

more: bigdev.de/teaching

Der Avnesische Restsatz

Chinesisches Restsatz - Intro

Wir wollen jetst wicht unt eine einzelne flongruenz løsen wie × = 2 mod 4, sondern mehrere gleich zeitig; 2.B. folgendes Problem:

Tute mit x Grunnibarchen: 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. × = 2 mod 4 Kongruendsystem

× = 3 mod 7

Wie löse ich das 2

 $7 \cdot x_1 = 1 \mod 4 \quad x_1 = 3$ $1 \cdot x_2 = 1 \mod 7 \quad x_2 = 2$ $1 \cdot x_1 = 2 \mod 7 \quad x_2 = 2$ $1 \cdot x_2 = 2 \cdot 3 \cdot 3 \cdot 4 \cdot 2 = 424 = 66$

Allewin. $\times \equiv a_1 \mod m_1 \times \equiv a_2 \mod m_2$

$$\times \equiv a_1 \mod m_1$$

 $\times \equiv a_2 \mod m_2$ (*

Wann gelt das?

- 1. Beredue $\times_{\Lambda_1} \times_2$ with $m_2 \cdot \times_{\Lambda} \equiv 1 \mod m_{\Lambda}$ $m_1 \times_2 \equiv 1 \mod m_2$
- 2 x := a₁-m₂-x₁ + a₂ m₁·x₂ ist eine Losung von (*).
- 3) Weitere Lösungen: x + 3. m, mz mit ze Z.

Benoùs. $x = a_1 m_2 x_1 + a_2 m_1 x_2 = a_1 \cdot m_2 \cdot x_1 = a_1 \cdot l = a_1 \mod m_1$

 $\times = \alpha_1 \underline{\mathsf{m}}_2 \times_1 + \alpha_2 \underline{\mathsf{m}}_1 \times_2 \equiv \alpha_2 \cdot \underline{\mathsf{m}}_1 \cdot \underline{\mathsf{x}}_2 \equiv \alpha_2 \quad \text{mod } \underline{\mathsf{m}}_2.$

Chinesischer Restsatz - Satz

Wir notieren jetzt den allgemeinen Chinesischen. Restsatz für v. Kongruenzgleichungen.

Chresischer Restsotz. Seien $m_1, m_n \in \mathbb{N}$ paerweise teilerfreud (d. h. $ggT(w_i, w_j) = 1 \quad \forall \quad 1 \leq i, j \leq n, \quad i \neq j$). Dann besitzt das Kongruenzsystem

 $\times \equiv a_n \mod m_n$ \vdots $\times \equiv a_n \mod m_n$

eine Lösung. × mod m, wobei m:= m, mn. Yede weitere Lösung y ist von der Form y = × + 2·m für ZEZ.

Beweis/Algorithmus. (O.) Wir bilden $k_i := \frac{m_1 \cdot w_1 \cdot w_n}{m_i} = \frac{m_1 \cdot w_1 \cdot w_n}{m_i}$

Dann gilt ggT(ki, mi) = 1.

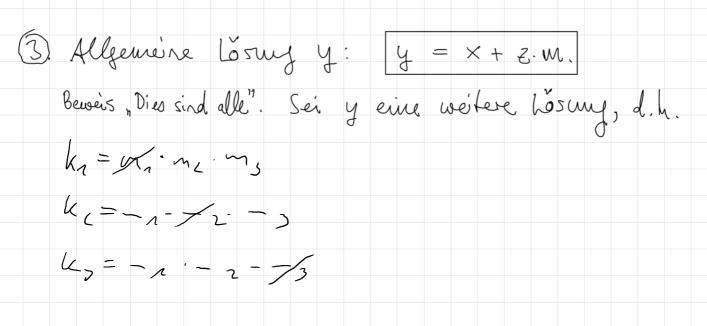
1) Beredue Inverse x; von k; mod m; : [k; x; = 1 mod m;

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

Baveis "Lösug: $x = k_1 \times_1 a_1 + ... + k_1 \times_2 a_1 + ... + k_n \times_n a_n \mod m_i$

und m: ki ±0 mod m; fir i ≠ j

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



(0.) Beredmen Sie
$$k_1 = 7.3.5 = 15$$

 $k_2 = 7.3.5 = 10$
 $k_3 = 2.3.8 = 6$

(1) Bereclinen Sie die Inversen
$$x_i$$
 von k_i mod m_i :

$$(5x_1 = k_1 \times_1 \equiv 1 \mod 2 \implies x_1 = 1)$$

$$(0x_2 = k_2 \times_2 \equiv 1 \mod 3 \implies x_2 = 1)$$

$$6x_3 = k_3 \times_3 \equiv 1 \mod 5 \implies x_3 \equiv 1$$