ČÍNSKÁ VĚTA O ZBYTCÍCH

(V:) Nechť $m_1, \dots, m_r$ je sada po dvou nesoudělných přirozených čísel.
Pak každá zbytková soustava $x = a_1 \pmod{Z_{m_1}}$
$\vdots$
$x = a_r \pmod{Z_{m_r}}$
má řešení a to je jediné $\pmod{Z_M}$,
kde M je ~~součet~~ součin řady $M = \prod_1^r m_i$

(DK) Existuje řešení (že je jediné - viz skripta)

Nejdříve vyřešíme speciální zbytkové soustavy
$x = 1 \pmod{Z_{m_i}}$
$x = 0 \pmod{Z_{m_j}}$, $j \neq i$

Řešení označím q_i, bzn. budeme řešit pro čísla $1 \leq i \leq r$.

Takto: $q_i = \left(\prod_{j \neq i} m_j\right) \cdot t$, kde $t = \left(\prod_{j \neq i} m_j\right)^{-1} \pmod{Z_{m_i}}$

(pak $q_i = 1 \pmod{Z_{m_i}}$)

↓
inverz existuje díky nesoudělnosti sady

[Bzn.: q_i počítám $\pmod{Z_M}$!]

- Potom řešení zadané soustavy bude
$x = a_1 q_1 + \dots a_r q_r \pmod{Z_M}$
protože např. $\pmod{Z_{m_i}}$ $x = a_1 \cdot 1 + a_2 \cdot 0 + \dots a_r \cdot 0$
$x = a_1$
atd.

(PŘ) Úloha $3, 4, 11 \rightarrow M = 3.4.11 = 132$

Řešte $x = 1 \pmod{3}$, $x = 2 \pmod{4}$, $x = 4 \pmod{11}$.

Nejdříve vypočteme q_i [označme raději q_{m_i}]

$\pmod{\mathbb{Z}_{132}}$ $q_3 = 4.11.\lambda$

[$\pmod{\mathbb{Z}_3}$ $4.11.\lambda = 1$

$1.2.\lambda = 1$

$2\lambda = 1$

$\lambda = 2^{-1} = 2$]

$q_3 = 4.11.2 = 88$

$\pmod{\mathbb{Z}_{132}}$ $q_4 = 3.11.\lambda$

[$\pmod{\mathbb{Z}_4}$ $3.11.\lambda = 1$

$\lambda = 9\lambda = 3.3.\lambda = 1$]

$q_4 = 3.11.1 = 33$

$\pmod{\mathbb{Z}_{132}}$ $q_{11} = 3.4.\lambda = \cancel{12\lambda}$

[$\pmod{\mathbb{Z}_{11}}$ $12\lambda = 1$

$1\lambda = 1$]

$q_{11} = 3.4.1 = 12$

Pak dosadím:

$x = 1q_3 + 2q_4 + 4q_{11} = 1.88 + 2.33 + 4.12 = 88 + 66 + 48$

$= 202 \leftarrow$ jedno řešení

$\pmod{\mathbb{Z}}$ další řešení $x = 202 + k.3.4.11 = 202 + k.132$

$\pmod{\mathbb{Z}_{132}}$ jediné řešení $x = (202 - 132) = 70$

Použití Č.V. o zbytcích → REZIDUÁLNÍ ARITMETIKA

Při +, · je respektována ≡ (~~mod~~ mod n)
 ↖ kongruence

Chci spočítat $A \cdot B$, A^3 v $\mathbb{Z}_n$

Pokud rozložím $n = m_1 \dots m_r$ → nesoudělná sada
 např. $n = p_1^{k_1} \dots p_r^{k_r}$ pro p_i různá prvočísla
 jsou $m_i = p_i^{k_i}$ nesoud. $1 \leq i \leq r$

mohu $A \cdot B$, A^3 počítat v každém $\mathbb{Z}_{m_i}$

Tím získám zbytkovou posl. pro $A \cdot B$, A^3 a Č.V. o zb. spočte $A \cdot B$, B^2 v $\mathbb{Z}_n$

(PŘ) Spočtěte reziduálně v $\mathbb{Z}_{132}$ $A \cdot B$, A^3
 pro $A = 1234567890 1$
 pro $B = 312131213121$

tím $132 = 2^2 \cdot 3 \cdot 11$ (NE $2 \cdot 2 \cdot 3 \cdot 11$)
 sada 4, 3, 11 — nesoudělná
 $q_3 = 88$, $q_4 = 33$, $q_{11} = 12$

Budu počítat v $\mathbb{Z}_3$, $\mathbb{Z}_4$, $\mathbb{Z}_{11}$

~~A·B~~ počítám $A \cdot B$

v $\mathbb{Z}_3$ $A \cdot B = (1+2+3 \dots +0+1) \cdot (3+1+ \dots) = 46 \cdot 21 = 0$ (21 → 0)

v $\mathbb{Z}_4$ $A \cdot B = 1 \cdot 21 = 1$

v $\mathbb{Z}_{11}$ $A \cdot B = (1 - \dots -8+9-0+1) \cdot (\dots -3+1-2+1) =$
 sepisuji odzadu

$= 6 \cdot (-9) = 12 = 1$

$\downarrow$

2

$\curvearrowright Z_{132} \quad A.B = 0q_3 + 1q_4 + 1q_{11} = 33 + 12 = 45$

Spočítám A^B

$\curvearrowright Z_3 \quad A^B = 46^B = 1^B = 1$

$\curvearrowright Z_4 \quad 1^B = 1$

$\curvearrowright Z_{11} \quad 6^B = 6^1 = 6$

$GCD(6, 11) = 1 \Rightarrow$ lze E.-F.

$\curvearrowright Z_{11} \; 6^{10} = 1 \Rightarrow$ exponent mod 10

$B \equiv 1 \pmod{10}$

$\curvearrowright Z_{132} \quad A^B = 1q_3 + 1q_4 + 6q_{11} = 88 + 33 + 6 \cdot 12 = 193 = \underline{61}$

POZN: Lze i použít jako 3. metodu pro hledání $A^{-1} \curvearrowright Z_n$

$\downarrow$

rekurzivně