11MAG – 3. cvičení
Modulární inverze. Rozšířený Euklidův algoritmus.

14. října 2013

1 Výpočet modulární inverze [20 min]

Vytvořte funkci `x=modinv(a,m)` pro výpočet modulární inverze čísla a v aritmetice modulo m. Výpočet bude probíhat metodou hrubé síly, budete tedy postuipně testovat, zda

$$a \cdot x \equiv 1 (\mod m)$$

pro $x = 1, 2, \ldots, m-1$.

2 Rozšířený Euklidův algoritmus [30 min]

Vytvořte funkci `[d,e]=gcd_ext(a,b)` pro výpočet nejvyššího společného dělitele čísel a a b rozšířeným Eukleidovým algoritmem.

3 Algoritmus modulárního mocnění [30 min]

Vytvořte funkci `r=modpow(x,n,m)` pro efektivní výpočet modulární mocniny

$$r \equiv x^n (\mod m)$$

pomocí opakovaného mocnění, tedy rozkladem n na binární číslo a výpočtem$x^2 (\mod m), x^4 (\mod m), x^4 (\mod m), \ldots,$