6. cvičení z MB154, podzim 2021

Příklad 1. Najděte primitivní kořen modulo 23 a demonstrujte DH protokol pro $a = 7$ a $b = 13$.

Pro nalezení primitivního kořene spíš jen říkejte, co je potřeba ověřit, a počítejte na kalkulačce – prvně by mělo vyjít 5. Zbytek pořádně se zápisem, zkuste modulární umocňování počítat systémem úprav výrazů (pro počítání mocniny začínáte s $x = 1$, pak se to bude měnit) $x \cdot y^{2z} \equiv x \cdot (y^2)^z \equiv \cdots$, resp. $x \cdot y^{2z+1} \equiv (x \cdot y) \cdot (y^2)^z \equiv \cdots$ (v každém kroku spočítáte explicitně y^2, případně $x \cdot y$).

Příklad 2. Tomáš a Petr chtějí komunikovat šifrou ElGamal. Tomáš si zvolil prvočíslo $p = 31$, primitivní kořen $g = 12$ a číslo $x = 6$. Zveřejnil pak trojici $(31, 12, h)$, kde $h \equiv 12^6 \pmod{31}$. Petr mu poslal dvojici $(21, 27)$. Jakou zprávu poslal Petr Tomášovi?

Příklad 3. V Rabinově kryptosystému Alice zvolila za svůj soukromý klíč $p = 19, q = 23$, veřejným klíčem je pak $n = p \cdot q = 437$. Zašifrujte pro Alici zprávu $m \equiv 327 \pmod{437}$ a ukažte, jak bude Alice tuto zprávu dešifrovat.

Příklad 4. Vyřešte diofantickou rovnici $21x + 34y = 1597$, prvně nad $\mathbb{Z}$, pak se pokuste odpovědět nad $\mathbb{N}_0$, měly by vyjít dvě řešení.

Přepíšete modulo 21, vyřešíte y a pak dořešíte x, tentokrát už v $\mathbb{Z}$.

Příklad 5. Vyřešte diofantickou rovnici $50x + 70y + 57z = 1234$, prvně nad $\mathbb{Z}$, pak se pokuste odpovědět nad $\mathbb{N}_0$, mělo by vyjít šest řešení.

Přepíšete modulo $10 = (50, 70)$, vyřešíte z (formálně si můžete převést z napravo a ptát se, kdy to bude mít řešení – no právě když bude pravá strana dělitelná tou 10, tak to vezmete modulo 10), převedete jej napravo a pak jak v předchozím, tj. přepíšete modulo 50, vyřešíte y a pak dořešíte x, tentokrát už v $\mathbb{Z}$.

Kódování bych asi úplně nezačínal, spíš bych se snažil před písemkou zopakovat, co jim dělalo problém z dosavadních příkladů – podle jejich přání. Ale pokud nic chtít nebudou, můžete to kódování klidně začít.

Příklad 6. Určete všechna kódová slova $(3, 2)$-kódu generovaného polynomem $x + 1$.

Příklad 7. Určete generující matici polynomiálního kódu z předchozího příkladu.

Příklad 8. Určete generující matici a matici kontroly parity $(7, 2)$-kódu generovaného polynomem $x^5 + x^4 + x^2 + 1$. Dekódujte přijaté slovo 0010111 za předpokladu, že při přenosu došlo k nejmenšímu možnému množství chyb.