ALGEBRA UND ZAHLENTHEORIE FÜR LEHRER

Wintersemester 2011/12, Universität Jena

Burkhard Külshammer

0. VORBEMERKUNGEN

In dieser Vorlesung verwenden wir häufig die folgenden Mengen:

$\mathbb{N} = \{1, 2, 3, \ldots\}$, die Menge der **natürlichen** Zahlen,

$\mathbb{N}_0 = \{0, 1, 2, 3, \ldots\}$,

$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \ldots\}$, die Menge der **ganzen** Zahlen.

Dabei setzen wir die üblichen Rechenregeln für $+, -, \cdot$ als bekannt voraus. Wichtig ist die folgende Eigenschaft:

$(*)$ *Jede nichtleere Teilmenge von* $\mathbb{N}$ *enthält ein kleinstes Element.*

Entsprechendes gilt auch für $\mathbb{N}_0$ statt $\mathbb{N}$. Auf $(*)$ beruht das **Prinzip der vollständigen Induktion**:

$(**)$ *Hat man für* $n \in \mathbb{N}$ *eine Aussage* $A(n)$ *und gilt* $A(1)$ *sowie* $A(n) \Longrightarrow A(n+1)$ *für jedes* $n \in \mathbb{N}$*, so gilt* $A(n)$ *für jedes* $n \in \mathbb{N}$*.*

[Denn andernfalls ist $\emptyset \neq M := \{m \in \mathbb{N} : A(m) \text{ gilt nicht}\} \subseteq \mathbb{N}$. Wegen $(*)$ enthält M ein kleinstes Element x. Da $A(1)$ gilt, $A(x)$ aber nicht, ist $x \neq 1$. Daher ist $x - 1 \in \mathbb{N}$, aber $x - 1 \notin M$. Also gilt $A(x-1)$. Wegen $A(x-1) \Longrightarrow A(x)$ gilt auch $A(x)$. Widerspruch!]

Es gibt viele Varianten von $(*)$, die wir auch verwenden werden, z.B.:

$(***)$ $A(1)$ *und* $A(1) \wedge \ldots \wedge A(n-1) \Longrightarrow A(n)$,

$(****)$ $A(1)$ *und* $A(2)$ *und* $A(n-1) \wedge A(n) \Longrightarrow A(n+1)$.

1. TEILBARKEIT

1.1 Satz. (Division mit Rest)
Zu $a \in \mathbb{Z}$ *und* $m \in \mathbb{N}$ *existieren stets eindeutig bestimmte* $q, r \in \mathbb{Z}$ *mit* $a = qm + r$ *und* $0 \leq r < m$*. (Dann heißen* q *und* r **Quotient** *bzw.* **Rest** *bei dieser Division.)*

Beispiel. $100 = \mathbf{7} \cdot 13 + \mathbf{9}$.

Beweis. Sei $R := \{a - qm : q \in \mathbb{Z}\}$. Dann ist $R \cap \mathbb{N}_0 \neq \emptyset$; denn für $a \geq 0$ ist $a - 0m = a \in \mathbb{N}_0$, und für $a < 0$ ist $a - am = a(1-m) \in \mathbb{N}_0$. Wegen $(*)$ existiert $r := \min(R \cap \mathbb{N}_0)$. Wir schreiben $r = a - qm$ mit $q \in \mathbb{Z}$. Dann ist $r \geq 0$, aber $r - m = a - (q+1)m < 0$ nach Wahl von r. Also ist $r < m$, wie gewünscht.
Seien auch $q', r' \in \mathbb{Z}$ mit $a = q'm + r'$ und $0 \leq r' < m$. Dann ist $r - r' = (q' - q)m$. Wegen $|q' - q|m = |r - r'| < m$ folgt $q' - q = 0$, d.h. $q' = q$ und $r' = r$.

1.2 Satz. (b-adische Entwicklung)
Sei $1 \neq b \in \mathbb{N}$. Für $n \in \mathbb{N}_0$ existieren dann eindeutig bestimmte

$$r_0, r_1, r_2, \ldots \in \{0, 1, \ldots, b-1\}$$

mit $|\{i \in \mathbb{N}_0 : r_i \neq 0\}| < \infty$ und $n = \sum_{i=0}^{\infty} r_i b^i$. (Dabei heißt b **Basis**, *und die r_i's heißen* **Ziffern** *oder* **Koeffizienten** *dieser Entwicklung von n.)*

Beispiel. Sei $b := 6$ und $n := 100$. Wegen $100 = 16 \cdot 6 + 4$ und $16 = 2 \cdot 6 + 4$ ist $100 = r_0 + r_1 \cdot 6 + r_2 \cdot 6^2$ mit $r_0 = r_1 = 4$ und $r_2 = 2$.

Beweis. *Existenz:* (Induktion nach n)
Im Fall $n = 0$ setzen wir $r_0 := r_1 := r_2 := \ldots := 0$. Sei also $n > 0$ und die Behauptung für alle $m < n$ schon gezeigt. Division mit Rest liefert dann $q, r_0 \in \mathbb{Z}$ mit $n = qb + r_0$ und $0 \leq r_0 < b$. Wegen $q = \frac{n-r_0}{b} \leq \frac{n}{b} < n$ existieren nach Induktionsvoraussetzung Elemente $r_1, r_2, \ldots \in \{0, 1, \ldots, b-1\}$ mit $|\{i \in \mathbb{N} : r_i \neq 0\}| < \infty$ und $q = \sum_{j=0}^{\infty} r_{j+1} b^j$. Dann ist $|\{i \in \mathbb{N}_0 : r_i \neq 0\}| < \infty$ und $n = qb + r_0 = \sum_{j=0}^{\infty} r_{j+1} b^{j+1} + r_0 = \sum_{i=0}^{\infty} r_i b^i$.
Eindeutigkeit: (Induktion nach n)
Seien $n \in \mathbb{N}_0$ und $s_0, s_1, s_2, \ldots \in \{0, 1, \ldots, b-1\}$ mit $|\{i \in \mathbb{N}_0 : s_i \neq 0\}| < \infty$ und $n = \sum_{i=0}^{\infty} s_i b^i$. Im Fall $n = 0$ folgt $s_i = 0$ für $i \in \mathbb{N}_0$. Sei also $n > 0$ und die Behauptung für alle $m < n$ schon gezeigt. Wegen $n = (\sum_{i=1}^{\infty} s_i b^{i-1})b + s_0$ und $0 \leq s_0 < b$ ist s_0 der Rest bei der Division von n durch b. Nach Satz 1.1 ist also s_0 eindeutig bestimmt. Analog ist $q := \sum_{i=1}^{\infty} s_i b^{i-1}$ eindeutig bestimmt. Wegen $q < n$ sind nach Induktionsvoraussetzung $s_1, s_2, \ldots$ eindeutig bestimmt.

1.3 Definition. Seien $a, b \in \mathbb{Z}$. Existiert ein $c \in \mathbb{Z}$ mit $b = ac$, so schreiben wir $a \mid b$ und sagen: a **teilt** b, a ist **Teiler** von b, b ist durch a **teilbar**, b ist **Vielfaches** von a, etc.

Beispiel. $12 \mid 36$, $24 \nmid 36$.

Satz. *Für alle $a, b, c, x, y \in \mathbb{Z}$ gilt:*
(i) $a \mid 0$, $1 \mid a$, $a \mid a$;
(ii) $a \mid b \Longrightarrow \pm a \mid \pm b$;
(iii) $a \mid b \wedge b \mid a \Longrightarrow a = \pm b$;
(iv) $a \mid b \wedge b \mid c \Longrightarrow a \mid c$;
(v) $a \mid b \wedge a \mid c \Longrightarrow a \mid bx + cy$;
(vi) $0 \mid a \Longleftrightarrow a = 0$;
(vii) $a \mid b \wedge a, b \in \mathbb{N} \Longrightarrow a \leq b$.

Beweis. Wir beweisen nur (v). [Der Rest geht analog.] Nach Voraussetzung existieren $g, h \in \mathbb{Z}$ mit $b = ag$ und $c = ah$. Daher ist $bx + cy = a(gx + hy)$, d.h. $a \mid bx + cy$.

1.4 Definition. Seien $a_1, \ldots, a_n, t \in \mathbb{Z}$ mit $t \mid a_1$, …, $t \mid a_n$. Dann heißt t **gemeinsamer Teiler** von $a_1, \ldots, a_n$. Mit $\mathrm{gT}(a_1, \ldots, a_n)$ bezeichnen wir die Menge aller gemeinsamen Teiler von $a_1, \ldots, a_n$.

Bemerkung. Wegen $\mathrm{gT}(a_1, \ldots, a_n) = \mathrm{gT}(\pm a_1, \ldots, \pm a_n)$ kann man beim Rechnen meist $a_1, \ldots, a_n \in \mathbb{N}_0$ annehmen. Da man $a_1, \ldots, a_n$ auch permutieren darf, kann man ferner $a_1 \geq \ldots \geq a_n$ annehmen. Man kann sogar $a_1 > \ldots > a_n$ annehmen. Im Fall $n \geq 2$ liefert

Satz 1.1 Elemente $q, r \in \mathbb{Z}$ mit $a_1 = qa_n + r$ und $0 \leq r < a_n$. Aus Satz 1.3 folgt leicht: $\mathrm{gT}(a_1, \ldots, a_n) = \mathrm{gT}(a_1 - qa_n, a_2, \ldots, a_n)$; dabei ist $a_1 - qa_n = r$ und $r + a_2 + \ldots + a_n < a_1 + \ldots + a_n$. Eine Iteration dieser Schritte liefert $\mathrm{gT}(a_1, \ldots, a_n) = \mathrm{gT}(b)$ für ein $b \in \mathbb{N}_0$. Dieses Verfahren heißt **euklidischer Algorithmus** (EUKLID, 365-300).

Beispiel. $\mathrm{gT}(45, 27, 12) = \mathrm{gT}(45 - 3 \cdot 12, 27, 12) = \mathrm{gT}(9, 27, 12) = \mathrm{gT}(27, 12, 9) = \mathrm{gT}(27 - 3 \cdot 9, 12, 9) = \mathrm{gT}(0, 12, 9) = \mathrm{gT}(12, 9) = \mathrm{gT}(12 - 1 \cdot 9, 9) = \mathrm{gT}(3, 9) = \mathrm{gT}(9, 3) = \mathrm{gT}(9 - 3 \cdot 3, 3) = \mathrm{gT}(0, 3) = \mathrm{gT}(3) = \{\pm 1, \pm 3\}$.

1.5 Definition. Seien $a_1, \ldots, a_n \in \mathbb{Z}$. Ein $d \in \mathbb{N}_0 \cap \mathrm{gT}(a_1, \ldots, a_n)$ heißt **größter gemeinsamer Teiler** (ggT) von $a_1, \ldots, a_n$, wenn d durch jedes $t \in \mathrm{gT}(a_1, \ldots, a_n)$ teilbar ist.

Satz. *Zu $a_1, \ldots, a_n \in \mathbb{Z}$ existiert stets genau ein ggT d.*

Beweis. Nach Bemerkung 1.4 ist $\mathrm{gT}(a_1, \ldots, a_n) = \mathrm{gT}(b)$ für ein $b \in \mathbb{N}_0$. Dann ist b ein ggT von $a_1, \ldots, a_n$. Ist b' ein weiterer ggT von $a_1, \ldots, a_n$, so gilt: $b \mid b' \mid b$, also $b' = \pm b$ nach Satz 1.3. Wegen $b, b' \in \mathbb{N}_0$ folgt $b' = b$.

Bemerkung. (i) Man schreibt: $d = \mathrm{ggT}(a_1, \ldots, a_n)$.
(ii) Dann gilt auch: $d = \mathrm{ggT}(\mathrm{ggT}(a_1, \ldots, a_{n-1}), a_n)$.
[Denn wegen $d \mid a_1$, …, $d \mid a_n$ ist $d \mid \mathrm{ggT}(a_1, \ldots, a_{n-1})$ und $d \mid a_n$, d.h.

$$d \in \mathrm{gT}(\mathrm{ggT}(a_1, \ldots, a_{n-1}), a_n).$$

Ferner gilt für beliebige $t \in \mathrm{gT}(\mathrm{ggT}(a_1, \ldots, a_{n-1}), a_n)$: $t \mid a_n$ und $t \mid \mathrm{ggT}(a_1, \ldots, a_{n-1}) =: s$ und $s \mid a_1$, …, $s \mid a_{n-1}$, also auch $t \mid a_1$, …, $t \mid a_{n-1}$, $t \mid a_n$, d.h. $t \mid d$.]
(iii) Wegen (ii) genügt es meist, den ggT von *zwei* Zahlen zu bestimmen.

1.6 Satz. (Erweiterter euklidischer Algorithmus)
Seien $a, b \in \mathbb{N}$. Wir setzen

$$(x_0, y_0, z_0) := (1, 0, a) \quad \textit{und} \quad (x_1, y_1, z_1) := (0, 1, b) \quad \textit{und} \quad i := 1.$$

Im Fall $z_i = 0$ brechen wir ab. Im Fall $z_i \neq 0$ liefert Division mit Rest Elemente $q_i, r_i \in \mathbb{Z}$ mit $z_{i-1} = q_i z_i + r_i$ und $0 \leq r_i < z_i$. Wir setzen

$$(x_{i+1}, y_{i+1}, z_{i+1}) := (x_{i-1} - q_i x_i, y_{i-1} - q_i y_i, z_{i-1} - q_i z_i = r_i),$$

erhöhen i um 1 und iterieren. Dieses Verfahren bricht ab, und am Ende ist

$$\mathrm{ggT}(a, b) = z_{i-1} = x_{i-1} a + y_{i-1} b.$$

Beispiel. Für $a = 143$ und $b = 39$ ergibt der erweiterte euklidische Algorithmus:

x_i	y_i	z_i	q_i
1	0	143	
0	1	39	3
1	−3	26	1
−1	4	13	2
		0	

Daher gilt: $\mathrm{ggT}(143, 39) = 13 = (-1) \cdot 143 + 4 \cdot 39$.

Beweis. Wegen $b = z_1 > z_2 > \ldots \geq 0$ bricht das Verfahren ab. Am Anfang ($i = 1$) ist $\mathrm{ggT}(a, b) = \mathrm{ggT}(z_{i-1}, z_i)$, und das bleibt während des Verfahrens erhalten; denn es gilt:

$$\mathrm{ggT}(z_i, z_{i+1}) = \mathrm{ggT}(z_i, z_{i-1} - q_i z_i) = \mathrm{ggT}(z_i, z_{i-1}).$$

Am Ende ist $\mathrm{ggT}(z_i, z_{i-1}) = \mathrm{ggT}(0, z_{i-1}) = z_{i-1}$.
Am Anfang ($i = 0, 1$) ist auch $x_i a + y_i b = z_i$, und dies bleibt während des Verfahrens erhalten:

$$\begin{aligned} x_{i+1}a + y_{i+1}b &= (x_{i-1} - q_i x_i)a + (y_{i-1} - q_i y_i)b \\ &= x_{i-1}a + y_{i-1}b - q_i(x_i a + y_i b) = z_{i-1} - q_i z_i = z_{i+1}. \end{aligned}$$

Bemerkung. Der erweiterte euklidische Algorithmus liefert also nicht nur $d := \mathrm{ggT}(a, b)$, sondern auch $x, y \in \mathbb{Z}$ mit $d = xa + yb$. Braucht man x, y nicht, so kann man bei der Iteration die x_i's und die y_i's weglassen.

1.7 Satz. *Für $a_1, \ldots, a_n, b \in \mathbb{Z}$ gilt:*

$$\mathrm{ggT}(a_1, \ldots, a_n) \mid b \Longleftrightarrow \exists x_1, \ldots, x_n \in \mathbb{Z} : b = x_1 a_1 + \ldots + x_n a_n.$$

Beweis. "$\Longleftarrow$": Seien $x_1, \ldots, x_n \in \mathbb{Z}$ mit $b = x_1 a_1 + \ldots + x_n a_n$. Für $t \in \mathrm{gT}(a_1, \ldots, a_n)$ gilt dann: $t \mid b$; insbesondere ist $\mathrm{ggT}(a_1, \ldots, a_n) \mid b$.
"$\Longrightarrow$": Sei $d := \mathrm{ggT}(a_1, \ldots, a_n) \mid b$, etwa $b = cd$. Es genügt, $y_1, \ldots, y_n \in \mathbb{Z}$ mit $d = y_1 a_1 + \ldots + y_n a_n$ zu finden; denn dann ist $b = cd = cy_1 a_1 + \ldots + cy_n a_n$ mit $cy_1, \ldots, cy_n \in \mathbb{Z}$. Die Existenz von $y_1, \ldots, y_n$ zeigen wir induktiv. Für $n = 1$ ist $d = \pm a_1$. Für $n = 2$ folgt die Existenz von y_1, y_2 aus Satz 1.6. Für $n > 2$ existieren nach Induktionsvoraussetzung Elemente $z_1, \ldots, z_{n-1} \in \mathbb{Z}$ mit $\mathrm{ggT}(a_1, \ldots, a_{n-1}) = z_1 a_1 + \ldots + z_{n-1} a_{n-1}$. Ferner existieren $v_1, v_2 \in \mathbb{Z}$ mit

$$\begin{aligned} d &= \mathrm{ggT}(\mathrm{ggT}(a_1, \ldots, a_{n-1}), a_n) = v_1 \mathrm{ggT}(a_1, \ldots, a_{n-1}) + v_2 a_n \\ &= v_1 z_1 a_1 + \ldots + v_1 z_{n-1} a_{n-1} + v_2 a_n. \end{aligned}$$

Bemerkung. Daher gilt: $\mathrm{ggT}(a_1, \ldots, a_n) = 1 \Longleftrightarrow \exists x_1, \ldots, x_n \in \mathbb{Z} : x_1 a_1 + \ldots + x_n a_n = 1$. Ggf. heißen $a_1, \ldots, a_n$ **teilerfremd**.

Beispiel. Wir suchen $x_1, x_2, x_3 \in \mathbb{Z}$ mit $45x_1 + 27x_2 + 12x_3 = 21$. Der erweiterte euklidische Algorithmus liefert $\mathrm{ggT}(45, 27) = 9 = (-1) \cdot 45 + 2 \cdot 27$ und $\mathrm{ggT}(45, 27, 12) = \mathrm{ggT}(9, 12) = 3 = 1 \cdot 12 - 1 \cdot 9 = 1 \cdot 12 - [(-1) \cdot 45 + 2 \cdot 27] = 1 \cdot 12 + 1 \cdot 45 - 2 \cdot 27$. Daher ist $21 = 7 \cdot 3 = \mathbf{7} \cdot 45 - \mathbf{14} \cdot 27 + \mathbf{7} \cdot 12$. (Probe!)

1.8 Definition. Eine natürliche Zahl $p \neq 1$ heißt **Primzahl**, falls $\pm 1, \pm p$ ihre einzigen Teiler sind. Wir setzen $\mathbb{P} := \{p \in \mathbb{N} : p \text{ Primzahl}\}$. Sind $a \in \mathbb{Z}$ und $p \in \mathbb{P}$ mit $p \mid a$, so heißt p **Primteiler** oder **Primfaktor** von a.

Beispiel. $\mathbb{P} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, \ldots\}$.

Satz. (i) *Jede natürliche Zahl $a \neq 1$ hat einen Primteiler.*
(ii) *Für $a, b \in \mathbb{Z}$ ist jeder Primteiler p von ab ein Teiler von a oder b.*

Beweis. (i) Wegen $1 \neq a \mid a$ ist $D := \{d \in \mathbb{N} : 1 \neq d \mid a\} \neq \emptyset$. Nach $(*)$ existiert also $p := \min(D)$. Wäre $p \notin \mathbb{P}$, so hätte p einen Teiler $t \in \mathbb{N}$ mit $1 \neq t \neq p$. Dann wäre aber $t \in D$ und $t < p$, im Widerspruch zur Wahl von p. Also ist $p \in \mathbb{P}$.
(ii) O.B.d.A. sei $p \nmid a$. Dann existieren $x, y \in \mathbb{Z}$ mit $1 = \mathrm{ggT}(p, a) = xp + ya$. Daher gilt: $p \mid xpb + yab = (xp + ya)b = 1 \cdot b = b$.

Bemerkung. Induktiv folgt: Sind $a_1, \ldots, a_r \in \mathbb{Z}$ und ist p ein Primteiler von $a_1 \ldots a_r$, so ist $p \mid a_i$ für ein $i \in \{1, \ldots, r\}$.

1.9 Satz. (EUKLID)

$$|\mathbb{P}| = \infty.$$

Beweis. Seien $p_1, \ldots, p_r \in \mathbb{P}$. Nach Satz 1.8 hat $m := p_1 \ldots p_r + 1$ einen Primteiler p_{r+1}. Wegen $p_1 \nmid m$, …, $p_r \nmid m$ ist $p_{r+1} \notin \{p_1, \ldots, p_r\}$.

Bemerkung. Die größte *bekannte* Primzahl ist $2^{43.112.609} - 1$. Sie wurde 2008 gefunden und hat fast 13 Millionen Dezimalstellen. (`http://primes.utm.edu/largest.html`)

2. DIE PRIMFAKTORZERLEGUNG

2.1 Satz. (Eindeutige Primfaktorzerlegung)
Sei $1 \neq m \in \mathbb{N}$. Dann existieren $p_1, \ldots, p_r \in \mathbb{P}$ mit $m = p_1 \ldots p_r$. Sind auch $q_1, \ldots, q_s \in \mathbb{P}$ mit $m = q_1 \ldots q_s$, so ist $r = s$, und nach Umnummerierung gilt: $p_i = q_i$ für $i = 1, \ldots, r$.

Beweis. *Existenz:* Nach Satz 1.8 hat m einen Primteiler p. Im Fall $m = p$ sind wir fertig. Andernfalls ist $\frac{m}{p} \in \mathbb{N}$ und $1 < \frac{m}{p} < m$. Induktiv kann man annehmen, dass $p_1, \ldots, p_{r-1} \in \mathbb{P}$ mit $\frac{m}{p} = p_1 \ldots p_r$ existieren. Dann ist $m = p_1 \ldots p_{r-1} p$.
Eindeutigkeit: Aus $p_1 \ldots p_r = m = q_1 \ldots q_s$ folgt $p_r \mid q_1 \ldots q_s$, also $p_r \mid q_i$ für ein $i \in \{1, \ldots, s\}$; o.B.d.A. sei $p_r \mid q_s$. Wegen $q_s \in \mathbb{P}$ folgt $p_r = q_s$, d.h. $p_1 \ldots p_{r-1} = q_1 \ldots q_{s-1}$. Induktiv ist also $r - 1 = s - 1$ und $p_i = q_i$ für $i = 1, \ldots, r - 1$ (nach Umnummerierung).

Bemerkung. (i) $m = p_1 \ldots p_r$ heißt **Primfaktorzerlegung** von m. Nach Zusammenfassen mehrfach vorkommender Faktoren kann man diese auch in der Form $m = q_1^{a_1} \ldots q_t^{a_t}$ mit paarweise verschiedenen $q_1, \ldots, q_t \in \mathbb{P}$ und beliebigen $a_1, \ldots, a_t \in \mathbb{N}$ schreiben.
Eine weitere Schreibweise ist $m = \prod_{p \in \mathbb{P}} p^{b_p}$, wobei $b_p \in \mathbb{N}_0$ für alle $p \in \mathbb{P}$ und $|\{p \in \mathbb{P} : b_p \neq 0\}| < \infty$ ist. Auf diese Weise kann man auch $1 = \prod_{p \in \mathbb{P}} p^0$ als Primfaktorzerlegung von 1 auffassen.
(ii) Aus Satz 2.1 folgt leicht, dass die Teiler von $m = \prod_{p \in \mathbb{P}} p^{b_p}$ genau die Zahlen $\pm \prod_{p \in \mathbb{P}} p^{t_p}$ mit $t_p \leq b_p$ für alle $p \in \mathbb{P}$ sind.
(iii) Die gemeinsamen Teiler von $m = \prod_{p \in \mathbb{P}} p^{b_p}$ und $n = \prod_{p \in \mathbb{P}} p^{c_p}$ sind also genau die Zahlen $\pm \prod_{p \in \mathbb{P}} p^{t_p}$ mit $t_p \leq \min\{b_p, c_p\}$ für alle $p \in \mathbb{P}$. Daher gilt:

$$\mathrm{ggT}(m, n) = \prod_{p \in \mathbb{P}} p^{\min\{b_p, c_p\}}.$$

(iv) Die Konstruktion großer Primzahlen und die Primfaktorzerlegung großer natürlicher Zahlen haben erhebliche Bedeutung für die Kryptographie, d.h. die Lehre vom Verschlüsseln und Entschlüsseln geheimer Nachrichten (EC-Karte, Passwörter, etc.). Darauf werden wir in Kapitel 8 zurückkommen.

2.2 Satz. (EULER, 1707-1783)

$$\sum_{p\in\mathbb{P}} \frac{1}{p} = \infty.$$

Beweis. Wir setzen $p_1 := 2$, $p_2 := 3$, $p_3 := 5$, usw. Dann gilt für $k \in \mathbb{N}$:

$$\prod_{i=1}^{k} \frac{1}{1-\frac{1}{p_i}} = (1+\frac{1}{p_1}+\frac{1}{p_1^2}+\ldots)\cdots(1+\frac{1}{p_k}+\frac{1}{p_k^2}+\ldots) = \sum_n \frac{1}{n},$$

wobei n alle natürlichen Zahlen durchläuft, deren Primteiler sämtlich in $\{p_1,\ldots,p_k\}$ liegen. Für alle $x \in \mathbb{R}$ mit $0 < x \leq \frac{1}{2}$ ist $x - 2x^2 = x(1-2x) \geq 0$, also $(1-x)(1+2x) = 1 + x - 2x^2 \geq 1$, d.h.

$$\frac{1}{1-x} \leq 1 + 2x < \sum_{k=0}^{\infty} \frac{(2x)^k}{k!} = e^{2x}.$$

Daher gilt:

$$\sum_n \frac{1}{n} = \prod_{i=1}^{k} \frac{1}{1-\frac{1}{p_i}} \leq \prod_{i=1}^{k} e^{\frac{2}{p_i}} = e^{2\sum_{i=1}^{k}\frac{1}{p_i}}.$$

Im Fall $C := \sum_{i=1}^{\infty} \frac{1}{p_i} < \infty$ wäre also $\sum_n \frac{1}{n} \leq e^{2C} < \infty$. Der Grenzübergang $k \longrightarrow \infty$ würde also liefern: $\sum_{n=1}^{\infty} \frac{1}{n} \leq e^{2C} < \infty$. Dies ist ein Widerspruch; denn aus der Analysis ist bekannt: $\sum_{n=1}^{\infty} \frac{1}{n} = \infty$.

2.3 Satz. *Seien $x \in \mathbb{Q}$ und $c_0,\ldots,c_{k-1} \in \mathbb{Z}$ mit $x^k + c_{k-1}x^{k-1} + \ldots + c_1 x + c_0 = 0$. Dann ist $x \in \mathbb{Z}$.*

Beweis. O.B.d.A. sei $x \neq 0$. Wir schreiben $x = \frac{a}{b}$ mit teilerfremden $a, b \in \mathbb{Z}$. Dann ist $0 = b^k \cdot 0 = a^k + bz$ mit $z := c_{k-1}a^{k-1} + \ldots + c_1 ab^{k-2} + c_0 b^{k-1} \in \mathbb{Z}$. Daher ist jeder Primteiler von b auch einer von a^k und damit einer von a. Wegen $\mathrm{ggT}(a,b) = 1$ folgt: $b = \pm 1$, d.h. $x = \pm a \in \mathbb{Z}$.

Bemerkung. Seien $k, n \in \mathbb{N}$ mit $x := \sqrt[k]{n} \in \mathbb{Q}$. Wegen $x^k - n = 0$ ist dann $x \in \mathbb{Z}$ und damit sogar $x \in \mathbb{N}$.

Beispiel. $\sqrt{2} \notin \mathbb{Q}$.

2.4 Satz. (LAMBERT, 1728-1777)
(i) $e = \sum_{k=1}^{\infty} \frac{1}{k!} \notin \mathbb{Q}$;
(ii) $\pi \notin \mathbb{Q}$.

Beweis. (i) Sonst wäre $m!e \in \mathbb{N}$ für ein $m \in \mathbb{N}$. Dann wäre $r := m!e - \sum_{k=0}^{m} \frac{m!}{k!} \in \mathbb{Z}$. Andererseits gilt für $q := \frac{1}{m+2}$:

$$0 < r = \sum_{k=m+1}^{\infty} \frac{m!}{k!} = \frac{1}{m+1}(1 + \frac{1}{m+2} + \frac{1}{(m+2)(m+3)} + \ldots)$$
$$< \frac{1}{m+1}(1 + \frac{1}{q} + \frac{1}{q^2} + \ldots) = \frac{1}{m+1}\sum_{j=0}^{\infty} q^j = \frac{1}{m+1} \cdot \frac{1}{1-q} = \frac{m+2}{(m+1)^2} < 1.$$

Widerspruch!
(ii) Sonst wäre $\pi = \frac{a}{b}$ mit teilerfremden $a, b \in \mathbb{N}$. Für $n \in \mathbb{N}$ und $x \in \mathbb{R}$ sei

$$f(x) := f_n(x) := \frac{x^n(a-bx)^n}{n!} = \frac{1}{n!}\sum_{i=n}^{2n} c_i x^i$$

($c_i \in \mathbb{Z}$) und

$$F(x) := F_n(x) := f_n(x) + \sum_{k=1}^{n} (-1)^k f_n^{(2k)}(x).$$

Dann gilt:

$$f^{(n)}(x) = \sum_{i=n}^{2n} \frac{c_i}{n!} i(i-1)\ldots(i-n+1)x^{i-n} = \sum_{i=n}^{2n} c_i \binom{i}{n} x^{i-n},$$

also $f^{(k)}(0) \in \mathbb{Z}$ für $k \geq n$. Wegen $f^{(0)}(0) = \ldots = f^{(n-1)}(0) = 0$ folgt $f^{(k)}(0) \in \mathbb{Z}$ für $k \in \mathbb{N}_0$. Wegen

$$f(\pi - x) = \frac{(\pi - x)^n(a - b\pi + bx)^n}{n!} = \frac{(a-bx)^n x^n}{n!} = f(x)$$

ist auch $f^{(k)}(\pi) \in \mathbb{Z}$ für $k \in \mathbb{N}_0$, d.h. $F(0), F(\pi) \in \mathbb{Z}$. Wegen

$$\begin{aligned}(F'(x)\sin(x) - F(x)\cos(x))' \\ &= F''(x)\sin(x) + F'(x)\cos(x) - F'(x)\cos(x) - F(x)(-\sin(x)) \\ &= (F''(x) + F(x))\sin(x) = f(x)\sin(x)\end{aligned}$$

gilt:

$$I := \int_0^{\pi} f(x)\sin(x)dx = F'(\pi)\sin(\pi) - F(\pi)\cos(\pi) - F'(0)\sin(0) + F(0)\cos(0)$$
$$= F(\pi) + F(0) \in \mathbb{Z}.$$

Andererseits gilt für $0 < x < \pi$: $0 < f(x)\sin(x) \leq f(x) < \frac{\pi^n a^n}{n!}$, also

$$0 < I = \int_0^{\pi} f(x)\sin(x)dx < \frac{\pi^{n+1}a^n}{n!}.$$

Nach der Stirling-Formel gilt für große $n \in \mathbb{N}$: $n! \geq \frac{n^n}{e^n}$. Damit haben wir den Widerspruch

$$0 < I < \pi(\frac{\pi a e}{n})^n < 1.$$

2.5 Definition. Für $x \in \mathbb{R}$ definiert man die **Gauß-Klammer** $[x] := \lfloor x \rfloor$ als die größte ganze Zahl n mit $n \leq x$ (d.h. $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$).

Beispiel. $\lfloor \pi \rfloor = 3$, $\lfloor e \rfloor = 2$; man rundet also stets zu einer ganzen Zahl ab.

Satz. *Für $x, y \in \mathbb{R}$ gilt:* $\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x + y \rfloor \leq \lfloor x \rfloor + \lfloor y \rfloor + 1$.

Beweis. Wegen $0 \leq \rho := x - \lfloor x \rfloor < 1$ und $0 \leq \sigma := y - \lfloor y \rfloor < 1$ gilt:

$$\begin{aligned} \lfloor x \rfloor + \lfloor y \rfloor &= \lfloor \lfloor x \rfloor + \lfloor y \rfloor \rfloor \leq \lfloor \lfloor x \rfloor + \rho + \lfloor y \rfloor + \sigma \rfloor = \lfloor x + y \rfloor \\ &= \lfloor \lfloor x \rfloor + \rho + \lfloor y \rfloor + \sigma \rfloor = \lfloor x \rfloor + \lfloor y \rfloor + \lfloor \rho + \sigma \rfloor \leq \lfloor x \rfloor + \lfloor y \rfloor + 1. \end{aligned}$$

2.6 Definition. Sei $1 \neq b \in \mathbb{N}$, und sei $n \in \mathbb{N}_0$ mit b-adischer Entwicklung $n = \sum_{i=0}^{\infty} a_i b^i$ (d.h. $a_0, a_1, a_2, \ldots \in \{0, 1, \ldots, b-1\}$). Dann heißt $s_b(n) := \sum_{i=0}^{\infty} a_i$ **Quersumme** von n (bzgl. b).

Beispiel. Wegen $135 = 5 \cdot 10^0 + 3 \cdot 10^1 + 1 \cdot 10^2$ ist $s_{10}(135) = 5 + 3 + 1 = 9$; wegen $135 = 1 \cdot 2^7 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0$ ist $s_2(135) = 1 + 1 + 1 + 1 = 4$.

Satz. *Seien $p \in \mathbb{P}$, $n \in \mathbb{N}$ und $m \in \mathbb{N}_0$ maximal mit $p^m \mid n!$. Dann gilt:*

$$m = \frac{n - s_p(n)}{p - 1} = \lfloor \frac{n}{p} \rfloor + \lfloor \frac{n}{p^2} \rfloor + \lfloor \frac{n}{p^3} \rfloor + \cdots$$

Beweis. Von den Zahlen $1, 2, \ldots, n$ sind genau $\lfloor \frac{n}{p} \rfloor$ Zahlen durch p teilbar, genau $\lfloor \frac{n}{p^2} \rfloor$ durch p^2, genau $\lfloor \frac{n}{p^3} \rfloor$ durch p^3, usw. Daher gilt:

$$m = \lfloor \frac{n}{p} \rfloor + \lfloor \frac{n}{p^2} \rfloor + \lfloor \frac{n}{p^3} \rfloor + \ldots.$$

Die p-adische Entwicklung von n sei $n = a_0 + a_1 p + \ldots + a_r p^r$. Dann gilt:

$$\begin{aligned} \lfloor \frac{n}{p} \rfloor &= a_1 + a_2 p + \ldots + a_r p^{r-1}, \\ \lfloor \frac{n}{p^2} \rfloor &= a_2 + a_3 p + \ldots + a_r p^{r-2}, \\ &\ldots \\ \lfloor \frac{n}{p^i} \rfloor &= a_i + a_{i+1} p + \ldots + a_r p^{r-i}. \end{aligned}$$

Daraus folgt:

$$\begin{aligned} m &= a_1 + a_2(p+1) + a_3(p^2+p+1) + \ldots + a_r(p^{r-1} + \ldots + p + 1) \\ &= a_1\frac{p-1}{p-1} + a_2\frac{p^2-1}{p-1} + a_3\frac{p^3-1}{p-1} + \ldots + a_r\frac{p^r-1}{p-1} \\ &= \frac{a_1p + a_2p^2 + \ldots + a_rp^r - a_1 - a_2 - \ldots - a_r}{p-1} = \frac{n - s_p(n)}{p-1}. \end{aligned}$$

2.7 Beispiel. Sei $n := 100$. Für $p = 2$ ist dann $m = 50 + 25 + 12 + 6 + 3 + 1 = 97$, für $p = 3$ ist $m = 33 + 11 + 3 + 1 = 48$, für $p = 5$ ist $m = 20 + 4 = 24$, und für $p = 7$ ist $m = 14 + 2 = 16$. Daher ist $100! = 2^{97}3^{48}5^{24}7^{16} \cdot \ldots$.

Satz. *Für alle $x \in \mathbb{R}$ mit $x \geq 2$ gilt:* $(*)$ $\prod_{p\in\mathbb{P},\, p\leq x} p < 4^x$.

Beweis. Sicher gilt $(*)$ für $2 \leq x \leq 5$.
Ist $n \in \mathbb{N}$ ungerade mit $n \geq 5$ und gilt $\prod_{p\in\mathbb{P},p\leq n} p < 4^n$, so gilt $(*)$ auch für alle $x \in \mathbb{R}$ mit $n \leq x < n + 2$.
Daher genügt zu zeigen: $(*)$ gilt für alle ungeraden $x = n \in \mathbb{N}$. Der Induktionsanfang $n = 5$ ist klar. Sei also $n \geq 7$ ungerade und $k := \frac{n\pm1}{2}$, wobei das Vorzeichen so gewählt wird, dass k ungerade ist. Dann ist $k \geq 3$ und $n - k = \frac{n\mp1}{2}$ gerade. Daher gilt:

$$\prod_{p\in\mathbb{P},k<p\leq n} p \leq \binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

Andererseits ist $2^n = (1+1)^n = \sum_{i=0}^{n}\binom{n}{i} > \binom{n}{k} + \binom{n}{n-k} = 2\binom{n}{k}$, d.h. $\binom{n}{k} < 2^{n-1}$. Nach Induktionsvoraussetzung ist $\prod_{p\in\mathbb{P},p\leq k} p < 4^k$. Daher gilt insgesamt:

$$\prod_{p\in\mathbb{P},p\leq n} p = \prod_{p\in\mathbb{P},p\leq k} p \prod_{p\in\mathbb{P},k<p\leq n} p < 4^k \cdot 2^{n-1} = 2^{2k+n-1} \leq 2^{2n} = 4^n.$$

2.8 Satz. (BERTRANDs Postulat, 1822-1900)
Für $1 \neq n \in \mathbb{N}$ existiert ein $p \in \mathbb{P}$ mit $n < p < 2n$.

Beispiel. Für $n = 2$ nimmt man $p = 3$; für $n = 3$ nimmt man $p = 5$; für $4 \leq n \leq 6$ nimmt man $p = 7$; für $7 \leq n \leq 12$ nimmt man $p = 13$; für $13 \leq n \leq 22$ nimmt man $p = 23$; für $23 \leq n \leq 42$ nimmt man $p = 43$; für $43 \leq n \leq 82$ nimmt man $p = 83$; für $83 \leq n \leq 162$ nimmt man $p = 163$.

Beweis. Wir nehmen das Gegenteil an. Dann ist $n \geq 163$, und $\binom{2n}{n} = \frac{(2n)!}{n!n!}$ hat eine Primfaktorzerlegung der Form

$$\binom{2n}{n} = \prod_{p\in\mathbb{P},p\leq 2n} p^{\mu_p} = \prod_{p\in\mathbb{P},p\leq n} p^{\mu_p}.$$

Sei $p \in \mathbb{P}$, und sei $\nu_p \in \mathbb{N}_0$ mit $p^{\nu_p} \leq 2n < p^{\nu_p+1}$. Dann gilt nach Satz 2.6 und Satz 2.5:

$$\mu_p = \sum_{j=1}^{\nu_p} (\lfloor \frac{2n}{p^j} \rfloor - 2\lfloor \frac{n}{p^j} \rfloor) \leq \nu_p.$$

Wir unterscheiden drei Fälle:
Fall 1: $\frac{2n}{3} < p \leq n$, d.h. $1 \leq \frac{n}{p} < \frac{3}{2}$.
Dann ist $2 \leq \frac{2n}{p} < 3$ und $\mu_p = \lfloor \frac{2n}{p} \rfloor - 2\lfloor \frac{n}{p} \rfloor = 2 - 2 \cdot 1 = 0$.
Fall 2: $\sqrt{2n} < p \leq \frac{2n}{3}$.
Dann ist $p^2 > 2n$, d.h. $\mu_p \leq \nu_p \leq 1$.
Fall 3: $p \leq \sqrt{2n}$.
Dann ist $p^{\mu_p} \leq p^{\nu_p} \leq 2n$.
Insgesamt haben wir:

$$\binom{2n}{n} = \prod_{p \leq \sqrt{2n}} p^{\mu_p} \prod_{\sqrt{2n} < p \leq \frac{2n}{3}} p^{\mu_p} \prod_{\frac{2n}{3} < p \leq n} p^{\mu_p} \leq \prod_{p \leq \sqrt{2n}} (2n) \prod_{p \leq \frac{2n}{3}} p.$$

Es gibt genau $\lfloor \sqrt{2n} \rfloor$ natürliche Zahlen zwischen 1 und $\sqrt{2n}$. Wieviele davon sind Primzahlen? Natürlich sind 1 und die von 2 verschiedenen geraden Zahlen keine Primzahlen. Das sind also $\lfloor \sqrt{2n} \rfloor/2$ (falls $\lfloor \sqrt{2n} \rfloor$ gerade) bzw. $(\lfloor \sqrt{2n} \rfloor - 1)/2$ (falls $\lfloor \sqrt{2n} \rfloor$ ungerade) Zahlen. Wegen $n > 128$, d.h. $\sqrt{2n} > 16$ gilt auch: $9, 15 \notin \mathbb{P}$. Daher liegen zwischen 1 und $\sqrt{2n}$ höchstens $(\lfloor \sqrt{2n} \rfloor)/2 - 2$ bzw. $(\lfloor \sqrt{2n} \rfloor + 1)/2 - 2$ Primzahlen. Das sind also höchstens $\sqrt{2n}/2 - 1$ Primzahlen. Mit Satz 2.7 folgt:

$$\binom{2n}{n} < (2n)^{\frac{1}{2}\sqrt{2n}-1} \cdot 4^{\frac{2n}{3}}.$$

Andererseits ist $2^{2n} = (1+1)^{2n} = \sum_{i=0}^{2n} \binom{2n}{i}$. Das sind $2n+1$ Summanden, und $\binom{2n}{n}$ ist der größte davon. (Man denke dabei an das Pascalsche Dreieck.) Daher ist $2^{2n} \leq 2n \binom{2n}{n}$, d.h.

$$\frac{2^{2n}}{2n} \leq \binom{2n}{n} < (2n)^{\frac{1}{2}\sqrt{2n}-1} 4^{\frac{2n}{3}}.$$

Umformen ergibt: $2^{\frac{2}{3}n} < (2n)^{\frac{1}{2}\sqrt{2n}}$, d.h. $\frac{2}{3}n\log(2) < \frac{1}{2}\sqrt{2n}\log(2n)$. Daraus folgt:

$$\sqrt{8n}\log(2) - 3\log(2n) < 0.$$

Für die Funktion $f : I := [128, \infty[\longrightarrow \mathbb{R}$, $x \longmapsto \sqrt{8x}\log(2) - 3\log(2x)$, gilt: $f(128) = 8\log(2) > 0$. Ferner ist $f'(x) = \frac{1}{x}(\sqrt{2x}\log(2) - 3) > 0$ für $x \in I$, d.h. f wächst monoton; insbesondere ist $f(x) > 0$ für $x \in I$.

2.9 Bemerkung. (Sieb des ERATOSTHENES, 276-196)
Seien $n \in \mathbb{N}$ und $\{p \in \mathbb{P} : p \leq \sqrt{n}\} = \{2, 3, 5, \ldots, q\}$. Aus der Reihe der Zahlen $2, 3, 4, 5, \ldots, n$ streichen wir alle durch $2, 3, 5, \ldots, q$ teilbaren Zahlen. Dann bleiben die $p \in \mathbb{P}$ mit $\sqrt{n} < p \leq n$ übrig.

Beispiel. Im Fall $n = 100$ ist $\sqrt{n} = 10$ und $\{p \in \mathbb{P} : p \leq 10\} = \{2, 3, 5, 7\}$. Das Sieb des Eratosthenes liefert in diesem Fall die Primzahlen $11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97$:

1	~~2~~	~~3~~	~~4~~	~~5~~	~~6~~	~~7~~	~~8~~	~~9~~	~~10~~
11	~~12~~	**13**	~~14~~	~~15~~	~~16~~	**17**	~~18~~	**19**	~~20~~
~~21~~	~~22~~	**23**	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	**29**	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	**37**	~~38~~	~~39~~	~~40~~
41	~~42~~	**43**	~~44~~	~~45~~	~~46~~	**47**	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	**53**	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	**59**	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	**67**	~~68~~	~~69~~	~~70~~
71	~~72~~	**73**	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	**79**	~~80~~
~~81~~	~~82~~	**83**	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	**89**	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	**97**	~~98~~	~~99~~	~~100~~

2.10 Definition. Für $x \in \mathbb{R}$ setzt man $\pi(x) := |\{p \in \mathbb{P} : p \leq x\}|$.

Beispiel. $\pi(10) = 4$, $\pi(100) = 25$.

Satz. (TSCHEBYSCHEFF, 1821-1894)
Mit $a := \frac{1}{4}\log(2) \sim 0,17$ *und* $A := 6\log(2) \sim 4,16$ *gilt für alle* $x \in \mathbb{R}$ *mit* $x \geq 2$*:*

$$a\frac{x}{\log(x)} < \pi(x) < A\frac{x}{\log(x)}.$$

Beweis. Für $n \in \mathbb{N}$ gilt nach Bertrands Postulat:

$$n^{\pi(2n)-\pi(n)} < \prod_{p\in\mathbb{P}, n<p\leq 2n} p \leq \binom{2n}{n} = \frac{(2n)!}{n!n!} < \sum_{j=0}^{2n}\binom{2n}{j} = (1+1)^{2n} = 2^{2n}.$$

Wir setzen $n = 2^{k-1}$ für ein $k \in \mathbb{N}$ und erhalten: $(2^{k-1})^{\pi(2^k)-\pi(2^{k-1})} < 2^{2^k}$, d.h.

$$(k-1)(\pi(2^k) - \pi(2^{k-1})) < 2^k$$

und $k\pi(2^k) < (k-1)\pi(2^{k-1}) + \pi(2^k) + 2^k$. Sicher ist $\pi(2^k) \leq 2^{k-1}$; denn 1 und die geraden Zahlen (außer 2) sind keine Primzahlen. Daher ist $k\pi(2^k) < (k-1)\pi(2^{k-1}) + 3 \cdot 2^{k-1}$, d.h. $\pi(2^k) < \frac{k-1}{k}\pi(2^{k-1}) + 3 \cdot \frac{2^{k-1}}{k}$. Wir zeigen induktiv, dass für $k \in \mathbb{N}$ gilt:

$$(*) \qquad \pi(2^k) < 3 \cdot \frac{2^k}{k}.$$

Für $k = 1$ gilt $(*)$ wegen $\pi(2) = 1 < 6$. Sei also $k > 1$ fest und schon gezeigt:

$$\pi(2^{k-1}) < 3 \cdot \frac{2^{k-1}}{k-1}.$$

Dann folgt:

$$\pi(2^k) < \frac{k-1}{k} \cdot 3 \cdot \frac{2^{k-1}}{k-1} + 3 \cdot \frac{2^{k-1}}{k} = 3 \cdot \frac{2^k}{k}.$$

Daher gilt $(*)$. Für $x \in \mathbb{R}$ mit $2^k \leq x < 2^{k+1}$ folgt:

$$\pi(x) \leq \pi(2^{k+1}) < 3 \cdot \frac{2^{k+1}}{k+1} = 6\log(2)\frac{2^k}{\log(2^{k+1})} \leq A\frac{x}{\log(x)}.$$

Damit ist die obere Schranke bewiesen. Wir wenden uns also der unteren Schranke zu. Die Primfaktorzerlegung von $\binom{2n}{n}$ sei $\prod_{p\in\mathbb{P}} p^{\mu_p}$. Ferner sei $\nu_p \in \mathbb{N}_0$ mit $p^{\nu_p} \leq 2n < p^{\nu_p+1}$. Dann gilt nach Satz 2.5: $\mu_p = \sum_{j=1}^{\nu_p}(\lfloor \frac{2n}{p^j} \rfloor - 2\lfloor \frac{n}{p^j} \rfloor) \leq \nu_p$, d.h. $p^{\mu_p} \leq p^{\nu_p} \leq 2n$. Daher gilt:

$$\binom{2n}{n} = \prod_{p\in\mathbb{P}, p\leq 2n} p^{\mu_p} \leq (2n)^{\pi(2n)}.$$

Andererseits ist

$$\binom{2n}{n} = \frac{2n}{n} \cdot \frac{2n-1}{n-1} \cdots \frac{n+1}{1} \geq 2^n,$$

d.h. $2^n \leq (2n)^{\pi(2n)}$. Wir setzen wieder $n = 2^{k-1}$ für ein $k \in \mathbb{N}$. Dann folgt: $2^{k\pi(2^k)} \geq 2^{2^{k-1}}$, d.h. $\pi(2^k) \geq \frac{2^{k-1}}{k} = \frac{2^k}{2k}$. Für $x \in \mathbb{R}$ mit $2^k \leq x < 2^{k+1}$ folgt:

$$\pi(x) \geq \pi(2^k) \geq \frac{2^k}{2k} = \frac{\log(2)}{4} \cdot \frac{2^{k+1}}{\log(2^k)} > a\frac{x}{\log(x)}.$$

Bemerkung. HADAMARD (1865-1963) und DE LA VALLEE–POUSSIN (1866-1962) haben gezeigt:

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\log(x)} = 1 \quad (\textbf{Primzahlsatz}).$$

Der Beweis ist schwieriger.

Beispiel.

x	$x/\log(x)$	$\pi(x)$	$\frac{\pi(x)}{x/\log(x)}$
10	$4,3$	4	$0,92$
100	$21,7$	25	$1,51$
1000	$144,7$	168	$1,16$

3. PRIMZAHLEN

3.1 Satz. *Es gibt beliebig große Primzahllücken.*

Beweis. Für $n \in \mathbb{N}$ gilt: $2 \mid (n+1)! + 2$, $3 \mid (n+1)! + 3$, ..., $n+1 \mid (n+1)! + (n+1)$, d.h. $(n+1)! + 2, \ldots, (n+1)! + (n+1) \notin \mathbb{P}$.

3.2 Satz. *Seien $k \in \mathbb{N}$ und $a_0, \ldots, a_k \in \mathbb{Z}$ mit $a_k \neq 0$. Setzt man $f := a_k x^k + \ldots + a_1 x + a_0$, so existieren unendlich viele $n \in \mathbb{N}$ mit $|f(n)| \notin \mathbb{P}$.*

Beweis. O.B.d.A. sei $a_k > 0$, d.h. $\lim_{n\to\infty} f(n) = \infty$. Daher existiert ein $N \in \mathbb{N}$ mit $f(n) > 1$ für alle $n \in \mathbb{N}$ mit $n \geq N$. Insbesondere ist $d := f(N) = a_k N^k + \ldots + a_1 N + a_0 > 1$. Für $m \in \mathbb{N}$ ist dann

$$\begin{aligned} f(md+N) &= a_k(md+N)^k + a_{k-1}(md+N)^{k-1} + \ldots + a_1(md+N) + a_0 \\ &= zmd + a_k N^k + a_{k-1}N^{k-1} + \ldots + a_1 N + a_0 = zmd + f(N) = zmd + d \end{aligned}$$

für ein $z \in \mathbb{Z}$. Daher gilt: $d \mid f(md+N)$; insbesondere ist $f(md+N) \notin \mathbb{P}$ für unendlich viele $m \in \mathbb{N}$.

Beispiel. $x^2 - 79x + 1601 \in \mathbb{P}$ für $x = 1, \ldots, 79$.

Bemerkung. (i) Nach dem **Primzahlsatz von** DIRICHLET (1805-1859) existieren für beliebige $a, b \in \mathbb{N}$ mit $\mathrm{ggT}(a,b) = 1$ unendlich viele Primzahlen der Form $p = ax + b$ $(x \in \mathbb{Z})$.
(ii) Man weiß nicht, ob unendlich viele Primzahlen der Form $p = x^2 + 1$ $(x \in \mathbb{Z})$ existieren.

3.3 Definition. Seien $p \in \mathbb{P}$, $a_0, \ldots, a_k \in \mathbb{Z}$ und $f := a_k X^k + \ldots + a_1 X + a_0$. Existiert ein $n \in \mathbb{N}$ mit $p \mid f(n)$, so heißt p **Primteiler** von f.

Satz. *Seien $a_0, \ldots, a_k \in \mathbb{Z}$ mit $k > 0$ und $a_k \neq 0$. Dann hat $f := a_k X^k + \ldots + a_1 X + a_0$ unendlich viele Primteiler.*

Beweis. O.B.d.A. sei $a_0 \neq 0$; sonst ist die Behauptung trivial. Dann gilt:

$$f(a_0 Y) = a_k(a_0 Y)^k + \ldots + a_1(a_0 Y) + a_0 = a_0 g(Y);$$

dabei ist $g = b_k Y^k + \ldots + b_1 Y + 1$ mit $b_1, \ldots, b_k \in \mathbb{Z}$ und $b_k \neq 0$. Daher genügt zu zeigen, dass g unendlich viele Primteiler hat.
Sicher hat g mindestens einen Primteiler. Sind $p_1, \ldots, p_r$ Primteiler von g, so gilt für $n \in \mathbb{N}$:

$$g(np_1 \ldots p_r) = h(n)p_1 \ldots p_r + 1;$$

dabei ist h ein ganzzahliges Polynom vom Grad $k > 0$. Es gibt also unendlich viele $n \in \mathbb{N}$ mit $h(n)p_1 \ldots p_r + 1 \neq \pm 1$. Jedes solche n liefert einen Primteiler $p_{r+1} \notin \{p_1, \ldots, p_r\}$ von g.

3.4 Satz. *Seien $a, n \in \mathbb{N} \setminus \{1\}$ mit $a^n + 1 \in \mathbb{P}$. Dann ist a gerade, und n ist eine Potenz von 2.*

Beweis. Wäre a ungerade, so wäre $a^n + 1$ gerade, also $a^n + 1 = 2$, d.h. $a^n = 1$. Widerspruch!
Wäre n keine Potenz von 2, so wäre $n = 2^k m$, wobei $1 \neq m \in \mathbb{N}$ ungerade und $k \in \mathbb{N}_0$ ist. Dann wäre aber

$$a^n + 1 = a^{2^k m} + 1 = (a^{2^k(m-1)} - a^{2^k(m-2)} + - \ldots - a^{2^k} + 1)(a^{2^k} + 1) \notin \mathbb{P}.$$

Definition. Primzahlen der Form $p = 2^{2^m} + 1$ heißen **Fermat-Primzahlen** (FERMAT, 1601-1665).

Bemerkung. (i) Für $m = 0, 1, 2, 3, 4$, d.h. $2^{2^m} + 1 = 3, 5, 17, 257, 65.537$ ist $2^{2^m} + 1 \in \mathbb{P}$. Man weiß nicht, ob es weitere Fermat-Primzahlen gibt. Z.B. gilt: $641 \mid 2^{2^5} + 1$. Bekannt ist: $2^{2^m} + 1 \notin \mathbb{P}$ für $m = 5, \ldots, 32$. Man weiß auch nicht, ob $2^{2^m} + 1 \notin \mathbb{P}$ für unendlich viele $m \in \mathbb{N}$ gilt.
(ii) GAUSS (1777-1855) hat gezeigt, dass sich ein regelmäßiges n-Eck genau dann nur mit Zirkel und Lineal konstruieren lässt, wenn n Produkt einer 2-Potenz mit paarweise verschiedenen Fermat-Primzahlen ist.

3.5 Satz. *Sind $a, n \in \mathbb{N} \setminus \{1\}$ mit $a^n - 1 \in \mathbb{P}$, so gilt: $a = 2$ und $n \in \mathbb{P}$.*

Beweis. Wegen $a - 1 \mid a^n - 1 \in \mathbb{P}$ ist $a - 1 = 1$, d.h. $a = 2$. Für $k, l \in \mathbb{N}$ ist ferner $a^k - 1 \mid a^{kl} - 1$.

Definition. Primzahlen der Form $p = 2^n - 1$ ($n \in \mathbb{N}$) heißen **Mersenne-Primzahlen** (MERSENNE, 1588-1648).

Bemerkung. Die kleinsten Mersenne-Primzahlen entstehen für $n = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127$. Bis heute (2012) kennt man 47 Mersenne-Primzahlen. Man weiß nicht, ob es unendlich viele Mersenne-Primzahlen gibt. Man weiß auch nicht, ob $2^p - 1 \notin \mathbb{P}$ für unendlich viele $p \in \mathbb{P}$ gilt.

3.6 Definition. Eine natürliche Zahl n heißt **vollkommen**, wenn die Summe ihrer echten Teiler $d \in \mathbb{N}$ gleich n ist.

Beispiel. $6 = 1 + 2 + 3$ und $28 = 1 + 2 + 4 + 7 + 14$ sind vollkommen.

Satz. *Eine gerade Zahl $n \in \mathbb{N}$ ist genau dann vollkommen, wenn sie die Form $n = 2^{p-1}(2^p - 1)$ mit einer Mersenne-Primzahl $2^p - 1$ hat.*

Beweis. "$\Longleftarrow$": (EUKLID)
Sei $n = 2^{p-1}(2^p - 1)$ mit $2^p - 1 \in \mathbb{P}$. Die positiven Teiler von n sind dann genau die Zahlen 2^i und $2^i(2^p - 1)$ mit $i \in \{0, 1, \ldots, p-1\}$. Die Summe dieser Teiler ist also

$$\sum_{i=0}^{p-1}(2^i + 2^i(2^p - 1)) = \sum_{i=0}^{p-1} 2^i 2^p = 2^p(2^p - 1) = 2n.$$

Die Summe der echten Teiler von n ist also n, d.h. n ist vollkommen.
"$\Longrightarrow$": (EULER)

Wir schreiben $n = 2^r m$ mit $r, m \in \mathbb{N}$ und $2 \nmid m$. Im folgenden sei $\sigma(n)$ die Summe *aller* (positiven) Teiler von n (d.h. $\sigma(6) = 1 + 2 + 3 + 6 = 12$.) Dann gilt:

$$2^{r+1}m = 2n = \sigma(n) = \sum_{i=0}^{r} \sum_{d|m} 2^i d = (1 + 2 + \ldots + 2^r) \sum_{d|m} d = (2^{r+1} - 1)\sigma(m).$$

Daher gilt: $2^{r+1} - 1 \mid m$, etwa $m = (2^{r+1} - 1)M$ mit $M \in \mathbb{N}$. Dann ist $2^{r+1}M = \sigma(m) \geq m + M = 2^{r+1}M$. Folglich ist $m \in \mathbb{P}$ und $M = 1$. Wegen $m = 2^{r+1} - 1$ ist m eine Mersenne-Primzahl, und $n = 2^r(2^{r+1} - 1)$.

Bemerkung. Man weiß nicht, ob es ungerade vollkommene Zahlen gibt.

3.7 Definition. Paare von Primzahlen der Form $(p, p + 2)$ heißen **Primzahlzwillinge**.

Beispiel. $(3, 5)$, $(5, 7)$, $(11, 13)$, $(17, 19)$, ... sind Primzahlzwillinge.

Bemerkung. (i) Man vermutet, dass es unendlich viele Primzahlzwillinge gibt.
(ii) Man weiß (BRUN, 1885-1978): $\sum_{p \in \mathbb{P}, p+2 \in \mathbb{P}} \frac{1}{p} + \frac{1}{p+2} < 2$.
Das größte *bekannte* Paar von Primzahlzwillingen hat über 200.000 Dezimalstellen (2011).

3.8 Bemerkung. Die **Goldbach-Vermutung** (GOLDBACH, 1690-1764) besagt, dass sich jede gerade natürliche Zahl $n \geq 4$ als Summe von zwei Primzahlen schreiben lässt; sie ist unbewiesen.
Aus dieser Vermutung würde folgen, dass sich jede ungerade natürliche Zahl $n \geq 7$ als Summe von 3 Primzahlen schreiben lässt; auch das ist unbewiesen.
VINOGRADOV hat aber 1937 gezeigt, dass sich jede genügend große ungerade natürliche Zahl n als Summe von 3 ungeraden Primzahlen schreiben lässt. Man weiß heute, dass dabei $n > 10^{1350}$ ausreicht.
RAMAREE hat 1995 gezeigt, dass sich jede gerade natürliche Zahl als Summe von höchstens 6 Primzahlen schreiben lässt.
Über die Goldbach-Vermutung gibt es einen Roman: A. Doxiadis, *Onkel Petros und die Goldbachsche Vermutung.*

3.9 Bemerkung. CATALAN (1814-1894) vermutete, dass die Gleichung

$$x^p - y^q = 1 \qquad (x, y \in \mathbb{N},\ p, q \in \mathbb{N} \setminus 1)$$

nur die Lösung $x^p = 9$, $y^q = 8$ hat; dies wurde 2002 von MIHAILESCU bewiesen.

3.10 Definition. Eine Primzahl p mit $2p + 1 \in \mathbb{P}$ heißt **Sophie-Germain-Primzahl** (SOPHIE GERMAIN, 1776-1831).

Beispiel. $2, 3, 5, 11$ sind Sophie-Germain-Primzahlen.

Bemerkung. (i) Man vermutet, dass es unendliche viele Sophie-Germain-Primzahlen gibt.
(ii) Sophie-Germain-Primzahlen wurden im Zusammenhang mit der **Fermat-Vermutung** eingeführt (vgl. Kapitel 13).

(iii) Die Fermat-Vermutung besagt, dass die Gleichung $x^n + y^n = z^n$ $(x, y, z \in \mathbb{N})$ für $n \geq 3$ keine Lösung hat. Diese Vermutung wurde 1995 von A. WILES bewiesen.

4. KONGRUENZEN

4.1 Bemerkung. Bekanntlich ist eine **Relation** ein Tripel (M, N, R) von Mengen M, N, R mit $R \subseteq M \times N$. Statt $(x, y) \in R$ schreibt man oft xRy. Eine Relation der Form (M, M, R) heißt **Äquivalenzrelation**, wenn gilt:
(i) $x \in M \Longrightarrow xRx$; (*Reflexivität*)
(ii) $xRy \Longrightarrow yRx$; (*Symmetrie*)
(iii) $xRy \wedge yRz \Longrightarrow xRz$. (*Transitivität*)
Beispiele für Äquivalenzrelationen sind die Kongruenz oder die Ähnlichkeit von Dreiecken. Für eine beliebige Äquivalenzrelation (M, M, R) und $x \in M$ heißt

$$[x]_R := \{y \in M : xRy\}$$

Äquivalenzklasse von x bzgl. R. Die Menge aller Äquivalenzklassen bezeichnet man mit

$$M/R = \{[x]_R : x \in M\}.$$

Bekanntlich sind für $x, y \in M$ die folgenden Bedingungen gleichwertig:

(1) xRy; (2) $[x]_R = [y]_R$; (3) $[x]_R \cap [y]_R \neq \emptyset$.

Daher ist M/R eine **Partition** von M, d.h. eine Menge nichtleerer, paarweise disjunkter Teilmengen von M mit Vereinigung M.
Bekanntlich liefert umgekehrt jede Partition $\mathfrak{P}$ einer Menge M eine Äquivalenzrelation (M, M, R) durch folgende Vorschrift:

$$xRy :\Longleftrightarrow \exists P \in \mathfrak{P} : x, y \in P.$$

Ferner ist dann $M/R = \mathfrak{P}$. Daher sind Äquivalenzrelationen auf einer Menge M und Partitionen von M nur verschiedene Sichtweisen des gleichen mathematischen Sachverhalts.

4.2 Definition. Seien $a, b \in \mathbb{Z}$ und $m \in \mathbb{N}$ mit $m \mid a - b$. Dann heißt a **kongruent** zu b **modulo** m. Man schreibt: $a \equiv b \pmod{m}$.

Satz. *Die Kongruenz modulo m ist eine Äquivalenzrelation. Ferner ist sie mit Addition und Multiplikation* **verträglich**, *d.h. es gilt:*

$$a \equiv a' \pmod{m} \wedge b \equiv b' \pmod{m} \Longrightarrow a+b \equiv a'+b' \pmod{m} \wedge ab \equiv a'b' \pmod{m}.$$

Beweis. *Reflexivität:* $a \in \mathbb{Z} \Longrightarrow m \mid 0 = a - a \Longrightarrow a \equiv a \pmod{m}$.
Symmetrie: $a \equiv b \pmod{m} \Longrightarrow m \mid a - b \Longrightarrow m \mid -(a - b) = b - a \Longrightarrow b \equiv a \pmod{m}$.
Transitivität: $a \equiv b \pmod{m} \wedge b \equiv c \pmod{m} \Longrightarrow m \mid a - b \wedge m \mid b - c \Longrightarrow m \mid (a - b) + (b - c) = a - c \Longrightarrow a \equiv c \pmod{m}$.

Verträglichkeit: Es sei $a \equiv a' \pmod m$ und $b \equiv b' \pmod m$, d.h. $m \mid a - a'$ und $m \mid b - b'$. Dann gilt: $m \mid (a - a') + (b - b') = (a + b) - (a' + b')$, d.h. $a + b \equiv a' + b' \pmod m$.
Ferner gilt: $m \mid (a - a')b + a'(b - b') = ab - a'b'$, d.h. $ab \equiv a'b' \pmod m$.

Bemerkung. Für $a \in \mathbb{Z}$ und $m \in \mathbb{N}$ heißt

$$a + m\mathbb{Z} := \{a + mz : z \in \mathbb{Z}\} = \{\ldots, a - 2m, a - m, a, a + m, a + 2m, \ldots\}$$

Restklasse von a modulo m. Dies ist die Äquivalenzklasse von a bzgl. der Kongruenz modulo m; z.B. ist

$$2 + 6\mathbb{Z} = \{\ldots, -10, -4, 2, 8, 14, \ldots\} = 8 + 6\mathbb{Z} = -4 + 6\mathbb{Z} = \cdots$$

Warum heißt $a + m\mathbb{Z}$ Restklasse? Division mit Rest liefert $q, r \in \mathbb{Z}$ mit $a = qm + r$ und $0 \le r < m$. Wegen $m \mid qm = a - r$ ist dann $a \equiv r \pmod m$, d.h. $a + m\mathbb{Z} = r + m\mathbb{Z}$. Die Menge aller Restklassen modulo m ist also

$$\{a + m\mathbb{Z} : a \in \mathbb{Z}\} = \{0 + m\mathbb{Z}, 1 + m\mathbb{Z}, \ldots, m - 1 + m\mathbb{Z}\} =: \mathbb{Z}/m\mathbb{Z}.$$

Sind $r, s \in \{0, 1, \ldots, m - 1\}$ mit $r \equiv s \pmod m$, so ist $m \mid r - s$ und $|r - s| < m$, d.h. $r - s = 0$, also $r = s$. Daher gilt:

$$|\mathbb{Z}/m\mathbb{Z}| = m.$$

Beispiel. Wegen $2^{16} = (2^8)^2 = (256)^2 = 65.536 \equiv 154 \pmod{641}$ und $2^{32} = (2^{16})^2 \equiv (154)^2 = 23.716 \equiv -1 \pmod{641}$ ist $641 \mid 2^{32} + 1 = 2^{2^5} + 1$, d.h. $2^{2^5} + 1 \notin \mathbb{P}$. (Vgl. Bemerkung 3.4.)

4.3 Satz. *Für $a, b, c \in \mathbb{Z}$ und $m \in \mathbb{N}$ gilt:*
(i) $m \mid ab \wedge \mathrm{ggT}(a, m) = 1 \Longrightarrow m \mid b$.
(ii) $ab \equiv ac \pmod m \Longleftrightarrow b \equiv c \pmod{\frac{m}{\mathrm{ggT}(a,m)}}$.

Beweis. (i) Sei $\mathrm{ggT}(a, m) = 1$. Dann existieren $x, y \in \mathbb{Z}$ mit $xa + ym = 1$, d.h. $xab + ymb = b$. Aus $m \mid ab$ folgt also: $m \mid b$.
(ii) "$\Longrightarrow$": Sei $ab \equiv ac \pmod m$, d.h. $a(b - c) = zm$ für ein $z \in \mathbb{Z}$. Dann ist $\frac{a}{d}(b - c) = z\frac{m}{d}$ mit $d := \mathrm{ggT}(a, m)$. Wegen $1 = \mathrm{ggT}(\frac{a}{d}, \frac{m}{d})$ folgt aus (i): $\frac{m}{d} \mid b - c$, d.h. $b \equiv c \pmod{\frac{m}{d}}$.
"$\Longleftarrow$": Sei $b \equiv c \pmod{\frac{m}{d}}$, d.h. $b - c = z\frac{m}{d}$ für ein $z \in \mathbb{Z}$. Dann ist $a(b - c) = zm\frac{a}{d}$, d.h. $ab \equiv ac \pmod m$.

4.4 Satz. *Seien $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$ und $d := \mathrm{ggT}(a, m)$. Genau dann hat die Kongruenz $ax \equiv b \pmod m$ eine Lösung $x \in \mathbb{Z}$, wenn $d \mid b$ gilt. Ggf. bilden die Lösungen eine Restklasse modulo $\frac{m}{d}$.*

Beweis. "$\Longrightarrow$": Sei $x \in \mathbb{Z}$ mit $ax \equiv b \pmod m$, d.h. $ax - b = my$ für ein $y \in \mathbb{Z}$. Dann gilt: $d \mid ax - my = b$.
"$\Longleftarrow$": Sei $d \mid b$, $a' := \frac{a}{d}$, $m' := \frac{m}{d}$ und $b' := \frac{b}{d}$. Wegen $\mathrm{ggT}(a', m') = 1$ existieren $y', z' \in \mathbb{Z}$ mit $1 = a'y' + m'z'$. Dann ist $b = ba'y' + bm'z' = ab'y' + mb'z' \equiv ax' \pmod m$ mit $x' := b'y'$. Für $x \in \mathbb{Z}$ gilt also nach Satz 4.3:

$$ax \equiv b \pmod m \Longleftrightarrow ax \equiv ax' \pmod m \Longleftrightarrow x \equiv x' \pmod{m'} \Longleftrightarrow x \in x' + m'\mathbb{Z}.$$

Beispiel. Wir wollen die Kongruenz $23x \equiv 17 \pmod{100}$ lösen. Der erweiterte euklidische Algorithmus liefert: $1 = 3 \cdot 100 - 13 \cdot 23 \equiv 23 \cdot (-13) \pmod{100}$. Daher ist $17 \equiv 23 \cdot (-13) \cdot 17 \equiv 23 \cdot (-221) \equiv 23 \cdot \mathbf{79} \pmod{100}$. (Probe!)

4.5 Definition. Seien $a_1, \ldots, a_n \in \mathbb{Z}$. Jedes $m \in \mathbb{Z}$ mit $a_1 \mid m$, ..., $a_n \mid m$ heißt **gemeinsames Vielfaches** von $a_1, \ldots, a_n$. Ein gemeinsames Vielfaches $v \in \mathbb{N}_0$ von $a_1, \ldots, a_n$ heißt **kleinstes gemeinsames Vielfaches** (kgV) von $a_1, \ldots, a_n$, wenn v jedes gemeinsame Vielfache von $a_1, \ldots, a_n$ teilt.

Bemerkung. Im Fall $a_i = 0$ für ein $i \in \{1, \ldots, n\}$ ist 0 das einzige gemeinsame Vielfache, also auch das einzige kgV von $a_1, \ldots, a_n$. Sei also $a_i \neq 0$ und $a_i = \prod_{p \in \mathbb{P}} p^{b_{ip}}$ für $i = 1, \ldots, n$. Die gemeinsamen Vielfachen von $a_1, \ldots, a_n$ haben dann die Form $\pm \prod_{p \in \mathbb{P}} p^{c_p}$ mit $c_p \geq \max\{b_{1p}, \ldots, b_{np}\}$ für $p \in \mathbb{P}$. Daher ist $v := \prod_{p \in \mathbb{P}} p^{\max\{b_{1p}, \ldots, b_{np}\}}$ das einzige kgV von $a_1, \ldots, a_n$. Insbesondere haben beliebige $a_1, \ldots, a_n \in \mathbb{Z}$ stets genau ein kgV v. Man schreibt: $v = \mathrm{kgV}(a_1, \ldots, a_n)$.

Satz. *Für $a_1, \ldots, a_n \in \mathbb{Z}$ gilt stets:*
(i) $\mathrm{kgV}(a_1, \ldots, a_n) = \mathrm{kgV}(\mathrm{kgV}(a_1, \ldots, a_{n-1}), a_n)$*;*
(ii) $\mathrm{kgV}(a_1, \mathrm{ggT}(a_2, \ldots, a_n)) = \mathrm{ggT}(\mathrm{kgV}(a_1, a_2), \ldots, \mathrm{kgV}(a_1, a_n))$*;*
(iii) $\mathrm{ggT}(a_1, \mathrm{kgV}(a_2, \ldots, a_n)) = \mathrm{kgV}(\mathrm{ggT}(a_1, a_2), \ldots, \mathrm{ggT}(a_1, a_n))$.

Beweis. Wir beweisen nur (iii). [Der Rest geht analog.] Im Fall $a_1 = 0$ steht auf beiden Seiten $\mathrm{kgV}(a_2, \ldots, a_n)$. Sei also $a_1 \neq 0$. Im Fall $a_i = 0$ für ein $i \in \{2, \ldots, n\}$ steht links $\mathrm{ggT}(a_1, 0) = \pm a_1$. Wegen $\mathrm{ggT}(a_1, a_2), \ldots, \mathrm{ggT}(a_1, a_n) \mid \pm a_1 = \mathrm{ggT}(a_1, a_i)$ steht auch rechts $\pm a_1$.
Sei also $a_i \neq 0$ und $a_i = \prod_{p \in \mathbb{P}} p^{b_{ip}}$ für $i = 1, \ldots, n$. Dann steht links:

$$\prod_{p \in \mathbb{P}} p^{\min\{b_{1p}, \max\{b_{2p}, \ldots, b_{np}\}\}}.$$

Und rechts steht:

$$\prod_{p \in \mathbb{P}} p^{\max\{\min\{b_{1p}, b_{2p}\}, \ldots, \min\{b_{1p}, b_{np}\}\}}.$$

Beide Seiten stimmen überein, da stets die Exponenten gleich sind:

$$\min\{b_1, \max\{b_2, \ldots, b_n\}\} = \max\{\min\{b_1, b_2\}, \ldots, \min\{b_1, b_n\}\}.$$

[Zum Beweis sei o.B.d.A. $b_2 \leq \ldots \leq b_n$. Dann gilt:

$$\min\{b_1, \max\{b_2, \ldots, b_n\}\} = \min\{b_1, b_n\}$$

und $\min\{b_1, b_2\} \leq \min\{b_1, b_3\} \leq \ldots \leq \min\{b_1, b_n\}$, d.h.

$$\max\{\min\{b_1, b_2\}, \ldots, \min\{b_1, b_n\}\} = \min\{b_1, b_n\}.]$$

4.6 Satz. (WILSON, 1741-1793)

$p \in \mathbb{P} \Longrightarrow (p-1)! \equiv -1 \pmod{p}$.

Beweis. Für $a \in \{1, \ldots, p-1\}$ existiert nach Satz 4.4 genau ein $a' \in \{1, \ldots, p-1\}$ mit $aa' \equiv 1 \pmod{p}$. Wir fassen also $1, 2, \ldots, p-1$ zu Paaren (a, a') zusammen. Das geht, außer im Fall $a = a'$, d.h. $a^2 \equiv 1 \pmod{p}$. Das bedeutet aber $p \mid a^2 - 1 = (a+1)(a-1)$, d.h. $p \mid a+1$ oder $p \mid a-1$, also $a \in \{p-1, 1\}$. Daher gilt: $(p-1)! = 1 \cdot 2 \cdots (p-1) \equiv 1 \cdot (p-1) \equiv -1 \pmod{p}$.

Beispiele. Für $p = 2$ ist $1 \equiv 1 \pmod{2}$; für $p = 3$ ist $2 \equiv -1 \pmod{3}$; für $p = 5$ ist $24 \equiv -1 \pmod{5}$.

Bemerkung. Für $2 \neq p \in \mathbb{P}$ folgt aus dem Satz von Wilson leicht:

$$\left(\frac{p-1}{2}!\right)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p};$$

denn es gilt:

$$\begin{aligned} -1 &\equiv 1 \cdot 2 \cdots \frac{p-1}{2} \cdot \frac{p+1}{2} \cdots (p-1) \\ &\equiv 1 \cdot 2 \cdots \frac{p-1}{2} \cdot (p - \frac{p-1}{2}) \cdots (p-1) \\ &\equiv 1 \cdot 2 \cdots \frac{p-1}{2} \cdot (-\frac{p-1}{2}) \cdots (-1) \\ &\equiv (\frac{p-1}{2}!)^2 (-1)^{\frac{p-1}{2}} \pmod{p}. \end{aligned}$$

Für $p \equiv 1 \pmod{4}$ ist also $(\frac{p-1}{2}!)^2 \equiv -1 \pmod{p}$, und für $p \equiv 3 \pmod{4}$ ist $(\frac{p-1}{2}!)^2 \equiv 1 \pmod{p}$. Darauf werden wir im Zusammenhang mit dem Quadratischen Reziprozitätsgesetz noch zurückkommen.

4.7 Satz. (Chinesischer Restsatz)
Seien $a_1, \ldots, a_n \in \mathbb{Z}$ und $m_1, \ldots, m_n \in \mathbb{N}$. Genau dann existiert ein $x \in \mathbb{Z}$ mit

$$x \equiv a_i \pmod{m_i} \quad \text{für} \quad i = 1, \ldots, n,$$

wenn gilt:

$$a_i \equiv a_j \pmod{\mathrm{ggT}(m_i, m_j)} \quad \text{für alle} \quad i, j \in \{1, \ldots, n\}.$$

Ggf. bilden die $x \in \mathbb{Z}$ mit $x \equiv a_i \pmod{m_i}$ für $i = 1, \ldots, n$ genau eine Restklasse modulo $\mathrm{kgV}(m_1, \ldots, m_n)$.

Beweis. "$\Longrightarrow$": Sei $x \in \mathbb{Z}$ mit $x \equiv a_i \pmod{m_i}$ für $i = 1, \ldots, n$. Für $i, j \in \{1, \ldots, n\}$ gilt dann: $a_i \equiv x \equiv a_j \pmod{\mathrm{ggT}(m_i, m_j)}$.
"$\Longleftarrow$": (Induktion nach n)
Im Fall $n = 1$ setzen wir $x := a_1$ und sind fertig. Im Fall $n = 2$ gilt nach Voraussetzung: $d := \mathrm{ggT}(m_1, m_2) \mid a_1 - a_2$. Ferner existieren $v_1, v_2 \in \mathbb{Z}$ mit $m_1 v_1 + m_2 v_2 = d$. Für $z := \frac{v_1(a_2 - a_1)}{d} \in \mathbb{Z}$ gilt dann:

$$m_1 z \equiv (d - m_2 v_2) \frac{a_2 - a_1}{d} \equiv a_2 - a_1 - m_2 v_2 \frac{a_2 - a_1}{d} \equiv a_2 - a_1 \pmod{m_2}.$$

Für $x := a_1 + m_1 z$ gilt also: $x \equiv a_1 \pmod{m_1}$ und $x \equiv a_1 + (a_2 - a_1) \equiv a_2 \pmod{m_2}$. Damit ist der Fall $n = 2$ erledigt.
Sei also $n > 2$ und die Behauptung für $n-1$ schon bewiesen. Es existiert dann ein $y \in \mathbb{Z}$ mit $y \equiv a_i \pmod{m_i}$ und damit auch $y \equiv a_i \equiv a_n \pmod{\text{ggT}(m_i, m_n)}$ für $i = 1, \ldots, n-1$ nach Voraussetzung. Daher ist $y - a_n$ teilbar durch

$$\text{kgV}(\text{ggT}(m_1, m_n), \ldots, \text{ggT}(m_{n-1}, m_n)) = \text{ggT}(\text{kgV}(m_1, \ldots, m_{n-1}), m_n).$$

Der Fall $n = 2$ liefert also ein $x \in \mathbb{Z}$ mit $x \equiv y \pmod{\text{kgV}(m_1, \ldots, m_{n-1})}$ und $x \equiv a_n \pmod{m_n}$. Für $i = 1, \ldots, n-1$ ist dann auch $x \equiv y \equiv a_i \pmod{m_i}$.
Eindeutigkeit: Seien $x, x' \in \mathbb{Z}$ mit $x \equiv a_i \equiv x' \pmod{m_i}$ für $i = 1, \ldots, n$. Dann ist $x' - x$ durch $m_1, \ldots, m_n$, also auch durch $M := \text{kgV}(m_1, \ldots, m_n)$ teilbar. Folglich gilt $x' \equiv x \pmod{M}$.
Umgekehrt gilt für $z \in \mathbb{Z}$ und $i = 1, \ldots, n$: $x + Mz \equiv x \equiv a_i \pmod{m_i}$.

4.8 Satz. *Seien $m_1, \ldots, m_n \in \mathbb{N}$ paarweise teilerfremd. Zu beliebigen $a_1, \ldots, a_n \in \mathbb{Z}$ existiert dann ein $x \in \mathbb{Z}$ mit $x \equiv a_i \pmod{m_i}$ für $i = 1, \ldots, n$, und diese x bilden genau eine Restklasse modulo $m_1 \ldots m_n$.*

Beweis. Das folgt unmittelbar aus Satz 4.7.

Beispiel. Wir suchen ein $x \in \mathbb{Z}$ mit

$$x \equiv 2 \pmod{10}, \quad x \equiv 7 \pmod{15}, \quad x \equiv 4 \pmod{21}.$$

Wir setzen zunächst $x_1 := 2$. Dann ist sicher $x_1 \equiv 2 \pmod{10}$. Dann machen wir den Ansatz $x_2 = 2 + 10y$ mit $y \in \mathbb{Z}$. Dann gilt:

$$x_2 \equiv 7 \pmod{15} \iff 10y \equiv 5 \pmod{15} \iff 2y \equiv 1 \pmod{3}.$$

Wir setzen also $y := 2$, d.h. $x_2 = 22$. Dann gilt:

$$x_2 \equiv 2 \pmod{10} \quad \text{und} \quad x_2 \equiv 7 \pmod{15}.$$

Wir machen den Ansatz $x_3 = 22 + 30z$ mit $z \in \mathbb{Z}$. Dann gilt:

$$x_3 \equiv 4 \pmod{21} \iff 30z \equiv 3 \pmod{21} \iff 10z \equiv 1 \pmod{7}.$$

Wir setzen also $z := -2$, d.h. $x_3 = 22 - 60 = -38$. (Probe!). Wegen $\text{kgV}(10, 15, 21) = 210$ ist die Lösungsmenge also $-38 + 210\mathbb{Z}$.

5. GRUPPEN

5.1 Definition. Eine **Verknüpfung** auf einer Menge M ist eine Abbildung $M \times M \longrightarrow M$. Das Bild von $(a, b) \in M \times M$ unter dieser Abbildung schreibt man oft in der Form $a * b$, $a \circ b$, $a + b$, $a \cdot b$ oder ab.

Beispiel. (i) Addition, Multiplikation und Subtraktion auf $\mathbb{Q}$ oder $\mathbb{R}$, aber nicht die Division, da z.B. $5/0$ nicht definiert ist;
(ii) $\wedge$, $\vee$, $\Longrightarrow$ auf $M = \{w, f\}$;
(iii) $\cap$, $\cup$, $\setminus$ auf der Potenzmenge $\mathfrak{P}(X) = 2^X$ einer Menge X;
(iv) Komposition $\circ$ auf $M = \mathrm{Abb}(X, X) = \{f : X \longrightarrow X \mid f \text{ Abbildung}\}$.

5.2 Definition. Eine **Gruppe** ist ein Paar $(G, *)$, das aus einer Menge G und einer Verknüpfung $*$ auf G mit folgenden Eigenschaften besteht:
(i) $(a * b) * c = a * (b * c)$ für alle $a, b, c \in G$ (*Assoziativgesetz*);
(ii) Es existiert ein Element $e \in G$ (**neutrales Element**) mit $e * a = a = a * e$ für alle $a \in G$;
(iii) Zu jedem $a \in G$ existiert ein $a' \in G$ (**inverses Element**) mit $a * a' = e = a' * a$.

Bemerkung. (i) Das Element e in (ii) ist eindeutig bestimmt; denn ist auch $f \in G$ mit $f * a = a = a * f$ für alle $a \in G$, so folgt $e = e * f = f$. Jede Gruppe enthält also *genau ein* neutrales Element; dieses bezeichnet man oft mit 1 oder 0.
(ii) Für $a \in G$ ist das Element a' in (iii) eindeutig bestimmt; denn ist auch $\tilde{a} \in G$ mit $a * \tilde{a} = e = \tilde{a} * a$, so gilt:

$$\tilde{a} = \tilde{a} * e = \tilde{a} * (a * a') = (\tilde{a} * a) * a' = e * a' = a'.$$

Jedes $a \in G$ hat also *genau ein* inverses Element a'; dieses bezeichnet man oft mit a^{-1} oder $-a$.
(iii) Wegen (i) lässt man Klammern häufig weg und schreibt: $a * b * c$.
(iv) Gilt $a * b = b * a$ für alle $a, b \in G$, so heißt $(G, *)$ **kommutative** oder **abelsche** Gruppe (N. H. ABEL, 1802-1829).

Beispiel. (a) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ und $(\mathbb{R}, +)$ sind abelsche Gruppen; neutrales Element ist 0, und $-x$ ist jeweils invers zu x. Dagegen ist $(\mathbb{N}, +)$ *keine* Gruppe (denn es existiert zum Beispiel kein neutrales Element). Auch $(\mathbb{N}_0, +)$ ist keine Gruppe (denn zum Beispiel hat 2 kein Inverses).
(b) $(\mathbb{Q} \setminus \{0\}, \cdot)$ und $(\mathbb{R} \setminus \{0\}, \cdot)$ sind abelsche Gruppen; neutrales Element ist 1, und $\frac{1}{x}$ ist jeweils invers zu x. Dagegen ist $(\mathbb{Z} \setminus \{0\}, \cdot)$ *keine* Gruppe (denn zum Beispiel hat 2 kein Inverses).
(c) Für jede Menge X ist $\mathrm{Sym}(X) := \{f \in \mathrm{Abb}(X, X) : f \text{ bijektiv}\}$ eine Gruppe bzgl. $\circ$; neutrales Element ist die **Identitätsabbildung** $\mathrm{id}_X : X \longrightarrow X$, $x \longmapsto x$, und invers zu $f \in \mathrm{Sym}(X)$ ist die Umkehrabbildung $f^{-1} : X \longrightarrow X$. Man nennt $(\mathrm{Sym}(X), \circ)$ **symmetrische Gruppe** auf X; ihre Elemente, d.h. die bijektiven Abbildungen $f : X \longrightarrow X$, heißen **Permutationen** auf X. Im Fall $X = \{1, \ldots, n\}$ für ein $n \in \mathbb{N}$ schreibt man:

$$f = \begin{pmatrix} 1 & 2 & \ldots & n \\ f(1) & f(2) & \ldots & f(n) \end{pmatrix}.$$

Für $X = \{1, 2, 3\}$ besteht $\mathrm{Sym}(X)$ aus den folgenden Permutationen:

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

$$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}, \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix};$$

insbesondere ist $|\mathrm{Sym}(X)| = 6$. Diese Gruppe ist nichtabelsch; denn es gilt:

$$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} \circ \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix},$$

$$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} \circ \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}.$$

Für $X = \{1, \ldots, n\}$ ist $|\mathrm{Sym}(X)| = n!$; denn für $f(1)$ hat man n Möglichkeiten, für $f(2)$ hat man noch $n-1$ Möglichkeiten, für $f(3)$ hat man noch $n-2$ Möglichkeiten, usw.
(d) Für Gruppen $(G_1, *), \ldots, (G_n, *)$ mit neutralen Elementen $e_1, \ldots, e_n$ ist auch ihr **direktes Produkt** $(G_1 \times \ldots \times G_n, *)$ eine Gruppe, wenn man definiert:

$$(a_1, \ldots, a_n) * (b_1, \ldots, b_n) := (a_1 * b_1, \ldots, a_n * b_n) \qquad (a_1, b_1 \in G_1, \ldots, a_n, b_n \in G_n).$$

Neutrales Element in $G_1 \times \ldots \times G_n$ ist $(e_1, \ldots, e_n)$, und invers zu $(a_1, \ldots, a_n)$ ist das Element $(a_1^{-1}, \ldots, a_n^{-1})$.

Satz. *Sei $(G, *)$ eine Gruppe mit neutralem Element e. Dann gilt für alle $a, b \in G$:*
(i) $e^{-1} = e$;
(ii) $(a^{-1})^{-1} = a$;
(iii) $(a * b)^{-1} = b^{-1} * a^{-1}$. (!)

Beweis. (i) $e * e = e \Longrightarrow e^{-1} = e$.
(ii) $a^{-1} * a = e = a * a^{-1} \Longrightarrow (a^{-1})^{-1} = a$.
(iii) Wegen $(a*b)*(b^{-1}*a^{-1}) = ((a*b)*b^{-1})*a^{-1} = (a*(b*b^{-1}))*a^{-1} = (a*e)*a^{-1} = a*a^{-1} = e$ und $(b^{-1}*a^{-1})*(a*b) = \ldots = e$ ist $(a*b)^{-1} = b^{-1}*a^{-1}$.

5.3 Bemerkung. Sei $(G, *)$ eine Gruppe. Im folgenden lassen wir $*$ oft weg und sagen kurz: Sei G eine Gruppe. Für $a \in G$ und $n \in \mathbb{Z}$ definieren wir die n-te **Potenz** von a durch $a^n := a \cdots a$ (n Faktoren), falls $n > 0$; außerdem setzen wir $a^0 := 1$ und $a^n := (a^{-1})^{-n}$ für $n < 0$. Dann hat man die folgenden Rechenregeln:

$$a^m a^n = a^{m+n} \quad \text{und} \quad (a^m)^n = a^{mn} \qquad (m, n \in \mathbb{Z}).$$

I.Allg. ist dagegen $(ab)^n \neq a^n b^n$ für $a, b \in G$. Ist G aber abelsch, so gilt auch $(ab)^n = a^n b^n$ für alle $a, b \in G$. Oft schreibt man dann $+$ statt $\cdot$ und na statt a^n. Die Rechenregeln nehmen dann die folgende Form an:

$$ma + na = (m+n)a, \quad n(ma) = (nm)a, \quad [n(a+b) = na + nb].$$

Die **Ordnung** $|G|$ von G ist definiert als die Anzahl der Elemente in G.

5.4 Definition. Eine Teilmenge $H \neq \emptyset$ einer Gruppe G heißt **Untergruppe** von G, falls gilt:

(i) $a, b \in H \Longrightarrow ab \in H$;
(ii) $a \in H \Longrightarrow a^{-1} \in H$.
Ggf. schreibt man: $H \leq G$, im Fall $H \neq G$ auch $H < G$.

Bemerkung. (i) Sei $H \leq G$. Dann existiert ein Element $a \in H$. Nach Definition ist also auch $a^{-1} \in H$ und $1 = aa^{-1} \in H$. Daher ist H selbst eine Gruppe mit der entsprechend eingeschränkten Verknüpfung. Die neutralen Elemente in G und H stimmen überein.
(ii) Eine Teilmenge $H \neq \emptyset$ einer Gruppe G ist genau dann eine Untergruppe von G, wenn gilt: $(*)$ $a, b \in H \Longrightarrow ab^{-1} \in H$. Der Beweis ist eine leichte Übung.
(iii) Für Untergruppen H, K von G gilt: $H \cap K \leq G$.

Beispiel. (i) Wir haben Untergruppen $(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +)$ und $(\mathbb{Q} \setminus \{0\}, \cdot) \leq (\mathbb{R} \setminus \{0\}, \cdot)$.
(ii) Für jede Gruppe G ist $\{1\} \leq G$ und $G \leq G$; man nennt $\{1\}$ die **triviale** Untergruppe von G. Die Untergruppen $H < G$ heißen **echte** Untergruppen von G.
(iii) Für jede Gruppe G und jedes Element $a \in G$ ist $\langle a \rangle := \{a^n : n \in \mathbb{Z}\} \leq G$; man nennt $\langle a \rangle$ die von a **erzeugte zyklische** Untergruppe von G. Für $G = (\mathbb{Z}, +)$ und $a = 5$ ist also

$$\langle 5 \rangle = \{0, \pm 5, \pm 10, \ldots\} =: 5\mathbb{Z}.$$

Für $G = \mathrm{Sym}(3) := \mathrm{Sym}(\{1, 2, 3\})$ und $a := \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ ist $a^2 = 1$, $a^3 = a$, …, $a^{-1} = a$. Daher ist $\langle a \rangle = \{1, a\}$.

5.5 Definition. Sei G eine Gruppe und $H \leq G$. Für $a \in G$ heißt $aH := \{ah : h \in H\}$ **Linksnebenklasse** und $Ha := \{ha : h \in H\}$ **Rechtsnebenklasse** von a nach H. Mit $G/H := \{aH : a \in G\}$ und $H\backslash G := \{Ha : a \in G\}$ bezeichnet man die Menge aller Linksnebenklassen bzw. Rechtsnebenklassen von G nach H.

Bemerkung. (i) Für $a \in G$ ist

$$Ha^{-1} = \{ha^{-1} : h \in H\} = \{k^{-1}a^{-1} : k \in H\} = \{(ak)^{-1} : k \in H\}.$$

Für jede Linksnebenklasse X nach H ist also $X^{-1} = \{x^{-1} : x \in X\}$ eine Rechtsnebenklasse nach H. Die Anzahl $|G : H|$ aller Linksnebenklassen nach H in G stimmt also mit der Anzahl der Rechtsnebenklassen nach H in G überein; man nennt $|G : H|$ **Index** von H in G.
(ii) Für $a, b \in G$ gilt:

$$aH \cap bH \neq \emptyset \Longleftrightarrow aH = bH \Longleftrightarrow a^{-1}b \in H;$$

zum Beweis sei zunächst $c \in aH \cap bH$. Wir schreiben $c = ah_0$ mit $h_0 \in H$. Für $h \in H$ ist dann $ch = ah_0h \in aH$ und $ah = ch_0^{-1}h \in cH$. Daher ist $cH = aH$. Analog ist $cH = bH$, d.h. $aH = bH$.
Sei jetzt $aH = bH$. Dann ist $a = a \cdot 1 \in aH = bH$, d.h. $a = bh$ für ein $h \in H$. Daher ist $a^{-1}b = h^{-1} \in H$.
Sei schließlich $a^{-1}b \in H$. Dann ist $b = a \cdot a^{-1}b \in aH \cap bH$.

(iii) Für $a \in G$ ist $H \longrightarrow aH$, $h \longmapsto ah$, bijektiv; insbesondere ist $|aH| = |H|$.

Satz. (LAGRANGE, 1736-1813)
Für jede Gruppe G und alle $H \leq G$ gilt: $|G| = |G : H| \cdot |H|$; insbesondere sind $|H|$ und $|G : H|$ im Fall $|G| < \infty$ Teiler von $|G|$.

Beweis. Nach der obigen Bemerkung liegt jedes Element $a \in G$ in genau einer Linksnebenklasse nach H. Es gibt genau $|G : H|$ Linksnebenklassen, und jede davon enthält genau $|H|$ Elemente.

Beispiel. (i) Für $G := \mathrm{Sym}(3)$ und $H := \langle a \rangle$ mit $a := \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ ist $|G| = 6$ und $|H| = 2$, also $|G : H| = 3$. (Probe!)
(ii) Für $G = \mathbb{Z}$ und $H = 5\mathbb{Z}$ hat man die folgenden Linksnebenklassen:

$$\begin{aligned} 0 + 5\mathbb{Z} &= \{\ldots, -10, -5, 0, 5, 10, \ldots\}, \\ 1 + 5\mathbb{Z} &= \{\ldots, -9, -4, 1, 6, 11, \ldots\}, \\ 2 + 5\mathbb{Z} &= \{\ldots, -8, -3, 2, 7, 12, \ldots\}, \\ 3 + 5\mathbb{Z} &= \{\ldots, -7, -2, 3, 8, 13, \ldots\}, \\ 4 + 5\mathbb{Z} &= \{\ldots, -6, -1, 4, 9, 14, \ldots\}. \end{aligned}$$

Daher ist $|\mathbb{Z} : 5\mathbb{Z}| = 5$. Analog ist $|\mathbb{Z} : n\mathbb{Z}| = n$ für $n \in \mathbb{N}$.
(iii) Eine Gruppe der Ordnung 12 kann nach dem Satz von Lagrange keine Untergruppen der Ordnung 7 enthalten. Solche Beobachtungen sind wichtig bei der Bestimmung aller Untergruppen einer gegebenen Gruppe.

5.6 Definition. Für jede Gruppe G und jedes Element $a \in G$ heißt $|\langle a \rangle|$ **Ordnung** von a.

Bemerkung. Wir unterscheiden zwei Fälle:
Fall I: Alle a^n $(n \in \mathbb{Z})$ sind verschieden.
Dann ist $|\langle a \rangle| = \infty$.
Fall II: Es gibt $m, n \in \mathbb{Z}$ mit $m < n$ und $a^m = a^n$.
Dann ist $n - m \in \mathbb{N}$ und $a^{n-m} = a^n a^{-m} = a^m a^{-m} = 1$. Sei $k \in \mathbb{N}$ minimal mit $a^k = 1$. Für $l \in \mathbb{Z}$ liefert dann Division mit Rest Elemente $q, r \in \mathbb{Z}$ mit $l = qk + r$ und $0 \leq r < k$. Daher ist $a^l = (a^k)^q a^r = 1^q a^r = a^r$. Also ist

$$\langle a \rangle = \{a^0 = 1, a^1 = a, a^2, \ldots, a^{k-1}\}.$$

Dabei sind $a^0, a^1, \ldots, a^{k-1}$ paarweise verschieden; denn ist $a^i = a^j$ und $1 \leq i \leq j < k$, so ist $0 \leq j - i < k$ und $a^{j-i} = a^j a^{-i} = a^i a^{-i} = 1$, d.h. $j - i = 0$ nach Wahl von k.
In diesem Fall ist also $|\langle a \rangle| = k$.
In beiden Fällen gilt daher:

$$|\langle a \rangle| = \inf\{k \in \mathbb{N} : a^k = 1\}.$$

Satz. *Sei G eine endliche Gruppe, und sei $a \in G$ ein Element der Ordnung m. Dann gilt für $i, j \in \mathbb{Z}$:*

(i) $a^i = 1 \iff m \mid i$; *insbesondere ist* $a^{|G|} = 1$ (FERMAT).
(ii) $a^i = a^j \iff i \equiv j \pmod{m}$.
(iii) $|\langle a^i \rangle| = \frac{m}{\mathrm{ggT}(m,i)}$.
(iv) *Ist G abelsch, ist $b \in G$ ein Element der Ordnung n und ist* $\mathrm{ggT}(m,n) = 1$*, so hat ab die Ordnung mn.*

Beweis. (i) "$\Longrightarrow$": Es sei $a^i = 1$. Nach der Bemerkung ist auch $a^m = 1$. Division mit Rest liefert Elemente $q, r \in \mathbb{Z}$ mit $i = qm + r$ und $0 \leq r < m$. Dann ist $1 = a^i = (a^m)^q a^r = 1^q a^r = a^r$. Also ist $r = 0$ nach der Bemerkung, d.h. $m \mid i$.
"$\Longleftarrow$": Sei $m \mid i$, d.h. $i = ml$ für ein $l \in \mathbb{Z}$. Dann ist $a^i = (a^m)^l = 1^l = 1$.
Nach dem Satz von Lagrange ist $m = |\langle a \rangle| \,\big|\, |G|$, also $a^{|G|} = 1$.
(ii) Sei $a^i = a^j$, d.h. $a^{i-j} = a^i a^{-j} = a^j a^{-j} = 1$. Nach (i) ist dann $m \mid i - j$, d.h. $i \equiv j \pmod{m}$.
Sei umgekehrt $i \equiv j \pmod{m}$, d.h. $m \mid i - j$. Dann ist $1 = a^{i-j} = a^i a^{-j}$ nach (i), d.h. $a^j = a^i$.
(iii) Wegen $m \mid \frac{im}{\mathrm{ggT}(m,i)}$ gilt nach (i): $1 = a^{\frac{im}{\mathrm{ggT}(m,i)}} = (a^i)^{\frac{m}{\mathrm{ggT}(m,i)}}$. Mit (i), angewandt auf a^i statt a, folgt: $t := |\langle a^i \rangle| \,\big|\, \frac{m}{\mathrm{ggT}(m,i)}$. Andererseits ist $a^{it} = (a^i)^t = 1$ nach (i), angewandt auf a^i statt a. Wegen (i) ist also $m \mid it$. Daher gilt: $\frac{m}{\mathrm{ggT}(m,i)} \mid \frac{i}{\mathrm{ggT}(m,i)} t$. Da $\frac{m}{\mathrm{ggT}(m,i)}$ und $\frac{i}{\mathrm{ggT}(m,i)}$ teilerfremd sind, folgt: $\frac{m}{\mathrm{ggT}(m,i)} \mid t$. Insgesamt ist also $t = \frac{m}{\mathrm{ggT}(m,i)}$.
(iv) Wegen $\langle a \rangle \cap \langle b \rangle \leq \langle a \rangle$ ist $|\langle a \rangle \cap \langle b \rangle| \,\big|\, |\langle a \rangle| = m$. Analog ist $|\langle a \rangle \cap \langle b \rangle| \,\big|\, n$. Daher ist $|\langle a \rangle \cap \langle b \rangle| \,\big|\, \mathrm{ggT}(m,n) = 1$, d.h. $\langle a \rangle \cap \langle b \rangle = \{1\}$. Sei $k := |\langle ab \rangle|$. Dann ist $1 = (ab)^k = a^k b^k$, d.h. $a^k = b^{-k} \in \langle a \rangle \cap \langle b \rangle = \{1\}$; insbesondere ist $a^k = 1$. Wegen (i) folgt: $m \mid k$. Analog gilt: $n \mid k$. Daher ist $mn \mid k$. Andererseits ist $(ab)^{mn} = (a^m)^n (b^n)^m = 1^n 1^m = 1$, d.h. $k \mid mn$ nach (i), angewandt auf ab statt a.

5.7 Satz. *Für jede Gruppe G und alle $H \leq G$ sind äquivalent:*
(1) $aH = Ha$ *für alle* $a \in G$;
(2) $aHa^{-1} = H$ *für alle* $a \in G$;
(3) $aHa^{-1} \subseteq H$ *für alle* $a \in G$.

Beweis. (1) $\iff$ (2) $\Longrightarrow$ (3): Klar!
(3) $\Longrightarrow$ (2): Sei (3) erfüllt und $a \in G$. Dann ist $H = aa^{-1}H(a^{-1})^{-1}a^{-1} \subseteq aHa^{-1}$.

Definition. Ggf. heißt H **normal** oder **Normalteiler** in G. Man schreibt $H \trianglelefteq G$, im Fall $H \neq G$ auch $H \triangleleft G$.

Beispiel. (i) Stets ist $\{1\} \trianglelefteq G$ und $G \trianglelefteq G$.
(ii) Aus $H, K \trianglelefteq G$ folgt $H \cap K \trianglelefteq G$; denn für $a \in G$ gilt:

$$a(H \cap K)a^{-1} \subseteq aHa^{-1} \cap aKa^{-1} \subseteq H \cap K.$$

(iii) In einer abelschen Gruppe ist jede Untergruppe normal.
(iv) Jede Untergruppe H einer Gruppe G mit $|G : H| = 2$ ist normal in G; denn die beiden Linksnebenklassen (Rechtsnebenklassen) nach H in G sind H und $G \setminus H$.
(v) Es seien $G := \mathrm{Sym}(3)$ und $H := \langle b \rangle$ mit $b := \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$. Dann ist $H = \{1, b, b^2\}$ (nachrechnen!), also $|H| = 3$, d.h. $|G : H| = 2$ nach dem Satz von Lagrange. Daher gilt: $H \trianglelefteq G$.

(vi) Es seien $G := \mathrm{Sym}(3)$ und $H := \langle a \rangle$ mit $a := \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$. Dann ist $H \not\trianglelefteq G$ wegen

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} H = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

und

$$H \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\}.$$

5.8 Satz *Für jeden Normalteiler N einer Gruppe G wird G/N zu einer Gruppe, wenn man definiert:*

$$(aN)(bN) := (ab)N \qquad (a, b \in G).$$

Definition. G/N heißt **Faktorgruppe** von G nach N.

Beweis. Wir zeigen zunächst, dass die Verknüpfung in G/N *wohldefiniert* ist, d.h. nicht von der Schreibweise der Nebenklassen abhängt. Dazu seien $a, a', b, b' \in G$ mit $aN = a'N$ und $bN = b'N$. Dann ist $a^{-1}a' \in N$, also auch $b^{-1}a^{-1}a'b \in N$. Folglich ist $abN = a'bN$. Analog ist $a'bN = a'b'N$.
Offensichtlich ist die Verknüpfung in G/N assoziativ, neutrales Element in G/N ist $1N = N$, und es gilt: $(aN)^{-1} = a^{-1}N$ für $a \in G$.

Beispiel. Für $G = \mathbb{Z}$ und $N = 5\mathbb{Z}$ ist

$$G/N = \mathbb{Z}/5\mathbb{Z} = \{0 + 5\mathbb{Z}, 1 + 5\mathbb{Z}, \ldots, 4 + 5\mathbb{Z}\}$$

eine Gruppe der Ordnung 5 bzgl. $+$. Zum Beispiel gilt:

$$(3 + 5\mathbb{Z}) + (4 + 5\mathbb{Z}) = 7 + 5\mathbb{Z} = 2 + 5\mathbb{Z}.$$

6. HOMOMORPHISMEN

6.1 Definition. Seien G, H Gruppen. Eine Abbildung $f : G \longrightarrow H$ mit $f(ab) = f(a)f(b)$ für alle $a, b \in G$ heißt **Homomorphismus**. Wir setzen

$$\mathrm{Hom}(G, H) := \{h : G \longrightarrow H \mid h \text{ Homomorphismus}\}.$$

Bemerkung. (i) Ggf. ist $f(1_G) = f(1_G)1_H = f(1_G)f(1_G)f(1_G)^{-1} = f(1_G1_G)f(1_G)^{-1} = f(1_G)f(1_G)^{-1} = 1_H$, d.h. $f(1_G) = 1_H$.
(ii) Daher gilt für $a \in G$: $f(a^{-1}) = f(a^{-1})1_H = f(a^{-1})f(a)f(a)^{-1} = f(a^{-1}a)f(a)^{-1} = f(1_G)f(a)^{-1} = 1_H f(a)^{-1} = f(a)^{-1}$, d.h. $f(a^{-1}) = f(a)^{-1}$.

(iii) Für Gruppen G, H, K und $f \in \mathrm{Hom}(G,H)$, $g \in \mathrm{Hom}(H,K)$ ist $g \circ f \in \mathrm{Hom}(G,K)$; denn für $a, b \in G$ gilt:

$$(g \circ f)(ab) = g(f(ab)) = g(f(a)f(b)) = g(f(a))g(f(b)) = (g \circ f)(a) \cdot (g \circ f)(b).$$

Beispiel. (i) Für beliebige Gruppen G, H ist $G \longrightarrow H$, $g \longmapsto 1$, ein Homomorphismus.
(ii) $f : (\mathbb{R}, +) \longrightarrow (\mathbb{R} \setminus \{0\}, \cdot)$, $x \longmapsto 2^x$, ist ein Homomorphismus; denn für $x, y \in \mathbb{R}$ ist $f(x+y) = 2^{x+y} = 2^x 2^y = f(x)f(y)$.
(iii) Für $n \in \mathbb{N}$ und jeden Körper K ist $\mathrm{GL}(n,K) \longrightarrow K \setminus \{0\}$, $A \longmapsto \det(A)$, ein Homomorphismus.

Satz. *Für Gruppen G, H und $f \in \mathrm{Hom}(G,H)$ gilt:*
(i) *Für $U \leq G$ ist $f(U) \leq H$; insbesondere ist $\mathrm{Bld}(f) = f(G) \leq H$.*
(ii) *Für $U \trianglelefteq G$ ist $f(U) \trianglelefteq f(G)$, aber nicht unbedingt $f(U) \trianglelefteq H$.*
(iii) *Für $V \leq H$ ist $f^{-1}(V) \leq G$.*
(iv) *Für $V \trianglelefteq H$ ist $f^{-1}(V) \trianglelefteq G$.*

Beweis. (i) Wegen $U \neq \emptyset$ ist $f(U) \neq \emptyset$. Seien $x, y \in f(U)$. Wir schreiben $x = f(a)$, $y = f(b)$ mit $a, b \in U$. Dann ist $xy^{-1} = f(a)f(b)^{-1} = f(a)f(b^{-1}) = f(ab^{-1}) \in f(U)$ wegen $ab^{-1} \in U$.
(ii) Für $a \in G$ und $u \in U$ ist $f(a)f(u)f(a)^{-1} = f(aua^{-1}) \in f(U)$ wegen $aua^{-1} \in U$. Daher gilt: $f(U) \trianglelefteq f(G)$.
Seien $G := \langle \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \rangle$, $H := \mathrm{Sym}(3)$ und $f : G \longrightarrow H$, $g \longmapsto g$, die Inklusionsabbildung. Dann ist $G \trianglelefteq G$, aber $f(G) = G \not\trianglelefteq H$. (Vgl. Beispiel 5.7 (vi)).
(iii) Wegen $f(1_G) = 1_H \in V$ ist $1_G \in f^{-1}(V)$, d.h. $f^{-1}(V) \neq \emptyset$. Seien $a, b \in f^{-1}(V)$, d.h. $f(a), f(b) \in V$. Dann gilt: $f(ab^{-1}) = f(a)f(b)^{-1} \in V$, d.h. $ab^{-1} \in f^{-1}(V)$.
(iv) Seien $a \in G$ und $b \in f^{-1}(V)$, d.h. $f(b) \in V$. Dann ist $f(aba^{-1}) = f(a)f(b)f(a)^{-1} \in V$, d.h. $aba^{-1} \in f^{-1}(V)$.

6.2 Bemerkung. Für Gruppen G, H und $f \in \mathrm{Hom}(G,H)$ ist

$$\mathrm{Ker}(f) := f^{-1}(\{1_H\}) = \{a \in G : f(a) = 1_H\} \trianglelefteq G;$$

man nennt $\mathrm{Ker}(f)$ den **Kern** von f.

Beispiel. Für $n \in \mathbb{N}$ und jeden Körper K ist

$$\mathrm{SL}(n,K) := \mathrm{Ker}(\det) = \{A \in \mathrm{GL}(n,K) : \det(A) = 1\} \trianglelefteq \mathrm{GL}(n,K);$$

$\mathrm{SL}(n,K)$ heißt **spezielle lineare Gruppe** des **Grades** n über K, und $\mathrm{GL}(n,K)$ ist die allgemeine lineare Gruppe des Grades n über K.

Satz. *Für Gruppen G, H und $f \in \mathrm{Hom}(G,H)$ gilt:* f injektiv $\Longleftrightarrow \mathrm{Ker}(f) = \{1_G\}$.

Beweis. "$\Longrightarrow$": Sei f injektiv. Wegen $\mathrm{Ker}(f) \leq G$ ist $1_G \in \mathrm{Ker}(f)$, d.h. $\{1_G\} \subseteq \mathrm{Ker}(f)$. Sei umgekehrt $x \in \mathrm{Ker}(f)$, d.h. $f(x) = 1 = f(1_G)$. Daher ist $x = 1_G$, da f injektiv ist. Dies zeigt: $\mathrm{Ker}(f) = \{1_G\}$.

"$\Longleftarrow$": Sei $\mathrm{Ker}(f) = \{1_G\}$. Für $x, y \in G$ mit $f(x) = f(y)$ gilt dann: $1 = f(x)f(y)^{-1} = f(xy^{-1})$. Daher ist $xy^{-1} \in \mathrm{Ker}(f) = \{1_G\}$, d.h. $xy^{-1} = 1_G$ und damit $x = y$.

6.3 Definition. Ein injektiver Homomorphismus heißt **Monomorphismus**, ein surjektiver Homomorphismus **Epimorphismus** und ein bijektiver Homomorphismus **Isomorphismus**.

Beispiel. (i) Für jede Untergruppe H einer Gruppe G ist die Inklusionsabbildung $H \longrightarrow G$, $h \longmapsto h$, ein Monomorphismus.
(ii) Für jeden Normalteiler N von G ist $f : G \longrightarrow G/N$, $a \longmapsto aN$, ein Epimorphismus. Man nennt f den **kanonischen Epimorphismus** von G auf G/N. Dann ist $\mathrm{Ker}(f) = N$; denn für $a \in G$ gilt:

$$a \in \mathrm{Ker}(f) \Longleftrightarrow aN = 1N \Longleftrightarrow a \in N.$$

(iii) Stets ist $\mathrm{id}_G : G \longrightarrow G$, $a \longmapsto a$, ein Isomorphismus.
(iv) Ist $f : G \longrightarrow H$ ein Isomorphismus, so auch $f^{-1} : H \longrightarrow G$; denn für $a, b \in H$ gilt:

$$f^{-1}(ab) = f^{-1}(f(f^{-1}(a)) \cdot f(f^{-1}(b))) = f^{-1}(f(f^{-1}(a) \cdot f^{-1}(b))) = f^{-1}(a) \cdot f^{-1}(b).$$

Bemerkung. Gruppen G und H heißen **isomorph** ($G \cong H$), wenn ein Isomorphismus $f : G \longrightarrow H$ existiert. Man zeigt leicht, dass $\cong$ reflexiv, symmetrisch und transitiv ist.

Satz. (Homomorphiesatz)
Seien G, H Gruppen, $f \in \mathrm{Hom}(G, H)$ und $K := \mathrm{Ker}(f)$. Dann ist

$$F : G/K \longrightarrow \mathrm{Bld}(f), \quad aK \longmapsto f(a),$$

ein Isomorphismus; insbesondere ist $G/\mathrm{Ker}(f) \cong \mathrm{Bld}(f)$.

Beweis. Wir zeigen zunächst, dass F wohldefiniert ist. Dazu seien $a, a' \in G$ mit $aK = a'K$, d.h. $a^{-1}a' \in K = \mathrm{Ker}(f)$. Dann ist $1 = f(a^{-1}a') = f(a)^{-1}f(a')$, d.h. $f(a) = f(a')$.
Für $a, b \in G$ ist $F(aK \cdot bK) = F(abK) = f(ab) = f(a)f(b) = F(aK)F(bK)$. Daher ist F ein Homomorphismus. Offensichtlich ist F surjektiv.
Sei $aK \in \mathrm{Ker}(F)$, d.h. $1 = F(aK) = f(a)$. Dann ist $a \in \mathrm{Ker}(f) = K$, d.h. $aK = 1K$. Dies zeigt: $\mathrm{Ker}(F) = \{1\}$, d.h. F ist injektiv.

6.4 Beispiel. Für $n \in \mathbb{N}$ und jeden Körper K folgt aus dem Homomorphiesatz:

$$\mathrm{GL}(n, K)/\mathrm{SL}(n, K) \cong K \setminus \{0\}.$$

Definition. Ein **Endomorphismus** (bzw. **Automorphismus**) einer Gruppe G ist ein Homomorphismus (bzw. Isomorphismus) $f : G \longrightarrow G$.

Bemerkung. Man zeigt leicht: $\mathrm{Aut}(G) := \{f : G \longrightarrow G \mid f \text{ Automorphismus}\} \leq \mathrm{Sym}(G)$; man nennt $\mathrm{Aut}(G)$ die **Automorphismengruppe** von G.

6.5 Definition. Eine Gruppe G heißt **zyklisch**, falls ein $a \in G$ mit $G = \langle a \rangle = \{a^n : n \in \mathbb{Z}\}$ existiert.

Beispiel. (i) $(\mathbb{Z},+)=\langle 1\rangle$ ist eine unendliche zyklische Gruppe.
(ii) Für $n\in\mathbb{N}$ ist $(\mathbb{Z}/n\mathbb{Z},+)=\langle 1+n\mathbb{Z}\rangle$ eine zyklische Gruppe der Ordnung n.
(iii) Jede Gruppe G von Primzahlordnung ist zyklisch; denn für $1\neq a\in G$ ist $1\neq |\langle a\rangle| \,\big|\, |G|$, also $|\langle a\rangle|=|G|$ und damit $\langle a\rangle=G$.

Satz. (i) *Jede unendliche zyklische Gruppe $G=\langle a\rangle$ ist zu $(\mathbb{Z},+)$ isomorph.*
(ii) *Jede zyklische Gruppe $G=\langle a\rangle$ der Ordnung $n<\infty$ ist zu $(\mathbb{Z}/n\mathbb{Z},+)$ isomorph.*

Beweis. (i) $f:\mathbb{Z}\longrightarrow G$, $k\longmapsto a^k$, ist wegen $a^{k+l}=a^ka^l$ für $k,l\in\mathbb{Z}$ ein Homomorphismus und nach Bemerkung 5.6 bijektiv.
(ii) $f:\mathbb{Z}\longrightarrow G$, $k\longmapsto a^k$, ist wieder ein Homomorphismus und surjektiv. Aus dem Homomorphiesatz folgt: $\mathbb{Z}/\mathrm{Ker}(f)\cong \mathrm{Bld}(f)=G$. Dabei gilt nach Satz 5.6:

$$\mathrm{Ker}(f)=\{k\in\mathbb{Z}:a^k=1\}=\{k\in\mathbb{Z}:n\mid k\}=n\mathbb{Z}.$$

6.6 Satz. *Jede Untergruppe einer zyklischen Gruppe ist wieder zyklisch. Genauer gilt:*
(i) *Jede unendliche zyklische Gruppe $G=\langle a\rangle$ hat für $d\in\mathbb{N}$ genau eine Untergruppe vom Index d, nämlich $\langle a^d\rangle$. Zusammen mit der trivialen Untergruppe $\{1\}$ erhält man so alle Untergruppen von G.*
(ii) *Jede zyklische Gruppe $G=\langle a\rangle$ der Ordnung $n<\infty$ hat für jeden (positiven) Teiler d von n genau eine Untergruppe vom Index d, nämlich $\langle a^d\rangle$. So erhält man alle Untergruppen von G.*

Beweis. (i) Sei $G=\langle a\rangle$ unendlich. Für $d\in\mathbb{N}$ ist $U:=\langle a^d\rangle\leq G$ und $f:\mathbb{Z}\longrightarrow G\longrightarrow G/U$, $k\longmapsto a^k\longmapsto a^kU$, ein Epimorphismus. Dabei gilt:

$$k\in\mathrm{Ker}(f)\Longleftrightarrow a^kU=1\Longleftrightarrow a^k\in U=\langle a^d\rangle=\{a^{dn}:n\in\mathbb{Z}\}\Longleftrightarrow k\in d\mathbb{Z}.$$

Dies zeigt: $\mathrm{Ker}(f)=d\mathbb{Z}$. Aus dem Homomorphiesatz folgt: $\mathbb{Z}/d\mathbb{Z}\cong\mathrm{Bld}(f)=G/U$. Insbesondere ist $|G:U|=|G/U|=|\mathbb{Z}/d\mathbb{Z}|=d$.
Dies zeigt: Für $d\in\mathbb{N}$ ist $\langle a^d\rangle$ eine Untergruppe von G vom Index d.
Sei jetzt $1\neq U\leq G$ und $1\neq u\in U$. Wir schreiben $u=a^m$ mit $0\neq m\in\mathbb{Z}$. Wegen $1\neq u^{-1}=a^{-m}\in U$ ist $M:=\{k\in\mathbb{N}:a^k\in U\}\neq\emptyset$. Sei $d:=\min(M)$. Dann ist $a^d\in U$, d.h. $\langle a^d\rangle\subseteq U$.
Sei umgekehrt $a^k\in U$ mit $k\in\mathbb{Z}$. Division mit Rest liefert $q,r\in\mathbb{Z}$ mit $k=qd+r$ und $0\leq r<d$. Dann ist $a^r=a^{k-qd}=a^k(a^d)^{-q}\in U$, d.h. $r=0$ nach Wahl von d. Also ist $a^k=(a^d)^q\in\langle a^d\rangle$. Dies zeigt: $U=\langle a^d\rangle$.
(ii) Sei $G=\langle a\rangle$ und $|G|=n<\infty$. Für $d\in\mathbb{N}$ mit $d\mid n$ ist $U:=\langle a^d\rangle\leq G$, und $|U|=\frac{n}{d}$ nach Satz 5.6. Aus dem Satz von Lagrange folgt: $|G:U|=d$.
Dies zeigt: Für $d\in\mathbb{N}$ mit $d\mid n$ ist $\langle a^d\rangle\leq G$ und $|G:\langle a^d\rangle|=d$.
Sei umgekehrt $U\leq G$ beliebig. Nach dem Satz von Lagrange ist $d:=|G:U| \,\big|\, |G|=n$. Daher folgt aus Satz 5.6: $a^dU=(aU)^d=(aU)^{|G/U|}=1$ in G/U, d.h. $a^d\in U$ und damit $\langle a^d\rangle\subseteq U$. Wegen

$$d=|G:\langle a^d\rangle|=\frac{|G|}{|\langle a^d\rangle|}\geq\frac{|G|}{|U|}=|G:U|=d$$

folgt $|\langle a^d\rangle|=|U|$, d.h. $U=\langle a^d\rangle$.

7. RINGE

7.1 Definition. Ein **Ring** ist ein Tripel $(R, +, \cdot)$, das aus einer Menge R und Verknüpfungen $+, \cdot$ auf R mit folgenden Eigenschaften besteht:
(i) $(R, +)$ ist eine abelsche Gruppe;
(ii) $a, b, c \in R \Longrightarrow (ab)c = a(bc)$;
(iii) $a, b, c \in R \Longrightarrow a(b + c) = ab + ac \wedge (a + b)c = ac + bc$;
(iv) Es gibt ein Element $1 \in R$ (**Einselement**) mit $1a = a = a1$ für alle $a \in R$.

Bemerkung. (i) Wie bei Gruppen zeigt man, dass 1 in (iv) eindeutig bestimmt ist. Man schreibt: $1 = 1_R$.
(ii) Analog enthält R genau ein Element 0 (**Nullelement**) mit $a + 0 = a$ für alle $a \in R$. Man schreibt: $0 = 0_R$.
(iii) Ferner existiert zu jedem $a \in R$ genau ein Element $-a \in R$ (**negatives Element**) mit $a+(-a) = 0$. Dabei gilt: $-(-a) = a$ und $0a = 0 = a0$ [wegen $0a+0a = (0+0)a = 0a$] und $a(-b) = (-a)b = -(ab)$ [wegen $ab+a(-b) = a(b+(-b)) = a0 = 0$ und $(-a)b+ab = \ldots = 0$]. Statt $a + (-b)$ schreibt man $a - b$.
(iv) Ein Ring $R = (R, +, \cdot)$ mit $ab = ba$ für alle $a, b \in R$ heißt **kommutativ**.
(v) Ein kommutativer Ring R mit $|R| \geq 2$ heißt **Integritätsbereich**, falls für alle $a, b \in R$ gilt: $ab = 0 \Longrightarrow a = 0 \vee b = 0$.
(vi) Ein kommutativer Ring K mit $|K| \geq 2$ heißt **Körper**, falls zu jedem $a \in K \setminus \{0\}$ ein $a' \in K$ mit $aa' = 1$ existiert. Ggf. ist a' durch a eindeutig bestimmt, und $a' \neq 0$. Man nennt a' **invers** zu a und schreibt: $a' =: a^{-1}$.
Jeder Körper ist ein Integritätsbereich; denn aus $ab = 0$ und $a \neq 0$ folgt $b = 1b = a^{-1}ab = a^{-1}0 = 0$. Ferner ist $(K \setminus \{0\}, \cdot)$ eine Gruppe, die **multiplikative Gruppe** von K.
Beachte: $1 \neq 0$; denn sonst wäre $a = a1 = a0 = 0$ für $a \in K$, d.h. $|K| = 1$.
(vii) Wir verwenden die Konvention: *Punktrechnung vor Strichrechnung.*

Beispiel. (a) $(\mathbb{Z}, +, \cdot)$ ist ein Integritätsbereich; $(\mathbb{Q}, +, \cdot)$ und $(\mathbb{R}, +, \cdot)$ sind Körper, $(\mathbb{N}, +, \cdot)$ und $(\mathbb{N}_0, +, \cdot)$ sind keine Ringe.
(b) Für $n \in \mathbb{N}$ und jeden Körper K ist die Menge $K^{n\times n}$ aller $n \times n$-Matrizen mit Koeffizienten in K ein Ring mit der üblichen Addition und Multiplikation von Matrizen. Für $n \geq 2$ ist $K^{n\times n}$ nicht kommutativ.
(c) $\{0\}$ ist ein kommutativer Ring, aber kein Integritätsbereich.

7.2 Definition. Ein Element a eines Rings R heißt **invertierbar** oder **Einheit**, falls ein $a' \in R$ mit $aa' = 1 = a'a$ existiert.

Bemerkung. Stets ist $R^\times := \{a \in R : a \text{ Einheit}\}$ eine Gruppe bzgl. $\cdot$; man nennt $R^\times$ die **Einheitengruppe** von R.

Beispiel. (i) Für $n \in \mathbb{N}$ und jeden Körper K ist $(K^{n\times n})^\times = \mathrm{GL}(n, K)$; insbesondere ist $K^\times = K \setminus \{0\}$.
(ii) $\mathbb{Z}^\times = \{1, -1\}$.

7.3 Definition. Eine Teilmenge S eines Rings R mit $1_R \in S$ und $a - b, ab \in S$ für alle $a, b \in S$ heißt **Teilring** von R.

Bemerkung. Ggf. ist auch $0_R = 1_R - 1_R \in S$. Daher gilt: $(S,+) \leq (R,+)$. Ferner ist S mit den entsprechend eingeschränkten Verknüpfungen ein Ring. Dabei ist $0_S = 0_R$ und $1_S = 1_R$.

Beispiel. (a) Wir haben Teilringe $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$.
(b) Für $n \in \mathbb{N}$ und jeden Körper K bilden die oberen Dreiecksmatrizen [bzw. die Diagonalmatrizen] einen Teilring von $K^{n\times n}$.

7.4 Definition. Sei R ein Ring. Eine Untergruppe $(I,+) \leq (R,+)$ mit $ax, xa \in I$ für alle $a \in R$, $x \in I$ heißt **Ideal** von R. Man schreibt: $I \trianglelefteq R$.

Beispiel. (a) In jedem Ring R sind $\{0\}$ und R Ideale.
(b) Für Ideale I, J in einem Ring R sind auch $I \cap J$ und $I + J := \{x + y : x \in I,\ y \in J\}$ Ideale.
(c) Sei R ein kommutativer Ring und $a \in R$. Dann ist $(a) := Ra := \{ra : r \in R\}$ ein Ideal in R, das man das von a **erzeugte Hauptideal** in R nennt.
(d) Insbesondere ist $(n) = \mathbb{Z}n = n\mathbb{Z}$ für $n \in \mathbb{N}_0$ ein Ideal in $\mathbb{Z}$. Nach Satz 6.6 hat jedes Ideal (sogar jede Untergruppe) von $\mathbb{Z}$ diese Form.

Satz. *Für jedes Ideal I in einem Ring R wird die Faktorgruppe $R/I = \{a + I : a \in R\}$ zu einem Ring mit Einselement $1 + I$, wenn man definiert:*

$$(a + I)(b + I) := ab + I \qquad (a, b \in R).$$

Beweis. Wir zeigen zunächst, dass die Multiplikation in R/I wohldefiniert ist. Dazu seien $a, a', b, b' \in R$ mit $a + I = a' + I$ und $b + I = b' + I$, d.h. $a - a', b - b' \in I$. Dann ist $ab - a'b' = (a - a')b + a'(b - b') \in I$, d.h. $ab + I = a'b' + I$. Damit ist $\cdot$ wohldefiniert. Wie früher gezeigt, ist $(R/I,+)$ eine abelsche Gruppe. Für $a, b, c \in R$ gilt ferner:

$$\begin{aligned}((a + I)(b + I))(c + I) &= (ab + I)(c + I) = (ab)c + I = a(bc) + I = (a + I)(bc + I)\\ &= (a + I)((b + I)(c + I)),\end{aligned}$$

$$\begin{aligned}((a + I) + (b + I))(c + I) &= (a + b + I)(c + I) = (a + b)c + I = ac + bc + I\\ &= (ac + I) + (bc + I) = (a + I)(c + I) + (b + I)(c + I),\end{aligned}$$

$$(a + I)((b + I) + (c + I)) = \ldots = (a + I)(b + I) + (a + I)(c + I),$$

$$(1 + I)(a + I) = 1a + I = a + I,$$

$$(a + I)(1 + I) = \ldots = a + I.$$

7.5 Definition. Für jedes Ideal I in einem Ring R heißt der Ring R/I aus Satz 7.4 **Restklassenring** modulo I. Seine Elemente heißen **Restklassen** modulo I. Statt $a + I = b + I$ schreibt man auch $a \equiv b \pmod{I}$.

Beispiel. Für $n \in \mathbb{N}$ ist $I := (n) = n\mathbb{Z}$ ein Ideal in $\mathbb{Z}$. Für $a, b \in \mathbb{Z}$ gilt dabei:

$$a \equiv b \pmod{n\mathbb{Z}} \iff a + n\mathbb{Z} = b + n\mathbb{Z} \iff a - b \in n\mathbb{Z} \iff a \equiv b \pmod{n}.$$

Satz. $(\mathbb{Z}/n\mathbb{Z})^\times = \{a + n\mathbb{Z} : a \in \mathbb{Z},\ \mathrm{ggT}(a,n) = 1\}$ *für* $n \in \mathbb{N}$.

Beweis. Für $a \in \mathbb{Z}$ gilt: $a + n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times \iff \exists b \in \mathbb{Z} : (a + n\mathbb{Z})(b + n\mathbb{Z}) = 1 + n\mathbb{Z} \iff \exists b \in \mathbb{Z} : ab \equiv 1 \pmod{n} \iff \mathrm{ggT}(a,n) = 1$. (Vgl. Satz 4.4).

Bemerkung. $\mathbb{Z}/n\mathbb{Z}$ heißt **Restklassenring** und $(\mathbb{Z}/n\mathbb{Z})^\times$ **prime Restklassengruppe** modulo n. Die Elemente in $(\mathbb{Z}/n\mathbb{Z})^\times$ heißen **prime Restklassen** modulo n. Zum Beispiel ist $(\mathbb{Z}/6\mathbb{Z})^\times = \{1 + 6\mathbb{Z}, 5 + 6\mathbb{Z}\}$.

7.6 Definition. Die **Euler-Funktion** $\varphi : \mathbb{N} \longrightarrow \mathbb{C}$ wird definiert durch

$$\begin{aligned}\varphi(n) &:= |(\mathbb{Z}/n\mathbb{Z})^\times| = |\{a + n\mathbb{Z} : a \in \mathbb{Z},\ \mathrm{ggT}(a,n) = 1\}| \\ &= |\{a \in \mathbb{N} : 1 \le a \le n,\ \mathrm{ggT}(a,n) = 1\}|\end{aligned}$$

für $n \in \mathbb{N}$.

Satz. *Für* $n \in \mathbb{N}$ *mit Primfaktorzerlegung* $n = p_1^{a_1} \dots p_r^{a_r}$ *gilt:*

$$\varphi(n) = (p_1^{a_1} - p_1^{a_1 - 1}) \dots (p_r^{a_r} - p_r^{a_r - 1}) = n(1 - \frac{1}{p_1}) \dots (1 - \frac{1}{p_r}).$$

Beispiel. $\varphi(1000) = \varphi(2^3 5^3) = (2^3 - 2^2)(5^3 - 5^2) = 4 \cdot 100 = 400$.

Beweis. Die Abbildung

$$f : (\mathbb{Z}/n\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/p_1^{a_1}\mathbb{Z})^\times \times \dots \times (\mathbb{Z}/p_r^{a_r}\mathbb{Z})^\times, \quad b + n\mathbb{Z} \longmapsto (b + p_1^{a_1}\mathbb{Z}, \dots, b + p_r^{a_r}\mathbb{Z}),$$

ist wohldefiniert; denn aus $\mathrm{ggT}(b,n) = 1$ folgt $\mathrm{ggT}(b, p_i^{a_i}) = 1$ für $i = 1, \dots, r$, und aus $b + n\mathbb{Z} = b' + n\mathbb{Z}$, d.h. $b \equiv b' \pmod{n}$, folgt $b \equiv b' \pmod{p_i^{a_i}}$, d.h. $b + p_i^{a_i}\mathbb{Z} = b' + p_i^{a_i}\mathbb{Z}$ für $i = 1, \dots, r$.
f ist injektiv; denn sind $b, c \in \mathbb{Z}$ mit $b + p_i^{a_i}\mathbb{Z} = c + p_i^{a_i}\mathbb{Z}$, d.h. $b \equiv c \pmod{p_i^{a_i}}$ für $i = 1, \dots, r$, so ist $b \equiv c \pmod{n}$, d.h. $b + n\mathbb{Z} = c + n\mathbb{Z}$.
f ist surjektiv; denn ist $c_i + p_i^{a_i}\mathbb{Z} \in (\mathbb{Z}/p_i^{a_i}\mathbb{Z})^\times$ für $i = 1, \dots, r$, so existiert nach dem Chinesischen Restsatz ein $c \in \mathbb{Z}$ mit $c \equiv c_i \pmod{p_i^{a_i}}$ für $i = 1, \dots, r$. Dabei ist $p_i \nmid c_i$, also auch $p_i \nmid c$ für $i = 1, \dots, r$. Daher ist $\mathrm{ggT}(n,c) = 1$, d.h. $c + n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times$ und $f(c + n\mathbb{Z}) = (c_1 + p_1^{a_1}\mathbb{Z}, \dots, c_r + p_r^{a_r}\mathbb{Z})$.
Dies zeigt: f ist bijektiv; insbesondere ist $\varphi(n) = \varphi(p_1^{a_1}) \dots \varphi(p_r^{a_r})$. Daher genügt zu zeigen, dass für $p \in \mathbb{P}$ und $k \in \mathbb{N}$ gilt: $\varphi(p^k) = p^k - p^{k-1}$. Dies gilt; denn von den Zahlen $1, \dots, p^k$ sind genau die Zahlen px mit $x \in \{1, \dots, p^{k-1}\}$ durch p teilbar.

7.7 Satz. (EULER-FERMAT)
Für $a \in \mathbb{Z}$ *und* $n \in \mathbb{N}$ *mit* $\mathrm{ggT}(a,n) = 1$ *ist* $a^{\varphi(n)} \equiv 1 \pmod{n}$. *Insbesondere gilt für* $a \in \mathbb{Z}$ *und* $p \in \mathbb{P}$ *mit* $p \nmid a$: $a^{p-1} \equiv 1 \pmod{p}$.

Beweis. $G := (\mathbb{Z}/n\mathbb{Z})^\times$ ist eine Gruppe der Ordnung $\varphi(n)$. Nach Satz 5.6 (i) gilt für $a + n\mathbb{Z} \in G$: $1 + n\mathbb{Z} = (a + n\mathbb{Z})^{\varphi(n)} = a^{\varphi(n)} + n\mathbb{Z}$, d.h. $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Bemerkung. Für $a \in \mathbb{Z}$ und $p \in \mathbb{P}$ ist also $a^p \equiv a \pmod{p}$.

7.8 Satz. *Für jede zyklische Gruppe G der Ordnung $n < \infty$ ist*

$$\varphi(n) = |\{a \in G : \langle a \rangle = G\}|,$$

d.h. $\varphi(n)$ ist die Anzahl der **Erzeuger** *von G.*

Beweis. Wir schreiben $G = \langle a \rangle = \{1, a, a^2, \ldots, a^{n-1}\} = \{a, a^2, \ldots, a^n\}$. Für $k = 1, \ldots, n$ hat a^k nach Satz 5.6 die Ordnung $\frac{n}{\mathrm{ggT}(k,n)}$. Dies ist gleich n genau dann, wenn $\mathrm{ggT}(k, n) = 1$ ist. Daher gilt: $\langle a^k \rangle = G \iff \mathrm{ggT}(k, n) = 1$.

7.9 Satz. *Für $n \in \mathbb{N}$ ist $\sum_{d|n} \varphi(d) = n$; dabei durchläuft die Summe alle (positiven) Teiler d von n.*

Beispiel. Für $n = 6$ ist $\varphi(1) + \varphi(2) + \varphi(3) + \varphi(6) = 1 + 1 + 2 + 2 = 6$.

Beweis. Es sei G eine zyklische Gruppe der Ordnung n (z.B. $G = \mathbb{Z}/n\mathbb{Z}$). Wir bestimmen die Anzahl der Elemente in

$$M := \{(g, U) : g \in G, U \leq G, U = \langle g \rangle\}$$

auf zwei Arten. Einerseits liefert jedes Element $g \in G$ genau ein Paar $(g, U) \in M$, nämlich $(g, U) := (g, \langle g \rangle)$. Daher ist $|M| = |G| = n$. Andererseits existiert zu jedem (positiven) Teiler d von $n = |G|$ nach Satz 6.6 genau eine Untergruppe U von G der Ordnung d; diese ist zyklisch und hat nach Satz 7.8 $\varphi(d)$ Erzeuger. Ferner erhält man so alle Untergruppen von G. Daher ist $|M| = \sum_{d|n} \varphi(d)$.

8. DAS RSA-VERFAHREN IN DER KRYPTOGRAPHIE

In diesem Kapitel gehen wir kurz auf eine moderne Anwendung der Zahlentheorie ein, das RSA-Verfahren in der Kryptographie. Dabei steht RSA für **R**IVEST, **S**HAMIR und **A**DLEMAN, drei Pioniere in der sogenannten Public-Key-Cryptography.

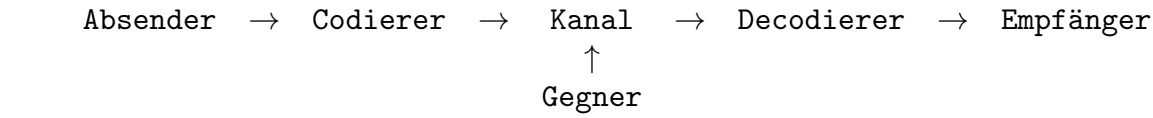
Ausgangspunkt des RSA-Verfahrens ist das folgende Problem. Personen $A, B, C, \ldots$ wollen miteinander über einen unsicheren Kanal kommunizieren. Dazu soll jede Nachricht so verschlüsselt werden, dass nur der richtige Empfänger sie entschlüsseln kann. Wie geht das?

Am Anfang wählt jeder Teilnehmer T zwei große verschiedene Primzahlen p_T, q_T (je ca. 100 Dezimalstellen) und eine große natürliche Zahl r_T, die zu $\varphi(p_T q_T) = (p_T - 1)(q_T - 1)$ teilerfremd ist. Mit dem erweiterten euklidischen Algorithmus berechnet er dann ein $s_T \in \mathbb{N}$ mit

$$r_T s_T \equiv 1 \pmod{\varphi(p_T q_T)}.$$

Die Zahlen p_T, q_T, s_T hält er geheim, die Zahlen $n_T := p_T q_T$ und r_T kommen in ein allgemein zugängliches "Telefonbuch". Der "Schlüssel" von T besteht also aus zwei Teilen, einem geheimen (p_T, q_T, s_T) und einem offenen (n_T, r_T).

Wir nehmen jetzt an, dass Teilnehmer A an Teilnehmer B eine Nachricht m schicken möchte. Dabei können wir annehmen, dass $m \in \mathbb{N}$ und $m < n_B$ ist. Dann geht Teilnehmer A folgendermaßen vor: Er berechnet zunächst das eindeutig bestimmte $m' \in \mathbb{N}$ mit $m' \equiv m^{r_B} \pmod{n_B}$ und $m' < n_B$. Das geht, weil n_B und r_B öffentlich bekannt sind. Obwohl r_B groß ist, lässt sich m' relativ schnell berechnen. Dann schickt Teilnehmer A die verschlüsselte Nachricht m' an B.



Wegen $r_B s_B \equiv 1 \pmod{(p_B-1)(q_B-1)}$ existiert ein $t_B \in \mathbb{N}$ mit

$$r_B s_B = 1 + t_B(p_B-1)(q_B-1).$$

Daher gilt:

$$(m')^{s_B} \equiv (m^{r_B})^{s_B} = m^{1+t_B(p_B-1)(q_B-1)} = m(m^{p_B-1})^{t_B(q_B-1)} \equiv m \pmod{p_B};$$

denn im Fall $p_B \nmid m$ folgt $m^{p_B-1} \equiv 1 \pmod{p_B}$ aus dem Satz von Euler-Fermat, und im Fall $p_B \mid m$ ist dies trivial.
Analog ist $(m')^{s_B} \equiv m \pmod{q_B}$. Insgesamt ist also $(m')^{s_B} \equiv m \pmod{p_B q_B}$. Teilnehmer B kann also die Nachricht m' entschlüsseln, indem er $(m')^{s_B}$ berechnet.

Wir nehmen jetzt an, dass ein "Gegner" die verschlüsselte Nachricht m' abhört. Kann er sie entschlüsseln?

Theoretisch ja: Schließlich muss er "nur" das öffentlich zugängliche n_B in Primfaktoren zerlegen. Dann kennt er p_B und q_B, kann also s_B mit dem erweiterten euklidischen Algorithmus berechnen und dann m' genauso wie B entschlüsseln.

Praktisch nein: Denn man kennt kein Verfahren, das "große" natürliche Zahlen "schnell" in Primfaktoren zerlegt. Auch kennt man keine anderen schnellen Methoden zur Entschlüsselung von m'. Daher ist das RSA-Verfahren in der Praxis gut etabliert. (Vgl. z.B. `www.rsa.com`).

9. ZAHLENTHEORETISCHE FUNKTIONEN

9.1 Definition. Eine **zahlentheoretische Funktion** ist eine Abbildung $\alpha : \mathbb{N} \longrightarrow \mathbb{C}$. Die Menge aller zahlentheoretischen Funktionen bezeichnen wir mit $\mathcal{Z}$. Für $\alpha, \beta \in \mathcal{Z}$ definiert man die Summe $\alpha + \beta \in \mathcal{Z}$ durch $(\alpha+\beta)(n) := \alpha(n) + \beta(n)$ für $n \in \mathbb{N}$.

Bemerkung. Man sieht sofort, dass $(\mathcal{Z}, +)$ eine abelsche Gruppe ist; neutrales Element ist die Nullfunktion $0 : \mathbb{N} \longrightarrow \mathbb{C}$, $n \longmapsto 0$. Invers zu $\alpha \in \mathcal{Z}$ ist $-\alpha : \mathbb{N} \longrightarrow \mathbb{C}$, $n \longmapsto -\alpha(n)$.

Beispiel. (i) Die Euler-Funktion φ.
(ii) Die **Möbius-Funktion** μ (MÖBIUS, 1790-1868); für $n \in \mathbb{N}$ mit Primfaktorzerlegung $n = p_1^{a_1} \dots p_r^{a_r}$ ist dabei $\mu(n) = (-1)^r$, falls $a_1 = \dots = a_r = 1$, und $\mu(n) := 0$ sonst. Insbesondere ist $\mu(1) = 1$.

(iii) $\nu_k : \mathbb{N} \longrightarrow \mathbb{C}$, $n \longmapsto n^k$, $(k \in \mathbb{N}_0)$; insbesondere $\iota := \nu_0 : \mathbb{N} \longrightarrow \mathbb{C}$, $n \longmapsto 1$, und $\nu := \nu_1 : \mathbb{N} \longrightarrow \mathbb{C}$, $n \longmapsto n$.

9.2 Definition. Für $\alpha, \beta \in \mathcal{Z}$ definiert man das **Dirichlet-Produkt** (DIRICHLET, 1805-1859) $\alpha * \beta \in \mathcal{Z}$ durch

$$(\alpha * \beta)(n) := \sum_{d|n} \alpha(d)\beta(\frac{n}{d}) = \sum_{xy=n} \alpha(x)\beta(y) \qquad (n \in \mathbb{N}).$$

Satz. *$(\mathcal{Z}, +, *)$ ist ein Integritätsbereich mit Einselement ε; dabei ist ε definiert durch $\varepsilon(1) := 1$ und $\varepsilon(n) := 0$ für $n \neq 1$.*

Beweis. Für $\alpha, \beta, \gamma \in \mathcal{Z}$ und $n \in \mathbb{N}$ gilt:

$$(\beta * \alpha)(n) = \sum_{xy=n} \beta(x)\alpha(y) = \sum_{yx=n} \alpha(y)\beta(x) = (\alpha * \beta)(n),$$

$$\begin{aligned}((\alpha * \beta) * \gamma)(n) &= \sum_{xy=n} (\alpha * \beta)(x) \cdot \gamma(y) = \sum_{xy=n} \sum_{uv=x} \alpha(u)\beta(v)\gamma(y) \\ &= \sum_{uvy=n} \alpha(u)\beta(v)\gamma(y) = \sum_{uz=n} \sum_{vy=z} \alpha(u)\beta(v)\gamma(y) \\ &= \sum_{uz=n} \alpha(u) \cdot (\beta * \gamma)(z) = (\alpha * (\beta * \gamma))(n)\end{aligned}$$

und

$$(\alpha * \varepsilon)(n) = \sum_{xy=n} \alpha(x)\varepsilon(y) = \alpha(n)\varepsilon(1) = \alpha(n).$$

Die Distributivgesetze sind offensichtlich. Seien schließlich $\alpha, \beta \in \mathcal{Z}\backslash\{0\}$, und seien $r, s \in \mathbb{N}$ minimal mit $\alpha(r) \neq 0 \neq \beta(s)$. Dann ist $(\alpha * \beta)(rs) = \sum_{xy=rs} \alpha(x)\beta(y) = \alpha(r)\beta(s) \neq 0$, d.h. $\alpha * \beta \neq 0$.

Beispiel. Nach Satz 7.9 ist $(\varphi * \iota)(n) = \sum_{d|n} \varphi(d)1 = n = \nu(n)$ für $n \in \mathbb{N}$. Daher ist

$$\varphi * \iota = \nu.$$

9.3 Satz. $\mathcal{Z}^\times = \{\alpha \in \mathcal{Z} : \alpha(1) \neq 0\}$.

Beweis. Für $\alpha, \beta \in \mathcal{Z}$ gilt:

$$\alpha * \beta = \varepsilon \Longleftrightarrow \alpha(1)\beta(1) = 1 \wedge \alpha(1)\beta(n) + \sum_{xy=n, y<n} \alpha(x)\beta(y) = 0 \text{ für } 1 \neq n \in \mathbb{N}.$$

Daraus folgt unmittelbar die Behauptung.

Bemerkung. Die Einheitengruppe $\mathcal{Z}^\times$ von $\mathcal{Z}$ ist also eine abelsche Gruppe bzgl. $*$. Für $\alpha \in \mathcal{Z}^\times$ bezeichnen wir das Inverse von α in $\mathcal{Z}^\times$ mit α^{-1}. [Dies ist nicht zu verwechseln mit der Umkehrabbildung; diese existiert hier nicht. (Warum?)]

9.4 Definition. Ein Element $\alpha \in \mathcal{Z} \setminus \{0\}$ heißt **multiplikativ**, falls $\alpha(mn) = \alpha(m)\alpha(n)$ für alle $m, n \in \mathbb{N}$ mit $\mathrm{ggT}(m, n) = 1$ gilt. Ist sogar $\alpha(mn) = \alpha(m)\alpha(n)$ für alle $m, n \in \mathbb{N}$, so heißt α **vollständig multiplikativ**.

Bemerkung. Sei $\alpha \in \mathcal{Z}$ multiplikativ. Dann existiert ein $m \in \mathbb{N}$ mit $0 \neq \alpha(m) = \alpha(1m) = \alpha(1)\alpha(m)$. Daher ist $\alpha(1) = 1 \neq 0$; insbesondere ist $\alpha \in \mathcal{Z}^\times$ nach Satz 9.3.
Für $n \in \mathbb{N}$ mit Primfaktorzerlegung $n = p_1^{a_1} \dots p_r^{a_r}$ gilt ferner:

$$\alpha(n) = \alpha(p_1^{a_1}) \dots \alpha(p_r^{a_r}).$$

Daher ist α durch seine Werte auf Primzahlpotenzen eindeutig festgelegt.

Satz. $\mathcal{M} := \{\alpha \in \mathcal{Z} : \alpha \text{ multiplikativ}\} \leq \mathcal{Z}^\times$.

Beweis. Nach Bemerkung 9.4 ist $\emptyset \neq \mathcal{M} \subseteq \mathcal{Z}^\times$. Für $\alpha, \beta \in \mathcal{M}$ und $m, n \in \mathbb{N}$ mit $\mathrm{ggT}(m, n) = 1$ gilt:

$$(\alpha * \beta)(mn) = \sum_{xy=mn} \alpha(x)\beta(y) = \sum_{x_1y_1=m, x_2y_2=n} \alpha(x_1x_2)\beta(y_1y_2);$$

denn jeder Teiler von mn lässt sich eindeutig in der Form $x = x_1x_2$ mit $x_1 \mid m$ und $x_2 \mid n$ schreiben. (Analog für y.) Daher gilt:

$$\begin{aligned}(\alpha * \beta)(mn) &= \sum_{x_1y_1=m, x_2y_2=n} \alpha(x_1)\alpha(x_2)\beta(y_1)\beta(y_2) \\ &= \sum_{x_1y_1=m} \alpha(x_1)\beta(y_1) \sum_{x_2y_2=n} \alpha(x_2)\beta(y_2) = (\alpha * \beta)(m) \cdot (\alpha * \beta)(n).\end{aligned}$$

Also ist $\alpha * \beta \in \mathcal{M}$. Wegen $\alpha(1) = 1$ existiert ferner genau ein $\gamma \in \mathcal{M}$ mit

$$0 = (\alpha * \gamma)(p^r) = \sum_{i=0}^{r} \alpha(p^i)\gamma(p^{r-i}) = \gamma(p^r) + \sum_{i=1}^{r} \alpha(p^i)\gamma(p^{r-i})$$

für alle $p \in \mathbb{P}$, $r \in \mathbb{N}$. Dann ist $(\alpha * \gamma)(p^r) = \varepsilon(p^r)$ für $p \in \mathbb{P}$, $r \in \mathbb{N}$. Wegen $\alpha * \gamma \in \mathcal{M}$ folgt: $\alpha * \gamma = \varepsilon$. Also ist $\alpha^{-1} = \gamma \in \mathcal{M}$.

Beispiel. (i) Wegen $\mu, \iota \in \mathcal{M}$ ist auch $\mu * \iota \in \mathcal{M}$, und für $p \in \mathbb{P}$, $r \in \mathbb{N}$ gilt:

$$(\mu * \iota)(p^r) = \sum_{i=0}^{r} \mu(p^i)1 = \mu(p) + \mu(1) = -1 + 1 = 0 = \varepsilon(p^r).$$

Daher ist $(\mu * \iota)(n) = \varepsilon(n)$ für $n \in \mathbb{N}$. Folglich gilt:

$$\mu = \iota^{-1}.$$

(ii) Für $k \in \mathbb{N}_0$ ist $\nu_k \in \mathcal{M}$, also auch $\sigma_k := \nu_k * \iota \in \mathcal{M}$; man nennt σ_k die k-te **Teilerfunktion**. Für $n \in \mathbb{N}$ ist

$$\sigma_k(n) = \sum_{d|n} \nu_k(d)1 = \sum_{d|n} d^k;$$

insbesondere gilt für $p \in \mathbb{P}$ und $r \in \mathbb{N}$:

$$\sigma_k(p^r) = \sum_{i=0}^{r} (p^i)^k = \sum_{i=0}^{r} (p^k)^i = \begin{cases} \frac{p^{k(r+1)}-1}{p^k-1}, & \text{falls } k \neq 0; \\ r+1, & \text{falls } k = 0. \end{cases}$$

Für $n \in \mathbb{N}$ ist $\sigma(n) := \sigma_1(n)$ die *Summe* aller Teiler von n, und $\tau(n) := \sigma_0(n)$ ist die *Anzahl* aller Teiler von n.
(iii) $\varphi \in \mathcal{M}$.

9.5 Bemerkung. (Möbius-Inversion)
Für $\gamma \in \mathcal{Z}$ heißt $\Gamma := \gamma * \iota$ **summatorische** Funktion von γ. Dann ist

$$\Gamma(n) = \sum_{d|n} \gamma(d)$$

für $n \in \mathbb{N}$. Ggf. ist $\gamma = \Gamma * \iota^{-1} = \Gamma * \mu$, d.h.

$$\gamma(n) = \sum_{d|n} \Gamma(d)\mu(\frac{n}{d}) = \sum_{d|n} \Gamma(\frac{n}{d})\mu(d) \qquad (n \in \mathbb{N}).$$

Satz. *Sei $\gamma \in \mathcal{Z}$ mit summatorischer Funktion Γ. Ist Γ multiplikativ, so auch γ, und für $p \in \mathbb{P}$, $r \in \mathbb{N}$ gilt: $\gamma(p^r) = \Gamma(p^r) - \Gamma(p^{r-1})$.*

Beweis. Aus $\Gamma, \mu \in \mathcal{M}$ folgt $\gamma = \Gamma * \mu \in \mathcal{M}$. Ferner gilt für $p \in \mathbb{P}$ und $r \in \mathbb{N}$:

$$\gamma(p^r) = \sum_{i=0}^{r} \Gamma(p^{r-i})\mu(p^i) = \sum_{i=0}^{1} \Gamma(p^{r-i})\mu(p^i) = \Gamma(p^r) - \Gamma(p^{r-1}).$$

Beispiel. Für $\gamma := \varphi$ ist $\Gamma := \nu$. Damit folgt aus dem Satz die schon bekannte Formel $\varphi(p^r) = p^r - p^{r-1}$ $(p \in \mathbb{P}, r \in \mathbb{N})$.

9.6 Bemerkung. Für vollständig multiplikative Funktionen $\alpha, \beta \in \mathcal{Z}$ ist $\alpha * \beta$ i.Allg. *nicht* vollständig multiplikativ; denn z.B. ist ι vollständig multiplikativ, aber $\iota * \iota = \tau$ nicht; denn $\tau(4) = 3$, aber $\tau(2)\tau(2) = 2 \cdot 2 = 4$.
I.Allg. ist auch α^{-1} *nicht* vollständig multiplikativ; denn z.B. gilt für $\iota^{-1} = \mu$: $\mu(4) = 0$, aber $\mu(2)\mu(2) = (-1)(-1) = 1$.

9.7 Bemerkung. Ein $n \in \mathbb{N}$ ist genau dann vollkommen, wenn $\sigma(n) = 2n$ gilt. Ein $n \in \mathbb{N}$ mit $\sigma(n) < 2n$ $[\sigma(n) > 2n]$ heißt **defizient** [bzw. **abundant**].

Satz. *Seien $p, q \in \mathbb{P}$ ungerade und verschieden. Für $r, s \in \mathbb{N}$ ist dann $n := p^r q^s$ defizient.*

Beweis. Dies folgt aus

$$\frac{\sigma(n)}{n} = \frac{\sigma(p^r)\sigma(q^s)}{p^r q^s} = \frac{p^{r+1}-1}{p^r(p-1)} \cdot \frac{q^{s+1}-1}{q^s(q-1)} < \frac{p}{p-1} \cdot \frac{q}{q-1} \leq \frac{3}{2} \cdot \frac{5}{4} = \frac{15}{8} < 2.$$

9.8 Satz. *Die Folge* $(\frac{\sigma(n)}{n})_{n\in\mathbb{N}}$ *ist nach oben unbeschränkt.*

Beweis. Für $n \in \mathbb{N}$ ist $\frac{\sigma(n)}{n} = \sum_{d|n} \frac{d}{n} = \sum_{d|n} \frac{1}{d}$. Wir setzen $n = m!$ für ein $m \in \mathbb{N}$. Dann gilt: $\frac{\sigma(n)}{n} \geq \sum_{k=1}^{m} \frac{1}{k}$. Die Behauptung folgt also wegen $\sum_{k=1}^{\infty} \frac{1}{k} = \infty$.

10. POLYNOME

Im Folgenden sei K ein Körper.

10.1 Definition. Ein **Polynom** mit Koeffizienten in K ist eine Folge $\alpha = (a_0, a_1, a_2, \ldots)$ von Elementen $a_i \in K$ mit $|\{i \in \mathbb{N}_0 : a_i \neq 0\}| < \infty$. [Diese Polynome bilden bekanntlich einen K-Vektorraum P mit

$$\alpha + \beta := (a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots),$$

$$r\alpha := (ra_0, ra_1, ra_2, \ldots)$$

für $\alpha = (a_0, a_1, a_2, \ldots), \beta = (b_0, b_1, b_2, \ldots) \in P$, $r \in K$.] Wir definieren eine Multiplikation auf P durch $\alpha\beta := (c_0, c_1, c_2, \ldots)$ mit

$$c_0 := a_0b_0, \quad c_1 := a_0b_1 + a_1b_0, \quad \ldots, \quad c_i := \sum_{j+k=i} a_jb_k, \quad \ldots$$

Satz. *So wird P zu einem kommutativen Ring mit Nullelement $(0, 0, 0, \ldots)$ und Einselement $(1, 0, 0, \ldots)$. Dabei gilt: $r(\alpha\beta) = (r\alpha)\beta = \alpha(r\beta)$ für $r \in K$, $\alpha, \beta \in P$.*

Beweis. Sind $\alpha, \beta \in P$ wie oben, so ist $\alpha\beta \in P$ wegen

$$\{i \in \mathbb{N}_0 : c_i \neq 0\} \subseteq \{j \in \mathbb{N}_0 : a_j \neq 0\} + \{k \in \mathbb{N}_0 : b_k \neq 0\}.$$

Wir zeigen nur die Assoziativität der Multiplikation; die übrigen Axiome beweist man analog. Dazu sei auch $\gamma = (c_0, c_1, c_2, \ldots) \in P$. Dann ist $\alpha\beta = (d_0, d_1, d_2, \ldots)$ mit $d_i = \sum_{j+k=i} a_jb_k$ für alle i, d.h. $(\alpha\beta)\gamma = (e_0, e_1, e_2, \ldots)$ mit

$$e_i = \sum_{j+k=i} d_jc_k = \sum_{j+k=i} \sum_{l+m=j} a_lb_mc_k = \sum_{l+m+k=i} a_lb_mc_k$$

für alle i. Analog ist $\alpha(\beta\gamma) = (f_0, f_1, f_2, \ldots)$ mit $f_i = \sum_{l+m+k=i} a_lb_mc_k$ für alle i. Also ist $(\alpha\beta)\gamma = \alpha(\beta\gamma)$.

Bemerkung. P heißt **Polynomring** über K und $(0, 0, 0, \ldots)$ **Nullpolynom**, $(1, 0, 0, \ldots)$ **Einspolynom**. Ferner heißt $X := (0, 1, 0, 0, \ldots)$ **Unbestimmte** oder **Variable** von P. Dann ist

$$X(a_0, a_1, a_2, \ldots) = (0, a_0, a_1, a_2, \ldots);$$

insbesondere ist $X^2 = (0, 0, 1, 0, 0, \ldots)$, $X^3 = (0, 0, 0, 1, 0, 0, \ldots)$, usw. Wegen $|\{i \in \mathbb{N}_0 : a_i \neq 0\}| < \infty$ ist also $(a_0, a_1, a_2, \ldots) = \sum_{i=0}^{\infty} a_iX^i$; dabei ist wie üblich X^0 das Einspolynom. Daher kann man jedes $\alpha \in P$ in der Form $\alpha = \sum_{i=0}^{\infty} a_iX^i$ mit eindeutig bestimmten

Koeffizienten $a_i \in K$ schreiben, von denen nur endlich viele von 0 verschieden sind. Dies werden wir in Zukunft stets tun. Für $\alpha = \sum_{i=0}^{\infty} a_i X^i, \beta = \sum_{i=0}^{\infty} b_i X^i \in P$ und $r \in K$ gilt dann:

- $\alpha = \beta \Longleftrightarrow a_i = b_i$ für alle i;
- $\alpha + \beta = \sum_{i=0}^{\infty}(a_i + b_i)X^i$;
- $r\alpha = \sum_{i=0}^{\infty}(ra_i)X^i$;
- $\alpha\beta = \sum_{i=0}^{\infty}(\sum_{j+k=i} a_j b_k)X^i$.

Statt P schreibt man meist $K[X]$. Für $0 \neq \alpha = \sum_{i=0}^{\infty} a_i X^i \in K[X]$ heißt

$$d := \deg(\alpha) := \max\{i \in \mathbb{N}_0 : a_i \neq 0\}$$

Grad von α. Dann ist also $\alpha = \sum_{i=1}^{d} a_i X^i$. Das Nullpolynom erhält den Grad $-\infty$.

10.2 Satz. *Für $\alpha, \beta \in K[X]$ und $0 \neq r \in K$ gilt:*
(i) $\deg(r\alpha) = \deg(\alpha)$*;*
(ii) $\deg(\alpha + \beta) \leq \max\{\deg(\alpha), \deg(\beta)\}$*;*
(iii) $\deg(\alpha) \neq \deg(\beta) \Longrightarrow \deg(\alpha + \beta) = \max\{\deg(\alpha), \deg(\beta)\}$*;*
(iv) $\deg(\alpha\beta) = \deg(\alpha) + \deg(\beta)$.

Beweis. Als Muster beweisen wir (iv); die übrigen Aussagen zeigt man analog. Wir schreiben $\alpha = \sum_{i=0}^{\infty} a_i X^i$, $\beta = \sum_{i=0}^{\infty} b_i X^i$, $\alpha\beta = \sum_{i=0}^{\infty} c_i X^i$ mit $a_i, b_i, c_i \in K$ für alle i und setzen $d := \deg(\alpha)$, $e := \deg(\beta)$; dabei sei o.B.d.A. $d \neq -\infty \neq e$. Für $i \in \mathbb{N}_0$ ist $c_i = \sum_{j+k=i} a_j b_k$. Wegen $a_j = 0$ für $j > d$ und $b_k = 0$ für $k > e$ gilt:

$$c_{d+e} = \sum_{j+k=d+e} a_j b_k = \sum_{j+k=d+e, j\leq d, k\leq e} a_j b_k = a_d b_e \neq 0,$$

und $c_i = 0$ für $i > d + e$. Also ist $\deg(\alpha\beta) = d + e = \deg(\alpha) + \deg(\beta)$.

Bemerkung. Für $r, s \in K$ gilt: $rX^0 \pm sX^0 = (r \pm s)X^0$ und $(rX^0)(sX^0) = (rs)X^0$. Daher kann man jeweils r mit rX^0 identifizieren und so K als Teilring von $K[X]$ auffassen. Die Elemente in K heißen dann auch **konstante** Polynome in $K[X]$.
Sei $0 \neq \alpha = \sum_{i=0}^{\infty} a_i X^i \in K[X]$ mit $d := \deg(\alpha)$ und $a_d = 1$. Dann heißt α **normiert**. Außerdem betrachtet man das Nullpolynom als normiert.
Wegen (iv) ist $K[X]$ ein Integritätsbereich.

10.3 Satz. (Division mit Rest)
Seien $\alpha, \beta \in K[X]$ mit $\beta \neq 0$. Dann existieren eindeutig bestimmte $\kappa, \rho \in K[X]$ mit $\alpha = \kappa\beta + \rho$ und $\deg(\rho) < \deg(\beta)$.

Beweis. *Eindeutigkeit:* Für $i = 1, 2$ sei $\alpha = \kappa_i\beta + \rho_i$ und $\deg(\rho_i) < \deg(\beta)$. Dann ist $\rho_2 - \rho_1 = (\kappa_1 - \kappa_2)\beta$. Im Fall $\kappa_1 \neq \kappa_2$ hätte man den Widerspruch

$$\deg(\beta) > \deg(\rho_2 - \rho_1) = \deg((\kappa_1 - \kappa_2)\beta) = \deg(\kappa_1 - \kappa_2) + \deg(\beta) \geq \deg(\beta).$$

Also ist $\kappa_1 = \kappa_2$ und damit $\rho_1 = \rho_2$.

Existenz: Im Fall $\deg(\alpha) < \deg(\beta)$ setzt man $\kappa := 0$ und $\rho := \alpha$. Sei also $m := \deg(\alpha) \geq \deg(\beta) =: n$. Wir schreiben $\alpha = \sum_{i=0}^{m} a_i X^i$, $\beta = \sum_{j=0}^{n} b_j X^j$ und setzen $\tilde{\alpha} := \alpha - \frac{a_m}{b_n} X^{m-n}\beta$. Dann ist $\deg(\tilde{\alpha}) < \deg(\alpha)$. Wir argumentieren jetzt mit Induktion nach m. Dann können wir voraussetzen, dass $\tilde{\kappa}, \tilde{\rho} \in K[X]$ mit $\tilde{\alpha} = \tilde{\kappa}\beta + \tilde{\rho}$ und $\deg(\tilde{\rho}) < n$ existieren. Dann ist

$$\alpha = \tilde{\alpha} + \frac{a_m}{b_n} X^{m-n}\beta = \kappa\beta + \rho$$

mit $\kappa := \tilde{\kappa} + \frac{a_m}{b_n} X^{m-n}$ und $\rho := \tilde{\rho}$, wie gewünscht.

Definition. Man nennt κ **Quotient** und ρ **Rest** bei der Division von α durch β. Im Fall $\rho = 0$ schreibt man auch $\kappa = \frac{\alpha}{\beta}$.

Beispiel. Für $\alpha = X^4 + X^3 + 1$ und $\beta = X^2 - X - 1$ erhält man leicht: $\kappa = X^2 + 2X + 3$ und $\rho = 5X + 4$.

10.4 Definition. Ein $\alpha \in K[X]$ heißt **Teiler** von $\beta \in K[X]$, falls $\beta = \alpha\gamma$ für ein $\gamma \in K[X]$ ist. Ggf. schreibt man $\alpha \mid \beta$.

Satz. *Für $\alpha, \beta, \gamma, \rho, \sigma \in K[X]$ gilt:*
(i) $\alpha \mid 0$, $1 \mid \alpha$, $\alpha \mid \alpha$;
(ii) $\alpha \mid \beta \wedge \beta \mid \gamma \Longrightarrow \alpha \mid \gamma$;
(iii) $\alpha \mid \beta \Longrightarrow a\alpha \mid b\beta$ *für* $a, b \in K^\times$;
(iv) $\alpha \mid \beta \wedge \beta \mid \alpha \Longrightarrow \exists c \in K^\times : \alpha = c\beta$;
(v) $0 \mid \alpha \Longleftrightarrow \alpha = 0$;
(vi) $\alpha \mid \beta \wedge \alpha \mid \gamma \Longrightarrow \alpha \mid \rho\beta + \sigma\gamma$.

Beweis. Als Muster beweisen wir (iv). [Der Rest geht ähnlich.] Sei also $\alpha \mid \beta$ und $\beta \mid \alpha$. Dann existieren $\gamma, \delta \in K[X]$ mit $\beta = \alpha\gamma$ und $\alpha = \beta\delta$. Daher ist $\alpha = \alpha\gamma\delta$, d.h. $\alpha(\gamma\delta - 1) = 0$. Im Fall $\alpha = 0$ ist $\beta = \alpha\gamma = 0$, d.h. $\alpha = 1\beta$. Sei also $\alpha \neq 0$. Da $K[X]$ ein Integritätsbereich ist, folgt $\gamma\delta - 1 = 0$, d.h. $\gamma\delta = 1$. Daher ist $0 = \deg(1) = \deg(\gamma) + \deg(\delta)$, d.h. $\deg(\gamma) = \deg(\delta) = 0$ und damit $\gamma, \delta \in K \setminus \{0\}$. Folglich ist $\alpha = c\beta$ mit $c := \delta \in K \setminus \{0\}$.

10.5 Definition. Ein $\tau \in K[X]$ mit $\tau \mid \alpha_1$, ..., $\tau \mid \alpha_n$ heißt **gemeinsamer Teiler** von $\alpha_1, \ldots, \alpha_n \in K[X]$. Die Menge aller gemeinsamen Teiler von $\alpha_1, \ldots, \alpha_n$ bezeichnen wir mit $\mathrm{gT}(\alpha_1, \ldots, \alpha_n)$. Ein normiertes $\delta \in \mathrm{gT}(\alpha_1, \ldots, \alpha_n)$ heißt **größter gemeinsamer Teiler** (ggT) von $\alpha_1, \ldots, \alpha_n$, falls $\tau \mid \delta$ für alle $\tau \in \mathrm{gT}(\alpha_1, \ldots, \alpha_n)$ gilt.

Bemerkung. Sind δ_1, δ_2 ggT's von $\alpha_1, \ldots, \alpha_n$, so gilt $\delta_1 \mid \delta_2 \mid \delta_1$. Nach Satz 10.4 existiert also ein $c \in K^\times$ mit $\delta_2 = c\delta_1$. Da δ_1, δ_2 normiert sind, folgt: $\delta_1 = \delta_2$. Das bedeutet: $\alpha_1, \ldots, \alpha_n$ haben höchstens einen ggT δ. Man schreibt: $\delta = \mathrm{ggT}(\alpha_1, \ldots, \alpha_n)$.

Satz. (Erweiterter euklidischer Algorithmus)
Seien $\alpha, \beta \in K[X]$. Wir setzen

$$(\lambda_0, \mu_0, \nu_0) := (1, 0, \alpha), \quad (\lambda_1, \mu_1, \nu_1) := (0, 1, \beta), \quad i := 1.$$

Im Fall $\nu_i = 0$ brechen wir ab. Im Fall $\nu_i \neq 0$ liefert Division mit Rest $\kappa_i, \rho_i \in K[X]$ mit $\nu_{i-1} = \kappa_i\nu_i + \rho_i$ und $\deg(\rho_i) < \deg(\nu_i)$. Wir setzen

$$(\lambda_{i+1}, \mu_{i+1}, \nu_{i+1}) := (\lambda_{i-1} - \kappa_i\lambda_i, \mu_{i-1} - \kappa_i\mu_i, \nu_{i-1} - \kappa_i\nu_i = \rho_i),$$

erhöhen i um 1 und wiederholen diesen Schritt.
Das Verfahren bricht ab, und am Ende existiert ein $c \in K$ mit $\nu_{i-1} = c \cdot \mathrm{ggT}(\alpha, \beta) = \lambda_{i-1}\alpha + \mu_{i-1}\beta$.

Beweis. Der Beweis verläuft ähnlich wie in $\mathbb{Z}$. Man beachte dabei: $\deg(\beta) > \deg(\nu_1) > \deg(\nu_2) > \ldots$

Beispiel. Führt man das Verfahren mit $\alpha = X^4 + X^3 + 2X^2 + X + 1$ und $\beta = X^4 - X^3 + 2X^2 - X + 1$ durch, so erhält man:

$$X^2 + 1 = \mathrm{ggT}(\alpha, \beta) = (-\frac{1}{2}X + \frac{1}{2})\alpha + (\frac{1}{2}X + \frac{1}{2})\beta.$$

(Probe!)

10.6 Bemerkung. Nach Satz 10.5 haben je zwei Polynome in $K[X]$ einen ggT. Daraus folgt leicht, dass endlich viele $\alpha_1, \ldots, \alpha_n \in K[X]$ stets einen ggT haben; denn wie in $\mathbb{Z}$ gilt:

$$\mathrm{ggT}(\alpha_1, \ldots, \alpha_n) = \mathrm{ggT}(\mathrm{ggT}(\alpha_1, \ldots, \alpha_{n-1}), \alpha_n).$$

Satz. *Seien $\alpha_1, \ldots, \alpha_n, \beta \in K[X]$. Genau dann existieren $\xi_1, \ldots, \xi_n \in K[X]$ mit $\beta = \alpha_1\xi_1 + \ldots + \alpha_n\xi_n$, wenn gilt:* $\mathrm{ggT}(\alpha_1, \ldots, \alpha_n) \mid \beta$.

Beweis. Wie in $\mathbb{Z}$.

10.7 Bemerkung. Wie in $\mathbb{Z}$ folgt auch, dass für $\alpha_1, \ldots, \alpha_n \in K[X]$ gilt:

$$\mathrm{ggT}(\alpha_1, \ldots, \alpha_n) = 1 \Longleftrightarrow \exists \xi_1, \ldots, \xi_n \in K[X] : \alpha_1\xi_1 + \ldots + \alpha_n\xi_n = 1.$$

Ggf. heißen $\alpha_1, \ldots, \alpha_n$ **teilerfremd**.

Definition. Ein normiertes Polynom $\pi \in K[X] \setminus K$ heißt **irreduzibel**, falls π keinen Teiler τ mit $0 < \deg(\tau) < \deg(\pi)$ hat.

Satz. (i) *Sei $\pi \in K[X]$ irreduzibel, und seien $\alpha, \beta \in K[X]$ mit $\pi \mid \alpha\beta$. Dann gilt: $\pi \mid \alpha \vee \pi \mid \beta$.*
(ii) *Jedes $\alpha \in K[X]$ hat einen irreduziblen Teiler.*

Beweis. (i) Wie in $\mathbb{Z}$.
(ii) Sei $\alpha \in K[X] \setminus K$. Dann ist $T := \{\tau \in K[X] \setminus K : \tau \text{ normiert}, \tau \mid \alpha\} \neq \emptyset$. Sei $\pi \in T$ derart, dass $\deg(\pi)$ möglichst klein ist. Dann ist π irreduzibel; denn sonst hätte π einen Teiler δ mit $0 < \deg(\delta) < \deg(\pi)$; o.B.d.A. sei δ normiert. Dann ist aber $\delta \in T$ im Widerspruch zur Wahl von π.

Beispiel. (i) Normierte Polynome vom Grad 1 sind stets irreduzibel.
(ii) $X^2 + 1$ ist irreduzibel in $\mathbb{R}[X]$, aber nicht in $\mathbb{C}[X]$; denn $X^2 + 1 = (X + i)(X - i)$.

10.8 Satz. (Eindeutige Primfaktorzerlegung)
Sei $\alpha \in K[X] \setminus K$. Dann existieren bis auf die Reihenfolge eindeutig bestimmte irreduzible Polynome $\pi_1, \ldots, \pi_r \in K[X]$ und ein eindeutig bestimmtes $c \in K$ mit $\alpha = c\pi_1 \ldots \pi_r$.

Beweis. *Existenz:* (Induktion nach $d := \deg(\alpha)$)

Im Fall $d = 1$ ist $\alpha = c(X - b)$ mit $b, c \in K$, und die Sache ist klar. Sei also $d > 1$. Nach Satz 10.7 hat α einen irreduziblen Teiler π_1. Wir schreiben $\alpha = \pi_1\beta$ mit $\beta \in K[X]$. Im Fall $\beta \in K$ sind wir fertig. Im Fall $\beta \notin K$ existieren nach Induktion $\pi_2, \ldots, \pi_r \in K[X]$ und $c \in K$ mit $\beta = c\pi_2 \ldots \pi_r$. Folglich ist $\alpha = c\pi_1 \ldots \pi_r$.
Eindeutigkeit: Sei $c\pi_1 \ldots \pi_r = d\rho_1 \ldots \rho_s$ mit $c, d \in K$ und irreduziblen Polynomen $\pi_1, \ldots, \pi_r, \rho_1, \ldots, \rho_s \in K[X]$. Wegen $\pi_1 \mid c\pi_1 \ldots \pi_r = d\rho_1 \ldots \rho_s$ ist $\pi_1 \mid \rho_i$ für ein $i \in \{1, \ldots, s\}$. O.B.d.A. sei $\pi_1 \mid \rho_1$ (nach Umnummerierung). Da ρ_1 irreduzibel ist, folgt $\pi_1 = \rho_1$. Daher ist $0 = \pi_1(c\pi_2 \ldots \pi_r - d\rho_2 \ldots \rho_s)$, d.h. $c\pi_2 \ldots \pi_r = d\rho_2 \ldots \rho_s$. Der Rest folgt induktiv.

10.9 Definition. Für $\alpha = \sum_{i=0}^{\infty} a_i X^i \in K[X]$ und $b \in K$ sei $\alpha(b) := \sum_{i=0}^{\infty} a_i b^i$. Man sagt, dass $\alpha(b)$ durch **Einsetzen** von b in α entsteht. Ist $\alpha(b) = 0$, so heißt b **Nullstelle** von α in K.
Bemerkung. Für $\alpha, \beta \in K[X]$ und $b \in K$ gilt:

$$(\alpha \pm \beta)(b) = \alpha(b) \pm \beta(b) \quad \text{und} \quad (\alpha\beta)(b) = \alpha(b)\beta(b).$$

Satz. *Für $\alpha \in K[X]$ und $b \in K$ ist $\alpha(b)$ der Rest bei der Division von α durch $X - b$. Insbesondere gilt: $\alpha(b) = 0 \iff X - b \mid \alpha$.*
Beweis. Division mit Rest liefert $\kappa, \rho \in K[X]$ mit $\alpha = (X - b)\kappa + \rho$ und $\rho \in K$. Nach der obigen Bemerkung ist $\alpha(b) = (b - b)\kappa(b) + \rho = \rho$. Daher gilt die erste Behauptung. Es folgt: $\alpha(b) = 0 \iff \rho = 0 \iff X - b \mid \alpha$.

10.10 Satz. *Jedes $\alpha \in K[X] \setminus \{0\}$ hat in K höchstens $n := \deg(\alpha)$ Nullstellen.*
Beweis. Seien $a_1, \ldots, a_m \in K$ paarweise verschiedene Nullstellen von α. Dann sind $X - a_1, \ldots, X - a_m$ paarweise verschiedene irreduzible Polynome in $K[X]$. Nach Satz 10.9 ist α durch $X - a_1, \ldots, X - a_m$ teilbar, also nach Satz 10.8 auch durch $(X - a_1) \ldots (X - a_m)$. Insbesondere ist $n = \deg(\alpha) \geq m$.

10.11 Definition. Für $\alpha = \sum_{i=0}^{\infty} a_i X^i \in K[X]$ heißt $\alpha' := \sum_{i=1}^{\infty} i a_i X^{i-1} \in K[X]$ (**formale**) **Ableitung** von α.
Satz. *Für $\alpha = \sum_{i=0}^{\infty} a_i X^i$, $\beta = \sum_{j=0}^{\infty} b_j X^j \in K[X]$ gilt:*
(i) $(\alpha + \beta)' = \alpha' + \beta'$;
(ii) $(\alpha\beta)' = \alpha'\beta + \alpha\beta'$;
(iii) $(\alpha \circ \beta)' = (\alpha' \circ \beta)\beta'$; *dabei ist $\alpha \circ \beta := \sum_{i=0}^{\infty} a_i \beta^i \in K[X]$.*
Beweis. (i) Offensichtlich ist

$$\begin{aligned}(\alpha + \beta)' = \Big(\sum_{i=0}^{\infty} (a_i + b_i) X^i\Big)' &= \sum_{i=1}^{\infty} i(a_i + b_i) X^{i-1} \\ &= \sum_{i=1}^{\infty} i a_i X^{i-1} + \sum_{i=1}^{\infty} i b_i X^{i-1} = \alpha' + \beta'.\end{aligned}$$

(ii) Für $i \in \mathbb{N}_0$ sei $\alpha_i := a_i X^i$. Im Fall $i = 0$ ist

$$(\alpha_0\beta)' = \Big(\sum_{j=0}^{\infty} a_0 b_j X^j\Big)' = \sum_{j=1}^{\infty} j a_0 b_j X^{j-1} = a_0\beta' = \alpha_0'\beta + \alpha_0\beta'.$$

Im Fall $i \neq 0$ ist

$$(\alpha_i\beta)' = (\sum_{j=0}^{\infty} a_i b_j X^{i+j})' = \sum_{j=0}^{\infty}(i+j)a_i b_j X^{i+j-1}$$
$$= \sum_{j=0}^{\infty} i a_i b_j X^{i+j-1} + \sum_{j=1}^{\infty} j a_i b_j X^{i+j-1} = \alpha_i'\beta + \alpha_i\beta'.$$

Daher gilt nach (i):

$$(\alpha\beta)' = (\sum_{i=0}^{\infty}\alpha_i\beta)' = \sum_{i=0}^{\infty}(\alpha_i\beta)' = \sum_{i=0}^{\infty}(\alpha_i'\beta + \alpha_i\beta')$$
$$= (\sum_{i=0}^{\infty}\alpha_i')\beta + (\sum_{i=0}^{\infty}\alpha_i)\beta' = \alpha'\beta + \alpha\beta'.$$

(iii) Für $i \in \mathbb{N}$ ist $(\beta^i)' = i\beta^{i-1}\beta'$; für $i = 1$ ist das trivial, und aus $(\beta^i)' = i\beta^{i-1}\beta'$ folgt mit (ii):

$$(\beta^{i+1})' = (\beta^i\beta)' = (\beta^i)'\beta + \beta'\beta^i = i\beta^{i-1}\beta'\beta + \beta'\beta^i = (i+1)\beta^i\beta'.$$

Also gilt nach (i):

$$(\alpha \circ \beta)' = (\sum_{i=0}^{\infty} a_i\beta^i)' = \sum_{i=0}^{\infty}(a_i\beta^i)' = \sum_{i=0}^{\infty} a_i(\beta^i)' = \sum_{i=1}^{\infty} a_i i\beta^{i-1}\beta' = (\alpha' \circ \beta)\beta'.$$

11. QUADRATISCHE RESTE

11.1 Satz. *Sei K ein Körper und $G \leq K^\times$ eine endliche Untergruppe. Dann ist G zyklisch, d.h. es existiert ein $a \in G$ mit $G = \langle a\rangle = \{1, a, a^2, \ldots\}$.*

Beweis. Für $g \in G$ ist $|\langle g\rangle| \mid |G| =: n$ nach dem Satz von Lagrange. Daher ist $n = \sum_{d|n}\psi(d)$ mit $\psi(d) := |\{g \in G : |\langle g\rangle| = d\}|$ für $d \in \mathbb{N}$.
Sei jetzt $d \mid n$ mit $\psi(d) > 0$. Dann existiert ein $g \in G$ mit $|\langle g\rangle| = d$. Für $i = 1, \ldots, d$ ist dann $(g^i)^d = (g^d)^i = 1^i = 1$. Da $X^d - 1 \in K[X]$ höchstens d Nullstellen in K hat, sind $g, g^2, \ldots, g^d$ genau die Nullstellen von $X^d - 1$ in K. Dabei gilt für $i = 1, \ldots, d$ nach Satz 5.5: $|\langle g^i\rangle| = d \Longleftrightarrow \mathrm{ggT}(i, d) = 1$. Daher haben genau $\varphi(d)$ der Elemente in $\{g, g^2, \ldots, g^d\}$ Ordnung d. Also ist $\psi(d) \leq \varphi(d)$ für alle $d \mid n$.
Folglich ist $n = \sum_{d|n}\psi(d) \leq \sum_{d|n}\varphi(d) = n$ nach Satz 7.9. Daher ist $\psi(d) = \varphi(d)$ für alle $d \mid n$; insbesondere ist $\psi(n) = \varphi(n) > 0$, d.h. G enthält ein Element a mit $|\langle a\rangle| = n$. Also ist $G = \langle a\rangle$.

Bemerkung. Für $p \in \mathbb{P}$ ist $\mathbb{Z}/p\mathbb{Z}$ wegen $|(\mathbb{Z}/p\mathbb{Z})^\times| = \varphi(p) = p - 1$ ein Körper. Daher existiert ein $a \in \mathbb{Z}$ mit

$$(\mathbb{Z}/p\mathbb{Z})^\times = \langle a + p\mathbb{Z}\rangle = \{1 + p\mathbb{Z}, a + p\mathbb{Z}, a^2 + p\mathbb{Z}, \ldots, a^{p-2} + p\mathbb{Z}\};$$

a heißt **Primitivwurzel** modulo p. Ggf. ist dann auch a^i für alle $i \in \mathbb{N}$ mit $\mathrm{ggT}(i, p-1) = 1$ eine Primitivwurzel modulo p.

Beispiel. Sei $p := 17$, d.h. $\varphi(p) = 16 = 2^4$. Wegen $2^8 = (2^4)^2 = 16^2 \equiv (-1)^2 \equiv 1 \pmod{17}$ ist 2 keine Primitivwurzel modulo 17. Wegen $3^8 \equiv (3^4)^2 \equiv 81^2 \equiv (-4)^2 \equiv 16 \equiv -1 \pmod{17}$ ist 3 Primitivwurzel modulo 17.

11.2 Bemerkung. Sei $G = \langle g \rangle$ eine zyklische Gruppe der Ordnung $2n$ für ein $n \in \mathbb{N}$. Dann enthält G genau eine Untergruppe der Ordnung 2, nämlich $\langle g^n \rangle$. Ferner ist $f : G \longrightarrow G$, $x \longmapsto x^2$, ein Homomorphismus. Jedes Element in $\mathrm{Ker}(f) \setminus \{1\}$ hat Ordnung 2, liegt also in $\langle g^n \rangle$. Daher ist $\mathrm{Ker}(f) = \langle g^n \rangle$.
Nach dem Homomorphiesatz ist $|\mathrm{Bld}(f)| = |G : \mathrm{Ker}(f)| = n$. Wegen

$$G = \{1, g, g^2, \ldots, g^{2n-1}\}$$

ist also $\mathrm{Bld}(f) = \{1, g^2, g^4, \ldots, g^{2n-2}\} = \langle g^2 \rangle$.

Definition. Sei $m \in \mathbb{N}$. Ein $a \in \mathbb{Z}$ heißt **quadratischer Rest** (QR) modulo m, falls ein $x \in \mathbb{Z}$ mit $x^2 \equiv a \pmod{m}$ existiert. Andernfalls heißt a **quadratischer Nichtrest** (QNR) modulo m.
Für $m = p \in \mathbb{P}$ und $p \nmid a$ heißt

$$\left(\frac{a}{p}\right) := \begin{cases} 1, & \text{falls } a \text{ QR modulo } p, \\ -1, & \text{falls } a \text{ QNR modulo } p, \end{cases}$$

Legendre-Symbol (LEGENDRE, 1752-1833). Man liest: a "nach" p.

Satz. (Euler-Kriterium)
Für $2 \neq p \in \mathbb{P}$ und $a \in \mathbb{Z}$ mit $p \nmid a$ gilt: $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

Beweis. Nach Satz 11.1 existiert ein $g \in \mathbb{Z}$ mit

$$(\mathbb{Z}/p\mathbb{Z})^\times = \langle g + p\mathbb{Z} \rangle = \{1 + p\mathbb{Z}, g + p\mathbb{Z}, \ldots, g^{p-2} + p\mathbb{Z}\}.$$

Dann ist $g^{p-1} \equiv 1 \pmod{p}$, aber $a := g^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}$, also $g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$; denn aus $a^2 \equiv 1 \pmod{p}$, d.h. $p \mid a^2 - 1 = (a+1)(a-1)$, folgt $p \mid a+1$ oder $p \mid a-1$.
Nach Bemerkung 11.2 sind $1 + p\mathbb{Z}, g^2 + p\mathbb{Z}, \ldots, g^{p-3} + p\mathbb{Z}$ Quadrate in $(\mathbb{Z}/p\mathbb{Z})^\times$, und $g + p\mathbb{Z}, g^3 + p\mathbb{Z}, \ldots, g^{p-2}\mathbb{Z}$ sind keine Quadrate in $(\mathbb{Z}/p\mathbb{Z})^\times$. Für $i = 0, \ldots, \frac{p-3}{2}$ gilt dabei:

$$(g^{2i} + p\mathbb{Z})^{\frac{p-1}{2}} = (g^{p-1})^i + p\mathbb{Z} = 1^i + p\mathbb{Z} = 1 + p\mathbb{Z},$$

$$(g^{2i+1} + p\mathbb{Z})^{\frac{p-1}{2}} = (g^{p-1})^i g^{\frac{p-1}{2}} + p\mathbb{Z} = -1 + p\mathbb{Z}.$$

Beispiel.

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \equiv \begin{cases} 1 \pmod{p}, & \text{falls } p \equiv 1 \pmod{4}, \\ -1 \pmod{p}, & \text{falls } p \equiv 3 \pmod{4}. \end{cases}$$

Daher gilt: (i) -1 QR modulo $p \iff p \equiv 1 \pmod{4}$;

(ii) -1 QNR modulo $p \iff p \equiv 3 \pmod 4$.

11.3 Bemerkung. Seien $2 \neq p \in \mathbb{P}$ und $a, b \in \mathbb{Z} \setminus p\mathbb{Z}$.
(i) Aus $a \equiv b \pmod p$ folgt $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.
(ii) Stets ist $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.
(iii) Ist $\rho_p(a) \in \{\frac{1-p}{2}, \ldots, \frac{p-1}{2}\}$ mit $a \equiv \rho_p(a) \pmod p$, so heißt $\rho_p(a)$ **absolut kleinster Rest** von a modulo p.

Satz. *Für $2 \neq p \in \mathbb{P}$ und $a \in \mathbb{Z}$ mit $p \nmid a$ ist $\left(\frac{a}{p}\right) = (-1)^\mu$ mit*

$$\mu := |\{j \in \mathbb{N} : 1 \leq j \leq \frac{p-1}{2},\ \rho_p(aj) < 0\}|.$$

Beweis. Seien $i, j \in \{1, \ldots, \frac{p-1}{2}\}$ mit $|\rho_p(ai)| = |\rho_p(aj)|$. Dann gilt:

$$ai \equiv \rho_p(ai) = \pm\rho_p(aj) \equiv \pm aj \pmod p,$$

d.h. $a(i \mp j) \equiv 0 \pmod p$. Daher ist $i \mp j \equiv 0 \pmod p$, d.h. $i = j$.
Dies zeigt: $\{|\rho_p(ai)| : i = 1, \ldots, \frac{p-1}{2}\} = \{1, 2, \ldots, \frac{p-1}{2}\}$. Folglich ist $\prod_{i=1}^{\frac{p-1}{2}} |\rho_p(ai)| = \left(\frac{p-1}{2}\right)!$ und $\prod_{i=1}^{\frac{p-1}{2}} \rho_p(ai) = (-1)^\mu \left(\frac{p-1}{2}\right)!$. Andererseits ist

$$\prod_{i=1}^{\frac{p-1}{2}} \rho_p(ai) \equiv \prod_{i=1}^{\frac{p-1}{2}} (ai) = a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv \left(\frac{a}{p}\right)\left(\frac{p-1}{2}\right)! \pmod p.$$

Die Behauptung folgt.
Beispiel. Für $a := 2$ und $j = 1, \ldots, \frac{p-1}{2}$ gilt:

$$\rho_p(aj) < 0 \iff \frac{p-1}{2} < 2j \leq p-1 \iff \frac{p-1}{4} < j \leq \frac{p-1}{2}.$$

Für $p \equiv 1 \pmod 4$ ist also $\mu = \frac{p-1}{4}$, und für $p \equiv 3 \pmod 4$ ist $\mu = \frac{p+1}{4}$. Daher gilt: μ gerade $\iff$ $p \equiv \pm 1 \pmod 8$. Daraus folgt leicht:

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

11.4 Satz. (EISENSTEIN, 1823-1852)
Für $p, q \in \mathbb{P} \setminus \{2\}$ mit $p \neq q$ und $k := \frac{p-1}{2}$, $l := \frac{q-1}{2}$ gilt:

$$\sum_{i=1}^{k} \lfloor \frac{iq}{p} \rfloor + \sum_{j=1}^{l} \lfloor \frac{jp}{q} \rfloor = kl.$$

Beweis. Wir nehmen zunächst an, dass $i \in \{1,\dots,k\}$ und $j \in \{1,\dots,l\}$ mit $iq - jp = 0$ existieren. Wegen $p \nmid q$ ist dann $p \mid i$. Dies ist aber ein Widerspruch wegen $1 \le i \le \frac{p-1}{2}$. Dieser Widerspruch zeigt: $iq - jp \neq 0$ für $i = 1,\dots,k$ und $j = 1,\dots,l$. Genau $S := \sum_{i=1}^{k} \lfloor \frac{iq}{p} \rfloor$ dieser Zahlen $iq - jp$ sind positiv; denn für ein festes i gilt: $iq > jp \iff j \in \{1,\dots,\lfloor \frac{iq}{p} \rfloor\}$.
Analog sind genau $T := \sum_{j=1}^{l} \lfloor \frac{jp}{q} \rfloor$ der Zahlen $iq - jp$ negativ. Insgesamt ist also $S+T = kl$.

11.5 Satz. (Quadratisches Reziprozitätsgesetz, GAUSS, 1777-1855)
Für $p, q \in \mathbb{P} \setminus \{2\}$ gilt:

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

d.h. $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$, *falls* $p \equiv 1 \pmod 4$ *oder* $q \equiv 1 \pmod 4$,
und $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$, *falls* $p \equiv 3 \equiv q \pmod 4$.

Bemerkung. Dazu gehören noch die beiden *Ergänzungssätze*:

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

d.h. $\left(\frac{-1}{p}\right) = 1 \iff p \equiv 1 \pmod 4$,
und $\left(\frac{2}{p}\right) = 1 \iff p \equiv \pm 1 \pmod 8$.

Beweis. Sei $i \in \{1,\dots,k := \frac{p-1}{2}\}$. Division mit Rest liefert dann: (1) $iq = p\lfloor \frac{iq}{p} \rfloor + r_i$ mit $1 \le r_i \le p-1$. Wir unterscheiden zwei Fälle:
Fall A: $r_i \le k$, d.h. $\rho_p(iq) = r_i > 0$.
Fall B: $r_i > k$, d.h. $\rho_p(iq) = r_i - p < 0$.
Der Fall B trete dabei genau μ-mal auf. Wir setzen $R := \sum_A r_i = \sum_A |\rho_p(iq)|$ und $R' := \sum_B (p - r_i) = \sum_B |\rho_p(iq)|$. Wie im Beweis von Satz 11.3 ist $\{|\rho_p(iq)| : i = 1,\dots,k\} = \{1,\dots,k\}$. Daher ist $R + R' = \sum_{i=1}^{k} i = \frac{k(k+1)}{2} = \frac{p^2-1}{8}$. Daher gilt:

$$(2) \qquad \frac{p^2-1}{8} = R + R' = \sum_A r_i + \mu p - \sum_B r_i.$$

Wir setzen $S(p,q) := \sum_{i=1}^{k} \lfloor \frac{iq}{p} \rfloor$. Summation von (1) liefert dann:

$$(3) \qquad \frac{p^2-1}{8} q = \sum_{i=1}^{k} iq = p\sum_{i=1}^{k} \lfloor \frac{iq}{p} \rfloor + \sum_{i=1}^{k} r_i = pS(p,q) + \sum_A r_i + \sum_B r_i.$$

Subtraktion von (2) und (3) ergibt:

$$(4) \qquad \frac{p^2-1}{8}(q-1) = pS(p,q) + 2\sum_B r_i - \mu p.$$

Wegen $\frac{p^2-1}{8} \in \mathbb{Z}$ und $p \equiv 1 \equiv q \pmod 2$ folgt: $\mu \equiv S(p,q) \pmod 2$. Nach Satz 11.3 ist $\left(\frac{q}{p}\right) = (-1)^{\mu} = (-1)^{S(p,q)}$. Analog ist $\left(\frac{p}{q}\right) = (-1)^{S(q,p)}$. Mit Satz 11.4 folgt: $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{S(p,q)+S(q,p)} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$.

Beispiel. Für die Primzahlen $p := 67$ und $q := 139$ ergibt sich:

$$\left(\frac{67}{139}\right) = -\left(\frac{139}{67}\right) = -\left(\frac{5}{67}\right) = -\left(\frac{67}{5}\right) = -\left(\frac{2}{5}\right) = 1.$$

So kann man das Legendre-Symbol schnell berechnen. Im folgenden präsentieren wir einige Anwendungen des Quadratischen Reziprozitätsgesetzes und seiner Ergänzungssätze.

11.6 Satz. $|\{p \in \mathbb{P} : p \equiv 1 \pmod 6\}| = \infty = |\{p \in \mathbb{P} : p \equiv -1 \pmod 6\}|$.

Beweis. Nach Satz 3.3 hat das Polynom $X^2 + 3$ unendlich viele Primteiler $p > 3$. Für jedes solche p existiert also ein $x \in \mathbb{Z}$ mit $x^2 + 3 \equiv 0 \pmod p$. Daher ist -3 QR modulo p, d.h.

$$1 = \left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}} = \left(\frac{p}{3}\right).$$

Daher ist p QR modulo 3, d.h. $p \equiv 1 \pmod 3$. Wegen $p \neq 2$ ist auch $p \equiv 1 \pmod 2$, d.h. $p \equiv 1 \pmod 6$.
Also ist $|\{p \in \mathbb{P} : p \equiv 1 \pmod 6\}| = \infty$.
Zum Beweis von $|\{p \in \mathbb{P} : p \equiv -1 \pmod 6\}| = \infty$ seien $2, 3, 5, \ldots, p \in \mathbb{P}$ und $n := 2\cdot 3\cdot 5\cdots p - 1$. Wegen $n \equiv -1 \pmod 6$ hat n einen Primteiler q mit $q \not\equiv 1 \pmod 6$, d.h. $q \equiv -1 \pmod 6$. Da n sicher nicht durch $2, 3, 5, \ldots, p$ teilbar ist, folgt: $q \notin \{2, 3, 5, \ldots, p\}$.

Beispiele. Die Folgen von Primzahlen $7, 13, 19, 31, 37, 43, \ldots$ und $5, 11, 17, 23, 29, 41, \ldots$ sind also beide unendlich.

11.7 Satz. *Für $1 \neq m \in \mathbb{N}$ gilt:* $2^m + 1 \in \mathbb{P} \iff 3^{2^{m-1}} \equiv -1 \pmod{2^m+1}$.

Bemerkung. Dies ist ein Test für Fermat-Primzahlen.

Beweis. "$\Longrightarrow$": Sei $p := 2^m + 1 \in \mathbb{P}$, also $p > 3$. Wegen $p \equiv (-1)^m + 1 \pmod 3$ ist m gerade, d.h. $m = 2s$ für ein $s \in \mathbb{N}$. Daher gilt: $p = 2^{2s} + 1 = 4^s + 1 \equiv 1^s + 1 = 2 \pmod 3$ und $p \equiv 1 \pmod 4$. Folglich ist $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = \left(\frac{2}{3}\right) = -1$, d.h. 3 ist QNR modulo p. Aus dem Euler-Kriterium ergibt sich: $3^{2^{m-1}} \equiv -1 \pmod p$.
"$\Longleftarrow$": Sei $3^{2^{m-1}} \equiv -1 \pmod{2^m+1}$ und $p \in \mathbb{P}$ mit $p \mid 2^m+1$, d.h. $p \neq 2$. Wegen $3^{2^m} \equiv 1 \pmod p$ ist $|\langle 3 + p\mathbb{Z}\rangle| \mid 2^m$, d.h. $2^m = |\langle 3 + p\mathbb{Z}\rangle| \mid |(\mathbb{Z}/p\mathbb{Z})^\times = p - 1$; insbesondere gilt: $2^m \leq p - 1$, d.h. $p = 2^m + 1$.

11.8 Satz. *Sei $1 \neq k \in \mathbb{N}$, und sei $p \in \mathbb{P}$ mit $p \mid 2^{2^k} + 1$. Dann gilt:* $2^{k+2} \mid p - 1$.

Beweis. Wegen $2^{2^k} \equiv -1 \pmod p$ ist $2^{2^{k+1}} \equiv 1 \pmod p$, d.h. $|\langle 2 + p\mathbb{Z}\rangle| = 2^{k+1}$. Folglich gilt: $2^{k+1} \mid |(\mathbb{Z}/p\mathbb{Z})^\times| = p - 1$, d.h. $p \equiv 1 \pmod{2^{k+1}}$. Folglich ist $p \equiv 1 \pmod 8$, d.h. 2 ist QR modulo p. Aus dem Euler-Kriterium folgt: $2^{\frac{p-1}{2}} \equiv \left(\frac{2}{p}\right) \equiv 1 \pmod p$. Also gilt: $2^{k+1} \mid \frac{p-1}{2}$ und damit $2^{k+2} \mid p - 1$.

Beispiel. Insbesondere hat also jeder Primteiler von $2^{2^5}+1$ die Form $p = 128n+1$. Wir probieren die verschiedenen n nacheinander durch:
$n = 1$: $128 \cdot 1 + 1 = 129 \notin \mathbb{P}$;
$n = 2$: $128 \cdot 2 + 1 = 257 = 2^{2^3}+1 \nmid 2^{2^5}+1$; denn es gilt:

$$2^{2^5}+1 \equiv (2^{2^3})^4 + 1 \equiv (-1)^4 + 1 \equiv 1+1 \equiv 2 \pmod{2^{2^3}+1};$$

$n = 3$: $128 \cdot 3 + 1 = 385 \notin \mathbb{P}$;
$n = 4$: $128 \cdot 4 + 1 = 513 \notin \mathbb{P}$;
$n = 5$: $128 \cdot 5 + 1 = 641$ Primteiler von $2^{2^5}+1$.

11.9 Definition. (JACOBI, 1804-1851)
Für $2 \neq p \in \mathbb{P}$ und $a \in \mathbb{Z}$ mit $p \mid a$ sei $\left(\frac{a}{p}\right) := 0$. Für $a \in \mathbb{Z}$ und ungerade $b \in \mathbb{N}$ mit Primfaktorzerlegung $b = p_1 \dots p_r$ sei $\left(\frac{a}{b}\right) := \left(\frac{a}{p_1}\right) \dots \left(\frac{a}{p_r}\right)$; insbesondere sei $\left(\frac{a}{1}\right) := 1$. Man nennt $\left(\frac{a}{b}\right)$ auch **Jacobi-Symbol**.

Bemerkung. (i) Das Jacobi-Symbol ist also eine Fortsetzung des Legendre-Symbols. Für $a \in \mathbb{Z}$ und ungerade $b \in \mathbb{N}$ ist $\left(\frac{a}{b}\right) \in \{1, 0, -1\}$. Dabei gilt: $\left(\frac{a}{b}\right) = 0 \Longleftrightarrow \mathrm{ggT}(a,b) \neq 1$.
(ii) Ist $b > 1$ und a QR modulo b, so ist $\left(\frac{a}{b}\right) = 1$, aber eventuell nicht umgekehrt.

Satz. *Für ungerade $b, b_1, b_2 \in \mathbb{N}$ und beliebige $a, a_1, a_2 \in \mathbb{Z}$ gilt:*
(i) $\left(\frac{a_1 a_2}{b}\right) = \left(\frac{a_1}{b}\right)\left(\frac{a_2}{b}\right)$ *und* $\left(\frac{a}{b_1 b_2}\right) = \left(\frac{a}{b_1}\right)\left(\frac{a}{b_2}\right)$.
(ii) $a_1 \equiv a_2 \pmod{b} \Longrightarrow \left(\frac{a_1}{b}\right) = \left(\frac{a_2}{b}\right)$.
(iii) $r \in \mathbb{N} \wedge \mathrm{ggT}(r,b) = 1 \Longrightarrow \left(\frac{ar^2}{b}\right) = \left(\frac{a}{b}\right)$.
(iv) $\left(\frac{-1}{b}\right) = (-1)^{\frac{b-1}{2}}$ *und* $\left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{8}}$.
(v) *a, b ungerade und teilerfremd* $\Longrightarrow \left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}}$.

Beweis. (i) - (iii) klar.
(iv) O.B.d.A. sei $b > 1$ mit Primfaktorzerlegung $b = p_1 \dots p_t$. Dann ist

$$\left(\frac{-1}{b}\right) = \prod_{i=1}^{t}\left(\frac{-1}{p_i}\right) = \prod_{i=1}^{t}(-1)^{\frac{p_i-1}{2}} = (-1)^{\sum_{i=1}^{t}\frac{p_i-1}{2}}.$$

Daher genügt zu zeigen: $\sum_{i=1}^{t}\frac{p_i-1}{2} \equiv \frac{p_1\dots p_t-1}{2} \pmod 2$, d.h. $\sum_{i=1}^{t}(p_i-1) \equiv p_1\dots p_t - 1 \pmod 4$. Dies stimmt sicher für $t = 1$. Sei also $t > 1$ und die Aussage für $t-1$ schon bewiesen. Dann gilt:

$$\begin{aligned} 0 &\equiv (p_1 \dots p_{t-1} - 1)(p_t - 1) \equiv p_1 \dots p_t - p_1 \dots p_{t-1} - p_t + 1 \\ &\equiv (p_1 \dots p_t - 1) - (p_1 \dots p_{t-1} - 1) - (p_t - 1) \\ &\equiv (p_1 \dots p_t - 1) - \sum_{i=1}^{t-1}(p_i - 1) - (p_t - 1) \equiv (p_1 \dots p_t - 1) - \sum_{i=1}^{t}(p_i - 1) \pmod 4. \end{aligned}$$

Analog ist

$$\left(\frac{2}{b}\right) = \prod_{i=1}^{t}\left(\frac{2}{p_i}\right) = \prod_{i=1}^{t}(-1)^{\frac{p_i^2-1}{8}} = (-1)^{\sum_{i=1}^{t}\frac{p_i^2-1}{8}}.$$

Daher genügt zu zeigen: $\sum_{i=1}^{t}\frac{p_i^2-1}{8} \equiv \frac{p_1^2\ldots p_t^2-1}{8} \pmod 2$, d.h. $\sum_{i=1}^{t}(p_i^2-1) \equiv p_1^2\ldots p_t^2-1 \pmod{16}$. Dies stimmt für $t=1$. Sei also $t>1$ und die Aussage für $t-1$ schon bewiesen. Dann gilt:

$$\begin{aligned}0 &\equiv (p_1^2\ldots p_{t-1}^2-1)(p_t^2-1) \equiv p_1^2\ldots p_t^2 - p_1^2\ldots p_{t-1}^2 - p_t^2 + 1\\ &\equiv (p_1^2\ldots p_t^2-1) - (p_1^2\ldots p_{t-1}^2-1) - (p_t^2-1)\\ &\equiv (p_1^2\ldots p_t^2-1) - \sum_{i=1}^{t-1}(p_i^2-1) - (p_t^2-1) \equiv (p_1^2\ldots p_t^2-1) - \sum_{i=1}^{t}(p_i^2-1) \pmod{16}.\end{aligned}$$

(v) O.B.d.A. sei $a \neq 1 \neq b$. Die Primfaktorzerlegungen von a und b seien $a = p_1\ldots p_r$ und $b = q_1\ldots q_s$. Dann gilt wie in (iv):

$$\begin{aligned}\left(\frac{a}{b}\right) &= \prod_{i=1}^{r}\prod_{j=1}^{s}\left(\frac{p_i}{q_j}\right) = \prod_{i=1}^{r}\prod_{j=1}^{s}\left(\frac{q_j}{p_i}\right)(-1)^{\frac{p_i-1}{2}\cdot\frac{q_j-1}{2}}\\ &= \left(\frac{b}{a}\right)(-1)^{\sum_{i=1}^{r}\frac{p_i-1}{2}\sum_{j=1}^{s}\frac{q_j-1}{2}} = \left(\frac{b}{a}\right)(-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}}.\end{aligned}$$

Beispiel. Diese Rechenregeln beschleunigen die Berechnung von Legendre-Symbolen; denn man braucht keine komplizierten Primfaktorzerlegungen mehr durchzuführen:

$$\begin{aligned}\left(\frac{10103}{7901}\right) &= \left(\frac{2202}{7901}\right) = \left(\frac{2}{7901}\right)\left(\frac{1101}{7901}\right) = -\left(\frac{7901}{1101}\right) = -\left(\frac{194}{1101}\right)\\ &= -\left(\frac{2}{1101}\right)\left(\frac{97}{1101}\right) = \left(\frac{97}{1101}\right) = \left(\frac{1101}{97}\right) = \left(\frac{34}{97}\right) = \left(\frac{2}{97}\right)\left(\frac{17}{97}\right)\\ &= \left(\frac{17}{97}\right) = \left(\frac{97}{17}\right) = \left(\frac{12}{17}\right) = \left(\frac{3}{17}\right) = \left(\frac{17}{3}\right) = \left(\frac{2}{3}\right) = -1.\end{aligned}$$

12. QUADRATSUMMEN

12.1 Satz. *Sei $2 \neq p \in \mathbb{P}$. Genau dann existieren $x, y \in \mathbb{Z}$ mit $p = x^2+y^2$, wenn gilt:* $p \equiv 1 \pmod 4$.

Beweis. "$\Longrightarrow$": Für $x \in \mathbb{Z}$ ist $x^2 \equiv 0 \pmod 4$ oder $x^2 \equiv 1 \pmod 4$. Für $y \in \mathbb{Z}$ ist also $x^2+y^2 \not\equiv 3 \pmod 4$.

"$\Longleftarrow$": Sei $p \equiv 1 \pmod 4$, d.h. $\left(\frac{-1}{p}\right) = 1$. Dann existiert ein $u \in \mathbb{N}$ mit $u^2 \equiv -1 \pmod p$. Wegen $(\lfloor\sqrt{p}\rfloor+1)^2 > p$ existieren verschiedene Paare $(x_1,y_1),(x_2,y_2)$ mit

$x_1, y_1, x_2, y_2 \in \{0, 1, \ldots, \lfloor\sqrt{p}\rfloor\}$ und $ux_1 - y_1 \equiv ux_2 - y_2 \pmod{p}$, d.h. $ux_0 \equiv y_0 \pmod{p}$ mit $x_0 := x_1 - x_2$ und $y_0 := y_1 - y_2$. Dann ist $y_0^2 \equiv u^2 x_0^2 \equiv -x_0^2 \pmod{p}$, d.h. $x_0^2 + y_0^2 \equiv 0 \pmod{p}$. Wegen $0 \leq |x_0| < \sqrt{p}$ und $0 \leq |y_0| < \sqrt{p}$ ist $0 < x_0^2 + y_0^2 < 2p$, d.h. $x_0^2 + y_0^2 = p$.
Beispiel. $29 = 5^2 + 2^2$, aber $31 \neq x^2 + y^2$ für $x, y \in \mathbb{Z}$.

12.2 Bemerkung. Für $a, b, c, d \in \mathbb{R}$ gilt:

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

Dies rechnet man nach, oder man beobachtet, dass es aus der Formel $|z_1 z_2| = |z_1| \cdot |z_2|$ $(z_1, z_2 \in \mathbb{C})$ folgt.
Satz. *Sei $n \in \mathbb{N}$ mit Primfaktorzerlegung $n = \prod_{p \in \mathbb{P}} p^{\alpha_p}$. Genau dann existieren $x, y \in \mathbb{Z}$ mit $n = x^2 + y^2$, wenn α_p für jedes $p \in \mathbb{P}$ mit $p \equiv 3 \pmod{4}$ gerade ist.*
Beweis. "$\Longleftarrow$": Für $p \in \mathbb{P}$ mit $p \equiv 1 \pmod{4}$ existieren $x_p, y_p \in \mathbb{Z}$ mit $p = x_p^2 + y_p^2$. Wegen $2 = 1^2 + 1^2$ folgt die Behauptung aus der Bemerkung.
"$\Longrightarrow$": Seien $x, y \in \mathbb{Z}$ mit $n = x^2 + y^2$, und sei $d := \mathrm{ggT}(x, y)$. Dann ist $n_1 = x_1^2 + y_1^2$ mit $n_1 := \frac{n}{d^2}$, $x_1 := \frac{x}{d}$, $y_1 := \frac{y}{d}$ und $\mathrm{ggT}(x_1, y_1) = 1$. Ist $2 \neq p \in \mathbb{P}$ mit $p \mid n_1$, so ist $p \nmid y_1$; denn sonst hätte man den Widerspruch $p \mid x_1$. Also existiert ein $z_1 \in \mathbb{Z}$ mit $y_1 z_1 \equiv 1 \pmod{p}$. Daher ist $(x_1 z_1)^2 \equiv -(y_1 z_1)^2 \equiv -1 \pmod{p}$, d.h. $\left(\frac{-1}{p}\right) = 1$ und damit $p \equiv 1 \pmod{4}$. Die Behauptung folgt.

12.3 Satz. *Seien $a, b \in \mathbb{N}$ und $p \in \mathbb{P}$. Seien ferner $u, v, x, y \in \mathbb{N}$ mit $(u, v) \neq (x, y)$ und $p = au^2 + bv^2 = ax^2 + by^2$. Dann gilt: $a = b = 1$ und $(u, v) = (y, x)$.*
Bemerkung. Im Wesentlichen ist die Darstellung $p = ax^2 + by^2$ also eindeutig.
Beweis. Wegen $p = au^2 + bv^2 > a$ ist $p \nmid a$. Wegen

$$\begin{aligned} a(vx + uy)(vx - uy) &= a(v^2x^2 - u^2y^2) = v^2(p - by^2) - au^2y^2 \\ &= pv^2 - (au^2 + bv^2)y^2 = pv^2 - py^2 \equiv 0 \pmod{p} \end{aligned}$$

ist also $vx \equiv \pm uy \pmod{p}$.
Fall 1: $vx \equiv uy \pmod{p}$.
Dann gilt:

$$\begin{aligned} p^2 &= (au^2 + bv^2)(ax^2 + by^2) = a^2u^2x^2 + b^2v^2y^2 + ab(u^2y^2 + v^2x^2) \\ &= (aux + bvy)^2 + ab(uy - vx)^2 > ab(uy - vx)^2 > 0; \end{aligned}$$

denn im Fall $uy = vx$ wäre $u \mid x \mid u$ wegen $\mathrm{ggT}(u, v) = 1 = \mathrm{ggT}(x, y)$, d.h. $u = x$ und damit $v = y$. Widerspruch!
Damit haben wir den Widerspruch $p^2 > ab(uy - vx)^2 \geq abp^2 \geq p^2$.
Fall 2: $vx \equiv -uy \pmod{p}$.
Dann gilt:

$$p^2 = (au^2 + bv^2)(ax^2 + by^2) = (aux - bvy)^2 + ab(uy + vx)^2 \geq ab(uy + vx)^2 > 0.$$

Also ist $p^2 \geq abp^2$, d.h. $a = b = 1$ und $ux = vy$. Wegen $\mathrm{ggT}(u,v) = 1 = \mathrm{ggT}(x,y)$ folgt $u \mid y \mid u$, d.h. $u = y$ und damit $x = v$.

12.4 Satz. (LAGRANGE)
Jedes $n \in \mathbb{N}$ lässt sich als Summe von höchstens 4 Quadratzahlen schreiben.

Bemerkung. Für $a, b, c, d, A, B, C, D \in \mathbb{R}$ gilt:

$$\begin{aligned}&(a^2+b^2+c^2+d^2)(A^2+B^2+C^2+D^2)\\&= (aA+bB+cC+dD)^2 + (aB-bA+cD-dC)^2\\&+ (aC-bD-cA+dB)^2 + (aD+bC-cB-dA)^2.\end{aligned}$$

(Nachrechnen!) Diese Formel versteht man am besten im Kontext der **Quaternionen** $\mathbb{H}$ (HAMILTON, 1805-1865).

Beweis. Nach der Bemerkung sei o.B.d.A. $n = p \in \mathbb{P}$. Wegen $2 = 1^2 + 1^2$ sei o.B.d.A. $p > 2$. Wegen Satz 12.1 sei o.B.d.A. $p \equiv 3 \pmod 4$. Sei $c \in \mathbb{N}$ minimal mit $\left(\frac{c}{p}\right) = -1$. Dann gilt: $2 \leq c \leq p-1$, $\left(\frac{c-1}{p}\right) = 1$ und $\left(\frac{-c}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{c}{p}\right) = (-1)^2 = 1$. Daher existieren $x, y \in \mathbb{Z}$ mit $x^2 \equiv c-1 \pmod p$ und $y^2 \equiv -c \pmod p$. Folglich ist $x^2 + y^2 + 1 \equiv 0 \pmod p$; dabei können wir $x, y \in \{0, \ldots, \frac{p-1}{2}\}$ annehmen.
Sei $h \in \mathbb{N}$ minimal derart, dass die Gleichung $x_1^2 + x_2^2 + x_3^2 + x_4^2 = hp$ in $\mathbb{Z}$ lösbar ist. Dann ist $1 \leq h < p$, und wir müssen $h = 1$ zeigen.
Wir nehmen zunächst an, dass h gerade ist. Dann ist $|\{i : 1 \leq i \leq 4,\ x_i \text{ ungerade}\}|$ gerade. Bei geeigneter Nummerierung sind also $x_1 \pm x_2$ und $x_3 \pm x_4$ gerade. Folglich gilt:

$$(\frac{x_1+x_2}{2})^2 + (\frac{x_1-x_2}{2})^2 + (\frac{x_3+x_4}{2})^2 + (\frac{x_3-x_4}{2})^2 = \frac{h}{2}p$$

im Widerspruch zur Wahl von h.
Also ist h ungerade. Wir nehmen $h \geq 3$ an. Für $i = 1, 2, 3, 4$ sei $y_i \in \mathbb{Z}$ mit $y_i \equiv x_i \pmod h$ und $|y_i| \leq \frac{h-1}{2}$. Dann ist $(y_1, y_2, y_3, y_4) \neq (0, 0, 0, 0)$; denn sonst wäre $h \mid x_1, \ldots, h \mid x_4$, also $h^2 \mid x_1^2 + x_2^2 + x_3^2 + x_4^2 = hp$ und damit $h \mid p$. Widerspruch!
Daher gilt: $0 < y_1^2 + y_2^2 + y_3^2 + y_4^2 < h^2$ und $y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \pmod h$, d.h. $y_1^2 + y_2^2 + y_3^2 + y_4^2 = kh$ mit $k < h$. Nach der obigen Bemerkung ist

$$hp \cdot kh = (x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = z_1^2 + z_2^2 + z_3^2 + z_4^2$$

mit

$$\begin{aligned}z_1 &= x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \pmod h,\\ z_2 &= x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3 \equiv x_1x_2 - x_2x_1 + x_3x_4 - x_4x_3 \equiv 0 \pmod h,\\ z_3 &= x_1y_3 - x_2y_4 - x_3y_1 + x_4y_2 \equiv x_1x_3 - x_2x_4 - x_3x_1 + x_4x_2 \equiv 0 \pmod h,\\ z_4 &= x_1y_4 + x_2y_3 - x_3y_2 - x_4y_1 \equiv x_1x_4 + x_2x_3 - x_3x_2 - x_4x_1 \equiv 0 \pmod h.\end{aligned}$$

Wir schreiben $z_i = ht_i$ mit $t_i \in \mathbb{Z}$ für $i = 1, \ldots, 4$. Dann ist $t_1^2 + t_2^2 + t_3^2 + t_4^2 = kp$ im Widerspruch zur Wahl von h.

12.5 Bemerkung. (i) Man hat auch eine Formel der Gestalt

$$(P^2+Q^2+\ldots+W^2)(p^2+q^2+\ldots+w^2)=a^2+b^2+\ldots+h^2$$

(jeweils 8 Summanden) mit

$$\begin{aligned}
a &= Pp-Qq-Rr-Ss-Tt-Uu-Vv-Ww\\
b &= Pq+Qp+Rs-Sr+Tu-Ut-Vw+Wv\\
c &= Pr-Qs+Rp+Sq+Tv+Uw-Vt-Wu\\
d &= Ps+Qr-Rq+Sp+Tw-Uv+Vu-Wt\\
e &= Pt-Qu-Rv-Sw+Tp+Uq+Vr+Ws\\
f &= Pu+Qt-Rw+Sv-Tq+Up-Vs+Wr\\
g &= Pv+Qw+Rt-Su-Tr+Us+Vp-Wq\\
h &= Pw-Qv+Ru+St-Ts-Ur+Vq+Wp
\end{aligned}$$

(Nachrechnen!) Diese Gleichungen führen auf die **Oktaven** $\mathbb{O}$ von CAYLEY (1821-1895). HURWITZ (1859-1919) hat gezeigt, dass es solche Gleichungen nur mit 1,2,4,8 Summanden geben kann. (Man braucht also nicht nach entsprechenden Formeln mit Summen von 16 Quadratzahlen zu suchen.)
(ii) GAUSS hat gezeigt, dass man ein $n\in\mathbb{N}$ genau dann *nicht* als Summe von höchstens 3 Quadratzahlen schreiben kann, wenn n die Form $n=4^km$ mit $k\in\mathbb{N}_0$ und $m\equiv 7 \pmod 8$ hat. Der Beweis ist schwieriger.
(iii) Man kann auf ähnliche Weise auch Gleichungen der Form $n=x_1^k+\ldots+x_r^k$ mit $k\geq 3$ untersuchen (WARING, 1736-1798); darauf gehen wir hier nicht ein.

12.6 Definition. Sind $x,y,z\in\mathbb{N}$ mit $x^2+y^2=z^2$, so heißt $(x,y,z)\in\mathbb{N}^3$ **pythagoräisches Tripel** (PYTHAGORAS, 569-475). Im Fall $\mathrm{ggT}(x,y,z)=1$ heißt (x,y,z) ein **primitives** pythagoräisches Tripel.

Bemerkung. (i) Für jedes pythagoräische Tripel (x,y,z) gilt:

$$\mathrm{ggT}(x,y,z)=1\Longleftrightarrow\mathrm{ggT}(x,y)=1\Longleftrightarrow\mathrm{ggT}(x,z)=1\Longleftrightarrow\mathrm{ggT}(y,z)=1.$$

(ii) Man erhält alle pythagoräischen Tripel aus den primitiven durch Multiplikation mit einem $m\in\mathbb{N}$.
(iii) Ist (x,y,z) ein primitives pythagoräisches Tripel, so ist entweder x oder y gerade; denn wegen $\mathrm{ggT}(x,y)=1$ können x,y nicht beide gerade sein. Wären x,y beide ungerade, so wäre $x^2\equiv 1\equiv y^2 \pmod 4$, d.h. $z^2\equiv 2 \pmod 4$. Widerspruch!

Satz. *Sei (x,y,z) ein primitives pythagoräisches Tripel und y gerade. Dann existieren $m,n\in\mathbb{N}$ mit $\mathrm{ggT}(m,n)=1$, $m>n$, $m\not\equiv n \pmod 2$ und*

$$x=m^2-n^2,\quad y=2mn,\quad z=m^2+n^2.$$

Umgekehrt liefern solche m,n stets ein primitives pythagoräisches Tripel (x,y,z), wobei y gerade ist.

Beweis. Sei (x, y, z) ein primitives pythagoräisches Tripel und y gerade. Dann ist $y^2 = z^2 - x^2 = (z + x)(z - x)$; dabei sind x, z ungerade, also $z + x, z - x$ gerade. Folglich ist $(\frac{y}{2})^2 = \frac{z+x}{2} \cdot \frac{z-x}{2}$ und $\mathrm{ggT}(\frac{z+x}{2}, \frac{z-x}{2}) \mid \mathrm{ggT}(x, z) = 1$. Daher sind $\frac{z+x}{2}$ und $\frac{z-x}{2}$ Quadratzahlen. Wir schreiben $\frac{z+x}{2} = m^2$ und $\frac{z-x}{2} = n^2$ mit $m, n \in \mathbb{N}$. Dann gilt: $m^2 - n^2 = x$, $y^2 = 2m^2 \cdot 2n^2 = 4m^2n^2$, d.h. $y = 2mn$, $m^2 + n^2 = z$, $\mathrm{ggT}(m, n) = 1$, $m > n$ und $m \not\equiv n \pmod 2$.
Seien umgekehrt $m, n \in \mathbb{N}$ mit $\mathrm{ggT}(m, n) = 1$, $m > n$ und $m \not\equiv n \pmod 2$. Wir setzen $x := m^2 - n^2$, $y := 2mn$, $z := m^2 + n^2$. Dann gilt:

$$x^2 + y^2 = m^4 - 2m^2n^2 + n^4 + 4m^2n^2 = m^4 + 2m^2n^2 + n^4 = z^2$$

und $\mathrm{ggT}(x, z) \mid \mathrm{ggT}(2m^2, 2n^2) \mid 2$. Wegen $m \not\equiv n \pmod 2$ ist x ungerade. Also sind x, z teilerfremd. Daher ist (x, y, z) ein primitives pythagoräisches Tripel, und y ist gerade.

Beispiel. Für $(m, n) = (2, 1), (3, 2), (4, 1), (4, 3), \ldots$ erhält man die primitiven pythagoräischen Tripel $(3, 4, 5), (5, 12, 13), (15, 8, 17), (7, 24, 25), \ldots$

12.7 Satz. *Es gibt keine $x, y, u \in \mathbb{N}$ mit $x^4 + y^4 = u^2$; insbesondere existieren keine $x, y, z \in \mathbb{N}$ mit $x^4 + y^4 = z^4$.*

Beweis. Wir nehmen an, dass $x, y, u \in \mathbb{N}$ mit $x^4 + y^4 = u^2$ existieren; dabei wählen wir u so klein wie möglich. Dann ist $d := \mathrm{ggT}(x, y) = 1$; denn sonst liefert die Division durch d einen Widerspruch zur Minimalität von u. Insbesondere ist x oder y ungerade.
Wären x, y beide ungerade, so hätte man den Widerspruch $u^2 \equiv x^4 + y^4 \equiv 1 + 1 \equiv 2 \pmod 4$.
Dieser Widerspruch zeigt: $x \not\equiv y \pmod 2$; o.B.d.A. sei x ungerade und y gerade. Dann ist (x^2, y^2, u) ein primitives pythagoräisches Tripel. Nach Satz 12.6 existieren also $a, b \in \mathbb{N}$ mit $x^2 = a^2 - b^2$, $y^2 = 2ab$, $u = a^2 + b^2$, $a > b$, $\mathrm{ggT}(a, b) = 1$ und $a \not\equiv b \pmod 2$.
Wäre a gerade und b ungerade, so hätte man den Widerspruch $x^2 \equiv -1 \pmod 4$.
Also ist a ungerade und b gerade, etwa $b = 2c$. Dann ist $y^2 = 4ac$, d.h. $(\frac{y}{2})^2 = ac$. Dabei ist $\mathrm{ggT}(a, c) = 1$ wegen $\mathrm{ggT}(a, b) = 1$. Folglich existieren $d, f \in \mathbb{N}$ mit $a = d^2$, $c = f^2$, $\mathrm{ggT}(d, f) = 1$ und d ungerade. Dann ist $x^2 = a^2 - b^2 = d^4 - 4f^4$, d.h. $x^2 + (2f^2)^2 = (d^2)^2$. Daher ist $(x, 2f^2, d^2)$ ein primitives pythagoräisches Tripel. Nach Satz 12.6 gibt es $l, m \in \mathbb{N}$ mit $x = l^2 - m^2$, $2f^2 = 2lm$, $d^2 = l^2 + m^2$ und $\mathrm{ggT}(l, m) = 1$. Wegen $f^2 = lm$ existieren $r, s \in \mathbb{N}$ mit $l = r^2$ und $m = s^2$. Dann ist $r^4 + s^4 = l^2 + m^2 = d^2$ mit $d \leq d^2 = a \leq a^2 < a^2 + b^2 = u$ im Widerspruch zur Minimalität von u.

13. ZUR FERMAT-VERMUTUNG

13.1 Bemerkung. In diesem Kapitel geht es um die Fermat-Vermutung für den Exponenten 3, d.h. die Gleichung

$$x^3 + y^3 = z^3$$

in $\mathbb{Z}$. Im folgenden sei $\zeta := \frac{-1+\sqrt{-3}}{2} \in \mathbb{C}$, also $\zeta^2 = \frac{-1-\sqrt{-3}}{2} = -\zeta - 1$ und $\zeta^3 = 1$. Dann ist

$$R := \mathbb{Z} + \mathbb{Z}\zeta = \{a + b\zeta : a, b \in \mathbb{Z}\}$$

ein Teilring von $\mathbb{C}$ und damit ein Integritätsbereich; denn für $a, b, c, d \in \mathbb{Z}$ gilt:

$$(a + b\zeta)(c + d\zeta) = (ac - bd) + (ad + bc - bd)\zeta \in R.$$

Analog ist $K := \mathbb{Q} + \mathbb{Q}\zeta = \{a + b\zeta : a, b \in \mathbb{Q}\}$ ein Teilring von $\mathbb{C}$. Wegen $\zeta = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$ und $\sqrt{-3} = 1 + 2\zeta$ ist auch

$$K = \mathbb{Q} + \mathbb{Q}\sqrt{-3} = \{x + y\sqrt{-3} : x, y \in \mathbb{Q}\}.$$

Ferner ist K sogar ein Körper; denn im Fall $x + y\sqrt{-3} \neq 0$ ist auch $0 \neq x - y\sqrt{-3}$ und damit $0 \neq (x + y\sqrt{-3})(x - y\sqrt{-3}) = x^2 + 3y^2$. Also ist

$$\frac{1}{x + y\sqrt{-3}} = \frac{x - y\sqrt{-3}}{x^2 + 3y^2} \in \mathbb{Q} + \mathbb{Q}\sqrt{-3} = K.$$

Die Abbildung $N : R \longrightarrow \mathbb{N}_0$, $\rho \longmapsto |\rho|^2 = \rho\overline{\rho}$, heißt **Norm**. Dann gilt für $\rho, \sigma \in R$ und $a, b \in \mathbb{Z}$: $N(\rho\sigma) = N(\rho)N(\sigma)$ und

$$N(a + b\zeta) = (a + b\zeta)(a + b\overline{\zeta}) = a^2 - ab + b^2 \in \mathbb{N}_0.$$

Satz. (Division mit Rest)
Zu $\alpha, \beta \in R$ mit $\beta \neq 0$ existieren stets $\kappa, \rho \in R$ mit $\alpha = \kappa\beta + \rho$ und $0 \leq N(\rho) < N(\beta)$.

Beweis. Wegen $\alpha, \beta \in K$ und $\beta \neq 0$ existieren $x, y \in \mathbb{Q}$ mit $\frac{\alpha}{\beta} = x + y\sqrt{-3}$. Wir wählen zunächst ein $v \in \mathbb{Z}$ mit $|y - \frac{v}{2}| \leq \frac{1}{4}$ und dann ein $u \in \mathbb{Z}$ mit $|x + \frac{v}{2} - u| \leq \frac{1}{2}$. Wir setzen $\kappa := u + v\zeta \in R$. Dann ist $\rho := \alpha - \kappa\beta \in R$ und

$$\frac{\rho}{\beta} = \frac{\alpha}{\beta} - \kappa = x + y\sqrt{-3} - u - v\frac{-1 + \sqrt{-3}}{2} = x - u + \frac{v}{2} + (y - \frac{v}{2})\sqrt{-3},$$

d.h. $|\frac{\rho}{\beta}|^2 = (x - u + \frac{v}{2})^2 + (y - \frac{v}{2})^2 3 \leq \frac{1}{4} + \frac{3}{16} = \frac{7}{16} < 1$. Also ist $0 \leq N(\rho) < N(\beta)$.

13.2 Satz. *Zu jedem Ideal I in R existiert ein $\alpha \in R$ mit $I = (\alpha)$.*

Beweis. O.B.d.A. sei $I \neq \{0\} = (0)$. Dann ist $\emptyset \neq \{N(\alpha) : 0 \neq \alpha \in I\} =: M \subseteq \mathbb{N}$. Sei $0 \neq \alpha \in I$ mit $N(\alpha) = \min(M)$. Dann ist $(\alpha) \subseteq I$.
Ist $\beta \in I$ beliebig, so liefert die Division mit Rest Elemente $\kappa, \rho \in R$ mit $\beta = \kappa\alpha + \rho$ und $0 \leq N(\rho) < N(\alpha)$.
Im Fall $\rho \neq 0$ wäre $\rho = \beta - \kappa\alpha \in I$, im Widerspruch zur Wahl von α.
Also ist $\rho = 0$ und damit $\beta = \kappa\alpha \in (\alpha)$. Insgesamt ist also $I = (\alpha)$.

13.3 Satz. *Für $\alpha, \beta \in R$ gilt: $(\beta) \subseteq (\alpha) \Longleftrightarrow \exists \rho \in R : \beta = \rho\alpha$.*

Beweis. "$\Longrightarrow$": Sei $(\beta) \subseteq (\alpha)$. Wegen $\beta = 1\beta \in (\beta) \subseteq (\alpha)$ existiert ein $\rho \in R$ mit $\beta = \rho\alpha$.
"$\Longleftarrow$": Sei $\rho \in R$ mit $\beta = \rho\alpha$. Dann ist $(\beta) = (\rho\alpha) \subseteq (\alpha)$.

Definition. Ggf. sagt man: α **teilt** β, α ist ein **Teiler** von β, β ist **Vielfaches** von α, usw. Man schreibt: $\alpha \mid \beta$.

Bemerkung. Wie in $\mathbb{Z}$ zeigt man, dass für $\alpha, \beta, \gamma, \rho, \sigma \in R$ gilt:
(i) $1 \mid \alpha$, $\alpha \mid \alpha$, $\alpha \mid 0$;
(ii) $0 \mid \alpha \Longleftrightarrow \alpha = 0$;
(iii) $\alpha \mid 1 \Longleftrightarrow \alpha \in R^\times$;
(iv) $\alpha \mid \beta \wedge \epsilon, \eta \in R^\times \Longrightarrow \epsilon\alpha \mid \eta\beta$;
(v) $\alpha \mid \beta \wedge \beta \mid \gamma \Longrightarrow \alpha \mid \gamma$;
(vi) $\alpha \mid \beta \wedge \alpha \mid \gamma \Longrightarrow \alpha \mid \rho\beta + \sigma\gamma$.

13.4 Satz. *Für $\alpha, \beta \in R$ sind äquivalent:*
(1) $\alpha \mid \beta \wedge \beta \mid \alpha$*;*
(2) $\alpha \mid \beta \wedge N(\alpha) = N(\beta)$*;*
(3) $\exists \epsilon \in R^\times : \beta = \epsilon\alpha$*;*
(4) $(\alpha) = (\beta)$.

Definition. Ggf. heißen α, β **assoziiert** ($\alpha \sim \beta$).

Beweis. (1) $\Longleftrightarrow$ (4): Dies folgt aus Satz 13.3.
(1) $\Longrightarrow$ (2): Sei $\alpha \mid \beta$ und $\beta \mid \alpha$. Wir schreiben $\beta = \rho\alpha$ mit $\rho \in R$.
Im Fall $\alpha = 0$ ist auch $\beta = 0$, d.h. $N(\alpha) = 0 = N(\beta)$.
Sei also $\alpha \neq 0$ und analog $\beta \neq 0$. Dann ist $\rho \neq 0$ und $N(\beta) = N(\rho)N(\alpha) \geq N(\alpha)$. Analog ist $N(\alpha) \geq N(\beta)$.
(2) $\Longrightarrow$ (3): Sei $\alpha \mid \beta$ und $N(\alpha) = N(\beta)$. Wir schreiben $\beta = \rho\alpha$ mit $\rho \in R$. Dann ist $N(\alpha) = N(\beta) = N(\rho)N(\alpha)$.
Im Fall $\alpha = 0$ ist auch $\beta = 0$ und daher $\beta = 1\alpha$ mit $1 \in R^\times$.
Sei also $\alpha \neq 0$, d.h. $N(\alpha) \neq 0$. Dann ist $1 = N(\rho) = \rho\overline{\rho}$. Dabei ist $\overline{\rho} \in R$ wegen $\overline{\zeta} = \zeta^2 \in R$. Also ist $\rho \in R^\times$ und $\beta = \rho\alpha$.
(3) $\Longrightarrow$ (4): Sei $\epsilon \in R^\times$ mit $\beta = \epsilon\alpha$. Dann ist $(\beta) = (\epsilon\alpha) \subseteq (\alpha)$. Wegen $\alpha = \epsilon^{-1}\beta$ ist analog $(\alpha) \subseteq (\beta)$.

Bemerkung. (i) $\sim$ ist eine Äquivalenzrelation auf R.
(ii) Für $\alpha, \alpha', \beta, \beta' \in R$ mit $\alpha \sim \alpha'$ und $\beta \sim \beta'$ gilt: $\alpha \mid \beta \Longleftrightarrow \alpha' \mid \beta'$.

13.5 Satz. $R^\times = \{\alpha \in R : \alpha \mid 1\} = \{\alpha \in R : \alpha \sim 1\} = \{\alpha \in R : N(\alpha) = 1\} = \{\pm 1, \pm\zeta, \pm\zeta^2\}$.

Beweis. (i) Sei $\alpha \in R^\times$. Dann gilt: $\alpha \mid 1$ nach Bemerkung 13.3.
(ii) Sei $\alpha \in R$ mit $\alpha \mid 1$. Wegen $1 \mid \alpha$ folgt dann: $\alpha \sim 1$.
(iii) Sei $\alpha \in R$ mit $\alpha \sim 1$. Nach Satz 13.4 ist dann $N(\alpha) = N(1) = 1$.
(iv) Sei $\alpha \in R$ mit $N(\alpha) = 1$. Wir schreiben $\alpha = a + b\zeta$ mit $a, b \in \mathbb{Z}$. Dann gilt:

$$1 = N(a + b\zeta) = a^2 - ab + b^2 = (a - \frac{b}{2})^2 + \frac{3}{4}b^2.$$

Folglich ist $|b| \leq 1$. Im Fall $b = 0$ ist $\alpha = a = \pm 1$.
Im Fall $b = 1$ ist $(a - \frac{1}{2})^2 = \frac{1}{4}$, d.h. $a - \frac{1}{2} = \pm\frac{1}{2}$ und damit $a \in \{0, 1\}$. Daher ist $\alpha = \zeta$ oder $\alpha = 1 + \zeta = -\zeta^2$.
Im Fall $b = -1$ ist $(a + \frac{1}{2})^2 = \frac{1}{4}$, d.h. $a + \frac{1}{2} = \pm\frac{1}{2}$ und damit $a \in \{0, -1\}$. Daher ist $\alpha = -\zeta$ oder $\alpha = -1 - \zeta = \zeta^2$.

(v) Sicher sind $\pm 1, \pm\zeta, \pm\zeta^2 \in R^\times$.

13.6 Satz. *Sei $0 \neq \pi \in R \setminus R^\times$. Dann sind äquivalent:*
(1) *Für alle $\alpha, \beta \in R$ gilt: $\pi \mid \alpha\beta \Longrightarrow \pi \mid \alpha \vee \pi \mid \beta$;*
(2) *Für alle $\alpha, \beta \in R$ gilt: $\pi = \alpha\beta \Longrightarrow \alpha \in R^\times \vee \beta \in R^\times$.*

Definition. Ggf. heißt π **Primelement** in R.

Beweis. (1) $\Longrightarrow$ (2): Sei (1) erfüllt und $\pi = \alpha\beta$ mit $\alpha, \beta \in R$. Dann gilt: $\pi \mid \alpha$ oder $\pi \mid \beta$; o.B.d.A. sei $\pi \mid \alpha$. Wegen $\alpha \mid \pi$ folgt $\alpha \sim \pi$, d.h. $\pi = \epsilon\alpha$ für ein $\epsilon \in R^\times$. Dann ist $0 = \pi - \pi = \alpha\beta - \alpha\epsilon = \alpha(\beta - \epsilon)$; dabei ist $\alpha \neq 0$ wegen $\pi \neq 0$. Also ist $\beta = \epsilon \in R^\times$.
(2) $\Longrightarrow$ (1): Sei (2) erfüllt, und seien $\alpha, \beta \in R$ mit $\pi \mid \alpha\beta$. Dann ist

$$I := \{\rho\pi + \sigma\alpha : \rho, \sigma \in R\}$$

ein Ideal in R. Nach Satz 13.2 existiert ein $\delta \in R$ mit $I = (\delta)$. Wegen $\pi \in I = (\delta)$ existiert ein $\gamma \in R$ mit $\pi = \gamma\delta$. Wegen (2) ist $\gamma \in R^\times$ oder $\delta \in R^\times$.
Im Fall $\gamma \in R^\times$ ist $\pi \sim \delta$, also $(\alpha) \subseteq I = (\delta) = (\pi)$, d.h. $\pi \mid \alpha$.
Im Fall $\delta \in R^\times$ ist $1 = \delta^{-1}\delta \in (\delta) = I$. Schreibt man $1 = \rho\pi + \sigma\alpha$ mit $\rho, \sigma \in R$, so gilt: $\pi \mid \rho\pi\beta + \sigma\alpha\beta = 1\beta = \beta$.

Bemerkung. Mit π ist auch jedes zu π assoziierte Element in R ein Primelement in R.

Beispiel. (i) $\sqrt{-3}$ ist ein Primelement in R; denn sind $\alpha, \beta \in R$ mit $\sqrt{-3} = \alpha\beta$, so ist $3 = N(\sqrt{-3}) = N(\alpha)N(\beta)$ mit $N(\alpha), N(\beta) \in \mathbb{N}$. Daher ist $N(\alpha) = 1$ oder $N(\beta) = 1$, d.h. $\alpha \in R^\times$ oder $\beta \in R^\times$.
(ii) Wegen $\lambda := 1 - \zeta = \zeta^2\sqrt{-3}$ ist auch λ ein Primelement in R. Dabei gilt: $\lambda^2 = -\zeta^4 3 = -3\zeta$.

13.7 Satz. (Eindeutige Primfaktorzerlegung)
Sei $0 \neq \alpha \in R \setminus R^\times$. Dann existieren Primelemente $\pi_1, \ldots, \pi_r \in R$ mit $\alpha = \pi_1 \ldots \pi_r$. Sind auch $\rho_1, \ldots, \rho_s \in R$ Primelemente mit $\alpha = \rho_1 \ldots \rho_s$, so ist $r = s$, und nach geeigneter Umnummerierung gilt: $\pi_i \sim \rho_i$ für $i = 1, \ldots, r$.

Beweis. Wir nehmen an, dass es ein Element $0 \neq \alpha \in R \setminus R^\times$ gibt, das sich nicht als Produkt von Primelementen schreiben lässt. Dann ist $N(\alpha) \in \mathbb{N}$; o.B.d.A. sei $N(\alpha)$ dabei so klein wie möglich. Sicher ist α kein Primelement. Daher existieren $\beta, \gamma \in R \setminus R^\times$ mit $\alpha = \beta\gamma$. Dann ist $0 \neq N(\alpha) = N(\beta)N(\gamma)$ mit $N(\beta) \neq 1 \neq N(\gamma)$. Daher ist $N(\beta) < N(\alpha)$ und $N(\gamma) < N(\alpha)$. Nach Wahl von α sind β, γ Produkte von Primelementen, also auch α. Mit diesem Widerspruch ist die erste Aussage gezeigt.
Sei jetzt $\pi_1 \ldots \pi_r = \rho_1 \ldots \rho_s$ mit Primelementen $\pi_1, \ldots, \pi_r, \rho_1, \ldots, \rho_s \in R$. Wir machen Induktion nach r. Im Fall $r = 1$ ist $\pi_1 = \rho_1 \ldots \rho_s$. Da π_1 ein Primelement ist, folgt $s = 1$ und damit $\pi_1 = \rho_1$.
Sei also $r > 1$. Dann gilt: $\pi_1 \mid \pi_1 \ldots \pi_r = \rho_1 \ldots \rho_s$. Da π_1 ein Primelement ist, folgt: $\pi_1 \mid \rho_j$ für ein $j \in \{1, \ldots, s\}$. O.B.d.A. sei $\pi_1 \mid \rho_1$. Da ρ_1 ein Primelement ist, folgt: $\pi_1 \sim \rho_1$, d.h. $\rho_1 = \epsilon\pi_1$ für ein $\epsilon \in R^\times$. Dann ist $\epsilon\rho_2$ ein Primelement in R, und $\pi_2 \ldots \pi_r = \epsilon\rho_2 \ldots \rho_s$. Nach Induktion ist $r - 1 = s - 1$, und nach geeigneter Umnummerierung ist $\pi_2 \sim \epsilon\rho_2$ und $\pi_3 \sim \rho_3, \ldots, \pi_r \sim \rho_r$. Die Behauptung folgt.

13.8 Bemerkung. Nach Beispiel 13.6 ist $\lambda := 1-\zeta \sim \sqrt{-3}$ ein Primelement in R. Daher ist $\lambda^2 \sim -3 \sim 3$ und

$$\begin{aligned} R/(\lambda) &= \{\rho + (\lambda) : \rho \in R\} = \{a + b\zeta + (\lambda) : a, b \in \mathbb{Z}\} \\ &= \{a + b + (\lambda) : a, b \in \mathbb{Z}\} = \{z + (\lambda) : z \in \mathbb{Z}\} = \{0 + (\lambda), \pm 1 + (\lambda)\}. \end{aligned}$$

Für $\tau \in R$ und $\sigma := 1 + \lambda\tau$ gilt:

$$\begin{aligned} \sigma^3 - 1 &= (\sigma - 1)(\sigma - \zeta)(\sigma - \zeta^2) = \lambda\tau(1 + \lambda\tau - \zeta)(1 + \lambda\tau - \zeta^2) \\ &= \lambda\tau(\lambda + \lambda\tau)(\lambda(1 + \zeta) + \lambda\tau) = \lambda^3\tau(1 + \tau)(\tau - \zeta^2) \end{aligned}$$

mit $\zeta^2 \equiv 1 \pmod{(\lambda)}$. Wegen $\tau + (\lambda) \in \{0 + (\lambda), \pm 1 + (\lambda)\}$ folgt: $\lambda^4 \mid \sigma^3 - 1$, d.h.

$$\sigma^3 \equiv 1 \pmod{\lambda^4} \quad \text{und} \quad (-\sigma)^3 \equiv -1 \pmod{\lambda^4}.$$

Satz. *Es gibt keine $\alpha, \beta, \gamma \in R \setminus \{0\}$, $\epsilon \in R^\times$ mit $\alpha^3 + \beta^3 = \epsilon\gamma^3$.*

Bemerkung. Insbesondere existieren keine $x, y, z \in \mathbb{Z} \setminus \{0\}$ mit $x^3 + y^3 = z^3$.

Beweis. Wir nehmen an, dass $\alpha, \beta, \gamma, \epsilon$ doch existieren. O.B.d.A. seien dabei α, β *teilerfremd*, d.h. es gibt kein Primelement $\pi \in R$ mit $\pi \mid \alpha$ und $\pi \mid \beta$.
Wir betrachten zunächst den Fall $\lambda \mid \alpha\beta$, d.h. $\lambda \mid \alpha$ oder $\lambda \mid \beta$. [Diesen Fall führen wir auf den Fall $\lambda \nmid \alpha\beta$ zurück.] O.B.d.A. sei $\lambda \mid \alpha$. [Sonst vertauschen wir α und β.] Dann gilt: $\lambda \nmid \beta$ und $\lambda \nmid \gamma$. Die obige Bemerkung impliziert:

$$\pm\epsilon \equiv \epsilon\gamma^3 \equiv \alpha^3 + \beta^3 \equiv \pm 1 \pmod{\lambda^2},$$

d.h. $3 \sim \lambda^2 \mid \epsilon \pm 1$. Wegen $R^\times = \{\pm 1, \pm\zeta, \pm\zeta^2 = \mp(\zeta + 1)\}$ ist also $\epsilon = \pm 1$. Daher ist $(\pm\gamma)^3 + (-\beta)^3 = \alpha^3$; dabei sind $\pm\gamma, \pm\beta \in R$ teilerfremd, und $\lambda \nmid (\pm\gamma)(-\beta)$. [Damit ist die Zurückführung geschafft.]
Im Folgenden sei also o.B.d.A. $\lambda \nmid \alpha\beta$. Unter allen Gegenbeispielen wählen wir $\alpha, \beta, \gamma, \epsilon$ so, dass

$$t := v(\gamma) := \max\{n \in \mathbb{N}_0 : \lambda^n \mid \gamma\}$$

so klein wie möglich ist [und außerdem α, β teilerfremd mit $\lambda \nmid \alpha\beta$ sind]. Wir unterscheiden drei Fälle.
Fall 1: $t = 0$, d.h. $\lambda \nmid \gamma$.
Nach der Bemerkung ist $\pm 1 \pm 1 \equiv \alpha^3 + \beta^3 = \epsilon\gamma^3 \equiv \pm\epsilon \pmod{\lambda^4}$. Wegen $\lambda^4 \sim 3^2 = 9 \nmid \epsilon$ folgt: $\epsilon \equiv \pm 2 \pmod 9$. Wir schreiben $\epsilon \mp 2 = 9(a + b\zeta)$ mit $a, b \in \mathbb{Z}$. Einsetzen von $\pm 1, \pm\zeta, \pm\zeta^2 = \mp(\zeta + 1)$ für ϵ liefert jeweils einen Widerspruch.
Fall 2: $t = 1$, d.h. $\lambda^2 \nmid \gamma$; insbesondere ist dann $\lambda^4 \nmid \gamma^3$.
Nach der Bemerkung ist $\epsilon\gamma^3 \equiv \alpha^3 + \beta^3 \equiv \pm 1 \pm 1 \equiv \pm 2 \pmod{\lambda^4}$, d.h. $\pm 2 \equiv \epsilon\gamma^3 \equiv 0 \pmod{\lambda^2}$ und damit $3 \sim \lambda^2 \mid 2$. Widerspruch!
Fall 3: $t \geq 2$.
Es genügt, ein Gegenbeispiel $\alpha', \beta', \gamma', \epsilon'$ mit $v(\gamma') < v(\gamma)$ zu konstruieren [wobei auch α', β' teilerfremd mit $\lambda \nmid \alpha'\beta'$ sind]. Wegen

$$(\alpha + \beta)(\alpha + \zeta\beta)(\alpha + \zeta^2\beta) = \ldots = \alpha^3 + \beta^3 = \epsilon\gamma^3$$

und $v(\epsilon\gamma^3) = 3v(\gamma) = 3t \geq 6$ ist $v(\alpha+\beta) \geq 2$ oder $v(\alpha+\zeta\beta) \geq 2$ oder $v(\alpha+\zeta^2\beta) \geq 2$. O.B.d.A. sei $v(\alpha+\beta) \geq 2$. [Sonst ersetzen wir β durch $\zeta\beta$ bzw. $\zeta^2\beta$.] Wegen $v(\lambda\beta) = 1$ folgt:

$$v(\alpha+\zeta\beta) = v(\alpha+\beta-(1-\zeta)\beta) = v(\alpha+\beta-\lambda\beta) = 1.$$

Analog ist $v(\alpha+\zeta^2\beta) = v(\alpha+\beta-(1-\zeta^2)\beta) = v(\alpha+\beta-(1-\zeta)(1+\zeta)\beta) = v(\alpha+\beta+\lambda\zeta^2\beta) = 1$. Also ist $v(\alpha+\beta) = 3v(\gamma) - 2 = 3t-2 \geq 4$. Im Folgenden sei $\pi \in R$ ein Primelement mit $\pi \not\sim \lambda$.

Wir nehmen an, dass gilt: $\pi \mid \alpha+\beta$ und $\pi \mid \alpha+\zeta\beta$. Dann ist $\pi \mid (1-\zeta)\beta = \lambda\beta$, d.h. $\pi \mid \beta$ und damit $\pi \mid \alpha$. Dies ist ein Widerspruch, da α, β teilerfremd sind.

Analog widerlegt man die Annahme $\pi \mid \alpha+\beta$ und $\pi \mid \alpha+\zeta^2\beta$ sowie die Annahme $\pi \mid \alpha+\zeta\beta$ und $\pi \mid \alpha+\zeta^2\beta$. Wegen der eindeutigen Primfaktorzerlegung in R existieren also paarweise teilerfremde Elemente $\rho, \sigma, \tau \in R$ sowie Einheiten $\epsilon_1, \epsilon_2, \epsilon_3 \in R^\times$ mit

$$(*) \qquad \alpha+\beta = \epsilon_1\rho^3\lambda^{3t-2},\ \alpha+\zeta\beta = \epsilon_2\sigma^3\lambda,\ \alpha+\zeta^2\beta = \epsilon_3\tau^3\lambda,\ \lambda \nmid \rho\sigma\tau.$$

Wir multiplizieren die erste Gleichung in $(*)$ mit 1, die zweite mit ζ, die dritte mit ζ^2, addieren und erhalten:

$$0 = \epsilon_1\rho^3\lambda^{3t-2} + \zeta\epsilon_2\sigma^3\lambda + \zeta^2\epsilon_3\tau^3\lambda.$$

Division durch λ ergibt: $0 = \epsilon_1\rho^3\lambda^{3(t-1)} + \zeta\epsilon_2\sigma^3 + \zeta^2\epsilon_3\tau^3$. Mit $\alpha_1 := \sigma$, $\beta_1 := \tau$, $\gamma_1 := \rho\lambda^{t-1}$ und geeigneten $\eta_1, \eta_2 \in R^\times$ gilt dann:

$$\alpha_1^3 + \eta_1\beta_1^3 = \eta_2\gamma_1^3.$$

Daher ist $0 \equiv \eta_2\gamma_1^3 \equiv \pm 1 \pm \eta_1 \pmod{\lambda^2}$, d.h. $3 \sim \lambda^2 \mid \pm 1 \pm \eta_1$. Wegen $R^\times = \{\pm 1, \pm\zeta, \pm\zeta^2 = \mp(\zeta+1)\}$ folgt: $\eta_1 = \pm 1$. Also ist

$$\alpha_1^3 + (\pm\beta_1)^3 = \eta_2\gamma_1^3,$$

wobei $\alpha_1, \beta_1 \in R$ teilerfremd mit $\lambda \nmid \alpha_1\beta_1$ und $\gamma_1 \in R$ mit $v(\gamma_1) = t-1 < t$ sind. Die Behauptung folgt.

LITERATUR

A. Bartholmé, J. Rung und H. Kern, *Zahlentheorie für Einsteiger*, Vieweg und Teubner, 2010

P. Bundschuh, *Einführung in die Zahlentheorie*, Springer-Verlag, 1996

K. Ireland and M. Rosen, *A classical introduction to modern number theory*, Springer-Verlag, 1990

E. Krätzel, *Zahlentheorie*, VEB Deutscher Verlag der Wissenschaften, 1981

A. Leutbecher, *Zahlentheorie - Eine Einführung in die Algebra*, Springer-Verlag, 1996

H. Menzer, *Zahlentheorie*, Oldenbourg-Verlag, 2010

S. Müller-Stach und J. Piontkowski, *Elementare und algebraische Zahlentheorie*, Vieweg, 2006

R. Remmert und P. Ullrich, *Elementare Zahlentheorie*, Birkhäuser-Verlag, 1995

H. Scheid und A. Frommer, *Zahlentheorie*, Spektrum Akademischer Verlag, 2007

J. Wolfart, *Einführung in die Zahlentheorie und Algebra*, Vieweg und Teubner, 2009