Mały Projekt nr 2.

Temat: ***Multiplikatywne grupy*** $(Z_n^*, \cdot_n)$

Niech n będzie ustaloną liczbą naturalną i niech $Z_n^* := \{k \in \mathbb{N} \mid 1 \leq k \leq n-1,\ \mathrm{NWD}(k,n) = 1\}$ będzie zbiorem liczb naturalnych mniejszych od n i względnie pierwszych z n. Określmy w Z_n^* binarne działanie w następujący sposób:

$$a \cdot_n b := (a \cdot b)_n.$$

($(a \cdot b)_n$ - reszta z dzielenia ab przez n)

Uwaga 1. *$(Z_n^*, \cdot_n)$ jest grupą.*

Niech $n \in \mathbb{N}$ oraz $a \in Z_n^*$. Przypomnijmy, najmniejszą dodatnią liczbę naturalną d taką, że

$$a^d \equiv_n 1$$

nazywamy *rzędem* elementu $a \in Z_n^*$ w grupie $(Z_n^*, \cdot_n)$.

Definicja 1. *Liczba $a \in Z_n^*$ jest pierwiastkiem pierwotnym modulo n, jeżeli rząd a jest równy $\varphi(n) = |Z_n^*|$.*

Twierdzenie 2. *Jeśli p jest liczbą pierwszą, to w grupie $(Z_p^*, \cdot_p)$ istnieje pierwiastek pierwotny modulo p. (Tzn., że grupa $(Z_p^*, \cdot_p)$ jest cykliczna.)*

Twierdzenie 3 (Test pierwszości Lucasa)**.** *Niech $n \in \mathbb{N}$ i $b \in \mathbb{Z}$ będą takie, że $2 \leq b \leq n-1$. Wtedy, jeśli dla każdego pierwszego podzielnika p liczby $n-1$ zachodzą warunki:*

- $b^{n-1} \equiv_n 1$,
- $b^{\frac{n-1}{p}} \neq 1 (mod\ n)$,

to n jest liczbą pierwszą.

Zadania do wykonania:

(a) Określić rzędy elementów w grupach $(Z_{19}^*, \cdot_{19})$ i $(Z_{24}^*, \cdot_{24})$.

(b) Znaleźć pierwiastki pierwotne w grupach $(Z_{19}^*, \cdot_{19})$ i $(Z_{41}^*, \cdot_{41})$.

(c) Sprawdzić, czy w grupie $(Z_{2^8}^*, \cdot_{2^8})$ istnieje pierwiastek pierwotny. Czy istnieje takie $n \geq 3$, że grupa $(Z_{2^n}^*, \cdot_{2^n})$ jest cykliczna?

(d) Znaleźć elementy odwrotne do wybranych elementów w grupach $(Z_{19}^*, \cdot_{19})$ i $(Z_{24}^*, \cdot_{24})$.

(e) Zastosować test Lucasa dla wybranych dużych liczb całkowitych.

(f)* Udowodnić Twierdzenie 3.