Cvičení 1. 3. 2012

Pro n přirozené číslo definujeme grupu $\mathbb{Z}_n^\star$ sestávající z čísel mezi 1 a n nesoudělných s n s operací násobení modulo n. Dá trochu práce dokázat, že je to grupa, ale je tomu tak. Počet prvků grupy $\mathbb{Z}_n^\star$ označme $\phi(n)$ (Eulerova funkce). Číslo $\phi(n)$ lze spočítat z prvočíselného rozkladu n (viz 5. příklad).

Platí Eulerova věta: Pokud je a celé číslo nesoudělné s n, tak $a^{\phi(n)} \equiv 1 \pmod{n}$.

Příklad 1 (Mini-verze čínské zbytkové věty)**.** Buďte $k, l \neq 0$ nesoudělná celá čísla. Dokažte, že potom $kl|n$, právě když $k|n$ a zároveň $l|n$.

Příklad 2. Dokažte, že:

1. $16|5^{80} - 1$
2. $198|13^{62} + 29$
3. $112|(835^5 + 6)^{18} - 1$

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

Příklad 4. Dokažte, že číslo tvaru $4k + 3, k \in \mathbb{N}$ nejde vyjádřit jako součet čtverců (tj. ve tvaru $a^2 + b^2$, kde a, b jsou celá).

Příklad 5. Dokažte, že pokud $n = p_1^{a_1} \cdots p_k^{a_k}$ je prvočíselný rozklad n, tak

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

Příklad 6. Dokažte:

1. Malou Fermatovu větu (Eulerova věta, kde n je prvočíslo)
2. Eulerovu větu.

Příklad 7. Dokažte, že číslo $19 \cdot 8^n + 17$ je složené pro každé n.