Zahlentheorie

Def. Teilbarkeit: Seien $a, b \in \mathbb{Z}$. $a|b \iff \exists c \in \mathbb{Z}: b = a \cdot c$

Teilbarkeits-Regeln:

- $\forall a \in \mathbb{Z}: \pm 1|a, \pm a|a$
  $a|0, \; 0|a \Rightarrow a = 0$
- $a|b \wedge b|c \Rightarrow a|c$
- $a|b \Rightarrow a \cdot c | b \cdot c \;\; \forall c \in \mathbb{Z}$
- $a_1|b_1 \wedge a_2|b_2 \Rightarrow a_1 a_2 | b_1 b_2$
- $a|b \wedge a|c \Rightarrow a|(rb + sc) \;\; \forall r, s \in \mathbb{Z}$
- $a|b \wedge b|a \Rightarrow b/a = \pm 1 \vee b = \pm a \vee |b| = |a|$
- $a|b \iff |a| \,\big|\, |b|$
- $a|b \Rightarrow |a| \leq |b|$
- a, b teilerfremd $\Rightarrow$ $a|bc \Rightarrow a|c$
  " $\Rightarrow$ $a|c \wedge b|c \Rightarrow a \cdot b | c$

Euklidischer Algorithmus

- Seien $a, b \in \mathbb{N}$. Dann $\exists q, r \in \mathbb{N}_0: a = q \cdot b + r, \; 0 \leq r < b$.
  (q und r sind eindeutig)
- OBdA sei $a > b$, $a = a_0$, $b = a_1$. Folge a_j im Algorithmus:
  $a_{j-1} = q_j \cdot a_j + a_{j+1} \;\; \forall j = 1..l$ (l Schritte $1 \leq l \leq b$).
  Wenn $a_{l+1} = 0$, dann $ggT(a,b) = a_l$ (vorletzter Schritt)

Bézout-Koeffizienten:

- $\exists r, s \in \mathbb{Z}: ggT(a,b) = r \cdot a + s \cdot b$.
- Berechne wie folgt: $r_0 = s_1 = 1$, $r_1 = s_0 = 0$. Folgen r_j, s_j:
  $r_{j+1} = r_{j-1} - r_j q_j$, $s_{j+1} = s_{j-1} - s_j q_j$, dann $r_l = r$, $s_l = s$.
- Oder „rückwärts einsetzen":
  letzte Zeile vom Alg. nach ggT umstellen (also $a_l = a_{l-2} - q_{l-1} a_{l-1}$),
  setze dann für a_{l-1} die vorherige, umgestellte Gleichung an
  (nicht alles ausmultiplizieren, s. Bsp.)

Primzahlen:

- $p \in \mathbb{N}$ prim $\iff p > 1 \wedge \forall a, b \in \mathbb{N}: p|ab \Rightarrow p|a \vee p|b$
- p unzerlegbar $\iff p > 1$ und einzige Teiler ± 1 und $\pm p$
- prim gdw. unzerlegbar (in $\mathbb{N}$)
- jedes $n > 1$ hat $p_{min}(n) = p$ kleinsten Primteiler mit $p|n$,
  p prim und kleinste solche Zahl
- n prim $\iff p_{min}(n) = n$
- impl.: einfache Vorwärtssuche für 2 bis n
  falls `n % j == 0`, return j ($O(10^d)$, d Stellen)
  (oder bis zur Wurzel; man lässt gerade Zahlen nach Prüfen von 2 weg)
- es gibt eine eindeutige Primfaktorzerlegung:
  $n = p_1^{v_1} \cdot \ldots \cdot p_k^{v_k} = \prod_{j=1}^{k} p_j^{v_j}$, die p_j sind prim

Def. ggT:

- $c \in \mathbb{Z}$ gem. Teiler von a und b
  wenn $c|a \wedge c|b$
- $d = ggT(a,b)$ wenn
  (1) $d \in \mathbb{N}$ (2) $d|a \wedge d|b$
  (3) $c|a \wedge c|b \Rightarrow c|d$
- $ggT(a,b)$ existiert & ist eindeutig
- impl.: naiv (suche bis $\min\{|a|, |b|\}$)
  Euklid. Alg.

ggT-Regeln:

- a, b teilerfremd $\iff ggT(a,b) = 1$
- $ggT(a,b) = ggT(|a|, |b|)$
- $ggT(a,b) \cdot kgV(a,b) = |a \cdot b|$

Bsp. Euklid. Alg.:

$ggT(37, 91) = ggT(91, 37)$

$a_0 = 91 = a$, $a_1 = 37 = b$

$a_{j-1} = q_j \cdot a_j + a_{j+1}$

1. $91 = 2 \cdot 37 + 17$
2. $37 = 2 \cdot 17 + 3$
3. $17 = 5 \cdot 3 + 2$
4. $3 = 1 \cdot 2 + 1 = ggT(37, 91)$

$2 = 2 \cdot 1 + 0$ STOP

Bsp. Bézout-Koeffizienten:

$ggT(37, 91) = 1 \quad (a = 91, b = 37)$ (4)
$= 3 - 1 \cdot 2$ (3)
$= 3 - 1 \cdot (17 - 5 \cdot 3)$ ausm.
$= (-1) \cdot 17 + 6 \cdot 3$ (2)
$= (-1) \cdot 17 + 6 \cdot (37 - 2 \cdot 17)$ ausm.
$= 6 \cdot 37 - 13 \cdot 17$ (1)
$= 6 \cdot 37 - 13 \cdot (91 - 2 \cdot 37)$ ausm.
$= (-13) \cdot 91 + 32 \cdot 37$
$= r \cdot a + s \cdot b$
$\Rightarrow r = -13, \; s = 32$

Restklassen:

- $a \equiv b \mod m \Leftrightarrow m \mid (a-b) \Leftrightarrow$ a, b selbe Restklasse ($\equiv$ ist sym./refl./trans.)
- $\overline{a} := [a]_m := \{b \in \mathbb{Z} \mid b \equiv a \mod m\}$ $= \{z = a + k \cdot m \mid k \in \mathbb{Z}\}$ ist Restklasse von a modulo m
- $[a]_m \cap [b]_m \neq \emptyset \Rightarrow [a]_m = [b]_m$
- $\mathbb{Z} = \bigcup_{a \in \mathbb{Z}} \overline{a} = \overline{0} \cup \overline{1} \cup \ldots \cup \overline{m-1}$

Kongruenzgleichungen:

- Sei $a_1 \equiv a_2 \mod m$, $b_1 \equiv b_2 \mod m$. Dann $a_1 \pm b_1 \equiv a_2 \pm b_2 \mod m$.
- $a \cdot x \equiv \mod m$ lösbar nach x $\Leftrightarrow ggT(a,m) \mid b$ (g Lösungen)
- a ist Einheit/invertierbar $\Leftrightarrow$ a, m teilerfremd
- a^{-1} ist die Lösung von $a \cdot x \equiv 1 \mod m$
- a^{-1} ist Bézout-s aus $ggT(a,m) = sa + rm$

Aus der Übung:

- $a_k := a_{k-1} + a_{k-2}$, $a_0 = a_1 = 1$ Fibonacci-Z.
- $a_k = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{k+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{k+1}\right)$ (Goldener Schnitt)
- $[z_0; z_1, \ldots, z_n] := z_0 + \cfrac{1}{z_1 + \cfrac{1}{\ddots + \cfrac{1}{z_{n-1} + \cfrac{1}{z_n}}}}$ heißt Kettenbruch (kann alle positiven Zahlen in $\mathbb{Q}$ darstellen)
- $l < \frac{\log_{10} b\sqrt{5}}{\log_{10} \gamma}$ mit $\gamma = \frac{1+\sqrt{5}}{2}$ für die Schrittanzahl l aus Euklid. Alg.
- für p prim und $\overline{a} \in \mathbb{Z}_p$, $\overline{a}$ Primitivwurzel: $\bigcup_{k=1}^{p-1} \overline{a}^k = \mathbb{Z}_p \setminus \{\overline{0}\}$ ($\overline{a} \neq \overline{0}$ immer, $\overline{a} = \overline{1} \Leftrightarrow p = 2$)
- diskreter Logarithmus von $\overline{b}$ zur Basis $\overline{a}$: $k \in \{1, \ldots, p-1\}$ s.d. $\overline{a}^k = \overline{b}$ (in $\mathbb{Z}_p$)

Restklassenringe/-körper/-faktorräume:

- $\mathbb{Z}_m := \mathbb{Z}/m\mathbb{Z} := \{\overline{a} \mid a \in \mathbb{Z}\}$ $= \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$
- $\left.\begin{array}{l} \overline{a} + \overline{b} := \overline{a+b} \\ \overline{a} \cdot \overline{b} := \overline{a \cdot b} \end{array}\right\}$ $\mathbb{Z}$ kom. unitärer Ring
  +, · ass./kom.; $\overline{0}, \overline{1}$ neutr. El., inv. El. für +, Distributivität
- $\mathbb{Z}_m$ Körper $\Leftrightarrow$ m prim (da alle a Einheiten)

Chinesischer Restsatz:

- für großes m statt x mod m: x mod m_j ($m_j = p_j^{k_j}$ aus Primfaktorzerlegung)
- kom. unit. Ring: $([a_1]_{m_1} \ldots [a_k]_{m_k})$ (mit Vektoraddition und -multiplikation)
- $\phi: \mathbb{Z}_m \to \mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_k}$ ist Homomorphismus mit $\phi([a]) := ([a]_{m_1} \ldots [a]_{m_k})$
- Ch. Restsatz: ϕ Isomorphismus (ϕ^{-1} existiert) für m_j Primfaktoren

Gleitkommazahlen:

- Rechnerzahlen $G(b, l, E_{min}, E_{max})$ zur Basis b, Mantissenlänge l, Exponentenschranken Emin/max, dann: $x = s\,(\underbrace{\textstyle\sum_{k=1}^{l} a_k b^{-k}}_{=:\,(0.a_1 \ldots a_l)_b})\, b^e$
- double $\hat{=}$ $G(2, 53, -1021, 1024)$ (64 bit)
- Problem: Auslöschung bei a − b, wobei $a \approx b$ und a, b nicht klein $\Rightarrow$ großer Fehler!