Der Chinesische Restsatz

Chinesischer Restsatz – Intro

Wir wollen jetzt nicht nur eine einzelne Kongruenz lösen wie $x \equiv 2 \mod 4$, sondern mehrere gleichzeitig; z.B. folgendes Problem:

Tüte mit x Gummibärchen: Wenn ich die GB an 4 Personen verteile, bleiben 2 übrig. Wenn ich sie an 7 Personen verteile, bleiben 3 übrig. Was ist x?

d.h.

$$\left.\begin{aligned} x &\equiv \quad \mod \\ x &\equiv \quad \mod \end{aligned}\right\} \textbf{Kongruenzsystem}$$

Wie löse ich das?

Allgemein:

$$\boxed{\begin{aligned} x &\equiv a_1 \mod m_1 \\ x &\equiv a_2 \mod m_2 \end{aligned}} \quad (*)$$

Wann geht das?

(1) Berechne x_1, x_2 mittels
$$m_2 \cdot x_1 \equiv 1 \mod m_1$$
$$m_1 \cdot x_2 \equiv 1 \mod m_2$$

(2) $\boxed{x := \qquad\qquad + \qquad\qquad}$ ist eine Lösung von $(*)$.

(3) Weitere Lösungen: $\boxed{x + \qquad\qquad}$ mit $z \in \mathbb{Z}$.

Beweis. $x = a_1 m_2 x_1 + a_2 m_1 x_2 \equiv \qquad \mod m_1$

$x = a_1 m_2 x_1 + a_2 m_1 x_2 \equiv \qquad \mod m_2$.

Chinesischer Restsatz – Satz

Wir notieren jetzt den allgemeinen Chinesischen Restsatz für n Kongruenzgleichungen.

<u>Chinesischer Restsatz</u>. Seien $m_1, \dots, m_n \in \mathbb{N}$ <u>paarweise teilerfremd</u> (d.h. $ggT(m_i, m_j) = 1 \ \forall\, 1 \leq i,j \leq n,\ i \neq j$). Dann besitzt das Kongruenzsystem

$$\boxed{\begin{array}{l} x \equiv a_1 \mod m_1 \\ \quad \vdots \\ x \equiv a_n \mod m_n \end{array}}$$

eine Lösung $x \mod m$, wobei $\boxed{m := m_1 \cdots m_n}$. Jede weitere Lösung y ist von der Form $y = x + z \cdot m$ für $z \in \mathbb{Z}$.

<u>Beweis / Algorithmus</u>. (0) Wir bilden $\boxed{k_i := \frac{m}{m_i} = \frac{m_1 \cdots \cancel{m_i} \cdots m_n}{\cancel{m_i}}}$.

Dann gilt $ggT(k_i, m_i) =$.

(1) Berechne Inverse x_i von $k_i \mod m_i$: $\boxed{k_i x_i \equiv 1 \mod m_i}$

(2) Berechne Lösung x : $\boxed{x = \sum_{j=1}^{n} k_j x_j a_j}$

Beweis „Lösung": $x = \underline{k_1} x_1 a_1 + \dots + \underline{k_i x_i} a_i + \dots + \underline{k_n} x_n a_n \mod \underline{m_i}$

(3) Allgemeine Lösung y: $\boxed{y = x + z \cdot m.}$

Beweis „Dies sind alle". Sei y eine weitere Lösung, d.h.

Ü

$x \equiv 1 \mod 2$

$x \equiv 2 \mod 3$

$x \equiv 3 \mod 5$

Lösen Sie das Kongruenzsystem, indem Sie folgende Schritte durchführen:

(0.) Berechnen Sie $k_1 =$
$k_2 =$
$k_3 =$

(1.) Berechnen Sie die Inversen x_i von $k_i \mod m_i$:

$= k_1 x_1 \equiv 1 \mod \quad \Rightarrow x_1 =$

$= k_2 x_2 \equiv 1 \mod \quad \Rightarrow x_2 =$

$= k_3 x_3 \equiv 1 \mod \quad \Rightarrow x_3 =$

(2.) Berechnen Sie $x =$

(3.) Allgemeine Lösung $y = x + z \cdot \underbrace{m}_{= m_1 m_2 m_3} =$