

2. Algebrou proti nadměrné radosti ze začátku semestru

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) $3^{57} \pmod{28}$ [19]

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

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

3. Dokažte, že pro každé prvočíslo $p \neq 2$ platí $p \mid 1^p + 2^p + 3^p + \dots + p^p$.

[počítejme modulo p a $p - 1$ -krát využijme Eulerovu větu]

Čínská věta 1.14 (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)
$$\begin{cases} 2x + 1 \equiv 2 \pmod{3} \\ 3x + 2 \equiv 3 \pmod{4} \\ 4x + 3 \equiv 2 \pmod{5}. \end{cases}$$

[$60m + 11, m \in \mathbb{Z}$; rovnice převedeme na tvar $x \equiv a \pmod{b}$ a pak postupujeme jako obvykle]

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

(a)
$$\begin{cases} x^2 \equiv 1 \pmod{3} \\ x^2 \equiv 1 \pmod{7}. \end{cases}$$
 [$x = 21m + 1, x = 21m + 8, x = 21m + 13$]

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)
$$\begin{cases} 10x \equiv 6 \pmod{32} \\ 3x \equiv 1 \pmod{5} \end{cases}$$
 [$80m + 7, m \in \mathbb{Z}$, pozor na soudělnost v první rovnici]

(c) $x^2 \equiv -1 \pmod{66}$. [\emptyset , protože $x^2 \equiv -1 \pmod{3}$ nemá řešení v \mathbb{Z}_3]

(d) $x^2 \equiv -1 \pmod{65}$. [$x = 65m + 8, x = 65m - 8, x = 65m + 18$ a $x = 65m - 18$,

kde $m \in \mathbb{Z}$; použijme ČVZ naopak: převedme 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 o zbytcích ve skriptech.

[Např.
$$\begin{cases} x \equiv 0 \pmod{2} \\ x \equiv 1 \pmod{4} \end{cases}$$
]

A pro odvážné několik zábavných příkladů navíc:

7. Určete poslední tři cifry čísla 249^{19} .
[249; zajímá nás $249^{19} \pmod{1000}$ a po litém boji zjistíme, že $249^2 \pmod{1000} = 1$]
8. Spočítejte
- (a) $3^{3^{3^{3^3}}} \pmod{28}$. [27; Eulerova věta stále dokola s tím, že $3^{3^{3^3}} \equiv 1 \pmod{2}$]
- (b) $3^{5^{7^{9^{11^{13}}}}} \pmod{28}$. [19, Eulerova věta stále dokola]
- (c) $130^{9^{3^{2021^{12^3}}}} \pmod{221}$. [91; buď pomocí Eulerovy věty (pozor na předpoklad nesoudělnosti) nebo skrze ČVZ rozdělením na dvě kongruence mod 17 a mod 13]
9. Dokažte, že
- (a) 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.]
- (b) $9 \mid 4^n + 6n - 1$ pro každé n přirozené. [indukcí dle n]
10. Najděte všechna $x \in \mathbb{Z}$ splňující $26^5 x \equiv 16 \pmod{11}$. [$5 + k \cdot 11, k \in \mathbb{Z}$; dá se využít faktu, že $26^5 \equiv 4^5 = 2^{10} \pmod{11}$ a nyní už jen použijme Eulerovu větu]
11. Najděte všechna $x \in \mathbb{Z}$, pro která platí $\begin{cases} 13x \equiv 15 \pmod{27} \\ 2x \equiv 1 \pmod{3} \end{cases}$ [∅]
12. Najděte všechna $x \in \mathbb{Z}$, pro která platí $\begin{cases} x^2 \equiv 36 \pmod{45} \\ x^2 \equiv -1 \pmod{65} \end{cases}$. [∅; lze si všimnout, že z první rovnice plyne $x^2 \equiv 1 \pmod{5}$, kdežto z druhé $x^2 \equiv -1 \pmod{5}$.]
13. Najděte všechna $x \in \mathbb{Z}$, pro která platí $\begin{cases} 3^x \equiv 1 \pmod{13} \\ 3x \equiv 1 \pmod{13} \end{cases}$. [$9 + 39k, k \in \mathbb{Z}$]
14. Buď $m, n \in \mathbb{N}$ nesoudělná. Nechť $1 = um + vn$. Dokažte, že prvek $x = bum + avn$ je řešením soustavy kongruencí $x \equiv a \pmod{m}$ a $x \equiv b \pmod{n}$. Na základě tohoto pozorování formulujte důkaz existenční části čínské věty o zbytcích.
15. Najděte všechna čísla n taková, že $\varphi(n) = 18$. [19, 27, 38, 54]
16. Najděte všechna čísla n taková, že $\varphi(n) \mid n$. [$n = 2^k \cdot 3^l$ pro $k, l \in \mathbb{N}$]
17. Označme $\sigma(n)$ součet všech dělitelů přirozeného čísla n . Najděte vzorec pro výpočet $\sigma(n)$, pokud znáte prvočíselný rozklad čísla n . Inspirujte se důkazem vzorce pro Eulerovu funkci. [řešení třeba tady]
18. 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 $x^6 \equiv 1 \pmod{7}$, tedy se rovnice redukuje na $x(1 + y) \equiv 0 \pmod{7}$, což je (díky tomu, že 7 je prvočíslo) ekvivalentní podmínce $x \equiv 0 \pmod{7} \vee y \equiv 6 \pmod{7}$]
19. Najděte všechna $x \in \{0, 1, \dots, 76\}$ splňující $x^2 + 8x \equiv 62 \pmod{77}$. [30, 39, 72, 74; převedme 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]
- 20.* 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.]