Autor: Krzysztof Zdon

Prowadzący: Krzysztof Zdon

Reszty kwadratowe

Wstęp teoretyczny

Def. 1 Niech p będzie liczbą pierwszą. Mówimy, że liczba a jest **resztą kwadratową modulo** p (w skrócie $a\mathbf{R}p$), jeśli istnieje rozwiązanie kongruencji $x^2 \equiv a\ (mod p)$. W przeciwnym razie nazywamy ją **nieresztą kwadratową modulo** p (w skrócie $a\mathbf{N}p$).

Uwaga 1. Powyższą definicję można łatwo rozszerzyć dla modułów m niebędących liczbami pierwszymi, należy jedynie zadbać, by $NWD(a, m) = 1$.

Twierdzenie 1. Dla każdej nieparzystej liczby pierwszej p mamy dokładnie $\frac{p-1}{2}$ niezerowych reszt kwadratowych.

Zadanie pomocnicze 1. Niech p będzie liczbą pierwszą, większą od 3. Udowodnij, że suma wszystkich reszt kwadratowych jest podzielna przez p.
Zadanie pomocnicze 2. Niech p będzie liczbą pierwszą. Udowodnij, że jeśli g jest dowolnym pierwiastkiem pierwotnym modulo p, to g^k jest resztą kwadratową modulo p wtedy i tylko wtedy, gdy $2|k$.

Def. 2 Niech p będzie nieparystą liczbą pierwszą i niech $a \in \mathbb{Z}$. Definiujemy symbol Legendre'a:

$$\left(\frac{a}{p}\right) = \begin{cases} +1, & gdy\ a\mathbf{R}p, \\ -1, & gdy\ a\mathbf{N}p, \\ 0, & gdy\ p|a. \end{cases}$$

Twierdzenie 2. (Kryterium Eulera) Niech p będzie nieparzystą liczbą pierwszą. Wtedy:

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\ (mod\, p)$$

Natychmiastowy Wniosek 1. Jeśli $a, b \in \mathbb{Z}$ oraz $p \in \mathbb{P}$, to:

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

Natychmiastowy Wniosek 2. Jeśli $p \in \mathbb{P}_{\geq 3}$, to

$$\left(\frac{-1}{p}\right) = \begin{cases} +1 & \iff p \equiv 1\,(mod\, 4), \\ -1 & \iff p \equiv 3\,(mod\, 4). \end{cases}$$

Prawo wzajemności reszt kwadratowych

Twierdzenie 3. Niech p i q będą różnymi nieparzystymi liczbami pierwszymi. Wtedy:

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

Natychmiastowy Wniosek 1. 3 jest resztą kwadratową mod p wtedy i tylko wtedy, gdy $p \equiv \pm 1\,(mod\, 12)$
Natychmiastowy Wniosek 2. 5 jest resztą kwadratową mod p wtedy i tylko wtedy, gdy $p \equiv \pm 1\,(mod\, 5)$

Twierdzenie 4. Jeśli $p \in \mathbb{P}_{\geq 3}$, to

$$\left(\frac{2}{p}\right) = \begin{cases} +1 \iff p \equiv \pm\,(mod\,8), \\ -1 \iff p \equiv \pm 3\,(mod\,8). \end{cases}$$

Zadania

Zadanie 1. Udowodnij, że $2^n + 1$ nie ma żadnego dzielnika pierwszego postaci $8k - 1$.
Zadanie 2. Udowodnij, że dla każdej liczby pierwszej $p \in \mathbb{P}_{\geq 7}$ istnieją dwie reszty kwadratowe różniące się o 1.
Zadanie 3. Załóżmy, że $NWD(a, p) = 1$, gdzie $p \in \mathbb{P}_{\geq 3}$. Udowodnij, że:

$$\sum_{i=1}^{p} \left(\frac{an+b}{p}\right) = 0 \text{ oraz } \sum_{i=1}^{p} \left(\frac{n^2+a}{p}\right) = -1$$

Zadanie 4. Niech $p \in \mathbb{P}_{\geq 7}$ i $A = \{b_1, ..., b_{\frac{p-1}{2}}\}$ będzie zbiorem wszystkich niezerowych reszt kwadratowych. Udowodnij, że nie istnieją takie liczby $a, c \in \mathbb{Z}_{\geq 1}$, że $NWD(ac, p) = 1$ oraz zbiór $B = \{ab_1 + c, ..., ab_{\frac{p-1}{2}} + c\}$ jest rozłączny z A mod p.
Zadanie 5. Niech n będzie liczbą całkowitą dodatnią i oznaczmy przez $k = 2^{2^n} + 1$. Udowodnij, że k jest pierwsze wtw, gdy $k \mid 3^{\frac{k-1}{2}}$.
Zadanie 6. Niech $a, b \in \mathbb{Z}_+$ będą takimi liczbami, że $2^a - 1 | 3^b - 1$. Udowodnij, że $a = 1$ lub $2|b$.
Zadanie 7. Niech $p \in \mathbb{P}_{\geq 3}$ i $n = \frac{p-1}{2}$. Znajdź wszystkie ń-krotki"$(x_1, ..., x_n)$, gdzie $x_i \in \{1, ..., p-1\}$, takie że:

$$\sum_{i=1}^{n} x_i \equiv \sum_{i=1}^{n} x_i^2 \equiv ... \equiv \sum_{i=1}^{n} x_i^n \;\; (mod\, p)$$

Zadanie 8. Niech $p > 3$ będzie liczbą pierwszą oraz niech $a, b, c \in \mathbb{Z}$, gdzie $a \neq 0$. Załóżmy, że $ax^2 + bx + c$ jest kwadratem dla $2p - 1$ kolejnych liczb całkowitych x. Udowodnij, że $p|b^2 - 4ac$.
Zadanie 9. Rozważmy ciąg liczb całkowitych $a_1, a_2, ...$ spełniający poniższą własność: Dla dowolnych dodatnich liczb całkowitych n i k liczba

$$\frac{a_n + a_{n+1} + ... + a_{n+k-1}}{k}$$

jest zawsze kwadratem liczby całkowitej. Udowodnij, że w istocie ten ciąg jest stały.
Zadanie 10. Załóżmy, że $\phi(5^m - 1) = 5^n - 1$ dla pewnej pary liczb całkowitych dodatnich m, n. Udowodnij, że $NWD(m, n) > 1$.