Cvičení 8. 3. 2013

Pro n přirozené definujeme grupu $\mathbb{Z}_n^\star$ sestávající z čísel mezi 1 a n nesoudělných s n s operací násobení modulo n. Buď a celé číslo nesoudělné s n.

Počet prvků grupy $\mathbb{Z}_n^\star$ označme $\phi(n)$ (Eulerova funkce). Číslo $\phi(n)$ lze spočítat z prvočíselného rozkladu $n = p_1^{a_1} \cdots p_k^{a_k}$ jako

$$\phi(n) = p_1^{a_1-1} \cdots p_k^{a_k-1}(p_1 - 1) \cdots (p_k - 1).$$

Řád prvku $a \in \mathbb{Z}_n^\star$ je nejmenší $m > 0$ takové, že $a^m \equiv 1 \pmod{n}$. Lagrangeova věta nám říká, že $m \mid \phi(n)$.

Pokud se situace zdá beznadějná, vzpomeňte si na čínskou zbytkovou větu.

Příklad 1. Nakreslete prvky $\mathbb{Z}_{36}$ uspořádané dělitelností. Vyznačte na obrázku podgrupy a řády prvků v grupě $(\mathbb{Z}_{36}, +)$. Co vidíte? Dokážete to zformulovat a dokázat jako větu?

Příklad 2. Najděte n, a takové, že $a \in \mathbb{Z}_n^\star, a \neq 1$ a prvek a má řád ostře menší než $\phi(n)$.

Příklad 3. Dokažte, že:

1. $16 \mid 5^{80} - 1$
2. $198 \mid 13^{62} + 29$

Příklad 4. Spočtěte $5^{20} \pmod{26}$, $9^{128} \pmod{48}$, $2^{3^{4^{5^{6^7}}}} \pmod{9}$.

Příklad 5. Vyřešte v $\mathbb{Z}$ rovnici

$$x^6 + x + xy \equiv 1 \pmod{7}$$

Příklad 6. Kolik existuje v grupě $\mathbb{Z}_n$ prvků k takových, že $\langle k \rangle = \mathbb{Z}_n$?

Příklad 7. Buď p prvočíslo. Kolik existuje v grupě $\mathbb{Z}_p^\star$ prvků řádu 2?

Příklad 8. Buď $n = p_1^{a_1} \cdots p_k^{a_k}$. Dokažte, že:

1. Okruh $\mathbb{Z}_n$ je isomorfní $\mathbb{Z}_{p_1^{a_1}} \times \mathbb{Z}_{p_2^{a_2}} \times \cdots \times \mathbb{Z}_{p_k^{a_k}}$,
2. grupa $\mathbb{Z}_n^\star$ je isomorfní $\mathbb{Z}_{p_1^{a_1}}^\star \times \mathbb{Z}_{p_2^{a_2}}^\star \times \cdots \times \mathbb{Z}_{p_k^{a_k}}^\star$.

Příklad 9. Spočtěte

$$\limsup_{n\to\infty} \phi(n),$$
$$\liminf_{n\to\infty} \phi(n).$$

Kreativní úlohy

Příklad 10 (Wilsonovo kritérium)**.** Dokažte, že číslo p je prvočíslo, právě když platí

$$(p-1)! \equiv -1 \pmod{p}.$$

Příklad 11 (návrat těžké úlohy)**.** Buď $p > 2$ prvočíslo. Dokažte, že p dělí čitatele zlomku

$$1 + 1/2 + \cdots + 1/(p-1).$$