Elementární teorie čísel

1 Elementární teorie čísel

1.1 NSD

1. Najděte NSD $(37, 10)$ a příslušné Bézoutovy koeficienty. [$1 = 3 \cdot 37 - 11 \cdot 10$; v $\mathbb{Z}_{37}$ tedy platí $10^{-1} = -11 \equiv 26 \pmod{37}$]

2. Najděte NSD $(1023, 96)$ a příslušné Bézoutovy koeficienty. [$3 = 1023 \cdot (-3) + 96 \cdot 32$]

3. Spočtěte NSD$(2^{92} - 1, 2^{31} - 1)$ a příslušné Bézoutovy koeficienty. [$1 = (-2) \cdot (2^{92} - 1) + \left[\left(2^{62} + 2^{31} + 1\right) \cdot \left(2^{31} - 1\right)\right]$]

4. Najděte 27^{-1} v tělese $\mathbb{Z}_{41}$. [38]

5. Spočtěte inverzní prvek 29^{-1} v tělese $\mathbb{Z}_{37}$. Je možné uvažovat inverzní prvek a^{-1} také modulo m, které není prvočíslo? Co třeba 29^{-1} nebo 33^{-1} v okruhu $\mathbb{Z}_{39}$? [23; 35; neexistuje např. protože $33 \cdot 26 \equiv 0 \pmod{39}$]

6. Rozmyslete si, že Eukleidův algoritmus lze provádět i s polynomy a že výsledkem bude NSD dvou polynomů. Spočtěte NSD$(x^3 + x^2 + x + 1, x^2 + 2x + 2)$ a příslušné Bézoutovy koeficienty. Zkuste úlohu vyřešit jak nad tělesem racionálních čísel, tak v nějakém konečném tělese, například $\mathbb{Z}_3$ nebo $\mathbb{Z}_5$. Vyjdou výsledky stejného stupně? (V tomto cvičení poněkud předbíháme, formálně si zavedeme polynomy a jejich dělitelnost později. Nicméně pokud jste někdy potkali dělení polynomů, úloha by měla být jasná.) [Pro $\mathbb{Q}$ a $\mathbb{Z}_3$: 5 s koeficienty $-x + 1$ a $x^2 - 2x + 2$, Pro $\mathbb{Z}_5$: $x + 3$ s koeficienty 1 a $1 - x$]

1.2 Kongruence a modulární aritmetika

1. Najděte všechna $x \in \mathbb{Z}$ splňující $10x \equiv 2 \pmod{14}$. [$x \in \{3 + 7k; k \in \mathbb{Z}\}$]

2. Najděte všechna $x \in \mathbb{Z}$ splňující $x^2 + 10x + 6 \equiv 0 \pmod{17}$. [$x \in \{j + 17k; j \in \{1, 6\}, k \in \mathbb{Z}\}$]

3. Dokažte, že

$$ca \equiv cb \pmod{m} \;\Leftrightarrow\; a \equiv b \pmod{m/\operatorname{NSD}(c, m)}.$$

4. Vyřešte v celých číslech následující rovnice:

1. $x \equiv 2 \pmod{8}$ [$x = 2 + 8k; k \in \mathbb{Z}$]
2. $3x \equiv 2 \pmod{5}$ [$x = 4 + 5k; k \in \mathbb{Z}$]
3. $6x \equiv 2 \pmod{8}$ [$x = 3 + 4k; k \in \mathbb{Z}$; pozor na změnu modulu, když „dělíme dvojkou“]
4. $x^2 \equiv 36 \pmod{45}$ [$\{6, 9\} + 15k, k \in \mathbb{Z}$]

5. Ukažte, že $n^2 \equiv 1 \pmod{8}$ pro každé liché $n \in \mathbb{N}$. [Jak vypadají lichá čísla mod 8?]

6. Buď p prvočíslo. Najděte všechna celočíselná řešení rovnice $x^2 \equiv 1 \pmod{p}$ a ukažte, že jsou opravdu všechna. [$x = \pm 1 + kp, k \in \mathbb{Z}$; převeďte na $p \mid (x + 1)(x - 1)$ a využijte charakterizace prvočísel]

1.3 Příklady navíc

1. Dokažte, že $\operatorname{NSD}(a, b) \cdot \operatorname{NSN}(a, b) = a \cdot b$, pro všechna $a, b \in \mathbb{N}$.

2. Spočtěte NSD$(2k - 1, 3k + 1)$ a příslušné Bézoutovy koeficienty v závislosti na $k \in \mathbb{N}$.

3. Najděte všechna $x, y, z \in \mathbb{Z}$ splňující $x^2 + y^2 + z^2 = 15w^2$. (*Návod:* řešte nejprve kongruenci modulo 8.)