3. cvičení z MB141, jaro 2023

Příklad. 1. Najděte inverzní prvek k číslu 157 modulo 2475, a to

a) pomocí Bezoutovy věty,
b) pomocí soustavy kongruencí, která vychází z rozkladu $2475 = 9 \cdot 11 \cdot 25$.

Řešení. 268. □

Příklad. 2. Pomocí malé Fermatovy věty najděte zbytek po dělení čísla $2^{97^{99}}$ číslem 26.

Řešení. 2. □

Příklad. 3. Najděte poslední dvě cifry čísla $3^{97^{99}}$. Hledáme zbytek po dělení 4 a pomocí Eulerovy věty zbytek po dělení 25.

Řešení. Po dělení 4 je zbytek 3, po dělení 25 je zbytek 23. Poslední dvě cifry jsou 23. □

Příklad. 4. Šifrou RSA s veřejným klíčem $n = 95$ a $e = 49$ bylo posláno číslo $Z = 42$. Šifru prolomte a určete zaslanou zprávu $M \in \{1, 2, \ldots, 94\}$.

Řešení. $95 = 5 \cdot 19$, $\varphi(95) = 4 \cdot 18 = 72$. Spočítáme inverzi d k exponentu $e = 49 \mod 72$, $d = 25$. Protože $Z = M^e$, je $M \equiv Z^d \equiv 42^{25} \equiv 93 \mod 95$. □

Příklad. 5. V šifrovacím systému RSA s veřejným klíčem skládajícím se z modulu $n = 2021$ a exponentu $e = 11$ došlo k prozrazení faktorizace $n = p \cdot q = 43 \cdot 47$. S její pomocí dešifrujte zprávu $c = 21$. Při výpočtu mocniny $c^d \mod 2021$ počítejte zvlášť modulo 43 a modulo 47 a tyto mezivýsledky pak dejte dohromady.

Řešení. $d = 527$, $c^d \equiv 11 \mod 43$, $c^d \equiv 34 \mod 47$, zpráva je 269. □

Příklad. 6. Najděte všechny primitivní kořeny modulo 26.

Řešení. $7, 19$. □

Příklad. 7. V ElGamalově šifrovacím systému si Alice zvolila veřejný klíč sestávající z prvočísla $p = 997$, primitivního kořene $g = 11$ a jeho mocniny g^x (kde exponent $x = 23$ je soukromý). Bob si pro komunikaci s Alicí zvolil soukromý klíč $y = 25$ a poslal jí svůj veřejný klíč g^y. Pomocí společného soukromého klíče g^{xy} pak zašifroval zprávu m a výslednou zprávu $c = 20$ poslal Alici. Jak ji bude Alice dešifrovat?

Řešení. Při počítání $\mod 997$ je $g^x \equiv 11^{23} \equiv 659$, $g^y \equiv 11^{25} \equiv 976$, $g^{xy} \equiv (g^y)^x \equiv 976^{23} \equiv 950$, inverze k němu je -297, $m \equiv c \cdot (-297) \equiv 42$. □