Matematyka Dyskretna

Ćwiczenia 8 (Szyfrowanie oraz ciąg dalszy teorii liczb)

Zadanie 1. Niech $a = 7$ i $b = 12$. Korzystając z przekształcenia afinicznego $C(x) = (ax + b) \bmod n$ zaszyfruj następujące wiadomości w 26-literowym alfabecie:

a) INFORMA

b) MATMA

c) DYSKRETNA

d) ANALIZA

Zadanie 2. Rozwiąż poniższe układy równań:

a) $\begin{cases} 3x + y = 1 \pmod{27} \\ 9x + y = 13 \pmod{27} \end{cases}$

b) $\begin{cases} 7x + y = 1 \pmod{37} \\ 5x + y = 5 \pmod{37} \end{cases}$

Zadanie 3. Wykonaj następujące polecenia, wiedząc że zachodzą następujące zależności w szyfrze liniowym: $C(E) = H$ oraz $C(T) = C$

a) Odszyfruj wiadomość WVB

b) Zaszyfruj wiadomość HIGH

Zadanie 4. Dla jakich par reszta a_1 i a_2 istnieją liczby spełniające poniższe układy kongurencji?

a) $\begin{cases} a_1 = a \pmod{4} \\ a_2 = a \pmod{6} \end{cases}$

b) $\begin{cases} a_1 = a \pmod{3} \\ a_2 = a \pmod{6} \end{cases}$

Zadanie 5. Rozwiąż poniższe układy kongurencji:

a) $\begin{cases} 1 = a \pmod{3} \\ 4 = a \pmod{5} \end{cases}$

b) $\begin{cases} 2 = a \pmod{3} \\ 3 = a \pmod{5} \end{cases}$

c) $\begin{cases} 2 = a \pmod{3} \\ 3 = a \pmod{5} \\ 5 = a \pmod{7} \end{cases}$

Zadanie 6. Oblicz resztę z dzielenia liczby 1997199919 przez 15.

Zadanie 7. Stosując algorytm mnożenia rosyjskich chłopów oblicz:

a) $36 \cdot 15$

b) $41 \cdot 21$

c) $111 \cdot 17$

d) $2048 \cdot 256$

Zadanie 8. Stosując algorytm mnożenia modulo oblicz:

a) $(36 \cdot 15) \mod 7$

b) $(41 \cdot 21) \mod 5$

c) $(111 \cdot 17) \mod 13$

d) $(2048 \cdot 256) \mod 17$

Zadanie 9. Stosując algorytm szybkiego potęgowania modulo oblicz:

a) $4^{14} \mod 15$

b) $8^{64} \mod 65$

c) $12^{64} \mod 65$

d) $10^{32} \mod 33$

Zadanie 10. Klucz publiczny Alicji to $(e, n) = (11, 85)$ ($p = 5,\ q = 17$). Stosując szyfrowanie RSA wykonaj następujące polecenia:

a) Zaszyfruj wiadomość 6.

b) Zaszyfruj wiadomość 23.

c) Odszyfruj wiadomość 22.

d) Odszyfruj wiadomość 29.