Chinesischer Restsatz

–

Chinese Remaindering

System von Kongruenzen

- Wir betrachten eine einfache Gleichung mit ganzzahligen Koeffizienten und einer ganzzahligen Lösung
- Und lösen sie mit modularer Arithmetik in $\mathbb{Z}_5$ und $\mathbb{Z}_7$

$$
\begin{aligned}
727x - 381 &= 17067 \mid +381 \\
727x &= 17448 \mid : 727 \\
x &= 24
\end{aligned}
$$

$$
\begin{aligned}
2x + 4 &= 2 \mod 5 \\
2x &= 3 \mod 5 \\
x &= 4 \mod 5
\end{aligned}
$$

$$
\begin{aligned}
6x + 4 &= 1 \mod 7 \\
6x &= 4 \mod 7 \\
x &= 3 \mod 7
\end{aligned}
$$

- Beachte: $24 = 4 \mod 5$ und $24 = 3 \mod 7$, da der Modulus der Lösung des Problems gleich der Lösung des modularen Problems ist.

System von Kongruenzen

- Das System von Kongruenzen des gezeigten Problems ist

$$x = 4 \mod 5 \qquad x = 3 \mod 7$$

- *Gegeben:* Ergebnis einer Rechnung in $\mathbb{Z}_m$ für verschiedene Werte von m
- *Gesucht:* ganze Zahl x, die die gegebenen Kongruenzen erfüllt.
- Lösung: *Chinese Remaindering* (im ersten Jahrhundert AD vom chinesischen Mathematiker Sun Tse entdeckt)

Beispiel

- Gegeben $a_1, a_2, m_1, m_2 \in \mathbb{Z}$ mit $\mathrm{ggT}(m_1, m_2) = 1$ so, dass

$$x = a_1 \mod m_1 \quad \text{und} \quad x = a_2 \mod m_2.$$

  Im Beispiel: $a_1 = 4, m_1 = 5, a_2 = 3, m_2 = 7$.

- Berechne die modularen Inversen ℓ_1 von m_2 in $\mathbb{Z}_{m_1}$ und ℓ_2 von m_1 in $\mathbb{Z}_{m_2}$:

$$\ell_1 m_2 = 1 \mod m_1 \quad \text{und} \quad \ell_2 m_1 = 1 \mod m_2.$$

  Im Beispiel: $\ell_1 = 3, \ell_2 = 3$.

- Dann ist *eine* ganzzahlige Lösung des Systems gegeben durch:

$$x = a_1 m_2 \ell_1 + a_2 m_1 \ell_2.$$

  Im Beispiel: $x = 129$.

Beispiel

- Dann ist *eine* ganzzahlige Lösung des Systems gegeben durch:

$$x = a_1 m_2 \ell_1 + a_2 m_1 \ell_2.$$

- Wegen $\ell_1 m_2 = 1 \mod m_1$ und $\ell_2 m_1 = 1 \mod m_2$ gilt:

$$a_1 \underbrace{m_2 \ell_1}_{=1 \mod m_1} + a_2 \underbrace{m_1 \ell_2}_{=0 \mod m_1} = a_1 \mod m_1,$$

und

$$a_1 \underbrace{m_2 \ell_1}_{=0 \mod m_2} + a_2 \underbrace{m_1 \ell_2}_{=1 \mod m_2} = a_2 \mod m_2,$$

Beispiel

- Dann ist *eine* ganzzahlige Lösung des Systems gegeben durch:

$$x = a_1 m_2 \ell_1 + a_2 m_1 \ell_2.$$

- Weitere ganzzahlige Lösungen sind gegeben durch

$$x = a_1 m_2 \ell_1 + a_2 m_1 \ell_2 + q m_1 m_2, \qquad \text{für } q \in \mathbb{Z},$$

  da $q m_1 m_2 = 0 \mod m_1$ und $q m_1 m_2 = 0 \mod m_2$.

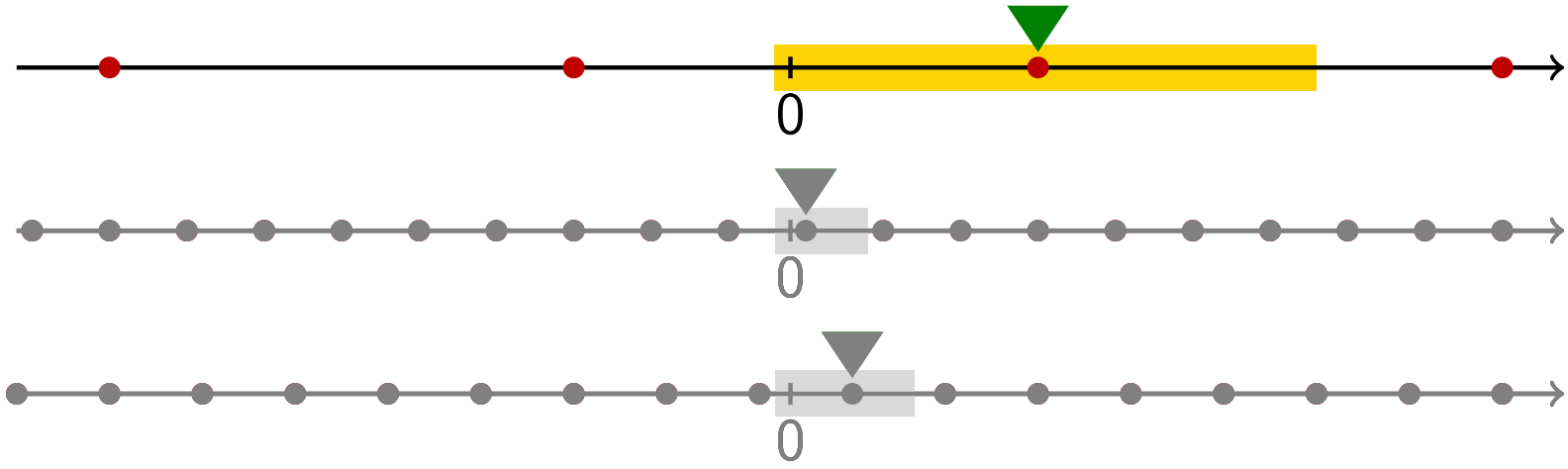
- Die kleinste nichtnegative Lösung des Systems ist der Repräsentant bezüglich Kongruenz modulo $M = m_1 m_2$ von x in $\mathbb{Z}_M$.
  Im Beispiel also $x = 129 = 24 \mod 35$.

Chinese Remaindering

- Weitere ganzzahlige Lösungen sind gegeben durch

$$x = a_1 m_2 \ell_1 + a_2 m_1 \ell_2 + q m_1 m_2, \qquad \text{für } q \in \mathbb{Z}.$$

$$x \in [x]_{m_1} \cap [x]_{m_2} = [x]_{m_1 m_2}$$



Chinesischer Restsatz

Seien $m_1, m_2, \ldots, m_n \in \mathbb{Z}$ paarweise relativ prim und das folgende System von Kongruenzen gegeben

$$\begin{aligned} x &= a_1 \mod m_1 \\ x &= a_2 \mod m_2 \\ &\vdots \\ x &= a_n \mod m_n \end{aligned}$$

mit $a_k \in \mathbb{Z}_{m_k}$. Dann existiert eine eindeutig bestimmte Lösung $x \in \mathbb{Z}_M$ mit $M = m_1 m_2 \cdots m_n$.

Chinese Remaindering Algorithm

1. Berechne $M_k = M/m_k$, d.h., M_k ist das Produkt aller Moduli ausser m_k (und damit gilt auch $\mathrm{ggT}(M_k, m_k) = 1$).
2. Für alle k berechne die modulare Inverse ℓ_k von M_k in $\mathbb{Z}_{m_k}$, also
$$\ell_k M_k = 1 \mod m_k.$$
3. Eine ganzzahlige Lösung des Systems ist gegeben durch
$$x = a_1 \underbrace{M_1\ell_1}_{=1 \mod m_1} + a_2 \underbrace{M_2\ell_2}_{=0 \mod m_1} + \cdots + a_n \underbrace{M_n\ell_n}_{=0 \mod m_1}.$$
4. Die eindeutig bestimmte Lösung in $\mathbb{Z}_M$ ist $\mathrm{rem}(x, M)$.