Algebros pratybos. Rimantas Grigutis

3 pratybos. *Lyginiai.*

1. Pasinaudoję EULERio teorema apskaičiuokite.

1) $7^{9999} \pmod{1000}$.

2) $11^{9999} \pmod{1000}$.

3) $13^{9999} \pmod{1000}$.

2. Išspręskite lyginių sistemas.

1) $\begin{cases} 2x \equiv -1 \pmod 3 \\ 3x \equiv 2 \pmod 5 \end{cases}$.

2) $\begin{cases} 3x \equiv 6 \pmod 9 \\ 5x \equiv 1 \pmod 8 \end{cases}$.

3) $\begin{cases} 11x \equiv 2 \pmod 5 \\ -x \equiv 3 \pmod 6 \end{cases}$.

4) $\begin{cases} 12x \equiv 15 \pmod{17} \\ 10x \equiv 4 \pmod{19} \\ 21x \equiv 16 \pmod{23} \end{cases}$.

5) $\begin{cases} 5x \equiv 1 \pmod{23} \\ 15x \equiv 11 \pmod{43} \\ 25x \equiv 21 \pmod{63} \end{cases}$.

6) $\begin{cases} 5x \equiv 1 \pmod{41} \\ 5x \equiv 1 \pmod{51} \\ 5x \equiv 1 \pmod{61} \end{cases}$.

7) $\begin{cases} 3x \equiv 1 \pmod{11} \\ 5x \equiv 2 \pmod{13} \\ 7x \equiv 3 \pmod{15} \end{cases}$.

3.1) Kurios iš primityviųjų klasių multiplikacinių grupių U_n , $2 \leq n \leq 20$, yra ciklinės. Atsakymą pagįskite.

2) Grupėje U_n raskite maksimalios eilės elementą. Atsakymą pagįskite.

4. Kriptografijos uždavinys. Apibrežkime kriptografijos uždavinį tokia schema:

$$\boxed{\text{Tekstas } \mathbf{T}} \overset{\text{šifravimas}}{\longrightarrow} \mathbf{T} \to \mathbf{x} \in \mathbf{Z}_n \overset{\text{įslaptinimas}}{\longrightarrow} \mathbf{y} = e(\mathbf{x}) = \mathbf{x}^{\mathbf{E}} \pmod n$$

$$\overset{y \text{ siuntimas}}{\rightsquigarrow} \mathbf{y} \in \mathbf{Z}_n \overset{\text{išslaptinimas}}{\longrightarrow} d(\mathbf{y}) = \mathbf{y}^{\mathbf{D}} = \mathbf{x}^{\mathbf{ED}(\bmod \varphi(n))} \equiv \mathbf{x} \pmod n \to \mathbf{x} \to \mathbf{T}.$$

Kriptosistemos $\{n, p, q, E, D\}$ parinkimas:

i) $n = p \cdot q$,čia p ir q pirminiai skaičiai;

ii) $\varphi(n) = (p-1)(q-1)$ ir E yra tarpusavyje pirminis $\varphi(n)$;
iii) D yra lyginio $Ex \equiv 1 \pmod{\varphi(n)}$ sprendinys: $D = E^{-1} \pmod{\varphi(n)}$.
1) Įslaptinkite ir išslaptinkite simbolį $\mathbf{x} = \mathbf{4}, \mathbf{7}, \mathbf{12}, \mathbf{18}$, kai
$n = 33, 39, 51, 57, 39, 35, 55, 85, 77$.
2) Išslaptinkite simbolį $\mathbf{y} = \mathbf{8}, \mathbf{12}, \mathbf{16}, \mathbf{23}$, kai
a) $n = 3397, E = 55$; b) $n = 4183,\ E = 85$; c) $n = 3869,\ E = 2205$.
3) Išslaptinkite simbolį $\mathbf{y} = \mathbf{8}, \mathbf{12}, \mathbf{16}, \mathbf{23}$, kai
a) $n = 11189, E = 17, \varphi(11189) = 10956$;
b) $n = 10229, E = 17, \varphi(10229) = 9984$;
c) $n = 8507, E = 17, \varphi(8507) = 8280$;
d) $n = 10207, E = 17, \varphi(10207) = 9976$.