Cvičení 2 – Eulerova věta, ČZV a RSA

7. října 2025

Algoritmus 1 (Lagrangeův)**.** Vstup: soustava k kongruencí $x \equiv x_i \bmod m_i$, kde $m_1, \ldots, m_k$ jsou navzájem nesoudělná.

Výstup: řešení kongruencí modulo $M := m_1 \cdot \cdots \cdot m_k$.

Postup:

1) $M_i = \frac{M}{m_i}$ pro všechna $i \in [k]$.
2) Spočítej a_i, b_i tak, že $a_i m_i + b_i M_i = 1$.
3) $x = \sum_{i=1}^{k} b_i M_i x_i$

Algoritmus 2 (Garnerův)**.** Vstup: soustava k kongruencí $x \equiv x_i \bmod m_i$, kde $m_1, \ldots, m_k$ jsou navzájem nesoudělná.

Výstup: řešení kongruencí modulo $M := m_1 \cdot \cdots \cdot m_k$.

Postup:

1) $(a_0, b_0, k_0) = (0, x_1, 1)$
2) $(a_i, b_i, k_i) = (a_{i-1} + b_{i-1}k_{i-1}, (x_{i+1} - a_i)c_i \bmod m_{i+1}, m_i k_{i-1}$, kde $c_i \equiv k_i^{-1} \bmod m_{i+1}$.
3) $x = a_{n-1} + b_{n-1}k_{n-1}$.

Příklad 1. Spočítejte následující úlohy:

a) $3^{40} \bmod 7$,

b) $3^{5^7} \bmod 28$,

c) jaká je poslední cifra čísla 1357^{246}?

Příklad 2. Nalezněte všechna $x \in \mathbb{Z}$ splňující následující rovnici:

a) $4^x \equiv 1 \bmod 7$,

b) $5^x \equiv 3 \bmod 13$.

Příklad 3. Dokažte, nebo vyvraťte následující tvrzení: Mějme zadané n a b. Pak jestliže pro všechna a taková, že $\mathrm{NSD}(a, n) = 1$, platí $a^b \equiv 1 \bmod n$, pak $b \equiv 0 \bmod \varphi(n)$.

Příklad 4. Najděte všechna $x \in \mathbb{Z}$ splňující:

a) $x \equiv 1 \bmod 3$, $x \equiv 3 \bmod 5$,

b) $x \equiv 2 \bmod 3$, $x \equiv 4 \bmod 7$, $x \equiv 3 \bmod 8$,

c) $10x \equiv 6 \bmod 32$, $3x \equiv 1 \bmod 5$

Příklad 5. Najděte příklad, kde bude vidět nezbytnost předpokladu na nesoudělnost čísel m_i z Čínské věty o zbytcích.

Příklad 6. Čínský velitel velel Zhuge Liang oddílu o 1000 mužích. Po bitvě u Chibi však mnoho jeho mužů padlo. Aby je nemusel každého po jednom počítat, nařídil jim, ať se nejprve seřadí po zástupu o 7 řadách, přičemž zbyli 2 muži. Následně jim nařídil se seřadit po 11, načež jich zbylo 6. Na závěr je seřadil po 13, kde zůstal jen jeden jediný. Nyní již velitel věděl, kolik mužů mu přežilo. Kolik to bylo?

Pozn: Zhuge Liang opravdu žil a bojoval v bitvě o Chibi, byl to stratég, vynálezce, filosof, správce provincie a asi i dobrý matematik, avšak Čínskou zbytkovou větu pravděpodobně neznal.

Příklad 7. Pomocí Čínské věty o zbytcích vypočtěte $12^{100} \bmod 30$.

Hint: použijte mod 5 *a mod* 6*.*

Příklad 8. Používáte systém RSA, zvolili jste si prvočísla 7 a 11. Jako exponent jste si zvolili 13.

a) Určete soukromý a vyřejný klíč.

b) Obdrželi jste zašifrovanou zprávu $c = 14$. Rozluštěte ji.

Příklad 9. Najděte m takové, aby rovnice $x^2 \equiv 1 \bmod m$ měla 3 řešení.

Příklad 10. Dokažte, že každá kvadratická rovnice nad $\mathbb{Z}_p$, kde p je prvočíslo, má nanejvýš 2 kořeny. Proč toto neplatí pro obecné n?

Příklad 11. Pro lichá n dokažte, že $n|2^{n!} - 1$.