

Logik und Diskrete Strukturen

Kapitel 3: Zahlentheorie und Arithmetik

Prof. Dr. Jasmin Blanchette

Lehr- und Forschungseinheit für Theoretische Informatik und Theorembeweisen

Sommersemester 2026

Basierend auf Folien von PD Dr. Jan Johannsen

Übersicht

Teilbarkeit und Primzahlen
Der euklidische Algorithmus
Restklassen
Der chinesische Restesatz

Ganzzahlige Division mit Rest

Für alle $a, b \in \mathbb{Z}$ mit $b \neq 0$ gibt es eindeutig bestimmte $q, r \in \mathbb{Z}$ mit

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

Notation: $q = \lfloor a/b \rfloor$ und $r = a \bmod b$

Für $a, b \in \mathbb{Z}$ ist definiert:

$$b \mid a \quad \text{gdw.} \quad a \bmod b = 0 \quad \text{gdw.} \quad a = q \cdot b \quad \text{für ein } q \in \mathbb{Z}$$

Jedes $a \in \mathbb{Z}$ mit $a \mid b$ ist ein **Teiler** von b .

Für alle $a \in \mathbb{Z}$ gilt $1 \mid a$ und $a \mid a$.

Auf \mathbb{N} ist die Relation \mid eine partielle Ordnung.

ggT und kgV

Für $a, b \in \mathbb{Z}$ definiere

- ▶ **größter gemeinsamer Teiler:** $ggT(a, b) := \max \{k \in \mathbb{N} \mid k \mid a \text{ und } k \mid b\}$
- ▶ **kleinstes gemeinsames Vielfaches:** $kgV(a, b) := \min \{k \in \mathbb{N} \mid a \mid k \text{ und } b \mid k\}$

Theorem (Lemma von Bézout)

Für $a, b \in \mathbb{Z}$ gibt es $s, t \in \mathbb{Z}$, sodass gilt:

$$ggT(a, b) = sa + tb$$

Damit folgt: $ggT(a, b)$ und $kgV(a, b)$ sind Infimum und Supremum von a, b in der Ordnung \mid .

Also ist \mathbb{N} mit der Ordnung \mid ein Verband.

Lemma von Bézout

Theorem (Lemma von Bézout)

Für $a, b \in \mathbb{Z}$ gibt es $s, t \in \mathbb{Z}$, sodass gilt:

$$\text{ggT}(a, b) = sa + tb$$

Beweis.

Wenn $a = 0$ oder $b = 0$ ist der Beweis trivial. Wir nehmen an, dass $a, b > 0$ gilt.

Sei $d > 0$ die kleinste natürliche Zahl von der Form $d = sa + tb$, für $s, t \in \mathbb{Z}$.

Es gilt $\text{ggT}(a, b) \mid a$ und $\text{ggT}(a, b) \mid b$. Daher $\text{ggT}(a, b) \mid sa + tb$ und $\text{ggT}(a, b) \mid d$.

Daher $\text{ggT}(a, b) \leq d$.

Es gibt $q, r \in \mathbb{Z}$ mit $0 \leq r < d$, sodass $a = qd + r$.

Dann ist $r = a - qd = a - q(sa + tb) = (a - qsa) - tqb = (1 - qs)a - tqb$.

Wegen der Minimalität von d kann r nur 0 sein. Das heißt, $d \mid a$.

Analog folgt, dass $d \mid b$. Damit ist $d \leq \text{ggT}(a, b)$.

Also $d = \text{ggT}(a, b)$.



Primzahlen

Eine Zahl $p \in \mathbb{N}$ mit $p \geq 2$ heißt **Primzahl**, wenn gilt:

$$a \mid p \text{ gilt nur für } a = 1 \text{ oder } a = p$$

Die ersten Primzahlen sind 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59.

Theorem von Euklid

Theorem (Euklid)

Es gibt unendlich viele Primzahlen.

Beweis.

Sei $P := \{p \in \mathbb{N} \mid p \text{ is prim}\}$.

Nehmen wir an, dass P endlich ist. Sei $n := |P|$.

Seien p_1, \dots, p_n alle Primzahlen.

Wir setzen $N := p_1 \cdot \dots \cdot p_n + 1$.

Da $N \bmod p_i = 1$, gilt $p_i \nmid N$ für alle $i \in \{1, \dots, n\}$.

Nach Beispiel in Kapitel 1 muss N ein Produkt von Primzahlen sein.

Diese sind aber nicht Teil von P . Widerspruch. □

Lemma von Euklid

Lemma (Euklid)

Für alle Primzahlen p und $a, b \in \mathbb{N}$ gilt:
Falls $p \mid a \cdot b$, dann $p \mid a$ oder $p \mid b$.

Beweis.

Sei $p \mid ab$, aber $p \nmid a$. Wir müssen zeigen, dass $p \mid b$.

Da $p \nmid a$, gilt $\text{ggT}(p, a) = 1$.

Durch das Lemma von Bézout gibt es $s, t \in \mathbb{Z}$, sodass $1 = sp + ta$.

Also $b = spb + tab$.

Da $p \mid ab$, ist $ab = cp$ für ein $c \in \mathbb{N}$.

$b = spb + tcp = p(sb + tc)$.

Somit $p \mid b$. □

Sieb des Erathosthenes

Algorithmus zur Berechnung der Primzahlen bis n

Liste := $[2, 3, 4, \dots, n]$

repeat

p := erstes unmarkiertes und nicht gestrichenes Element der Liste

 markiere p

 striche alle Vielfachen von p

until $p > \sqrt{n}$

Beispiel:

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

Fundamentalsatz der Arithmetik

Theorem (Fundamentalsatz der Arithmetik)

Für alle $n \in \mathbb{N} \setminus \{0\}$ gilt:

1. n ist Produkt von Primzahlen.
2. Die Primfaktorzerlegung von n ist bis auf die Reihenfolge der Faktoren eindeutig.

Beweis.

Punkt 1 wurde in Kapitel 1 gezeigt. Wir zeigen jetzt Punkt 2.

Sei $n \geq 2$ die kleinste natürliche Zahl mit zwei verschiedenen Primfaktorzerlegungen:

$$n = p_1^{c_1} \cdot \dots \cdot p_k^{c_k} = q_1^{d_1} \cdot \dots \cdot q_\ell^{d_\ell}.$$

Da $p_1 \mid n$, gilt nach dem Lemma von Euklid, dass $p_1 \mid q_i^{d_i}$ für ein i . Also $p_1 = q_i$.

$$\text{Dann ist } n/p_1 = p_1^{c_1-1} \cdot p_2^{c_2} \cdot \dots \cdot p_k^{c_k} = q_1^{d_1} \cdot \dots \cdot q_{i-1}^{d_{i-1}} \cdot q_i^{d_i-1} \cdot q_{i+1}^{d_{i+1}} \cdot \dots \cdot q_\ell^{d_\ell}.$$

Also ist $n/p_1 < n$ auch eine Zahl mit zwei verschiedenen Primfaktorzerlegungen.

Widerspruch zur Minimalität. □

Primzahlsatz

Definition: $\pi(n) := |\{p \in \mathbb{N} \mid p \leq n \text{ und } p \text{ ist Primzahl}\}|$

Es ist $\pi(10) = 4$, $\pi(20) = 8$, $\pi(30) = 10$, $\pi(100) = 25$.

Theorem (Primzahlsatz)

$$\pi(n) \sim n/\ln n, \quad \text{d.h.} \quad \lim_{n \rightarrow \infty} \frac{\pi(n)}{n/\ln n} = 1.$$

Der euklidische Algorithmus

Eingabe: $m, n \in \mathbb{N}$ mit $m \leq n$

Ausgabe: $ggT(m, n)$

Euklid(m, n)

if $m = 0$ then

return n

else if $m \mid n$ then

return m

else

return Euklid($n \bmod m, m$)

Korrektheit des euklidischen Algorithmus

Lemma

Sind $m, n \in \mathbb{N}$ mit $m \leq n$ und $m \nmid n$, so gilt:

$$\text{ggT}(m, n) = \text{ggT}(n \bmod m, m)$$

Beweis.

Seien $q := \lfloor n/m \rfloor$ und $r := n \bmod m$. Dann gilt $n = qm + r$.

Offensichtlich gilt $\text{ggT}(m, n) \mid m$ und $\text{ggT}(m, n) \mid n$.

Zudem gilt $\text{ggT}(m, n) \mid r$, denn $r = n - qm$.

Daher $\text{ggT}(m, n) \mid \text{ggT}(r, m)$.

Offensichtlich gilt $\text{ggT}(r, m) \mid r$ und $\text{ggT}(r, m) \mid m$.

Zudem gilt $\text{ggT}(r, m) \mid n$, denn $n = qm + r$.

Daher $\text{ggT}(r, m) \mid \text{ggT}(m, n)$.

Wegen der Antisymmetrie von \mid gilt $\text{ggT}(r, m) = \text{ggT}(m, n)$. □

Der erweiterte euklidische Algorithmus

Eingabe: $m, n \in \mathbb{N}$ mit $m \leq n$

Ausgabe: $s, t \in \mathbb{Z}$ mit $\text{ggT}(m, n) = sm + tn$

ErwEuklid(m, n)

if $m = 0$ then

return $(0, 1)$

else if $m \mid n$ then

return $(1, 0)$

else

$(s', t') := \text{ErwEuklid}(n \bmod m, m)$

$s = t' - s' \lfloor n/m \rfloor$

$t = s'$

return (s, t)

Korrektheit des erweiterten euklidischen Algorithmus

Lemma

Der Algorithmus berechnet für $m, n \in \mathbb{N}$ mit $m \leq n$ Zahlen $s, t \in \mathbb{Z}$ mit $\text{ggT}(m, n) = sm + tn$.

Beweis (durch vollständige Induktion über die Anzahl der rekursiven Aufrufe).

- ▶ **Induktionsanfang:** 0 rekursive Aufrufe.

Dann ist $m = 0$ oder $m \mid n$, und $\text{ggT}(m, n) = 0m + 1n$ oder $\text{ggT}(m, n) = 1m + 0n$.

- ▶ **Induktionsschritt:** $k + 1$ rekursive Aufrufe.

Dann ist $m \nmid n$ und n von der Form $qm + r$, mit $q = \lfloor n/m \rfloor$ und $r = n \bmod m$.

Wir müssen zeigen, dass $s, t \in \mathbb{Z}$ mit $\text{ggT}(m, n) = sm + tn$, unter Verwendung der Induktionshypothese, dass es $s', t' \in \mathbb{Z}$ mit $\text{ggT}(r, m) = s'r + t'm$ gibt.

Durch die Induktionshypothese und das letzte Lemma gilt

$$\begin{aligned}\text{ggT}(m, n) &= \text{ggT}(r, m) = s'r + t'm \\ &= s'(n - qm) + t'm = s'n - s'qm + t'm = (t' - s'q)m + s'n.\end{aligned}$$

Der Algorithmus setzt s zu $t' - s'q$ und t zu s' .



Ende der 4. Vorlesung

Modulare Arithmetik

Definiere die Äquivalenzrelation

$$a \equiv b \pmod{m} \quad \text{gdw.} \quad m \mid a - b$$

Die Äquivalenzklassen sind die **Restklassen** modulo m .

Vertretersystem: $\mathbb{Z}_m = \{0, 1, \dots, m - 1\}$

Modulare Arithmetik

Lemma

Die folgenden Aussagen sind äquivalent:

1. $a \equiv b \pmod{m}$
2. $a = b + t \cdot m$ für ein $t \in \mathbb{Z}$
3. $a \bmod m = b \bmod m$

Beweis.

- ▶ **1 \rightarrow 2:** $m \mid (a - b)$. Daher gibt es ein $t \in \mathbb{Z}$, sodass $a - b = tm$. Somit $a = b + tm$.
- ▶ **2 \rightarrow 3:** Es gibt $q, r \in \mathbb{Z}$, sodass $b = qm + r$ und $r = b \bmod m$.
Daher $a = qm + tm + r = (q + t)m + r$. Somit $r = a \bmod m$.
- ▶ **3 \rightarrow 1:** Es gibt $q_1, q_2, r \in \mathbb{Z}$, sodass $a = q_1m + r$ und $b = q_2m + r$.
Daher $a - b = q_1m - q_2m + r - r = (q_1 - q_2)m$. Somit $m \mid (a - b)$.



Modulares Rechnen

Lemma

Für alle $a, b, m \in \mathbb{Z}$ mit $m \geq 1$ gilt:

$$(a + b) \bmod m = (a \bmod m + b \bmod m) \bmod m$$

Beweis.

Es gibt $q_1, q_2, r_1, r_2 \in \mathbb{Z}$, sodass
$$\begin{cases} a = q_1 m + r_1 & \text{mit } r_1 = a \bmod m \\ b = q_2 m + r_2 & \text{mit } r_2 = b \bmod m \end{cases}$$

$$\begin{aligned} & (a + b) \bmod m \\ &= (q_1 m + r_1 + q_2 m + r_2) \bmod m \\ &= ((q_1 + q_2)m + r_1 + r_2) \bmod m \\ &= (r_1 + r_2) \bmod m, \text{ denn:} \end{aligned}$$

$m \mid ((q_1 + q_2)m + r_1 + r_2) - (r_1 + r_2)$, weil $m \mid (q_1 + q_2)m$,
das heißt, $(q_1 + q_2)m + r_1 + r_2 \equiv r_1 + r_2 \pmod{m}$. □

Modulares Rechnen

Lemma

Für alle $a, b, m \in \mathbb{Z}$ mit $m \geq 1$ gilt:

$$(a \cdot b) \bmod m = (a \bmod m \cdot b \bmod m) \bmod m$$

Beweis.

Es gibt $q_1, q_2, r_1, r_2 \in \mathbb{Z}$, sodass
$$\begin{cases} a = q_1 m + r_1 & \text{mit } r_1 = a \bmod m \\ b = q_2 m + r_2 & \text{mit } r_2 = b \bmod m \end{cases}$$

$$ab \bmod m$$

$$= ((q_1 m + r_1) \cdot (q_2 m + r_2)) \bmod m$$

$$= (q_1 q_2 m^2 + q_1 r_2 m + r_1 q_2 m + r_1 r_2) \bmod m$$

$$= ((q_1 q_2 m + q_1 r_2 + r_1 q_2) m + r_1 r_2) \bmod m$$

$$= r_1 r_2 \bmod m \quad (\text{siehe letzten Beweis}).$$



Schnelle Exponentiation

Berechne $a^b \bmod m$ wie folgt.

1. Zerlege b binär: finde $\beta_1 < \dots < \beta_k$ mit $\sum_{i=1}^k 2^{\beta_i} = b$

2. Berechne $\alpha_j = a^{2^j} \bmod m$ für $j \in \{0, \dots, \beta_k\}$:

$$\alpha_0 = a$$

$$\alpha_{j+1} = \alpha_j^2 \bmod m$$

3. Berechne $a^b \bmod m = (\prod_{i=1}^k \alpha_{\beta_i}) \bmod m$.

Kongruenz

Lemma

Für alle $a, b, c, d, m \in \mathbb{Z}$ mit $m \geq 1$ gilt: Sind

$$a \equiv b \pmod{m} \quad \text{und} \quad c \equiv d \pmod{m}$$

dann ist auch

$$a + c \equiv b + d \pmod{m}$$

Beweis.

Aus $a \equiv b \pmod{m}$ folgt $m \mid (a - b)$, d.h. es gibt $t_1 \in \mathbb{Z}$, sodass $a - b = t_1 m$.

Aus $c \equiv d \pmod{m}$ folgt $m \mid (c - d)$, d.h. es gibt $t_2 \in \mathbb{Z}$, sodass $c - d = t_2 m$.

Um $a + c \equiv b + d \pmod{m}$ zu zeigen, reicht es zu zeigen, dass $m \mid (a + c) - (b + d)$.

$$\begin{aligned} & (a + c) - (b + d) \\ &= (a - b) + (c - d) \\ &= t_1 m + t_2 m \\ &= (t_1 + t_2)m. \end{aligned}$$



Kongruenz

Lemma

Für alle $a, b, c, d, m \in \mathbb{Z}$ mit $m \geq 1$ gilt: Sind

$$a \equiv b \pmod{m} \quad \text{und} \quad c \equiv d \pmod{m}$$

dann ist auch

$$a \cdot c \equiv b \cdot d \pmod{m}$$

Beweis.

Aus $a \equiv b \pmod{m}$ folgt $m \mid (a - b)$, d.h. es gibt $t_1 \in \mathbb{Z}$, sodass $a - b = t_1 m$.

Aus $c \equiv d \pmod{m}$ folgt $m \mid (c - d)$, d.h. es gibt $t_2 \in \mathbb{Z}$, sodass $c - d = t_2 m$.

Um $ac \equiv bd \pmod{m}$ zu zeigen, reicht es zu zeigen, dass $m \mid (ac - bd)$.

$$ac - bd$$

$$= a(t_2 m + d) - (a - t_1 m)d$$

$$= at_2 m + ad - ad + t_1 md$$

$$= (at_2 + t_1 d)m.$$



Kongruenz

Lemma

Für alle $a, b, c, m \in \mathbb{Z}$ mit $m \geq 1$ gilt:

Ist $a + c \equiv b + c \pmod{m}$, dann auch $a \equiv b \pmod{m}$

Beweis.

Da $a + c \equiv b + c \pmod{m}$, gilt $m \mid (a + c) - (b + c) = a - b$.

Das heißt, $a \equiv b \pmod{m}$. □

Kongruenz

Lemma

Für alle $a, b, c, m \in \mathbb{Z}$ mit $m \geq 1$ und $\text{ggT}(c, m) = 1$ gilt:

Ist $a \cdot c \equiv b \cdot c \pmod{m}$, dann auch $a \equiv b \pmod{m}$

Beweis.

Da $ac \equiv bc \pmod{m}$, gilt $m \mid (ac - bc) = (a - b)c$.

Da $\text{ggT}(c, m) = 1$, gilt $m \mid (a - b)$. □

Lösen von Kongruenzen

Lemma

Für $a, b, m \in \mathbb{Z}$ mit $m \geq 1$ und $\text{ggT}(a, m) = 1$ hat die Kongruenz

$$a \cdot x \equiv b \pmod{m}$$

genau eine Lösung $x \in \mathbb{Z}_m$.

Beweis.

Aus $\text{ggT}(a, m) = 1$ und dem Lemma von Bézout folgt, dass es s, t gibt, sodass $sa + tm = 1$.

Daher $bsa + tbm = b$.

Daher $bsa \equiv b \pmod{m}$.

Daher $ax \equiv bsa \pmod{m}$ wegen $ax \equiv b \pmod{m}$.

Somit $x = bs + m$.

Diese Lösung ist eindeutig in \mathbb{Z}_m . □

Speziell für $b = 1$: Lösung von $ax \equiv 1 \pmod{m}$ ist **Inverses** von a modulo m .

Der chinesische Restesatz

Theorem (Chinesischer Restesatz)

Seien $b_1, \dots, b_k \in \mathbb{N}$ und $m_1, \dots, m_k \in \mathbb{N}$ mit

$$\text{ggT}(m_i, m_j) = 1 \quad \text{für } i \neq j$$

und sei $m = m_1 \cdot \dots \cdot m_k$. Dann existiert genau ein $x \in \mathbb{Z}_m$ mit

$$x \equiv b_i \pmod{m_i} \quad \text{für } i \in \{1, \dots, k\}$$

Beweis.

Wir definieren $f : \mathbb{Z}_m \rightarrow \mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_k}$, sodass $f(x) = (x \bmod m_1, \dots, x \bmod m_k)$.

Unten werden wir zeigen, dass f injektiv ist. Da $|\mathbb{Z}_m| = |\mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_k}|$, ist f bijektiv.

Das heißt, (b_1, \dots, b_k) hat genau ein Urbild x mit $f(x) = (b_1, \dots, b_k)$.

Injektivität von f : Seien $x_1, x_2 \in \mathbb{Z}_m$ mit $f(x_1) = f(x_2)$.

Das heißt, dass $x_1 \equiv x_2 \pmod{m_i}$ für alle $i \in \{1, \dots, k\}$ und deshalb $m_i \mid (x_1 - x_2)$.

Daher $m \mid (x_1 - x_2)$ wegen $\text{ggT}(m_i, m_j) = 1$.

Daher $x_1 \equiv x_2 \pmod{m}$. Somit $x_1 = x_2$, da $x_1, x_2 \in \mathbb{Z}_m$. □

Kleiner Satz von Fermat

Theorem (Kleiner Satz von Fermat)

Für alle $n \in \mathbb{N} \setminus \{0\}$ gilt:

n ist Primzahl gdw. $a^{n-1} \equiv 1 \pmod{n}$ für alle $a \in \mathbb{Z}_n \setminus \{0\}$

Beweis.

Richtung \leftarrow : Sei $d \mid n$, sodass $d < n$.

Daraus folgt, dass es t_1 gibt, sodass $n = t_1 d$.

Wir nehmen an, dass $a^{n-1} \equiv 1 \pmod{n}$ für alle $a \in \mathbb{Z}_n \setminus \{0\}$.

Insbesondere gilt $d^{n-1} \equiv 1 \pmod{n}$ und daher gibt es t_2 , sodass $d^{n-1} - 1 = t_2 n$.

Zusammen: $d^{n-1} - 1 = t_2 t_1 d$.

Dies ist nur dann möglich, wenn $d = 1$.

Da der Teiler d beliebig gewählt war, ist 1 der einzige Teiler von n zwischen 1 und $n - 1$.

Daher ist n eine Primzahl.

Kleiner Satz von Fermat

Definiere: $\mathbb{Z}_n^* := \{a \in \mathbb{Z}_n \setminus \{0\} \mid \text{ggT}(a, n) = 1\}$

$$\varphi(n) := |\mathbb{Z}_n^*|$$

Theorem (Satz von Euler)

Für alle $n \in \mathbb{N}$ mit $n \geq 1$ gilt:

$$a^{\varphi(n)} \equiv 1 \pmod{n} \quad \text{für alle } a \in \mathbb{Z}_n^*$$

Beweis im nächsten Kapitel.

Kleiner Satz von Fermat

Theorem (Satz von Euler)

Für alle $n \in \mathbb{N}$ mit $n \geq 1$ gilt:

$$a^{\varphi(n)} \equiv 1 \pmod{n} \quad \text{für alle } a \in \mathbb{Z}_n^*$$

Theorem (Kleiner Satz von Fermat)

Für alle $n \in \mathbb{N}$ mit $n \geq 1$ gilt:

$$n \text{ ist Primzahl} \quad \text{gdw.} \quad a^{n-1} \equiv 1 \pmod{n} \quad \text{für alle } a \in \mathbb{Z}_n \setminus \{0\}$$

Beweis.

Richtung \rightarrow : Aus Euler folgt Fermat:

Wenn n eine Primzahl ist, dann sind $\varphi(n) = n - 1$ und $\mathbb{Z}_n^* = \mathbb{Z}_n \setminus \{0\}$. □