Teoria liczb
reszty kwadratowe, 13-16 marca

Dla nieparzystej liczby pierwszej p oraz liczby całkowitej m definiujemy

$$\left(\frac{m}{p}\right) = \begin{cases} 0 & \text{jeśli } m \text{ jest podzielna przez } p, \\ 1 & \text{jeśli istnieje liczba całkowita } a \text{ taka, że } a^2 \equiv m \pmod{p}, \\ -1 & \text{w przeciwnych przypadkach.} \end{cases}$$

Wyrażenie tak zdefiniowane nazywa się *symbolem Legendre'*a. Jeśli $q \neq p$ jest inną nieparzystą liczbą pierwszą, to zachodzi *prawo wzajemności reszt kwadratowych*:

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

które udowodnimy na wykładzie.

Zadanie 1. (a) Oblicz $\left(\frac{m}{7}\right)$ dla $m = 0, 1, \ldots, 6$.

(b) Pokaż, że $\left(\frac{m}{p}\right) \equiv m^{\frac{p-1}{2}} \pmod{p}$.

(c) Pokaż, że dla ustalonego p i dowolnych m_1, m_2 zachodzi

$$\left(\frac{m_1}{p}\right) \cdot \left(\frac{m_2}{p}\right) = \left(\frac{m_1 m_2}{p}\right).$$

Zadanie 2. Użyj poprzedniego zadania i prawa wzajemności reszt, by obliczyć $\left(\frac{71}{113}\right)$, czyli stwierdzić, czy 71 jest resztą kwadratową modulo 113.

Niech p będzie nieparzystą liczbą pierwszą, jak poprzednio i niech m będzie niepodzielna przez p. *Najmniejszą resztą* $m \mod p$ nazwiemy liczbę $m' \in \mathbb{Z}$ taką, że $m' \equiv m \pmod{p}$ oraz $|m'|$ jest najmniejsze możliwe. Oznaczamy ją, na potrzeby tej serii zadań, r_m.

Zadanie 3. (a) Niech $p = 11$. Ile jest ujemnych elementów w zbiorze $r_2, r_4, \ldots, r_{\frac{p-1}{2}\cdot 2}$? Czy są w nim różne elementy o tej samej wartości bezwzględnej?

(b) Niech $p = 8k+s$, gdzie $0 < s < 8$. Oblicz, ile jest ujemnych elementów w zbiorze $r_2, r_4, \ldots, r_{\frac{p-1}{2}\cdot 2}$

Zadanie 4 (Lemat Gaussa)**.** (a) Ustalmy a niepodzielną przez p i weźmy $1 \leq k < l \leq \frac{p-1}{2}$. Pokaż, że $r_{ak} \neq r_{al}$ oraz $r_{ak} \neq -r_{al}$.

(b) Wywnioskuj z poprzedniego podpunktu, że zachodzi równość zbiorów

$$\left\{|r_a|, |r_{2a}|, \ldots, |r_{\frac{p-1}{2}\cdot a}|\right\} = \left\{1, 2, \ldots, \frac{p-1}{2}\right\}.$$

(c) Niech $\mathrm{N}(a)$ oznacza liczbę ujemnych liczb w zbiorze $\{r_a, \ldots, r_{\frac{p-1}{2}\cdot a}\}$. Pokaż, że

$$a \cdot (2a) \cdot \ldots \cdot \left(\frac{p-1}{2} \cdot a\right) \equiv (-1)^{\mathrm{N}(a)} \left(1 \cdot 2 \cdot \ldots \cdot \frac{p-1}{2}\right) \pmod{p}$$

Wywnioskuj, że $\left(\frac{a}{p}\right) = (-1)^{\mathrm{N}(a)}$.

(d) Połącz poprzednie podpunkty i poprzednie zadanie, by wywnioskować, że $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.

Zadanie 5. Pokaż, że istnieje nieskończenie wiele liczb pierwszych o pierwszej cyfrze jeden.

Zadanie 6. Pokaż, że każda liczba całkowita $n \geq 7$ może być zapisana jako suma różnych liczb pierwszych, nie większych od $\max(11, n-7)$. *Wskazówka: użyj indukcji, możesz założyć, że teza jest znana np. dla* $n \leq 50$.

Zadanie 7 ($\star\star$)**.** Użyj opisu z poprzednich zadań, by wykazać prawo wzajemności reszt kwadratowych.