Cvičení 22. 3. 2013

Díky čínské zbytkové větě víme:

$$\mathbb{Z}^\star_{p_1^{a_1}\cdots p_k^{a_k}} = \mathbb{Z}^\star_{p_1^{a_1}} \times \mathbb{Z}^\star_{p_2^{a_2}} \times \cdots \times \mathbb{Z}^\star_{p_k^{a_k}}.$$

Pro p liché prvočíslo je $(\mathbb{Z}_{p^n})^\star \simeq \mathbb{Z}_{p^{n-1}(p-1)}$, pro dvojku máme $\mathbb{Z}_2^\star$ triviální, $\mathbb{Z}_4^\star$ dvouprvkovou a v ostatních případech

$$(\mathbb{Z}_{2^n}) \simeq \mathbb{Z}_2 \times \mathbb{Z}_{2^{n-2}}.$$

Pro $n > 2$ lze každý prvek $\mathbb{Z}_{2^n}$ psát ve tvaru $(-1)^a 5^b$. Tyto skutečnosti mají mnoho praktických použití.

Příklad 1 (z minule)**.** Najděte všechna M taková, že $M^7 \equiv M \pmod{141}$.

Příklad 2. Sestrojte isomorfismus grup:

1. $\mathbb{Z}_{15}$ a $\mathbb{Z}_3 \times \mathbb{Z}_5$,
2. $\mathbb{Z}^\star_{13}$ a $\mathbb{Z}_{12}$,
3. $\mathbb{Z}^\star_7$ a $\mathbb{Z}_6$,
4. $\mathbb{Z}^\star_{75}$ a $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_5$.

Příklad 3. Najděte všechny prvky, které generují grupy:

1. $\mathbb{Z}^\star_7$,
2. $\mathbb{Z}^\star_{11}$,
3. $\mathbb{Z}^\star_{18}$,
4. $\mathbb{Z}^\star_{16}$.

Příklad 4 (Eulerova věta není optimální)**.** Jaké nejmenší $e \in \mathbb{N}$ můžeme zvolit, aby platila věta: „Pro každé a nesoudělné s 91 platí $a^e \equiv 1 \pmod{91}$“?

Příklad 5. Číslo n se nazývá Carmichaelovo číslo, pokud n není prvočíslo, ale platí $\forall a, (a,n) = 1 \Rightarrow a^{n-1} \equiv 1 \pmod{n}$. Dokažte, že číslo $3 \cdot 11 \cdot 17 = 561$ je Carmichaelovo číslo.

Příklad 6 (opakování z přednášky)**.** Dokažte, že pro každé $n \geq 1$ platí

$$5^{2^{n-3}} \equiv 1 + 2^{n-1} \pmod{2^n}.$$

Co z toho plyne pro řád prvku 5 v grupě $\mathbb{Z}_{2^n}^{\star}$?

Kreativní úlohy

Příklad 7. Buď $n > 1$. Dokažte, že grupa $\mathbb{Z}_n^{\star}$ je cyklická, právě když n má tvar 2, 4, p^m nebo $2p^m$ pro p liché prvočíslo.