}{2}\frac{q-1}{2}$

$$\Rightarrow \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) \overset{\text{Kor 58(ii)}}{=} \prod_{j=1}^{\frac{q-1}{2}} (-1)^{\left[\frac{p_j}{q}\right]} \prod_{i=1}^{\frac{p-1}{2}} (-1)^{\left[\frac{q_i}{q}\right]} = (-1)^{\sum_{i=1}^{\frac{q-1}{2}}\left[\frac{q_i}{p}\right]+\sum_{i=1}^{\frac{p-1}{2}}\left[\frac{p_j}{p}\right]=\frac{p-1}{2}\frac{q-1}{2}} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

□

Bemerkung 1. Das quadratische Reziprozitätsgesetz wird meist in der Form

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

angewandt.

2. Satz 59 impliziert, dass $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ wenn $p \equiv 1 \mod 4$ oder $q \equiv 1 \mod 4$ und $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$ wenn $p \equiv q \equiv 3 \mod 4$.

Beispiel
Ist $x^2 \equiv -21 \mod 61$ lösbar? (Beachte: 61 ist Primzahl und $\text{ggT}(61,-21)=1$)
1. Lösungsweg:

$$\left(\frac{-21}{61}\right) = \underbrace{\left(\frac{-1}{61}\right)}_{=(-1)^{30}=1 \text{ oder } 61\equiv 1 \mod 4} \left(\frac{3}{61}\right)\left(\frac{7}{61}\right) = \left(\frac{3}{61}\right)\left(\frac{7}{61}\right) =$$

$$= \underbrace{(-1)^{1\cdot 30}}_{=1 \text{ oder } 61\equiv 1 \mod 4} \left(\frac{61}{3}\right)\left(\frac{7}{61}\right) = \underbrace{\left(\frac{61}{3}\right)}_{=\left(\frac{1}{3}\right)=1 \text{ da } 61\equiv 1 \mod 3 \text{ und } 1=1^2} \left(\frac{7}{61}\right) =$$

$$= \underbrace{(-1)^{3\cdot 30}}_{=1 \text{ oder } 61\equiv 1 \mod 4} \underbrace{\left(\frac{61}{7}\right)}_{=\left(\frac{5}{7}\right) \text{ da } 61\equiv 5 \mod 7} = \left(\frac{5}{7}\right) =$$

$$= \underbrace{(-1)^{2\cdot 3}}_{=1 \text{ oder } 5\equiv 1 \mod 4} \underbrace{\left(\frac{7}{5}\right)}_{=\left(\frac{2}{5}\right) \text{ da } 7\equiv 2 \mod 5} = \left(\frac{2}{5}\right) = (-1)^{\frac{24}{8}} =$$

$$= \underbrace{(-1)^{3}}_{\text{oder } 5\equiv -3 \mod 8} = -1$$

2. Lösungsweg:

$$\left(\frac{-21}{61}\right) = \left(\frac{40}{61}\right) = \left(\frac{2^2\cdot 10}{61}\right) = \left(\frac{10}{61}\right) = \left(\frac{2}{61}\right)\left(\frac{5}{61}\right) = \underbrace{(-1)^{\frac{3720}{8}}}_{=(-1)^{465}=-1} \left(\frac{5}{61}\right) =$$

$$= - \underbrace{\left(\frac{5}{61}\right)}_{(-1)^{2\cdot 30}\left(\frac{61}{5}\right) \text{ bzw. } 5\equiv 61\equiv 1 \mod 4} = -\left(\frac{61}{5}\right) = -\left(\frac{1}{5}\right) = -1$$

D. h. -21 ist quadratischer Nichtrest modulo 61.

Korollar 60 (i) Es gibt unendlich viele Primzahlen $\equiv 1 \mod 6$

(ii) Es gibt unendlich viele Primzahlen $\equiv 1 \mod 3$

Beweis. (i) Angenommen, $p_1, \ldots, p_s$ wären alle Primzahlen $\equiv 1 \mod 6$.
Setze $N := 4(p_1 \cdots p_s)^2 + 3$. Sei p Primzahl mit $p \mid N$. Dann $p \notin \{2, 3, p_1, \ldots, p_s\}$
$\Rightarrow p \equiv 5 \mod 6$. Andererseits gilt $(2p_1 \cdots p_s)^2 \equiv -3 \mod p$

$$\Rightarrow 1 = \left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) \overset{\text{Kor 54}}{=} (-1)^{\frac{p-1}{2}} \left(\frac{3}{p}\right) \overset{\text{Satz 59}}{=} (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}\frac{3-1}{2}} \left(\frac{p}{3}\right) =$$
$$= (-1)^{p-1}\left(\frac{p}{3}\right) = \left(\frac{p}{3}\right)$$

Da $p \equiv 2 \mod 3$ muss aber $\left(\frac{p}{3}\right) = \left(\frac{2}{3}\right) = (-1)^{\frac{9-1}{8}} = -1$ folgen, Widerspruch!
Also $p \equiv 1 \mod 3$. Da auch $p \equiv 1 \mod 2$ folgt $p \equiv 1 \mod 6$, Widerspruch!

(ii) Folgt sofort aus (i) □

Bemerkung Wir haben die folgenden Spezialfälle des Dirichletschen Primzahlsatzes bewiesen: $p \equiv 1 \mod 2$ (trivial), $p \equiv 1 \mod 3$ (Korollar 60(ii)), $p \equiv 2 \mod 3$) (Bsp. 35), $p \equiv 1 \mod 4$ (Korollar 55), $p \equiv 3 \mod 4$ (Satz 14), $p \equiv 1 \mod 6$ (Korollar 60(i)), $p \equiv 5 \mod 6$ (Bsp. 36).
D. h., die Fälle $2, 3, 4, 6$ (als Modul) sind vollständig bewiesen.

Bemerkung Eine Erweiterung des Legendresymbols ist das JACOBI-Symbol $\left(\frac{a}{m}\right)$, das folgendermaßen definiert ist:
Sei $m \in \mathbb{N}$ ungerade und $m = p_1 \cdots p_k$ die Primfaktorzerlegung vom m mit (nicht notwendigerweise verschiedenen) Primzahlen $p_1, \ldots, p_k$ und $a \in \mathbb{Z}$ mit $\mathrm{ggT}\,(a, m) = 1$. Dann sei

$$\left(\frac{a}{m}\right) = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)$$

wobei $\left(\frac{a}{p_i}\right)$ das Legendresymbol bezeichnet (für $1 \leq i \leq k$).
Ist $\left(\frac{a}{m}\right) = -1$, so ist a quadratischer Nichtrest mod m, da dann $\exists i \in \{1, \ldots, k\} : \left(\frac{a}{p_i}\right) = -1$, d. h. $x^2 \equiv a \mod p_i$ ist unlösbar und daher auch $x^2 \equiv a \mod m$.
Ist $\left(\frac{a}{m}\right) = 1$, so kann a sowohl quadratischer Rest als auch quadratischer Nichtrest modulo m sein, z. B. ist $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1$, d. h. 2 ist quadratischer Nichtrest modulo 15 (da 2 quadratischer Nichtrest mod 3 bzw. 5 ist) aber $\left(\frac{2}{15}\right) = 1$.
Ist $a \equiv b \mod m$, so ist auch $\mathrm{ggT}\,(b, m) = 1$ und

$$\left(\frac{b}{m}\right) = \left(\frac{a}{m}\right) \qquad \left(\text{da } \left(\frac{b}{m}\right) = \prod_{i=1}^{k} \left(\frac{b}{p_i}\right) = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right) = \left(\frac{a}{m}\right)\right)$$

Sind $a, b \in \mathbb{Z}$ mit $\mathrm{ggT}\,(a, m) = \mathrm{ggT}\,(b, m) = 1$, so ist auch $\mathrm{ggT}\,(ab, m) = 1$ und

$$\left(\frac{ab}{m}\right) = \left(\frac{a}{m}\right)\left(\frac{b}{m}\right) \qquad \left(\text{da } \left(\frac{ab}{m}\right) = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)\left(\frac{b}{p_i}\right) = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right) \prod_{i=1}^{k} \left(\frac{b}{p_i}\right) = \left(\frac{a}{m}\right)\left(\frac{b}{m}\right)\right)$$

Ist m ungerade, so gelten

$$\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}} \qquad \text{und} \qquad \left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}$$

(Erster und zweiter Ergänzungssatz).
Sind $m, n \in \mathbb{N}$ ungerade und $\mathrm{ggT}\,(m, n) = 1$, so gilt:

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

(Quadratisches Reziprozitätsgesetz).

Kapitel 6

Kettenbrüche

Definition
i[Endlicher Kettenbruch] Seien $a_0, a_1, \ldots, a_n, c_1, \ldots, c_n \in \mathbb{R}$. Ein Ausdruck der Gestalt

$$a_0 + \cfrac{c_1}{a_1 + \cfrac{c_2}{a_2 + \cfrac{c_3}{\ddots + \cfrac{c_n}{a_n}}}}$$

wird endlicher Kettenbruch genannt.
Dabei setzen wir voraus, dass keiner der auftretenden Nenner $= 0$ ist.
Man schreibt stattdessen auch platzsparender

$$a_0 + \frac{c_1|}{|a_1} + \frac{c_2|}{|a_2} + \cdots + \frac{c_n|}{|a_n}$$

Zu diesem Kettenbruch definiert man zwei Folgen $(p_k)_{k\geq -2},\ (q_k)_{k\geq -2}$ folgendermaßen:

$$p_{-2} = 0,\ p_{-1} = 1,\ p_k = a_k p_{k-1} + c_k p_{k-2} \text{ für } k \geq 0$$
$$q_{-2} = 1,\ q_{-1} = 0,\ q_k = a_k q_{k-1} + c_k q_{k-2} \text{ für } k \geq 0$$

Satz 61
Seien $a_0, \ldots, a_n, c_0, \ldots, c_n \in \mathbb{R}$ wie oben. Dann gilt:

$$\frac{p_k}{q_k} = a_0 + \frac{c_1|}{|a_1} + \cdots + \frac{c_k|}{|a_k} \text{ für } k \geq 0$$

wobei man c_0 gleich 1 setzt.

Beweis. Induktion nach k:
k=0:

$$\frac{p_0}{q_0} = \frac{a_0 \cdot 1 + 1 \cdot 0}{a_0 \cdot 0 + 1 \cdot 1} = a_0$$

k=1:

$$\frac{p_1}{q_1} = \frac{a_0a_1 + c_1 \cdot 1}{a_1 \cdot 1 + c_1 \cdot 0} = \frac{a_0a_1 + c_1}{a_1} = a_0 + \frac{c_1}{a_1}$$

Induktionsschritt:

$$a_0 + \frac{c_1|}{|a_1} + \cdots + \frac{c_k|}{|a_k} + \frac{c_{k+1}|}{|a_{k+1}} = a_0 + \frac{c_1|}{|a_1} + \cdots + \frac{c_{k-1}|}{|a_{k-1}} + \frac{c_k|}{\left|a_k + \frac{c_{k+1}}{a_{k+1}}\right.} \overset{\text{IV}}{=}$$

$$\overset{\text{IV}}{=} \frac{(a_k + \frac{c_{k+1}}{a_{k+1}})p_{k-1} + c_kp_{k-2}}{(a_k + \frac{c_{k+1}}{a_{k+1}})q_{k-1} + c_kq_{k-2}} = \frac{a_kp_{k-1} + c_kp_{k-2} + \frac{c_{k+1}}{a_{k+1}}p_{k-1}}{a_kq_{k-1} + c_kq_{k-2} + \frac{c_{k+1}}{a_{k+1}}q_{k-1}} =$$

$$= \frac{p_k + \frac{c_{k+1}}{a_{k+1}}p_{k-1}}{q_k + \frac{c_{k+1}}{a_{k+1}}q_{k-1}} = \frac{a_{k+1}p_k + c_{k+1}p_{k-1}}{a_{k+1}q_k + c_{k+1}q_{k-1}} = \frac{p_{k+1}}{q_{k+1}}$$

□

Satz 62
Seien $a_0, a_1, \ldots, a_n, c_1, \ldots, c_n \in \mathbb{R}$ wie oben, dann gilt:

$$p_kq_{k-1} - q_kp_{k-1} = (-1)^{k-1}c_1 \cdots c_k \qquad \text{für} \qquad -1 \leq k \leq n$$

(für $k \in \{-1, 0\}$ ist $c_1 \cdots c_k = 1$, da es das leere Produkt ist.)

Beweis. Induktion nach k:

- $k = -1$: $p_{-1}q_{-2} - q_{-1}p_{-2} = 1 \cdot 1 - 0 \cdot 0 = 1 = (-1)^2 = (-1)^{-1-1}$
- $k = 0$: $p_0q_{-1} - q_0p_{-1} = a_0 \cdot 0 - 1 \cdot 1 = -1 = (-1)^{0-1}$
- $k - 1 \to k$: $p_kq_{k-1} - q_kp_{k-1} = (a_kp_{k-1} + c_kp_{k-2})q_{k-1} - (a_kq_{k-1} + c_kq_{k-2})p_{k-1} =$
  $= c_k(p_{k-2}q_{k-1} - q_{k-2}p_{k-1}) = -c_k(-1)^{k-2}c_1 \cdots c_{k-1} = (-1)^{k-1}c_1 \cdots c_k$ □

Definition „Regelmäßige Kettenbrüche“
Ein Kettenbruch $a_0 + \frac{c_1|}{|a_1} + \cdots + \frac{c_n|}{|a_n}$ heißt regelmäßig, wenn $a_0 \in \mathbb{Z}$, $c_i = 1$ für $1 \leq i \leq n$ und $a_1, \ldots, a_n \in \mathbb{N}$. Bei einem solchen Kettenbruch kann kein Nenner $= 0$ auftreten.
Statt $a_0 + \frac{1|}{|a_1} + \cdots + \frac{1|}{|a_n}$ schreibt man $[a_0; a_1, \ldots, a_n]$.

Satz 63
Sei $\frac{a}{b} \in \mathbb{Q}$ (mit $a \in \mathbb{Z}, b \in \mathbb{N}$). Dann gibt es $a_0 \in \mathbb{Z}, a_1, \ldots, a_n \in \mathbb{N}$ derart, dass $\frac{a}{b} = [a_0; a_1, \ldots, a_n]$.

Beweis. Wende (wie im euklidischen Algorithmus) fortwährend Division mit Rest auf a und b an:

$$\begin{aligned}
a &= a_0b + r_1 \\
b &= a_1r_1 + r_2 \\
r_1 &= a_2r_2 + r_3 \\
&\vdots \\
r_{n-2} &= a_{n-2}r_{n-1} + r_n \\
r_{n-1} &= a_nr_n
\end{aligned}$$

mit $b > r_1 > r_2 > \cdots > r_{n-1} > r_n > 0$. Zeige nun mit Induktion, dass für $1 \leq k \leq n$ gilt:

$$\frac{a}{b} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_{k-1} + \cfrac{r_k}{r_{k-1}}}}}} \qquad (*)$$

Für $k = 1$ ist $\frac{a}{b} = a_0 + \frac{r_1}{b} = a_0 + \frac{r_1}{r_0}$ (beachte $b = r_0$)
Sei die Behauptung für k bereits gezeigt. Wegen

$$r_{k-1} = a_k r_k + r_{k+1} \Rightarrow \frac{r_{k-1}}{r_k} = a_k + \frac{r_{k+1}}{r_k} \Rightarrow \frac{r_k}{r_{k-1}} = \cfrac{1}{a_k + \cfrac{r_{k+1}}{r_k}}$$

$$\Rightarrow \frac{a}{b} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_{k-1} + \cfrac{1}{a_k + \cfrac{r_{k+1}}{r_k}}}}}}$$

Für $k = n$ erhält man aus (*) die Behauptung, da $\frac{r_n}{r_{n-1}} = \frac{1}{a_n}$. □

Bemerkung Die regelmäßige Kettenbruchentwicklung einer rationalen Zahl ist nicht eindeutig. Ist $a_n > 1$, so ist $[a_0; a_1, \ldots, a_n] = [a_0; a_1, \ldots, a_n - 1, 1]$ (da $a_n = a_{n-1} + \frac{1}{1}$). Umgekehrt ist $[a_0; a_1, \ldots, a_{n-1}, 1] = [a_0; a_1, \ldots, a_{n-1} + 1]$ (da $a_{n-1} + \frac{1}{1} = a_{n-1} + 1$).

Beispiel 1. Entwickle $\frac{37}{49}$ in einen Kettenbruch:

$$\frac{37}{49} = 0 + \frac{1}{\frac{49}{37}} = 0 + \frac{1}{1 + \frac{12}{37}} = 0 + \frac{1}{1 + \frac{1}{\frac{37}{12}}} = 0 + \frac{1}{1 + \frac{1}{3 + \frac{1}{12}}} \left(= 0 + \frac{1}{1 + \frac{1}{3 + \frac{1}{11 + \frac{1}{1}}}} \right)$$

$\Rightarrow$ d. h. $\frac{37}{49} = [0; 1, 3, 12]$ $(= [0; 1, 3, 11, 1])$
Oder mittels Division mit Rest:

$$37 = \underbrace{0}_{=a_0} \cdot 49 + 37, \quad 49 = \underbrace{1}_{=a_1} \cdot 37 + 12, \quad 37 = \underbrace{3}_{=a_2} \cdot 12 + 1, \quad 12 = \underbrace{12}_{=a_3} \cdot 1 + 0$$

2. Bestimme den Wert des Kettenbruchs $[2; 1, 5, 2]$ $(= 2 + \frac{1}{1+\frac{1}{5+\frac{1}{2}}})$:

   Verwende die Rekursionsrelationen $p_{k+1} = a_{k+1}p_k + p_{k-1}$, $q_{k+1} = a_{k+1}q_k + q_{k-1}$

k	-2	-1	0	1	2	3
a_k	-	-	2	1	5	2
p_k	0	1	2	3	17	37
q_k	1	0	1	1	6	13

   d. h. $[2; 1, 5, 2] = \frac{p_3}{q_3} = \frac{37}{13}$

   Oder direkt:

$$2 + \frac{1}{1 + \frac{1}{5 + \frac{1}{2}}} = 2 + \frac{1}{1 + \frac{1}{\frac{11}{2}}} = 2 + \frac{1}{1 + \frac{2}{11}} = 2 + \frac{1}{\frac{13}{11}} = 2 + \frac{11}{13} = \frac{37}{13}$$

Definition „Näherungsbruch“
Sei $[a_0; a_1, \ldots, a_n]$ ein regelmäßiger Kettenbruch. Dann wird $\frac{p_k}{q_k} = [a_0; a_1, \ldots, a_k]$ mit $0 \leq k \leq n$ der k-te Näherungsbruch von $[a_0; a_1, \ldots, a_n]$ genannt.

Bemerkung 1. $(p_k)_{k\geq -2}$, $(q_k)_{k\geq -2}$ erfüllen die Rekursionsrelationen $p_{k+1} = a_{k+1}p_k + p_{k-1}, q_{k+1} = a_{k+1}q_k + q_{k-1}\ \forall k \geq -1$.

2. Da $[a_0; a_1, \ldots, a_n]$ regelmäßig ist, gilt $p_k, q_k \in \mathbb{Z}\ \forall k \geq -2$ und $q_k \in \mathbb{N}\ \forall k \geq 0$.

3. Aus Satz 62 folgt $p_k q_{k-1} - q_k p_{k-1} = (-1)^{k-1}\ \forall k \geq -1$

4. Aus Bemerkung 3 folgt sofort $\mathrm{ggT}\,(p_k, q_k) = 1\ \forall k \geq -2$
(und $\mathrm{ggT}\,(p_k, p_{k+1}) = \mathrm{ggT}\,(q_k, q_{k+1}) = 1$).

5. Die Folge $(q_k)_{k\geq 1}$ wächst exponentionell, genauer gilt $q_k \geq \sqrt{2}^{k-1}\ \forall \geq 0$
(Induktion nach k: $k = 0 : q_0 = 1 > \frac{1}{\sqrt{2}} = \sqrt{2}^{0-1}$, $k = 1 : q_1 = a_1 \geq 1 = \sqrt{2}^{1-1}$,
$q_{k+1} = a_{k+1}a_k + q_{k-1} \geq q_k + q_{k-1} \geq \sqrt{2}^{k-1} + \sqrt{2}^{k-2} = \sqrt{2}^{k-2}(\underbrace{\sqrt{2}+1}_{>2}) > 2\sqrt{2}^{k-2} = \sqrt{2}^{k}$.)

Korollar 64
Es seien $a \in \mathbb{Z}$, $b \in \mathbb{N}$, $\mathrm{ggT}(a, b) = 1$ und $\frac{a}{b} = [a_0; a_1, \ldots, a_n]$ (d.h. $\frac{a}{b} = \frac{p_n}{q_n}$). Dann ist $\big((-1)^{n-1}q_{n-1}, (-1)^n p_{n-1}\big)$ Lösung der linearen diophantischen Gleichung
$ax + by = 1$.

Beweis.

$$a(-1)^{n-1}q_{n-1} + b(-1)^n p_{n-1} = (-1)^{n-1}(p_n q_{n-1} - q_n p_{n-1}) = (-1)^{n-1}(-1)^{n-1} = 1$$

□

Satz 65
Sei $[a_0; a_1, \ldots, a_n]$ ein regelmäßiger Kettenbruch. Dann gilt

$$p_k q_{k-2} - q_k p_{k-2} = (-1)^k a_k \quad (\text{für } 0 \leq k \leq n)$$

Beweis.

$$\begin{aligned} p_k q_{k-2} - q_k p_{k-2} &= (a_k p_{k-1} + p_{k-2})q_{k-2} - (a_k q_{k-1} + q_{k-2})p_{k-2} = \\ &= a_k(p_{k-1}q_{k-2} - q_{k-1}p_{k-2}) = (-1)^k a_k \end{aligned}$$

□

Korollar 66
Sei $[a_0; a_1, \ldots, a_n]$ ein regelmäßiger Kettenbruch. Dann gelten:

$$\frac{p_{2k}}{q_{2k}} < \frac{p_{2(k+1)}}{q_{2(k+1)}} \quad (\text{für } 0 \leq k \leq \frac{n}{2} - 1) \quad \text{und} \quad \frac{p_{2k+1}}{q_{2k+1}} < \frac{p_{2k-1}}{q_{2k-1}} \quad (\text{für } 1 \leq k \leq \frac{n-1}{2})$$

Beweis. Aus Satz 61 folgt:

$$\frac{p_k}{q_k} - \frac{p_{k-2}}{q_{k-2}} = \frac{p_k q_{k-2} - q_k p_{k-2}}{q_k q_{k-2}} = (-1)^k \frac{a_k}{a_k q_{k-2}} = \begin{cases} > 0 & \text{für } 2 \mid k \\ < 0 & \text{für } 2 \nmid k \end{cases}$$

□

Definition „Unendlicher Kettenbruch“
Wir ordnen jedem $\alpha \in \mathbb{R}$ einen (möglicherweise) unendlichen Kettenbruch zu:

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}} = [a_0; a_1, a_2, \dots] \text{ mit } a_0 \in \mathbb{Z} \text{ und } a_i \in \mathbb{N}\ \forall i \geq 1$$

Sei $a_0 := [\alpha]$. Wenn $\alpha \in \mathbb{Z}$ fertig. Falls nicht ist $\alpha - a_0 \in (0,1)$ und $\exists \alpha_1 > 1$ (d. h. $\alpha_1 \in (1, +\infty)$) $\alpha = a_0 + \frac{1}{\alpha_1}$. Setze $a_1 := [\alpha_1]$. Falls $\alpha_1 \in \mathbb{N}$ fertig. Falls nicht, $\exists \alpha_2 > 1 : \alpha_1 = a_1 + \frac{1}{\alpha_2}$, usw.
Wenn $\alpha_n > 1$ schon definiert ist, setze $a_1 := [\alpha_n]$. Wenn $\alpha_n \in \mathbb{N}$ fertig. Falls nicht
$\exists \alpha_{n+2} > 1 : \alpha_n = a_n + \frac{1}{\alpha_{n+1}}$.
Falls $\alpha \in \mathbb{Q}$ bricht das Verfahren ab wie im Beweis von Satz 63.
Wenn $\alpha \in \mathbb{R} \setminus \mathbb{Q}$, dann folgt mit Induktion $\alpha \in \mathbb{R} \setminus \mathbb{Q}\ \forall n \geq 1$ und man erhält eine unendliche Folge $(a_n)_{n \geq 1}$ natürlicher Zahlen, die Teilnenner genannt werden. Man definiert wie im Fall endlicher Kettenbrüche die Näherungsbrüche $\frac{p_n}{q_n} = [a_0; a_1, \dots, a_n]$, die sämtliche Eigenschaften besitzen, die sie im Fall endlicher Kettenbrüche haben.

Lemma 67
Sei $[a_0; a_1, \dots, a_n]$ ein unendlicher Kettenbruch mit $a_0 \in \mathbb{Z}$ und $a_i \in \mathbb{N}\ \forall i \geq 1$. Dann konvergiert die Folge $\left(\frac{p_n}{q_n}\right)_{n \geq 0}$ der Näherungsbrüche gegen eine Zahl $\alpha \in \mathbb{R} \setminus \mathbb{Q}$. Dabei gilt

$$\frac{p_0}{q_0} < \frac{p_2}{q_2} < \frac{p_4}{q_4} < \dots < \alpha < \dots < \frac{p_5}{q_5} < \frac{p_3}{q_3} < \frac{p_1}{q_1}$$

Beweis. Nach Korollar 66 ist die Folge $\left(\frac{p_{2k}}{q_{2k}}\right)_{k \geq 0}$ streng monoton wachsend, die Folge $\left(\frac{p_{2k-1}}{q_{2k-1}}\right)_{k \geq 1}$ streng monoton fallend. Weiters ist $\frac{p_m}{q_m} < \frac{p_n}{q_n}$ für alle $m, n \in \mathbb{N} \cup \{0\}$ mit $2 \mid m$, $2 \nmid n$. Wegen $p_k q_{k-1} - q_k p_{k-1} = (-1)^{k-1}$ folgt

$$\frac{p_k}{q_k} - \frac{p_{k-1}}{q_{k-1}} = \frac{(-1)^{k-1}}{q_{k-1} q_k} \quad \begin{cases} > 0 & \text{für } 2 \nmid k \\ < 0 & \text{für } 2 \mid k \end{cases}$$

und daraus folgt $\frac{p_{k-1}}{q_{k-1}} < \frac{p_k}{q_k}$ für $2 \nmid k$ bzw. $\frac{p_k}{q_k} < \frac{p_{k-1}}{q_{k-1}}$ für $2 \mid k$. Ist $n < m$, so gilt $\frac{p_m}{q_m} < \frac{p_{m-1}}{q_{m-1}} \leq \frac{p_n}{q_n}$ und für $n > m$ gilt $\frac{p_m}{q_m} \leq \frac{p_{n-1}}{q_{n-1}} < \frac{p_n}{q_n}$. Insbesondere ist die Folge $\left(\frac{p_{2k}}{q_{2k}}\right)_{k \geq 0}$ nach oben beschränkt (z.B. durch $\frac{p_1}{q_1}$) und die Folge $\left(\frac{p_{2k-1}}{q_{2k-1}}\right)_{k \geq 1}$ nach unten beschränkt (z.B. durch $\frac{p_0}{q_0} = a_0$). Daher existieren $\alpha^- := \lim_{k \to \infty} \frac{p_{2k}}{q_{2k}}$ bzw. $\alpha^+ := \lim_{k \to \infty} \frac{p_{2k-1}}{q_{2k-1}}$ und wegen

$$0 \leq \alpha^+ - \alpha^- < \frac{p_{2k-1}}{q_{2k-1}} - \frac{p_{2k}}{q_{2k}} = \frac{q_{2k} p_{2k-1} - p_{2k} q_{2k-1}}{q_{2k-1} q_{2k}} = \frac{(-1)^{2k}}{q_{2k-1} q_{2k}} = \frac{1}{q_{2k-1} q_{2k}} \overset{k \to \infty}{\longrightarrow} 0$$

folgt daraus $\alpha^+ = \alpha^-$, d. h. $\alpha := \lim_{k \to \infty} \frac{p_k}{q_k}$ existiert. Wäre $\alpha \in \mathbb{Q}$. d. h. $\alpha = \frac{a}{b}$ mit $a \in \mathbb{Z}$, $b \in \mathbb{N}$, so würde aus $\frac{p_k}{q_k} \neq \alpha\ \forall k \geq 0$ folgen, dass

$$0 < \frac{1}{b q_k} \leq \left| \frac{a}{b} - \frac{p_k}{q_k} \right| = \left| \alpha - \frac{p_k}{q_k} \right| < \left| \frac{p_{k+1}}{q_{k+1}} - \frac{p_k}{q_k} \right| = \frac{1}{q_k q_{k+1}}$$

$\Rightarrow q_{k+1} < b \; \forall k \geq 1$, und dies ist ein Widerspruch zur Unbeschränktheit der Folge $(q_k)_{k\geq 0}$. $\square$

Lemma 68
Sei $\alpha \in \mathbb{R}$ und $[a_0; a_1, \ldots, a_n]$ der α zugeordnete (endliche oder unendliche) Kettenbruch. Dann gilt: $\left|\alpha - \frac{p_k}{q_k}\right| \leq \frac{1}{q_k q_{k+1}} \; \forall k \geq 0$

Beweis. Ist $\alpha \in \mathbb{Q}$ und $\alpha = [a_0; a_1, \ldots, a_n, \alpha_{n+1}] \; \forall k \geq 0$

$$\Rightarrow \alpha = \frac{\alpha_{k+1} p_k + p_{k-1}}{\alpha_{k+1} q_k + q_{k-1}} \; \forall k \geq 0 \Rightarrow \alpha - \frac{p_k}{q_k} = \frac{\alpha_{k+1} p_k + p_{k-1}}{\alpha_{k+1} q_k + q_{k-1}} - \frac{p_k}{q_k}$$
$$= \frac{q_k(\alpha_{k+1} p_k + p_{k-1}) - p_k(\alpha_{k+1} q_k + q_{k-1})}{q_k(\alpha_{k+1} q_k + q_{k-1})} = \frac{q_k p_{k-1} - p_k q_{k-1}}{q_k(\alpha_{k+1} q_k + q_{k-1})} = \frac{(-1)^k}{q_k(\alpha_{k+1} q_k + q_{k-1})}$$
$$\Rightarrow \left|\alpha - \frac{p_k}{q_k}\right| = \frac{1}{q_k(\alpha_{k+1} q_k + q_{k-1})} < \frac{1}{q_k(a_{k+1} q_k + q_{k-1})} = \frac{1}{q_k q_{k+1}}$$

$\square$

Bemerkung

1. Ist $\alpha \in \mathbb{R} \setminus \mathbb{Q}$, so gilt: $\left|\alpha - \frac{p_k}{q_k}\right| < \frac{1}{q_k q_{k+1}}$
2. Wegen $q_{k+1} \geq a_{k+1} q_k$ und $a_{k+1} \geq 1$ erhält mann aus Lemma 68 sofort die Abschätzungen $\left|\alpha - \frac{p_k}{q_k}\right| \leq \frac{1}{a_{k+1} q_k^2}$ und $\left|\alpha - \frac{p_k}{q_k}\right| < \frac{1}{q_k^2}$, die schwächer, aber oft praktischer sind.
3. Diese Abschätzungen zeigen, dass eine Zahl α durch ihre Näherungsbrüche sehr gut approximiert wird. Tatsächlich kann man zeigen: Die Näherungsbrüche von α sind die beiden rationalen Approximationen von α im folgenden Sinn: Ist $\frac{a}{b} \in \mathbb{Q}$ mit $0 < b < q_{n+1}$ und $\frac{a}{b} \neq \frac{p_{n+1}}{q_{n+1}}$, so gilt:

$$|b\alpha - a| \geq |q_n \alpha - p_n| > |q_{n+1} \alpha - p_{n+1}|$$

Satz 69
Jedes $\alpha \in \mathbb{R}$ lässt sich auf eindeutige Weise in einen (regelmäßigen) Kettenbruch entwickeln. Dieser ist genau dann endlich, wenn $\alpha \in \mathbb{Q}$ gilt. Dabei muss im Fall einer endlichen Kettenbruchentwicklung der letzte Teilnenner < 1 sein.

Beweis. In Satz 63 wurde gezeigt, dass sich jedes $\alpha \in \mathbb{Q}$ als Kettenbruch schreiben lässt. Ist $\alpha \in \mathbb{R} \setminus \mathbb{Q}$, so konvergiert der α zugeordnete Kettenbruch $[a_0; a_1, \ldots, a_n]$ nach Lemma 67 (in dem Sinn, dass $\lim_{k\to\infty} \frac{p_k}{q_k}$ existiert) und nach Lemma 68 gilt:

$$0 < \left|\alpha - \frac{p_k}{q_k}\right| < \frac{1}{q_k q_{k+1}} \overset{k \to \infty}{\longrightarrow} 0, \text{ d. h. } \lim_{k\to\infty} \frac{p_k}{q_k} = \alpha, \text{ d. h. } \alpha = [a_0; a_1, \ldots, a_n]$$

Zu zeigen bleibt die *Eindeutigkeit*: Angenommen, $\alpha \in \mathbb{R}$ besitzt zwei (endliche oder unendliche) Kettenbruchentwicklungen, $\alpha = [a_0; a_1, a_2, \ldots] = [b_0; b_1, b_2, \ldots]$. Diese sind dann beide endlich (falls $\alpha \in \mathbb{Q}$) oder unendlich (falls $\alpha \notin \mathbb{Q}$).
Sei zunächst $\alpha \notin \mathbb{Q}$. Induktion: Es ist $a_0 + \frac{1}{\alpha_1} = \alpha = b_0 + \frac{1}{\beta_1}$ mit $\alpha_1, \beta_1 > 1$, $\alpha_1 = [a_1; a_2, \ldots]$ und $\beta_1 = [b_1; b_2, \ldots] \Rightarrow |a_0 - b_0| = \left|\frac{1}{\alpha_1} - \frac{1}{\beta_1}\right| < 1$ (da $0 < \frac{1}{\alpha_1}, \frac{1}{\beta_1} < 1$) $\Rightarrow a_0 = b_0$.

Ist $a_i = b_i$ für $1 \leq i \leq n$ schon gezeigt, so gilt mit $\alpha_{n+1} = [a_{n+1}; a_{n+2}, \dots], \beta_{n+1} = [b_{n+1}; b_{n+2}, \dots]$ und:

$$\frac{\alpha_{n+1}p_n + p_{n-1}}{\alpha_{n+1}q_n + q_{n-1}} = [a_0; a_1, \dots, a_n, \alpha_{n+1}] = \alpha = [b_0; b_1, \dots, b_n, \beta_{n+1}] = \frac{\beta_{n+1}p_n + p_{n-1}}{\beta_{n+1}q_n + q_{n-1}}$$

$$\begin{aligned}
&\Rightarrow (\alpha_{n+1}p_n + p_{n-1})(\beta_{n+1}q_n + q_{n-1}) = (\beta_{n+1}p_n + p_{n-1})(\alpha_{n+1}q_n + q_{n-1}) \\
&\Rightarrow \alpha_{n+1}p_nq_{n-1} + \beta_{n+1}q_np_{n-1} = \beta_{n+1}p_nq_{n-1} + \alpha_{n+1}q_np_{n-1} \\
&\Rightarrow \alpha_{n+1}(p_nq_{n-1} - q_np_{n-1}) = \beta_{n+1}(p_nq_{n-1} - q_np_{n-1}) \\
&\Rightarrow \alpha_{n+1} = \beta_{n+1}
\end{aligned}$$

$$\begin{aligned}
&\Rightarrow a_{n+2} + \frac{1}{\alpha_{n+2}} = b_{n+1} + \frac{1}{\beta_{n+2}} \\
&\Rightarrow |a_{n+1} - b_{n+1}| = \left|\frac{1}{\alpha_{n+2}} - \frac{1}{\beta_{n+2}}\right| < 1 \\
&\Rightarrow a_{n+1} = b_{n+1}
\end{aligned}$$

Der Beweis für endliche Kettenbrüche erfordert nur geringe Modifikation (wobei man verwendet, dass endliche Kettenbrüche nicht auf den Teilnenner 1 enden dürfen). □

Beispiel 1. $[1; 1, 1, 1, \dots] = \frac{1+\sqrt{5}}{2}$. Sei $\alpha = [1; 1, 1, 1, \dots]$

$$\Rightarrow \alpha = 1 + \frac{1}{\alpha} \Rightarrow \alpha^2 - \alpha - 1 = 0 \Rightarrow \alpha = \frac{1}{2} \pm \sqrt{\frac{1}{4} + 1} = \frac{1 \pm \sqrt{5}}{2} \Rightarrow \alpha = \frac{1+\sqrt{5}}{2}$$

(Wegen $\alpha > 0$ ist $\alpha = \frac{1-\sqrt{5}}{2}$ unmöglich.)

2. $\forall a \in \mathbb{N} : [a; 2a, 2a, 2a, \dots] = \sqrt{a^2+1}$. Sei $\alpha = [2a; 2a, 2a, \dots]$. Dann

$$\alpha = 2a + \frac{1}{\alpha} \Rightarrow \alpha^2 - 2a\alpha - 1 \Rightarrow \alpha = a + \sqrt{a^2+1}$$

(Wegen $\alpha > 0$ ist $\alpha = a - \sqrt{a^2+1}$ unmöglich)

$$\Rightarrow \sqrt{a^2+1} = \alpha - a = [a; 2a, 2a, 2a, \dots]$$

Insbesondere ist $\sqrt{2} = [1; 2, 2, 2, \dots]$.

Definition „quadratische Irrationalzahl“
Ein $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ heißt quadratische Irrationalzahl wenn es ein Polynom $p(X) = AX^2 + BX + C \in \mathbb{Z}[X]$ (d. h. $A, B, C \in \mathbb{Z},\ A \neq 0$) gibt, dessen Nullstelle α ist (d. h. $p(\alpha) = 0$)

Lemma 70
Sei $\alpha \in \mathbb{R}$. Dann sind äquivalent:

(i) α ist quadratische Irrationalzahl

(ii) $\exists r, s \in \mathbb{Q},\ s \neq 0$ und $d \in \mathbb{Z},\ d \neq \{0, 1\},\ d$ quadratfrei (d. h. $\nexists$ Primzahl p mit $p^2 \mid d$) sodass $\alpha = r + s\sqrt{d}$

Beweis. (i) $\Rightarrow$ (ii): Sei $A\alpha^2 + B\alpha + C = 0$ $(A, B, C \in \mathbb{Z},\ a \neq 0) \Rightarrow \alpha = \frac{-B \pm \sqrt{B^2-4AC}}{2A}$, woraus (ii) folgt.
(ii) $\Rightarrow$ (i): Sei $q(X) = (X - r - s\sqrt{d})(X - r + s\sqrt{d}) = (X-r)^2 - ds^2 = X^2 - 2rX - r^2 - ds^2$ woraus man durch Multiplikation mit passendem $A \in \mathbb{Z} \setminus 0$ ein Polynom $p \in \mathbb{Z}[X]$ erhält, dessen Nullstelle α ist. □

Definition „Periodischer Kettenbruch“
Die Kettenbruchentwicklung $[a_0; a_1, a_2, \dots]$ heißt periodisch, wenn es $n, m \in \mathbb{N}$ mit der Eigenschaft $a_{i+m} = a_i\ \forall i \geq n$ gibt. D. h., die Kettenbruchentwicklung hat die Gestalt

$$[a_0; a_1, \dots, a_{n-1}, \underbrace{a_n, \dots, a_{n+m-1}}, \underbrace{a_n, \dots, a_{n+m-1}}, \dots]$$

Man schreibt dafür kurz $[a_0; a_1, \dots, a_{n-1}, \overline{a_n, \dots, a_{n+m-1}}]$.
(also z. B. $\sqrt{2} = [1; 2, 2, 2, \dots] = [1; \overline{2}]$.)

Satz 71
Sei $\alpha \in \mathbb{R}$. Dann sind äquivalent:

(i) α hat periodische Kettenbruchentwicklung

(ii) α ist quadratische Irrationalzahl

Beweis. (i) $\Rightarrow$ (ii): Es gibt $m, n \in \mathbb{N}$, sodass

$$\alpha = [a_0; a_1, \dots, a_{n-1}, \overline{a_n, \dots, a_{n+m-1}}] = [a_0; a_1, \dots, a_{n-1}, a_n, \dots, a_{n+m-1}, \overline{a_n, \dots, a_{n+m-1}}]$$
$$\Rightarrow \alpha = \frac{p_{n-1}\alpha_n + p_{n-2}}{q_{n-1}\alpha_n + q_{n-2}} = \frac{p_{n+m-1}\alpha_n + p_{n+m-2}}{q_{n+m-1}\alpha_n + q_{n+m-2}} \text{ mit } \alpha_n = [a_n; \overline{a_{n+1}, \dots, a_{n+m-1}}]$$
$$q_{n-1}\alpha_n\alpha + q_{n-2}\alpha = p_{n-1}\alpha_n + p_{n-2} \Rightarrow \alpha_n(q_{n-1}\alpha - p_{n-1} = -(q_{n-2}\alpha - p_{n-2})$$
$$\Rightarrow \alpha_n = -\frac{q_{n-2}\alpha - p_{n-2}}{q_{n-1}\alpha - p_{n-1}} \text{ und analog } \alpha_n = -\frac{q_{n+m-2}\alpha - p_{n+m-2}}{q_{n+m-1}\alpha - p_{n+m-1}}$$
$$\Rightarrow \frac{q_{n-2}\alpha - p_{n-2}}{q_{n-1}\alpha - p_{n-1}} = \frac{q_{n+m-2}\alpha - p_{n+m-2}}{q_{n+m-1}\alpha - p_{n+m-1}} \Rightarrow \dots \Rightarrow \text{ (ausmultiplizieren, sortieren)}$$
$$\Rightarrow (q_{n-2}q_{n+m-1} - q_{n-1}q_{n+m-2})\alpha^2 + (q_{n-1}p_{n+m-2} + p_{n-1}q_{n+m-2}$$
$$- q_{n-2}p_{n+m-1} - p_{n-2}q_{n+m-1})\alpha + (p_{n-2}p_{n+m-1} - p_{n-1}p_{n+m-2}) = 0$$

Dabei ist $q_{n-2}q_{n+m-1} - q_{n-1}q_{n+m-1} \neq 0$. Es ist $\text{ggT}\,(q_{n-2}, q_{n-1}) = \text{ggT}\,(q_{n+m-2}, q_{n+m-1}) = 1$. Wäre $q_{n-2}q_{n+m-1} = q_{n-1}$. Es folgt, $lq_{n-2}q_{n-1} = kq_{n-2}q_{n-1} \Rightarrow k = l \Rightarrow \text{ggT}\,(q_{n+m-2}, q_{n+m-1}) > 1$, Widerspruch!) Daher ist α quadratische Irrationalzahl.
(ii) $\Rightarrow$ (i): (ohne Beweis) □

Bemerkung Die regelmäßige Kettenbruchentwicklung ist nur für wenige Zahlen bekannt, z. B.: $e = [2; 1, 2, 1, 1, 4, 1, 1, 6, 1, \dots]$ und $\frac{e^{\frac{2}{k}}+1}{e^{\frac{2}{k}}-1} = [k; 3k, 5k, 7k, \dots]$.
Nicht bekannt sind aber z. B. schon die regelmäßigen Kettenbruchentwicklungen von $\sqrt[3]{2}$ oder π.