Elementární teorie čísel II

2 Elementární teorie čísel II

2.1 Eulerova věta a kryptosystém RSA

1. Určete hodnotu $\varphi(600)$ a $\varphi(7425)$. (Hint: $7425 = 27 \cdot 25 \cdot 11$) [160; 3600]

2. Spočítejte

1. $3^{5^7} \bmod 28$ [19]
2. $100^{99^{98}} \bmod 39$ [1]
3. $100^{99^{98}} \bmod 40$ [0; $10000 = 250 \cdot 40$]
4. $3^{3^{3^{3^3}}} \bmod 28$. [27; Eulerova věta + rozbor mocnin modulo 12]

3. Dokažte, že $13 \mid 16^{20} + 29^{21} + 42^{22}$ a $9 \mid 4^n + 6n - 1$ pro každé n přirozené. [Počítání modulo 13; Indukce + počítání modulo 9]

4. Dokažte, že pro každé prvočíslo $p \neq 2$ platí $p \mid 1^p + 2^p + 3^p + \ldots + p^p$. [Malá fermatova věta + součet aritmetické řady.]

5. 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 $x \equiv 0 \bmod 7 \vee y \equiv 6 \bmod 7$]

6. Najděte všechna $x \in \mathbb{Z}$ splňující $26^5 x \equiv 16 \pmod{11}$. [$x \in \{11k + 5; k \in \mathbb{Z}\}$]

7. Najděte všechna čísla n taková, že $\varphi(n) = 18$. [$19, 27, 38, 54$]

8. Najděte všechna čísla n taková, že $\varphi(n) \mid n$. [$n = 2^a 3^b; a > 0, b \geq 0$]

2.2 Čínská věta o zbytcích

1. Najděte všechna $x \in \mathbb{Z}$ splňující $\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 4 \pmod 7 \\ x \equiv 3 \pmod 8. \end{cases}$ [$168m + 11, m \in \mathbb{Z}$]

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

3. Najděte všechna $x \in \mathbb{Z}$ splňující $\begin{cases} x^2 \equiv 1 \pmod 3 \\ x^2 \equiv 1 \pmod 7). \end{cases}$ [$x = 21m + 1$, $x = 21m + 8$, $x = 21m + 13$ 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]

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

5. Najděte všechna $x \in \mathbb{Z}$ splňující $x^2 \equiv -1 \pmod{65}$. [$x = 65m + 8$, $x = 65m - 8$, $x = 65m + 18$ 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 všechna $x \in \mathbb{Z}$, pro která platí $3^x \equiv 1 \pmod{13}$ a $3x \equiv 1 \pmod{13}$. [$x \in \{39k + 9; k \in \mathbb{Z}\}$]