Algebrou proti koronaviru III

(cvičení cihlovou barvou jsme udělali na cvičení, a tak je můžete vynechat)

Eulerova funkce & Eulerova věta

1. Určete hodnotu

   (a) $\varphi(600)$. [160]

   (b) $\varphi(7425)$ (mohlo by se hodit vědět, že $7425 = 27 \cdot 25 \cdot 11$). [3600]

2. Spočítejte

   (a) $3^{5^7} \bmod 28$ [19]

   (b) $100^{99^{98}} \bmod 39$ [1]

   (c) $100^{99^{98}} \bmod 40$ [0; $10000 = 250 \cdot 40$]

3. Určete poslední tři cifry čísla 249^{19}. [249; zajímá nás $249^{19} \bmod 1000$ a po lítém boji zjistíme, že $249^2 \bmod 1000 = 1$]

Čínská věta 4.13 (o zbytcích)

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

   (a) $\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 4 \pmod 7 \\ x \equiv 3 \pmod 8. \end{cases}$ [$168m + 11, m \in \mathbb{Z}$]

   (b) $\begin{cases} 2x + 1 \equiv 2 \pmod 3 \\ 3x + 2 \equiv 3 \pmod 4 \\ 4x + 3 \equiv 2 \pmod 5. \end{cases}$ [$60m + 11, m \in \mathbb{Z}$; každou rovnici převeďme na tvar $x \equiv a \pmod b$ a pak postupujme jako obvykle]

5. Najděte všechna $x \in \mathbb{Z}$ splňující

   (a) $x^2 \equiv 1 \pmod 3$ a $x^2 \equiv 1 \pmod 7$. [$x = 21m + 1$, $x = 21m + 8$, $x = 21m + 13$ a $x = 21 + 20$, kde $m \in \mathbb{Z}$; z prvního cvičení víme, že rovnice $x^2 \equiv 1 \pmod p$ má pro prvočíslo p řešení právě $\pm 1 + k \cdot p, k \in \mathbb{Z}$, dostaneme tedy 4 možné soustavy (kombinace) lineárních rovnic]

   (b) $x^2 \equiv -1 \pmod{65}$. [$x = 65m + 8$, $x = 65m - 8$, $x = 65m + 18$ a $x = 65m - 18$, kde $m \in \mathbb{Z}$; použijme ČVZ naopak: převeďme na soustavu $\begin{cases} x^2 \equiv -1 \pmod 5 \\ x^2 \equiv -1 \pmod{13} \end{cases}$, kde je možné například řešení odhadnout, a následně „zvedněme“ řešení zpět $\pmod{65}$]

6. Najděte příklad, na kterém bude vidět nezbytnost předpokladu nesoudělnosti čísel m_i v Čínské **Větě 4.13** ve skriptech. [Např. $\begin{cases} x \equiv 0 \bmod 2 \\ x \equiv 1 \bmod 4 \end{cases}$]

A pro odvážné několik zábavných a zcela dobrovolných příkladů navíc:

7. $\begin{cases} 10x \equiv 6 \pmod{32} \\ 3x \equiv 1 \pmod{5} \end{cases}$ [$80m + 7, m \in \mathbb{Z}$]

8. Najděte všechna $x, y \in \mathbb{Z}$ splňující $x^6 + x + xy \equiv 1 \pmod 7$. [$x \not\equiv 0, y \equiv 6 \pmod 7$; podle Eulerovy věty pro nenulové x platí $x^6 \equiv 1 \bmod 7$, tedy se rovnice redukuje na $x(1 + y) \equiv 0 \bmod 7$, což je (díky tomu, že 7 je prvočíslo) ekvivalentní podmínce $x \equiv 0 \bmod 7 \vee y \equiv 6 \bmod 7$]

9. Najděte všechna $x \in \mathbb{Z}$ splňující $x^{11} \equiv 2 \pmod 5$ a $x^8 \equiv 1 \pmod 7$. [$x = 35m + 8$ a $x = 35m + 13$, $m \in \mathbb{Z}$]

10.⋆ Spočítejte

   (a) $3^{3^{3^{3^3}}} \bmod 28$. [27; Eulerova věta stále dokola s tím, že $3^{3^{3^3}} \equiv 1 \bmod 2$]

   (b) $3^{5^{7^{9^{11^{13}}}}} \bmod 28$. [19, Eulerova věta stále dokola]

11.⋆ Dokažte, že 13 dělí $23^{32} + 29^{33} + 36^{34}$. [skrze modulární aritmetiku, resp. Eulerovu větu zjistíme, že platí $23^{32} \equiv 9 \pmod{13}, 29^{33} \equiv 1 \pmod{13}, 36^{34} \equiv 3 \pmod{13}$ a součet je tedy modulo 13 roven 0.]

12.⋆ Spočtěte $130^{9^{3^{2021^{123}}}} \bmod 221$. [91; buď pomocí Eulerovy věty (pozor na předpoklad nesoudělnosti) nebo skrze ČVZ rozdělením na dvě kongruence mod 17 a mod 13]

13.⋆ Najděte všechna $x \in \{0, 1, \ldots, 76\}$ splňující $x^2 + 8x \equiv 62 \pmod{77}$. [$30, 39, 72, 74$; převeďme na $x^2 + 8x + 15 = (x + 3)(x + 5) \equiv 0 \pmod{77}$, pomocí ČVZ vyřešme modulo 7, resp. 11 čtyři možné případy a „zvedněme“ zpět modulo 77]

14.⋆ Nechť jsou p, q dvě různá prvočísla.

   (a) Dokažte, že má polynom $x^3 + 3x^2 + 2x$ v okruhu $\mathbb{Z}_{pq}$ právě 9 kořenů. [devět soustav $\begin{cases} x \equiv a \pmod p \\ x \equiv b \pmod q \end{cases}$, kde $a, b \in \{0, pq - 2, pq - 3\}$ dává díky ČVZ hledaných devět kořenů (proč jsou po dvou různé?, proč jsou všechny?)]

   (b) Rozhodněte, zda existují $a, b \in \mathbb{Z}_{pq}$, aby měl polynom $x^2 + ax + b$ v okruhu $\mathbb{Z}_{pq}$ právě 3 kořeny. [Neexistuje - viz předchozí úvahu: v $\mathbb{Z}_p$ by musel mít 3 kořeny (a v $\mathbb{Z}_q$ pak jeden), což pro kvadratický polynom nelze.]