Cvičení 5. 4. 2012

Pro počítání kvadratický zbytků modulo obecné složené číslo se nám hodí znát čínskou zbytkovou větu a strukturu grup $(\mathbb{Z}_{p^n})^\star$ (viz ukázka na tabuli).

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 $(-1)^a 5^b$.

Proto pro *liché* $n = p_1 \dots p_n$ definujeme Jacobiho symbol:

$$\left(\frac{a}{p_1 \dots p_n}\right) = \prod_i \left(\frac{a}{p_i}\right).$$

Jacobiho symboly zobecňují ty Legendreovy a lze je použít ve výpočtech (viz ukázka), ale z $\left(\frac{m}{n}\right) = 1$ už *neplyne*, že m je kvadratický zbytek modulo n.

S Jacobiho symboly jde počítat podobně jako s těmi Legendreovými:

1. Pokud $a \equiv b \pmod{n} p$, tak $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$,
2. platí $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right) \cdot \left(\frac{b}{n}\right)$,
3. platí $\left(\frac{-1}{n}\right) \equiv (-1)^{(p-1)/2} \pmod{p}$,
4. $\left(\frac{2}{n}\right) = 1$ pro $n \equiv 1, 7 \pmod{8}$ a -1 pro $n \equiv 3, 5 \pmod{8}$.
5. Pokud m, n jsou lichá, tak opět platí kvadratická reciprocita

$$\left(\frac{m}{n}\right)\left(\frac{m}{n}\right) = (-1)^{\frac{(m-1)(n-1)}{4}}.$$

(Tj. napravo vychází -1, právě když $m, n \equiv 3 \pmod{4}$, jinak vyjde 1.)

Příklad 1. Najděte všechny involuce (prvky řádu 2) v $\mathbb{Z}_{80}^\star$.

Příklad 2. Spočtěte pomocí Legendreových symbolů

1. $\left(\frac{35}{37}\right)$
2. $\left(\frac{63}{71}\right)$
3. $\left(\frac{36}{29}\right)$

4. $\left(\frac{129}{331}\right)$

Příklad 3. Kolik řešení (modulo 45) má rovnice $x^2 + 4x + 4 \equiv 0 \pmod{45}$?

Příklad 4. Najděte m, n, že $\left(\frac{m}{n}\right) = 1$, ale m není kvadratický zbytek modulo n. Je možné, aby $\left(\frac{m}{n}\right) = -1$, ale m byl kvadratický zbytek modulo n?

Příklad 5. 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 $\mathbb{Z}_{2^n}^\star$?

Příklad 6. 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.