# 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. $\left.\begin{array}{l} x \equiv 2 \mod 4 \\ x \equiv 3 \mod 7 \end{array}\right\}$ **Kongruenzsystem**

Wie löse ich das?

$$7 \cdot x_1 \equiv 1 \mod 4 \qquad x_1 = 3$$
$$4 \cdot x_2 \equiv 1 \mod 7 \qquad x_2 = 2$$
$$x = 2 \cdot 7 \cdot 3 + 3 \cdot 4 \cdot 2 = 42 + 24 = 66$$

Allgemein. $\boxed{\begin{array}{l} x \equiv a_1 \mod m_1 \\ x \equiv a_2 \mod m_2 \end{array}}$ (*) Wann geht das?

1. Berechne $x_1, x_2$ mittels $\begin{array}{l} m_2 \cdot x_1 \equiv 1 \mod m_1 \\ m_1 \cdot x_2 \equiv 1 \mod m_2 \end{array}$

2. $\boxed{x := a_1 \cdot m_2 \cdot x_1 + a_2 \cdot m_1 \cdot x_2}$ ist eine Lösung von (*).

3. Weitere Lösungen: $\boxed{x + z \cdot m_1 \cdot m_2}$ mit $z \in \mathbb{Z}$.

Beweis. $x = a_1 \underline{m_2 x_1} + a_2 \underline{m_1} x_2 \equiv a_1 \cdot m_2 \cdot x_1 \equiv a_1 \cdot 1 \equiv a_1 \mod \underline{m_1}$

$x = a_1 \underline{m_2} x_1 + a_2 \underline{m_1 x_2} \equiv a_2 \cdot m_1 \cdot x_2 \equiv a_2 \mod \underline{m_2}$.

# 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. $ggT(m_i, m_j) = 1 \quad \forall\, 1 \le i,j \le n,\ i \neq j$). Dann besitzt das Kongruenzsystem

$$\boxed{\begin{aligned} x &\equiv a_1 \mod m_1 \\ &\vdots \\ x &\equiv a_n \mod m_n \end{aligned}}$$

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 $ggT(k_i, m_i) = 1$.

(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": $x = k_1 x_1 a_1 + \dots + k_i x_i a_i + \dots + k_n x_n a_n \mod m_i$

$\mod m_i$: $k_j \equiv 0 \mod m_i$ für $i \neq j$

$$x = k_i \cdot x_i \cdot a_i \equiv 1 \cdot a_i \equiv a_i \mod m_i$$

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

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

$k_1 = \cancel{m_1} \cdot m_2 \cdot m_3$

$k_2 = -_1 \cdot \cancel{-_2} \cdot -_3$

$k_3 = -_1 \cdot -_2 \cdot \cancel{-_3}$

$\boxed{Ü}$

$x \equiv \underline{1} \bmod \underline{2}$

$x \equiv \underline{2} \bmod \underline{3}$

$x \equiv \underline{3} \bmod \underline{5}$

Lösen Sie das Kongruenzsystem, indem Sie folgende Schritte durchführen:

⓪ Berechnen Sie
$k_1 = \cancel{2} \cdot 3 \cdot 5 = 15$
$k_2 = 2 \cdot \cancel{3} \cdot 5 = 10$
$k_3 = 2 \cdot 3 \cdot \cancel{5} = 6$

① Berechnen Sie die Inversen $x_i$ von $k_i \bmod m_i$:

$15 x_1 = k_1 x_1 \equiv 1 \bmod 2 \Rightarrow x_1 = \underline{1}$
$10 x_2 = k_2 x_2 \equiv 1 \bmod 3 \Rightarrow x_2 = \underline{1}$
$6 x_3 = k_3 x_3 \equiv 1 \bmod 5 \Rightarrow x_3 = \underline{1}$

② Berechnen Sie $x = 15 \cdot 1 \cdot 1 + 10 \cdot 2 \cdot 1 + 6 \cdot 3 \cdot 1$

$= 53$

③ Allgemeine Lösung $y = x + z \cdot \underbrace{m}_{\substack{\| \\ m_1 m_2 m_3 \\ 2 \cdot 3 \cdot 5 \\ 30}} = 53 + z \cdot 30 = \ldots 53; 80; \ldots$
$\ldots; -7; 23;$