Der chinesische Restsatz

Wir haben bereits gesehen, wie wir lineare Kongruenzen der Form $a \cdot x \equiv b \bmod m$ lösen. In diesem Abschnitt möchten wir Systeme von linearen Kongruenzen lösen.

Satz 4.29 (Chinesischer Restsatz (CRS)) Buch Zhang ~400 n. Chr.

Seien $m_1, \dots, m_r \in \mathbb{N}^*$ mit $ggT(m_i, m_j) = 1 \ \forall i \neq j$.

Seien $a_1, \dots, a_r \in \mathbb{Z}$ beliebig.

(a) Es existiert ein $x \in \mathbb{Z}$ mit $x \equiv a_i \bmod m_i \ \forall i = 1, \dots, r$

(b) Die Lösung x aus a) ist eindeutig modulo $m = m_1 \cdot \dots \cdot m_r$

Beweis:

Für $M_j := \frac{m}{m_j} = \frac{m_1 \cdot \dots \cdot m_r}{m_j}$ ist $ggT(M_j, m_j) = 1$

$\Rightarrow [M_j]_{m_j} \in (\mathbb{Z}/m_j\mathbb{Z})^*$ (M_j hat also ein multiplikatives Inverses in $\mathbb{Z}/m_j\mathbb{Z}$)

$\Rightarrow \tilde{M}_j$ mit $M_j \cdot \tilde{M}_j \equiv 1 \bmod m_j$.

Wir definieren $x = \sum_{j=1}^{r} a_j M_j \tilde{M}_j$

Für $i \neq j$ ist $M_j = \frac{m}{m_j} \equiv 0 \bmod m_i$ da $m_i \mid M_j$

Also für festes j $M_j \tilde{M}_j a_j \equiv \begin{cases} 0 \bmod m_i \text{ für } i \neq j \\ 1 \cdot a_j \bmod m_j \end{cases}$

$\Rightarrow x \equiv 1 \cdot a_j \bmod m_j \ \forall j = 1, \dots, r$

$\Rightarrow x$ ist eine Lösung der Kongruenz. Dies zeigt (a).

Es bleibt die Eindeutigkeit dieser Lösung modulo m zu zeigen.

Sei $y \in \mathbb{Z}$ eine weitere Lösung.

Es ist also $x \equiv y \equiv a_i \bmod m_i \ \forall i = 1, \dots, r$

$\Rightarrow (x - y) \equiv 0 \bmod m_i \ \forall i = 1, \dots, r$

$\Rightarrow \forall i = 1 \dots r$ ist m_i ein Teiler von $(x-y)$. Da die m_i paarweise teilerfremd sind, ist also auch $m = m_1 \cdot \dots \cdot m_r$ ein Teiler von $(x-y)$

↪ x und y unterscheiden sich um ein Vielfaches von m

$\Rightarrow x \equiv y \bmod m$. ⇒

Bemerkung 4.30 (Alternative Formulierung d. CRS)

Seien $m_1, \dots, m_r \in \mathbb{N}^*$ mit $ggT(m_i, m_j) = 1 \ \forall i \neq j$

Sei ferner $m = m_1 \cdot \dots \cdot m_r$.

Die Abbildung $\Phi : \mathbb{Z}/m_1 \dots m_r\mathbb{Z} \longrightarrow \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \dots \times \mathbb{Z}/m_r\mathbb{Z}$

ist ein wohldef. Ringhomomorphismus

1) Zeige, dass $\mathbb{Z}/m_1\mathbb{Z} \times \dots \times \mathbb{Z}/m_r\mathbb{Z}$ bzgl. komponentenweiser Verknüpfung ein Ring ist.
2) Zeige die Wohldefiniertheit
3) Zeige die Homomorphie Eigenschaften

Φ ist zudem offensichtlich injektiv:

Ist $\Phi([x]_m) = 0$, so ist $x \equiv 0 \mod m_i \ \forall i = 1 \dots r$

$\Rightarrow [x]_m = [0]_m$

Satz 4.29 sagt, dass Φ surjektiv ist.

Ist $([a_1]_{m_1}, \dots, [a_r]_{m_r}) \in \mathbb{Z}/m_1\mathbb{Z} \times \dots \times \mathbb{Z}/m_r\mathbb{Z}$ &

x eine Lösung der simultanen Kongruenz

$x \equiv a_i \mod m_i \quad i = 1, \dots, r$

So ist $[x]_m$ das eindeutige Urbild von $([a_1]_{m_1}, \dots, [a_r]_{m_r})$ unter Φ.

Oft formuliert man den chinesischen Restsatz daher wie folgt:

Seien $m_1, \dots, m_r \in \mathbb{N}^*$ mit $ggT(m_i, m_j) = 1 \ \forall i \neq j$

Dann ist $\mathbb{Z}/m_1 \dots m_r\mathbb{Z} \simeq \mathbb{Z}/m_1\mathbb{Z} \times \dots \times \mathbb{Z}/m_r\mathbb{Z}$.

Beispiel 4.31

Wir betrachten die simultane Kongruenz

$x \equiv 2 \mod 20$

$x \equiv 6 \mod 9$

$x \equiv 5 \mod 7$

a_i	m_i

Bemerkung 4.26 13.06.18

Das obige Lemma folgt trivialerweise aus dem Indexsatz von Lagrange, einem allgemeinen Satz aus der Gruppentheorie.

Sei $(G,\circ)$ und $H \subset G$ eine Untergruppe. Dann definiert $a \sim b :\Leftrightarrow a^{-1} b \in H \Leftrightarrow \exists h \in H$ mit $b = a \cdot h$ eine Äquivalenzrelation auf G.

Die Äquivalenzklassen bzgl. dieser Äquivalenzrelation heißen (Links-) Nebenklassen

(Hätten wir als Äquivalenzrelation $a \sim b :\Leftrightarrow \exists h : b = h \cdot a$ heißen die Äquivalenzklassen Rechts-Nebenklassen).

Eine linksnebenklasse hat die Form $gH = \{gh \mid h \in H\}$

Die Anzahl der (unterschiedlichen) linksnebenklassen heißt der Index von H in G. Man schreibt hierfür $(G:H)$.

Indexsatz von Lagrange sagt: $|G| = (G:H) \cdot |H|$.

Insbesondere ist die Ordnung einer Untergruppe von $H \subset G$ ein Teiler der Ordnung von G.

Lemma 4.25 folgt nun für $G = (\mathbb{Z}/m\mathbb{Z})^*$ & für ein $a \in G$ betrachten wir die von a erzeugte Untergruppe von G.

$H = \{a^r \mid r \geq 1\} \subset G$.

Es ist $|H| = \mathrm{ord}_m(a)$ und $|G| = \varphi(m)$.

Beispiel 4.27 (Potenzen berechnen)

$m = 37$ (Primzahl) $\Rightarrow \varphi(m) = 36$

Wollen $\mathrm{ord}_m(8)$. Da nach 4.25 $\mathrm{ord}(8) \mid \varphi(m)$ ist

$\mathrm{ord}(8) \in \{2, 3, 4, 6, 9, 12, 18, 36\}$

$8^2 \equiv 64 \equiv 27 \mod 37$ $\quad 8^6 \equiv 8^4 \cdot 8^2 \equiv 36 \equiv -1 \mod 37$

$8^3 \equiv 8^2 \cdot 8 \equiv 31 \mod 37$ $\quad \Rightarrow 8^{12} = (8^6)^2 \equiv 1 \mod 37$

$8^4 \equiv (8^2)^2 \equiv 26 \mod 37$ $\quad \Rightarrow \mathrm{ord}(8) = 12$, falls $8^9 \not\equiv 1 \mod 37$

$8^9 \equiv 8^6 \cdot 8^3 \equiv -1 \cdot 31 \equiv 6 \mod 37$

Wollen $8^{1111} \mod 37$

$8^{1111} = 8^{92 \cdot 12} \cdot 8^7 = (8^{12})^{92} \cdot 8^7 \equiv 1 \cdot 8^7 \equiv 8 \cdot \underbrace{8^6}_{\equiv -1 \mod 37} \overset{29}{\equiv} -8 \mod 37$

Die Sätze von Euler & Fermat bzw. das obige Verfahren erlauben es in einigen Fällen Potenzen $a^e \mod p$ leicht zu berechnen.

Allgemeiner lassen sich solche Potenzen $a^e \mod p$ berechnen, indem man die binäre Entwicklung von e berechnet.

$e = \sum_{i=0}^{k} e_i 2^i \,, \; e_i \in \{0,1\}$

↝ Berechnen für $\forall i = 0, \dots, k$ $a^{2^i} \mod p$ indem man benutzt, dass $a^{2^{i+1}} = a^{2^i \cdot 2} = (a^{2^i})^2$

Benutze:

$a^e = a^{\sum e_i 2^i} = \prod_{i=0}^{k} a^{2^i \cdot e_i} = \prod_{i : e_i \neq 0}^{k} a^{2^i}$ ← Haben wir mod p berechnet!

Lemma 4.28

Sei $n \in \mathbb{N}^*$, dann gilt $n = \sum_{d \mid n} \varphi(d)$

Beweis:

Sei $M = \{1, \dots, n\}$ und $C_d = \{a \in M \mid ggT(a,n) = d\}$.

Für $d \neq d'$ gilt $C_d \cap C_{d'} = \emptyset \Rightarrow M = \dot{\bigcup}_{d \mid n} C_d$

Aus $ggT(a,n) = d$ folgt mit Prop. 3.10, dass $ggT\left(\frac{a}{d}, \frac{n}{d}\right) = 1$.

Also gilt für die Kardinalität von C_d:

$$|C_d| = \left|\left\{ \frac{a}{d} \;\middle|\; \frac{a}{d} \in M, ggT\left(\frac{a}{d}, \frac{n}{d}\right) = 1 \right\}\right| \overset{\text{Def. 4.18}}{=} \varphi\left(\frac{n}{d}\right)$$

Es folgt $n = |M| = \left|\dot{\bigcup}_{d \mid n} C_d\right| = \sum_{d \mid n} |C_d| = \sum_{d \mid n} \varphi\left(\frac{n}{d}\right) \overset{(*)}{=} \sum_{d \mid n} \varphi(d)$

(*) gilt da $\{\frac{n}{d} \mid d \text{ teilt } n\} = \{d \mid d \text{ teilt } n\}$

$\downarrow$

$n = \frac{n}{d} \cdot d$, wenn $d \mid n$, dann ist auch n/d ein Teiler von n.

Wir werden später nochmal auf die Eulersche φ-Fkt. zurückkommen

$m = m_1 \cdot m_2 \cdot m_3 = 20 \cdot 9 \cdot 7 = 1260$

$M_1 = \frac{m}{m_1} = \frac{1260}{20} = 9 \cdot 7 = 63$, $M_2 = \frac{1260}{9} = 20 \cdot 7 = 140$

$M_3 = \frac{1260}{7} = 20 \cdot 9 = 180$

Erw. euklidischer Algorithmus liefert:

$1 = ggT(M_1, m_1) = 7 \cdot 63 + 22 \cdot \underbrace{20}_{m_1} \Rightarrow \tilde{M}_1 = 7$

$1 = ggT(M_2, m_2) = 2 \cdot 140 - 31 \cdot 9 \Rightarrow \tilde{M}_2 = 2$

$1 = ggT(M_3, m_3) = 3 \cdot 180 - 77 \cdot 7 \Rightarrow \tilde{M}_3 = 3$

$\Rightarrow x = \sum_{j=1}^{3} M_j \cdot \tilde{M}_j \cdot a_j = 63 \cdot 7 \cdot 2 + 140 \cdot 2 \cdot 6 + 180 \cdot 3 \cdot 5$

$= 5262 \equiv 222 \mod \underbrace{m}_{1260}$

Was passiert, wenn die m_i nicht paarweise teilerfremd sind?

Beispiel 4.32

(a) Betrachte die simultane Kongruenz $x \equiv 2 \mod 10 = 2 \cdot 5$, $x \equiv 3 \mod 14 = 2 \cdot 7$

Es ist $ggT(10, 14) = 2$

Die erste Kongruenz liefert, dass $x \equiv 0 \mod 2$ ist

Die zweite Kongruenz liefert, dass $x \equiv 1 \mod 2$ ist

Da $0 \not\equiv 1 \mod 2$ hat die simultane Kongruenz keine Lsg.

(b) Betrachte $x \equiv ③ \mod 45 = ⑨ 5$, $x \equiv 7 \mod 756 = 9 \cdot 84$ } $ggT(45, 756) = 3^2 = 9$

Wegen $7 \not\equiv ③ \mod ⑨$ folgt wie in (a), dass keine Lsg. existiert.

Es gibt also, falls die m_i in der simultanen Kongruenz nicht teilerfremd sind 2 Möglichkeiten:

1) Die einzelnen Kongruenzen widersprechen sich & es existiert daher keine Lösung. Dies stellt man fest,

indem man die indizierten Kongruenzen modulo ggT($m_1, \ldots, m_r$) betrachtet.

2) Widersprechen sich die einzelnen Kongruenzen nicht, so kann man die simultane Kongruenz durch ein dazu "äquivalentes" System von Kongruenzen ersetzen. In diesem sind dann die "neuen m_i" paarweise teilerfremd.