Elementární teorie čísel

1 Elementární teorie čísel

1.1 NSD

1. Najděte NSD $(37, 10)$ a příslušné Bézoutovy koeficienty.

2. Najděte NSD $(1023, 96)$ a příslušné Bézoutovy koeficienty.

3. Spočtěte NSD$(2^{92} - 1, 2^{31} - 1)$ a příslušné Bézoutovy koeficienty.

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

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 $\mathbb{Z}_{39}$?

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.)

1.2 Kongruence a modulární aritmetika

1. Najděte všechna $x \in \mathbb{Z}$ splňující $10x \equiv 2 \pmod{14}$.

2. Najděte všechna $x \in \mathbb{Z}$ splňující $x^2 + 10x + 6 \equiv 0 \pmod{17}$.

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. $x \equiv 2 \,(\mathrm{mod}\, 8)$
2. $3x \equiv 2 \,(\mathrm{mod}\, 5)$
3. $6x \equiv 2 \,(\mathrm{mod}\, 8)$
4. $x^2 \equiv 36 \,(\mathrm{mod}\, 45)$

5. Ukažte, že $n^2 \equiv 1 \,(\mathrm{mod}\, 8)$ pro každé liché $n \in \mathbb{N}$.

6. Buď p prvočíslo. Najděte všechna celočíselná řešení rovnice $x^2 \equiv 1 \,(\mathrm{mod}\, p)$ a ukažte, že jsou opravdu všechna.

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.)