Algebra 21/22: 2. cvičení — skupina Ježil

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: $7425 = 27 \cdot 25 \cdot 11$)

2. Spočítejte

1. $3^{5^7} \bmod 28$
2. $100^{99^{98}} \bmod 39$
3. $100^{99^{98}} \bmod 40$
4. $3^{3^{3^{3^{3^{3^{3}}}}}} \bmod 28.$

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

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

5. Najděte všechna $x, y \in \mathbb{Z}$ splňující $x^6 + x + xy \equiv 1 \pmod 7$.

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

7. Najděte všechna čísla n taková, že $\varphi(n) = 18$.

8. Najděte všechna čísla n taková, že $\varphi(n) \mid n$.

2.2 Čínská věta o zbytcích

1. Najděte všechna $x \in \mathbb{Z}$ splňující $\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 4 \pmod 7 \\ x \equiv 3 \pmod 8. \end{cases}$

2. Najděte všechna $x \in \mathbb{Z}$ splňující $\begin{cases} 2x + 1 \equiv 2 \pmod 3 \\ 3x + 2 \equiv 3 \pmod 4 \\ 4x + 3 \equiv 2 \pmod 5. \end{cases}$

3. Najděte všechna $x \in \mathbb{Z}$ splňující $\begin{cases} x^2 \equiv 1 \pmod 3 \\ x^2 \equiv 1 \pmod 7. \end{cases}$

4. Najděte všechna $x \in \mathbb{Z}$ splňující $\begin{cases} 10x \equiv 6 \pmod{32} \\ 3x \equiv 1 \pmod 5 \end{cases}$

5. Najděte všechna $x \in \mathbb{Z}$ splňující $x^2 \equiv -1 \pmod{65}$.

6. Najděte všechna $x \in \mathbb{Z}$, pro která platí $3^x \equiv 1 \pmod{13}$ a $3x \equiv 1 \pmod{13}$.