Algebra — cvičení 3

(příklady cihlovou barvou jsme dělali on-line, na doma jsou ty ostatní bez hvězdiček, přičemž můžete vypustit libovolný jeden z nich)

Základní příklady

*Připomeňme z přednášky Eulerovu větu, která říká, že pro $a \in \mathbb{Z}$ a $m \in \mathbb{N}$ platí $a^{\varphi(m)} \equiv 1 \pmod m$, **pokud** jsou a, m nesoudělná. Jelikož lze každé $e \in \mathbb{N}$ zapsat ve tvaru $e = k\varphi(m) + z$, kde $0 \leq z < \varphi(m)$ a $k \in \mathbb{N}_0$, je možné — za předpokladu nesoudělných a, m — počítát pomocí Eulerovy věty*

$$a^e = a^{k\varphi(m)+z} = a^z a^{\varphi(m)^k} \equiv a^z \cdot 1^k = a^z \pmod m.$$

Zatímco tedy v základu můžeme kdykoliv „vymodulit" m, v exponentu lze kdykoliv „vymodulit" $\varphi(m)$, pokud je splněn předpoklad věty. Využíváme samozřejmě, že pro $1 < m = {p_1}^{e_1} \cdot \cdots \cdot {p_n}^{e_n}$, kde p_i jsou po dvou různá prvočísla, platí

$$\varphi(m) = \prod_{i=1}^{n} (p_i - 1){p_i}^{e_i - 1} \qquad \text{a} \quad \varphi(1) = 1.$$

1. Spočítejte
   (a) $100^{99^{98}} \bmod 40$.
   (b) $100^{99^{98}} \bmod 39$.
2. Spočítejte
   (a) $3^{3^{3^{3^3}}} \bmod 28$.
   (b) $3^{5^{7^{9^{11^{13}}}}} \bmod 28$.
3. Najděte všechna $x \in \mathbb{Z}$ splňující
   (a) $x \equiv 2 \pmod 3$, $x \equiv 4 \pmod 7$ a $x \equiv 3 \pmod 8$.
   (b) $2x + 1 \equiv 2 \pmod 3$, $3x + 2 \equiv 3 \pmod 4$ a $4x + 3 \equiv 2 \pmod 5$.
   (c) $10x \equiv 6 \pmod{32}$ a $3x \equiv 1 \pmod 5$.
4. Najděte všechna $x \in \mathbb{Z}$ splňující
   (a) $x^2 \equiv 1 \pmod 3$ a $x^2 \equiv 1 \pmod 7$.
   (b) $x^2 \equiv -1 \pmod{65}$.

Další počítání

5. Najděte všechna $x \in \mathbb{Z}$ splňující $x^{11} \equiv 2 \pmod 5$ a $x^8 \equiv 1 \pmod 7$.
6. Dokažte, že 13 dělí $23^{32} + 29^{33} + 36^{34}$.
7. Najděte všechna $x, y \in \mathbb{Z}$ splňující $x^6 + x + xy \equiv 1 \pmod 7$.
8. Určete poslední tři cifry čísla 249^{19}.

9. Najděte všechna $x \in \mathbb{Z}_{77}$ taková, že (v $\mathbb{Z}_{77}$) platí $x^2 + 8x = 62$.

10.* Spočtěte $130^{9^{3^{2021^{123}}}} \bmod 221$.

11.* 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.

(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.

12.* Dokažte, že $\lim_{n\to\infty} \varphi(n) = \infty$.

Pár řešení pro inspiraci.

1. (a) Pozor 40 a 100 jsou soudělné. Řešení je ale snadné $100 \cdot 100 \mod 40 = 5 \cdot 20 \cdot 2 \cdot 50 \mod 40 = 0 \implies 100^{99^{98}} \mod 40 = 0$.

1. (b) Jelikož jsou 39 a 100 nesoudělná, můžeme užít Eulerovu větu. Pro začátek máme $\varphi(39) = 2 \cdot 12 = 24$. Dále potřebujeme zjistit, kolik je $99^{98} \mod 24 = 3^{98} \mod 24$. Tady ale jsou 3 a 24 soudělná čísla, takže žádná Eulerova věta!

Můžeme si ale pomoci jinak. Mocnina trojky je jistě nějakým násobkem tří, takže si napíšeme $3x \equiv 3^{98} \pmod{24}$, což je ekvivalentní $x \equiv 3^{97} \pmod 8$. Již víme, že liché číslo na druhou modulo 8 je jedna, takže $3^{97} \mod 8 = 3$. Pro $x = 3$ pak dostáváme, že $3^{98} \mod 24 = 9$.

Víme tedy, že $99^{98} \mod 24 = 9$ a zbývá spočíst $100^9 \mod 39 = 22^9 \mod 39 = 2^9 \cdot 11^9 \mod 39$. Jelikož $11^2 \mod 39 = 2^2$, máme $2^9 \cdot 11^9 \mod 39 = 11 \cdot 2^{17} \mod 39 = 11 \cdot 4 \cdot (-7)^3 \mod 39$. Poslední krok plyne z $2^5 \equiv -7 \pmod{39}$. Konečně $11 \cdot 4 \cdot (-7)^3 \mod 39 = 5 \cdot (-7) \cdot 10 \mod 39 = 40 \mod 39 = 1$.

3. (a) Postupným dosazováním dostáváme: $x = 3k+2$ pro $k \in \mathbb{Z}$; $3k+2 \equiv 4 \pmod 7 \iff k \equiv 10 \equiv 3 \pmod 7$; máme $k = 7l + 3$ pro $l \in \mathbb{Z}$, a tedy $x = 3k + 2 = 3(7l + 3) + 2 = 21l + 11$; dosazením do poslední kongruence pak $21l + 11 \equiv 3 \pmod 8$, což je ekvivalentní $8 \mid 5l$, což je totéž jako $8 \mid l$. Dohromady proto $x = 21l + 11 = 21(8m) + 11 = 168m + 11$, kde $m \in \mathbb{Z}$.