Cvičení 24. 4. 2013

Pro $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ liché číslo definujeme Jacobiho symbol jako

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \cdots \left(\frac{a}{p_k}\right)^{\alpha_k}.$$

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 $a \equiv b \pmod{n}$, 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 $\left(\frac{-1}{n}\right) \equiv (-1)^{(n-1)/2}$,
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

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

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

Příklad 1 (rozcvička)**.** Kolik řešení má rovnice $x^2 + 4x + 5 \equiv 0 \pmod{85}$ v $\mathbb{Z}_{85}$?

Příklad 2. Spočtěte pomocí Jacobiho 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. 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 4. Buď n liché číslo složené. Rozhodněte, jestli pro každé $a \in \mathbb{Z}_n^{\star}$ platí $\left(\frac{a}{n}\right) \equiv a^{(n-1)/2} \pmod{n}$.

Kreativní úlohy

Příklad 5. Mějme veřejný klíč (n, e) pro RSA a šifrový text $C = M^e$. Ukažte, že z $C = M^e$ a n je možné zjistit Jacobiho symbol $\left(\frac{M}{n}\right)$.