# WSTĘP DO TEORII LICZB – ZADANIA

## Zestaw nr.10: Kongruencje, podzielność – różne problemy; liczby dwumianowe; chińskie twierdzenie o resztach

**Zad.1** Przypomnij sobie dwa twierdzenia i ich dowody (wykład):

a) jeżeli $b^a \equiv 1 \pmod{m}$, oraz $b^c \equiv 1 \pmod{m}$,
gdzie $b \perp m$, to zachodzi $b^d \equiv 1 \pmod{m}$, gdzie $d = NWD(a, c)$.

b) jeżeli $p \mid b^n - 1$ to albo $p \mid b^d - 1$, gdzie $d \mid n$ albo $n \mid p - 1$.
Dla *nieparzystego* $n$ (i nieparzystego $p$) mamy $2n \mid p - 1$.

**Zad.2** w oparciu o twierdzenia z punktu 1. znajdź faktoryzację $2^{11} - 1$, $2^{13} - 1$, $3^{12} - 1$, $2^{35} - 1$.

**Zad.3** to samo dla $5^{12} - 1$, $3^{15} - 1$, $3^{24} - 1$.

**Zad.4** to samo dla $10^5 - 1$, $10^6 - 1$, $10^8 - 1$.

**Zad.5** to samo dla $2^{33} - 1$, $2^{21} - 1$, $2^{15} - 1$, $2^{30} - 1$, $2^{60} - 1$.

**Zad.6** Oblicz:

a) $2^{1\,000\,000} \pmod{77}$

b) $6\,647^{362} \pmod{m}$ gdzie

$$m = 7\,785\,562\,197\,230\,017\,200 = 2^4 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 19 \cdot 31 \cdot 37 \cdot 41 \cdot 61 \cdot 73 \cdot 181$$

wskazówka: w obu przypadkach zacznij od znalezienia funkcji Carmichaela $\lambda(m)$ dla modułu.

**Zad.7** Liczba (dziesiętna) 3-cyfrowa daje resztę 7 przy dzieleniu przez 9 i przez 10, a resztę 3 przy dzieleniu przez 11. Liczba ta jest dzielnikiem $d$ liczby 6-cyfrowej $M$, która daje resztę 8 przy dzieleniu przez 9, resztę 7 przy dzieleniu przez 10 i przez 10 i resztę 1 przy dzieleniu przez 11. Znajdź iloraz $M/d$.

wsk: chińskie twierdzenie o resztach

**Zad.8** Główny sejf banku może otworzyć dyrektor banku. Kluczem zezwalającym na otwarcie sejfu jest duża (bardzo duża) liczba $N$. Rada nadzorcza podejmuje uchwałę, z której wynika, że możliwość otwarcia sejfu powinna być także być dostępna dla dowolnych trzech (ale działających wspólnie) członków rady nadzorczej, która liczy dziewięć osób. Dwóch członków (ani jeden) nie może mieć takiej (praktycznej) możliwości.

Chcemy korzystać z chińskiego twierdzenia o resztach; mamy do dyspozycji zbiór liczb pierwszych $p_i$; $i = 1, \ldots, 9$, które możemy „rozdzielić" pomiędzy członków rady nadzorczej. Jakie jeszcze informacje są potrzebne? Jakie powinny to być liczby $p_i$ w stosunku do liczby $N$?
Spróbuj swoje przemyślenia zilustrować przykładem liczbowym, wybierając $N$ rzędu 10 000 (to nie jest *duża* liczba, ale chcemy zaoszczędzić trudu przy rachunkach).