Pierwsze lepsze liczby

(1) Nie korzystając z kalkulatora oblicz:
a) $2^{100} \bmod 7$; b) $3^{200} \bmod 13$; c) $7^{111} \bmod 15$; d) $111^{111} \bmod 35$.

(2) Oblicz: a) $10^{-1} \mod 111$; b) $51^{-1} \mod 169$; c) $1000^{-1} \mod 1003$.

(3) Czy prawdą jest, że dla liczby pierwszej p zachodzi wynikanie

$$a^n \equiv b^n \bmod p \Rightarrow a \equiv b \bmod p?$$

(4) Znajdź resztę z dzielenia: 99!: a) przez 101; b) przez 111.

(5) Jakie wartości przyjmuje funkcja $f(n) = (n-1)! \mod n$?

(6) Niech $p > 3$ będzie liczbą pierwszą taką, że $p \equiv 2 \bmod 3$. Niech

$$a_k = k^2 + k + 1 \quad \text{dla } k = 1, 2, 3, ..., p-1.$$

Wykaż, że $a_1 a_2 ... a_{p-1} \equiv 3 \mod p$.

(7) Oblicz $\varphi(n)$ dla: a) $n = 1001$; b) 1331; c) 1001^{1001}.

(8) Jaki zachodzi związek pomiędzy $\varphi(2n)$ a $\varphi(n)$?

(9) Wykaż, że równanie $\varphi(n) = n/3$ ma nieskończenie wiele rozwiązań.

(10) Rozważmy RSA dla $n = 143$, $e = 7$.
a) Wyślij do Ali wiadomości $m = 100$, $m = 20$.
b) Znajdź klucz tajny d.
c) Pokaż rachunki, jakie trzeba przeprowadzić dla odszyfrowania wiadomości.

(11) Rozłóż $n = 35143$ na czynniki wiedząc, że jest ona iloczynem dwu liczb pierwszych, a $\phi(n) = 34720$.

(12) Zastosuj a-test Millera-Rabina do liczby n:
a) $n = 101$, $a = 2$; b) $n = 143$, $a = 12$; c) $n = 209$, $a = 56$.
Czy wynik jest pewny, czy tylko prawdopodobny?

(13) Rozłóż na czynniki za pomocą algorytmu Fermata (bez próbnego dzielenia):
a) 53357; b) 8858; c) 34571.

(14) Czy z danych $41^2 \equiv 2^4 \cdot 3$, $43^2 \equiv 2^3 \cdot 3^3$, $45^2 \equiv 2^3 \cdot 7^2 \mod 1633$ można wywnioskować rozkład 1633 na czynniki?

(15) Znajdź nietrywialny dzielnik N za pomocą algorytmu Dixona wykorzystując podane informacje:
a) $N = 61063$,

$$1882^2 \equiv 2 \cdot 3^3 \cdot 5 \mod 61063, \qquad 1898^2 \equiv 60750 \mod 61063.$$

b) $N = 52907$,

$$399^2 \equiv 2^2 \cdot 3 \cdot 5 \mod 52907, \quad 763^2 \equiv 2^6 \cdot 3 \mod 52907,$$
$$773^2 \equiv 2^6 \cdot 3^5 \mod 52907, \quad 976^2 \equiv 2 \cdot 5^3 \mod 52907.$$

(16) Rozłóż za pomocą algorytmu ρ-Pollarda: a) 221. b) 3959.

(17) Metodą $p-1$ Pollarda znajdź nietrywialny dzielnik liczby: a) 77; b) 247; c) 7991.