

#### 4. cvičení z MIN401 – soustavy kongruencí,

**Příklad 1:** Vyřešte následující kongruence:

(i)  $210x \equiv 40 \pmod{212}$ .

(ii)  $325x \equiv 694 \pmod{471}$ .

**Příklad 2:** Vyřešte následující soustavy kongruencí:

(i)  $2x \equiv 3 \pmod{7}$ ,  $x \equiv 8 \pmod{15}$ .

(ii)  $x \equiv 3 \pmod{10}$ ,  $x \equiv 8 \pmod{15}$ ,  $x \equiv 5 \pmod{84}$ .

(iii)  $21x \equiv 27 \pmod{24}$ ,  $26x \equiv 10 \pmod{25}$ ,  $27x \equiv 30 \pmod{17}$ .

**Příklad 3:** Najděte inverzní prvek k číslu 157 modulo 2475.

**Příklad 4:** [10.32, 10.33] Najděte primitivní kořeny modulo 8, 11, 20, 26, 41 a  $41^2$ .

**Příklad 5:** Šifrou RSA s veřejným klíčem  $n = 95$  a  $e = 55$  bylo posláno číslo  $Z = 42$ . Šifru prolomte a určete zaslanou zprávu  $M \in \{1, 2, \dots, 94\}$ .

**Příklad 6:** Veřejný klíč Honzy pro RSA šifru je  $(91, 23)$ . Zachytili jste jemu určenou zprávu 3. Dekódujte ji.

**Příklad 7:** 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  $c^d \pmod{2021}$  počítejte zvlášť modulo 43 a modulo 47 a tyto mezivýsledky pak dejte dohromady.

[Řešení:  $d = 527$ ,  $c^d \equiv 11 \pmod{43}$ ,  $c^d \equiv 34 \pmod{47}$ , zpráva je 269. ]

**Příklad 8:** V ElGamalově šifrovacím systému si Alice zvolila veřejný klíč sestávající z prvočísla  $p = 41$ , primitivního kořene  $g = 11$  a jeho mocniny  $g^a$  (kde exponent  $a = 10$  je soukromý). Bob poslal Alici svůj veřejný klíč  $g^b = 22$  a zašifrovanou zprávu  $c = 6$ . Pomozte Alici zprávu dešifrovat?

[Řešení:  $g^{ab} \equiv 22^a = 22^{10} \equiv 32 \pmod{41}$ . Inverze k  $32 \pmod{41}$  je  $d \equiv 9$ . Zpráva je  $m = 6 \cdot 9 \equiv 13 \pmod{41}$ . ]

**Příklad 9:** 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  $-297$ ,  $m \equiv c \cdot (-297) \equiv 42$ . ]