Cvičení 10. 5. 2012

Exponent grupy G je nejmenší přirozené číslo n takové, že $g^n = e$ pro každé $g \in G$. Je to nejmenší společný násobek řádů prvků G.

Na přednášce jste používali značení $\exp_n(k)$ pro řád prvku k v grupě $\mathbb{Z}_n^\star$ (pojem dává smysl jen pro k nesoudělné s n). Platí:

1. Pokud $a \equiv b \pmod{n}$, tak $\exp_n(a) = \exp_n(b)$
2. Pokud k, n jsou nesoudělná tak z Čínské zbytkové věty máme $\exp_{kn}(a) = nsn(\exp_k(a), \exp_n(a))$, stačí tedy znát $\exp_{p^i}(a)$ pro p prvočísla.
3. Vždy $\exp_n(a) \mid \varphi(n)$.
4. Pokud známe faktorizaci $\varphi(n) = q_1^{k_1} \dots q_l^{k_l}$, tak můžeme určit mocninu q_i v $\exp_n(a)$ jako minimální $0 \leq m \leq k_i$, že $a^{\varphi(n) q_i^{m-k_i}} \equiv 1 \pmod{n}$.

Pokud si zvolíme p pevné prvočíslo, a nesoudělné s k a $r_i = \exp_{p^i}(a)$, tak platí:

1. $r_i | r_{i+1}$
2. Buď $r_{i+1} = r_i$, nebo $r_{i+1} = p r_i$.
3. Pokud k je maximální takové, že $a^{r_2} \equiv 1 \pmod{p}^k$, tak

$$r_2 = r_3 = \dots = r_k$$

a navíc

$$r_{k+i} = p^i r_2.$$

Příklad 1. Dokažte, že pro každé $n \in \mathbb{N}$ je exponent grupy $\mathbb{Z}_n^\star$ dělitelem čísla $\varphi(n)$.

Příklad 2. Určete exponent grupy:

1. $\mathbb{Z}_{13}$
2. $\mathbb{Z}_2 \times \mathbb{Z}_2$
3. $\mathbb{Z}_{10}^\star$
4. $\mathbb{Z}_{256}^\star$

Příklad 3. Spočtěte řád prvku (v závislosti na i, pokud je přítomno):

1. $\exp_{13}(2)$
2. $\exp_{13}(3)$
3. $\exp_{113}(2)$
4. $\exp_{26}(11)$
5. $\exp_{2^i}(5)$
6. $\exp_{5^i}(9)$

Příklad 4. Dokažte, že pokud G je konečná komutativní grupa, tak existuje $g \in G$, že řád g je roven exponentu G. Pomocí tohoto zjištění a faktu, že $\mathbb{Z}_p$ je těleso pro p prvočíslo, dokažte, že $\mathbb{Z}_p^\star$ je cyklická pro každé p.

Příklad 5. Faktorizujte číslo $N = 6557$, víte-li, že je součinem dvou prvočísel p, q splňujících $|p - q| < 10$ (jde to bez kalkulačky!).

Příklad 6. Tři malá prasátka mají každé svůj privátní klíč (d_1, N_1), (d_2, N_2) a (d_3, N_3) a všechna používají veřejný exponent $e = 3$. Červená Karkulka poslala každému prasátku identickou pozvánku M na narozeninovou oslavu zašifrovanou pomocí jeho veřejného klíče, tj. zprávy mají tvar $C_1 = M^e \pmod{N_1}$, $C_2 = M^e \pmod{N_2}$, $C_3 = M^e \pmod{N_3}$.

Velký zlý vlk všechny tři zašifrované zprávy zachytil a zná veřejné klíče. Poraďte mu, jak z C_1, C_2, C_3 získat M.