Euklidischer Algorithmus

$x_0, x_1 \in \mathbb{Z} \quad \rightsquigarrow \quad x_i = d = ggT(x_0, x_1)$

$x_0 > x_1$ Korrektheit ✓ Theorem 4.29

$\sim 2 \cdot \log_2(|x_0|)$ viele Iterationen Laufzeit ✓ Theorem 4.31

(modulo - Berechnungen schnell ✓)

Auch (Rückwärtsrechnung) Darstellung des ggT's als Linearkombination ✓

$a \cdot x_0 + b \cdot x_1 = d$ a, b ausrechnen Lemma 4.30

1. Anwendung: Existenz in $\mathbb{Z}_p$ p Primzahl

$p, l \quad l \in \{1, 2, 3, \ldots, p-1\}, \quad ggT(p, l) = 1, \quad a \cdot l + b \cdot p = 1$

$\bar{a}$ Inverses zu $\bar{l}$ in $\mathbb{Z}_p$

2. Lösen von Kongruenzsystemen i) Existenz ✓

ii) Ausrechnen mit Euklid. Alg.

4.3.4 Chinesischer Restesatz (Anwendung!)

Lösen LGS

$a_1 \cdot x + b_1 \cdot y = c_1$ $\quad x, y$ Unbekannte!

$a_2 \cdot x + b_2 \cdot y = c_2$ $\quad$ 2 Gleichg., 2 Unbekannte!

$(\mathbb{Z}_n, \odot_n, \oplus_n)$

Gleichungssysteme $x \in \mathbb{Z}$

Kongruenzsysteme $a, b \in \mathbb{Z}$ $\quad n, m \in \mathbb{Z}$

$x \equiv a \bmod n$

$x \equiv b \bmod m$

Finde x! $\quad n, m \in \mathbb{N}$

$ggT(n, m) = 1$

(BSP)

$x \equiv 3 \mod 20$

$x \equiv \bar{5} \mod 153$

$x = 423$ ist Lsg.

$423 = 46 \cdot 20 + 3$

$423 = 6 \cdot 153 + \bar{5}$

modulo $20 \cdot 153$ gibt es reine Lsg.

$\mathbb{Z}_{20 \cdot 153} = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{20 \cdot 153 - 1}\}$

Theorem 4.32 Für alle $a, b \in \mathbb{Z}$ und $n, m \in \mathbb{N}$ mit $ggT(n,m) = 1$ existiert genau eine Lösung $x \in \{0, 1, 2, \ldots, m \cdot n - 1\}$ für das Kongruenzsystem:

$x \equiv a \mod n$

$x \equiv b \mod m.$

Beweis: (nicht konstruktiv !)

Beweis: $f: \mathbb{Z}_{n\cdot m} \longrightarrow \mathbb{Z}_n \times \mathbb{Z}_m$

Vorschrift: $\overline{x}_{n\cdot m} \longmapsto (\overline{x}_n, \overline{x}_m)$

wohldefiniert: $\overline{x}_{n\cdot m} = \overline{x'}_{n\cdot m} \quad x \neq x'$

$\overset{\forall}{\Rightarrow} f(\overline{x}_{n\cdot m}) = f(\overline{x'}_{n\cdot m})$

$\begin{cases} x = b'\cdot nm + \ell \\ x' = a'\cdot n\cdot m + \ell \\ x - x' = (b'-a')n\cdot m + \cancel{0} \end{cases}$

$\Rightarrow n\cdot m \mid x - x' \Rightarrow \begin{matrix} n \mid x-x' \\ m \mid x-x' \end{matrix} \Rightarrow \begin{matrix} \overline{x}_n = \overline{x'}_n \\ \overline{x}_m = \overline{x'}_m \end{matrix}$

Unabhängig von Repräsentanten $\forall$

$(\overline{x}_n, \overline{x}_m) = (\overline{x'}_n, \overline{x'}_m)$

Zeige: f ist bijektiv!

f ist injektiv

$$f(\bar{x}_{nm}) = f(\bar{\ell}_{nm})$$

$$\Leftrightarrow \left(\bar{x}_n, \bar{x}_m\right) = \left(\bar{\ell}_n, \bar{\ell}_m\right)$$

$$\Leftrightarrow \bar{x}_n = \bar{\ell}_n \quad , \quad \bar{x}_m = \bar{\ell}_m$$

$$\Leftrightarrow n \mid x-\ell \qquad m \mid x-\ell$$

$$\Rightarrow n \cdot m \mid x-\ell$$

n, m teilerfremd — Primfaktorzerlegung!

$$\Leftrightarrow \bar{x}_{n\cdot m} = \bar{\ell}_{n\cdot m}$$ ✓

2|12	3|18	n, m
9|18	3|18	n', m'

27×18

$6 \mid 18$ ⌟

Ann: Lsg. des Kongruenzsystem existiert laut

$\overset{!}{\Longrightarrow}$ endeutige Lsg. aus $\{0, 1, 2, \ldots, nm-1\}$

über Injektivität!

Indirekt, Sei $x, y \in \{0, 1, 2, \ldots, n \cdot m - 1\}$ $x \neq y$ Lsg.

$x \equiv a \bmod n$ $\quad y \equiv a \bmod n$

$x \equiv b \bmod m$ $\quad y \equiv b \bmod m$

$$\Rightarrow \quad f(\overline{x}_{n \cdot m}) = f(\overline{y}_{n \cdot m}) = (\overline{a}_n, \overline{b}_m)$$

$\overset{\text{Injektiv}}{\Longrightarrow}$ $\overline{x}_{n \cdot m} = \overline{y}_{n \cdot m} \Rightarrow x = y$ ↯

↑ wahl x, y aus $\{0, 1, \ldots, n \cdot m - 1\}$

Heißt: Endeutige Lsg. bei Existenz!

Noch 2.2: f_{sg} trivial auch!

Zeige: f ist surjektiv!

Für jedes Paar $(\bar{a}, \bar{b}) \in \mathbb{Z}_n \times \mathbb{Z}_m$ ex. Urbild $\bar{x}$ zu $(\bar{a}, \bar{b})$

$\bar{x} \in \mathbb{Z}_{nm}$ $f(\bar{x}) = (\bar{x}, \bar{x}) = (\bar{a}, \bar{b})$

Repräsentant aus $\{0, 1, \dots, n \cdot m - 1\}$ ex.

Allein über Kardinalität!

$|\mathbb{Z}_{nm}| = n \cdot m$ Halbbeweis!

$|\mathbb{Z}_n \times \mathbb{Z}_m| = n \cdot m$ Zielbereich!

Das Bild von f bzgl. $\mathbb{Z}_{nm}$ kann nicht kleiner werden wg. Injektivität!

$\Rightarrow$ f ist surjektiv! $\square$

Bis hierher: $a, b \in \mathbb{Z}$

$$x \equiv a \mod n$$
$$x \equiv b \mod m$$

$n, m \in \mathbb{N}$

$ggT(n, m) = 1$

$\Rightarrow$ eind. Lsg $\pmod{m \cdot n}$ $\quad x \in \{0, 1, 2, \ldots, n \cdot m - 1\}$

$\varphi : \mathbb{Z}_{n \cdot m} \to \mathbb{Z}_n \times \mathbb{Z}_m \qquad \varphi(\overline{x}_{nm}) = (\overline{x}_n, \overline{x}_m)$

Beweis: φ bijektiv

Jetzt: Konstruktiv! $\quad ggT(n, m) = 1$

Lemma 4.30 $\Rightarrow \exists\, v, w \in \mathbb{Z}$ mit

$$n \cdot v + m \cdot w = 1 \qquad \text{daraus ...}$$

Lsg.: $\quad x := b \cdot n \cdot v + a \cdot m \cdot w$

$\Rightarrow$ prüfen! (Das tut's!)

$$
\begin{aligned}
x &\equiv a \cdot m \cdot w \pmod{n} \\
&\equiv a \cdot n \cdot v + a \cdot m \cdot w \pmod{n} \\
&\equiv a\underbrace{(n \cdot v + m \cdot w)}_{=1} \pmod{n} \\
&\equiv a \pmod{n}
\end{aligned}
$$

$$
\begin{aligned}
x &\equiv b \cdot n \cdot v \pmod{m} \\
&\equiv b\underbrace{(n \cdot v + m \cdot w)}_{=1} \pmod{m} \\
&\equiv b \pmod{m}
\end{aligned}
$$

✓ fertig!

(BSP) Suche x!

$$x \equiv 3 \bmod 20 \quad | \; n$$
$$x \equiv 5 \bmod 153 \quad | \; m$$

Gleichung aufstellen!

$$\Rightarrow \quad m \cdot w + n \cdot v = 1$$

Euklidischer Alg:

$$153 = 7 \cdot 20 + 13 = x_2$$
$$20 = 1 \cdot 13 + 7 = x_3$$
$$13 = 1 \cdot 7 + 6 = x_4$$
$$7 = 1 \cdot 6 + 1 = x_5$$
$$6 = 6 \cdot 1 + 0 = x_6$$

$$x_5 = 1 = 7 - 1 \cdot 6$$
$$= (13 - 1 \cdot 7) - 1 \cdot 7$$
$$= -1 \cdot 13 + 2 \cdot 7$$
$$= 2 \cdot (20 - 1 \cdot 13) - 3 \cdot 13$$
$$= 2 \cdot 20 - 3 \cdot 13$$
$$= 2 \cdot 20 - 3 \cdot (153 - 7 \cdot 20)$$
$$= \underbrace{153}_{m}\underbrace{(-3)}_{w} + \underbrace{20}_{n} \cdot \underbrace{23}_{v} = 1$$

$$x = 9\,23$$

$$ggT(20, 153) = 1$$

$$x = a \cdot m \cdot w + b \cdot n \cdot v$$
$$= 3 \cdot 153 \cdot (-3) + 5 \cdot 20 \cdot 23$$

Erweiterungen: Verallgemeinerung!

Kongruenzsystem: $a_1, a_2, \dots, a_r \in \mathbb{Z}$

$$\begin{aligned} x &\equiv a_1 \bmod n_1 \\ x &\equiv a_2 \bmod n_2 \\ &\vdots \\ x &\equiv a_r \bmod n_r \end{aligned}$$

n_i paarweise teilerfremd.

$n_i \in \mathbb{N}$

$N = n_1 \cdot n_2 \cdot \dots \cdot n_r$

hat eind. Lsg. $x \in \{0, 1, 2, \dots, N-1\}$ $(\bmod N)$

Euklid: ggT darstellen $\quad n_i \cdot v_i + N_i w_i = 1$, $N_i = \frac{N}{n_i}$

$d_i = N_i \cdot w_i$ $\quad$ Lsg: $x = \sum_{i=1}^{r} a_i d_i$

$d_i \equiv 0 \bmod N_i$

$d_i \equiv 1 \bmod n_i$ $\quad i = 1, \dots, r$

(Idee)

4.3.5 RSA Kryptosystem

Rivest, Shamir, Adleman

Asymmetrische Verschlüsselung!

Schlüsselpaare: public key, private key

verschlüsseln entschlüsseln

Vorteil: Kein Schlüssel geheim austauschen!

Open PGP beruht darauf!

Idee: Ich generiere beide Schlüssel (public/private)

Gegenseite (jeder) kann mit public verschlüsseln. Nur ich mit private entschlüsseln.

Vorbereitungen dazu: $(\mathbb{Z}_n, \oplus_n, \odot_n)$

kommut. Ring mit 1.

Theorem 4.34 Im Ring $(\mathbb{Z}_n, \oplus_n, \odot_n)$ hat $\bar{a}$ genau dann ein multiplikatives Inverses, wenn $ggT(a,n) = 1$ gilt.

Beweis: "$\Rightarrow$" $\bar{a} \cdot \bar{b} = \bar{1}$ (modulo n)

$\Rightarrow n \mid a \cdot b - 1 \Rightarrow \exists v \in \mathbb{Z}$

Def. $|$ $ab - 1 = v \cdot n$

22: $ggT(a,n) = 1$

Sei q gemeinsamer Teiler von a und n

$\Rightarrow q \mid a$ und $q \mid n \Rightarrow \exists v' \in \mathbb{Z}$ $a \cdot b - v \cdot n = v' q$

$\Rightarrow q \mid \underbrace{ab - v \cdot n}_{=1} \Rightarrow q \mid 1$ d.h. $q = 1$, a, n teilerfremd.

BSP $\mathbb{Z}_6$

$\mathbb{Z}_6^* = \{\bar{1}, \bar{5}\}$

$ggT(2,6) = 2 = ggT(4,6)$

$ggT(3,6) = 3$

$$a \perp n \iff gg^{\top}(a,n) = 1$$

$$\Rightarrow \quad \exists\, v, w \in \mathbb{Z} \quad v \cdot a + w \cdot n = 1$$

(Lemma 4.30)

$$v \cdot a = 1 - w \cdot n$$

$$\Rightarrow \quad 1 \equiv v \cdot a \bmod n$$

$$\Rightarrow \quad \bar{1} = \overline{v \cdot a} = \bar{v} \cdot \bar{a}$$

$\bar{v}$ ist multiplikatives Inverses zu $\bar{a}$ ∎

Definition 4.33 Eulersche φ-Funktion $\varphi: \mathbb{N} \to \mathbb{N}$

$$\varphi(n) := \left| \{ x \in \{1, 2, 3, \ldots, n\} : gg^{\top}(x, n) = 1 \} \right|.$$

[Anzahl der Einheiten in $\mathbb{Z}_n$!] (BSP) $\mathbb{Z}_6^* = \{\bar{1}, \bar{5}\}$, $\varphi(6) = 2$,

$\varphi(24) = 8$, $\mathbb{Z}_{24}^* = \{\bar{1}, \bar{5}, \bar{7}, \bar{11}, \bar{13}, \bar{17}, \bar{19}, \bar{23}\}$]