Projekt nr 4.

Temat: ***Reszty kwadratowe***

Niech $2 \neq p$ będzie liczbą pierwszą, $a \in \mathbb{Z}$ i niech $\mathrm{NWD}(a,p) = 1$. Jeśli istnieje liczba $b \in \{1, \ldots, p-1\}$ taka, że $a \equiv_p b^2$ to powiemy, że a jest *resztą kwadratową* modulo p. W przeciwnym razie a nazywamy *niereszta̧ kwadratową* modulo p.
Symbol Legandre'a:

$$\left(\frac{a}{p}\right) := \begin{cases} 0, & \text{gdy } p|a, \\ +1, & \text{gdy } a \ - \text{reszta kwadratowa modulo } p, \\ -1, & \text{gdy } a \ - \text{niereszta kwadratowa modulo } p \end{cases}$$

Twierdzenie 1 (Kryterium Eulera)**.** *Niech p będzie liczbą pierwszą i $a \in \mathbb{Z}$. Wówczas a jest resztą kwadratową modulo p wtedy i tylko wtedy, gdy*

$$a^{\frac{p-1}{2}} \equiv_p 1. \tag{1}$$

Twierdzenie 2 (Prawo wzajemności reszt kwadratowych)**.** *Dla nieparzystych liczb pierwszych $p \neq q$*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Wniosek 3. *Niech $p \neq q$ będą nieparzystymi liczbami pierwszymi. Wtedy*

$$\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{p}{q}\right), & \text{gdy } p \equiv_4 1 \text{ lub } q \equiv_4 1 \\ -\left(\frac{p}{q}\right), & \text{gdy } p \equiv_4 3 \text{ oraz } q \equiv_4 3 \end{cases}$$

Uwaga 1. *Jeżeli n jest liczbą naturalną złożoną to dla około połowy liczb z przedziału* $[2, n-1]$ *warunek* (1) *nie zachodzi. Stąd wybierając losowo liczbę z tego przedziału mamy około* 50% *szans na odkrycie tego faktu.*

Zadania do wykonania:

Część teoretyczna.

(a) Niech $2 \neq p$ będzie liczbą pierwszą i $a, b \in \mathbb{Z}$. Udowodnić kryterium Eulera oraz pokazać, że

$$\left(\frac{a}{p}\right) \equiv_p a^{\frac{p-1}{2}}.$$

Stąd wywnioskować, że

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

(b) Podać opis protokołu rzutu monetą przez telefon.

(c) Przedstawić test Strassena-Solovaya rozpoznawania liczb pierwszych.

[2] Część praktyczna (z wykorzystaniem komputera).

(d) Wykonać testy prawdziwości kryterium Eulera oraz prawa wzajemności reszt kwadratowych.

(e) Zaimplementować własną funkcję obliczającą symbol Legendre'a.

(f) Zaimplementować test Strassena-Solovaya.

Literatura.

1. W. Marzantowicz, P. Zarzycki, *Elementarna teoria liczb*, Wydawnictwo Naukowe PWN, Warszawa, 2006.
2. S.Y. Yan, *Teoria liczb w informatyce*, WNT, Warszawa, 2006
3. M. Zakrzewski, *Markowe Wykłady z Matematyki. Teoria Liczb*, Oficyna Wydawnicza GiS, Wrocław, 2017.