6. procvičení z MB154, podzim 2023

Příklad 1. Najděte primitivní kořen modulo 19 a demonstrujte DH protokol pro $a = 5$ a $b = 7$. (Vyjde hned $g \equiv 2$, Alice pošle $2^5 \equiv 13$, Bob pošle $2^7 \equiv 14$, společný soukromý klíč $2^{5\cdot 7} \equiv 10$.)

Příklad 2. Tomáš a Petr chtějí komunikovat šifrou ElGamal. Tomáš si zvolil prvočíslo $p = 29$, primitivní kořen $g = 10$ a číslo $x = 7$. Zveřejnil pak trojici $(29, 10, h)$, kde $h \equiv 10^7 \pmod{29}$. Petr mu poslal dvojici $(2, 27)$. Jakou zprávu poslal Petr Tomášovi? (Společný soukromý klíč $2^7 \equiv 12$, dešifrovaná zpráva $M \equiv (12)^{-1} \cdot 27 \equiv 24$.)

Příklad 3. V Rabinově kryptosystému Alice zvolila za svůj soukromý klíč $p = 11, q = 19$, veřejným klíčem je pak $n = p \cdot q = 209$. Zašifrujte pro Alici zprávu $m \equiv 42 \pmod{209}$ a ukažte, jak bude Alice tuto zprávu dešifrovat. (Zašifrování $C \equiv 92$, dešifrování $M \equiv \pm 42, \pm 53$.)

Příklad 4. Vyřešte diofantickou rovnici $23x + 41y = 1693$, prvně nad $\mathbb{Z}$, pak se pokuste odpovědět nad $\mathbb{N}_0$. (Vyjde $x = -41t + 54$, $y = 23t + 11$; nezáporné pro $t = 0, 1$.)

Příklad 5. Vyřešte diofantickou rovnici $36x+60y+35z = 973$, prvně nad $\mathbb{Z}$, pak se pokuste odpovědět nad $\mathbb{N}_0$. (Například $x = -5s - 15t + 28$, $y = 3s + 2t$, $z = 12t - 1$; nad $\mathbb{N}_0$ čtyři řešení $(13, 2, 11)$, $(8, 5, 11)$, $(3, 8, 11)$, $(3, 1, 23)$.)