PODSTAWY TEORII LICZB – ZADANIA

Zestaw nr.6 – Rachunek Kongruencji

Zad.1 Wykaż, że dla *nieparzystych* m, $n \in \mathbb{N}$ zachodzi

$$S = 1^n + 2^n + \ldots + (m-1)^n \equiv 0 \mod m.$$

Zad.2 Udowodnij, że dla wszystkich $n \in \mathbb{N}$ i $p \in \mathbb{P}$ zachodzi

$$\binom{np}{p} \equiv n \mod p^2.$$

Zad.3 a) Wykaż, że dla $a \perp 7$ mamy $a^3 \equiv +1 \quad \text{lub} \quad -1 \pmod 7$.
wsk. rozważ $a = (7k \pm i)$, $i = 1, 2, 3$.

b) oblicz $2006^{2007} \pmod{11}$; wsk: wzór dwumianowy

c) Jakie są ostatnie dwie cyfry 9^{9^9}?

wsk. wykaż najpierw: $9^{10} \equiv 1 \pmod{100}$ oraz $9^9 \equiv 9 \pmod{10}$.

d)Jakie są ostatnie dwie cyfry $7^{7^{7^7}}$? wsk. wykaż najpierw: $7^{100} \equiv 1 \pmod{100}$ oraz $7^{7^7} = 7^{100t} \cdot 7^{43}$

Zad.4 Rozwiąż kongruencję $144x = 216 \pmod{360}$. Ile mamy rozwiązań?

Zad.5 Wykaż, że $2 \cdot 26! \equiv -1 \pmod{29}$ oraz $18! \equiv -1 \pmod{437}$, $437 = 19 \cdot 23$.

wsk. tw. Wilsona

Zad.6 Korzystając z chińskiego twierdzenia o resztach rozwiąż układ jednoczesnych kongruencji:

$x \equiv 3 \pmod{11}$, $\qquad x \equiv 5 \pmod{19}$, $\qquad x \equiv 10 \pmod{29}$.

wsk. standardowa procedura i wzór. $x \equiv 34\,433 \pmod{6061}$

Zad.7 Wykaż, że dla dowolnej liczby całkowitej n:

a) $n^7 \equiv n \mod 42$;

b)$\frac{1}{5}n^5 + \frac{1}{3}n^3 + \frac{7}{15}n$ jest liczbą całkowitą.

Zad.8 Rozwiąż kongruencje:

$$\begin{array}{ll} \text{a) } x^2 + 7x + 11 \equiv 0 \mod 5, & \text{c) } x^2 \equiv -1 \mod 29, \\ \text{b) } x^2 - 3x + 3 \equiv 0 \mod 7, & \text{d) } x^2 \equiv -1 \mod 37. \end{array}$$

Dodatkowe problemy – premiowane jako zadania trudniejsze

Zad.A Wykaż, że jeżeli p jest nieparzystą liczbą pierwszą oraz $a + b = p - 1$, to

$$a!b! + (-1)^a \equiv 0 \mod p.$$

Zad.B Niech p będzie liczba pierwszą większą od 3 i niech $f(x) = (x - 1)(x - 2) \ldots (x - p + 1)$. Wykaż, że $p \mid f'(0)$.

Zad.C Dla $p \in \mathbb{P}$ funkcję $f(x) = (1 - x)^p$ rozwijamy w szereg Maclaurina

$$(1 - x)^p = c_0 + c_1 x + c_2 x^2 + \ldots$$

Wykaż, że

$$c_i \begin{cases} \equiv 1 \mod p & \text{gdy } p \mid i \\ \equiv 0 \mod p & \text{gdy } p \nmid i \end{cases}$$

Zad.D Wykaż, że ciąg $10^{6k+4} + 3,\ k = 1, 2, \ldots$ zawiera wyłącznie liczby złożone (podzielne przez 7).

Zad.E Wykaż, że jeżeli $a \equiv b \pmod m$ to zachodzi $a^m \equiv b^m \pmod{m^2}$.

wsk. $a = b + t \cdot m$. Mamy więc $a^m - b^m = (a - b)(\ldots ? \ldots)$. Podstaw za potęgi a w drugim czynniku i rozważ podzielność *obu* czynników przez m.

Zad.F Uogólnij indukcyjnie powyższy wzór na:

dla $a \equiv b \pmod m$ o zachodzi $(a^m)^n \equiv (b^m)^n \pmod{m^{n+1}}$.

w oparciu o ten wzór określ, jaka jest reszta R dzielenia liczby n^{100} przez 125.