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

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

Rozwiązanie.
(b) Przypadek $m \equiv 0 \pmod{p}$ jest jasny. Dalej zakładamy $m \not\equiv 0 \pmod{p}$. Równanie $x^2 \equiv 1 \pmod{p}$ jest równoważne $p \mid (x-1)(x+1)$, więc ma rozwiązania $\pm 1 \pmod{p}$. Z małego twierdzenia Fermata wynika, że dla każdego m niepodzielnego przez p zachodzi $(m^{\frac{p-1}{2}})^2 \equiv 1 \pmod{p}$, zatem $m^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$. Z zadania 7 pierwszej serii zadań wynika, że $m^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ wtedy i tylko wtedy, gdy istnieje a takie, że $m \equiv a^2 \pmod{p}$. W przeciwnym przypadku musi więc zachodzi $m^{\frac{p-1}{2}} \equiv -1 \pmod{p}$, co kończy dowód.
(a) Na mocy punktu (b) mamy $\left(\frac{m}{7}\right) \equiv m^3 \pmod{7}$. Obliczamy bezpośrednio, że

$$\left(\frac{0}{7}\right) = 0,\ \left(\frac{1}{7}\right) = 1,\ \left(\frac{2}{7}\right) = 1,\ \left(\frac{3}{7}\right) = -1,\ \left(\frac{4}{7}\right) = 1,\ \left(\frac{5}{7}\right) = \left(\frac{-2}{7}\right) = -1,\ \left(\frac{6}{7}\right) = \left(\frac{-1}{7}\right) = -1$$

(c) Na mocy punktu (b) mamy

$$\left(\frac{m_1}{p}\right) \cdot \left(\frac{m_2}{p}\right) \equiv m_1^{\frac{p-1}{2}} \cdot m_2^{\frac{p-1}{2}} = (m_1 m_2)^{\frac{p-1}{2}} \equiv \left(\frac{m_1 m_2}{p}\right) \pmod{p}.$$

Obie strony należą do zbioru $\{-1, 0, -1\}$, więc wynika stąd równość $\left(\frac{m_1}{p}\right)\left(\frac{m_2}{p}\right) = \left(\frac{m_1 m_2}{p}\right)$.

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.

Rozwiązanie.

Obie liczby 71 i 113 są pierwsze. Na mocy prawa wzajemności reszt mamy $\left(\frac{71}{113}\right)\left(\frac{113}{71}\right) = (-1)^{35\cdot 56} = 1$. Pozostaje obliczyć $\left(\frac{113}{71}\right) = \left(\frac{113-71}{71}\right) = \left(\frac{42}{71}\right)$. Skoro $42 = 7 \cdot 3 \cdot 2$, to

$$\left(\frac{42}{71}\right) = \left(\frac{7}{71}\right) \cdot \left(\frac{3}{71}\right) \cdot \left(\frac{2}{71}\right) = (-1)^{3\cdot 35}\left(\frac{71}{7}\right) \cdot (-1)^{1\cdot 35}\left(\frac{71}{3}\right) \cdot (-1)^{(71^2-1)/8}.$$

Mamy $\left(\frac{71}{7}\right) = \left(\frac{1}{7}\right) = 1$ oraz $\left(\frac{71}{3}\right) = \left(\frac{-1}{3}\right) = -1$. Ponadto, liczba $71^2 - 1^2 = 70 \cdot 72$ jest podzielna przez 16, więc $(-1)^{(71^2-1)/8} = 1$. Łącznie otrzymujemy

$$\left(\frac{42}{71}\right) = -1 \cdot 1 \cdot (-1) \cdot (-1) \cdot 1 = -1.$$

Zatem $\left(\frac{71}{113}\right) = \left(\frac{42}{71}\right) = -1$.

Rozwiązanie.

Obie liczby 71 i 113 są pierwsze. Na mocy prawa wzajemności reszt mamy $\left(\frac{71}{113}\right)\left(\frac{113}{71}\right) = (-1)^{35\cdot 56} = 1$. Pozostaje obliczyć $\left(\frac{113}{71}\right) = \left(\frac{113-2\cdot 71}{71}\right) = \left(\frac{-29}{71}\right)$. Z multiplikatywności symbolu Legendre'a mamy $\left(\frac{-29}{71}\right) = \left(\frac{-1}{71}\right)\left(\frac{29}{71}\right) = (-1)^{35}\left(\frac{29}{71}\right) = -\left(\frac{29}{71}\right)$. Znowu na mocy prawa wzajemności, mamy $\left(\frac{29}{71}\right)\left(\frac{71}{29}\right) = (-1)^{14\cdot 35} = 1$. Ponadto $\left(\frac{71}{29}\right) = \left(\frac{13}{29}\right)$. Po raz kolejny z prawa wzajemności, mamy $\left(\frac{13}{29}\right)\left(\frac{29}{13}\right) = (-1)^{14\cdot 6} = 1$. Wreszcie, $\left(\frac{29}{13}\right) = \left(\frac{3}{13}\right)$. Korzystając jeszcze raz z wzajemności, mamy $\left(\frac{3}{13}\right)\left(\frac{13}{3}\right) = (-1)^{1\cdot 6} = 1$. Ponadto $\left(\frac{13}{3}\right) = \left(\frac{1}{3}\right) = 1$. Łącząc te przejścia, stwierdzamy, że

$$\left(\frac{71}{113}\right) = \left(\frac{-29}{71}\right) = -\left(\frac{13}{29}\right) = -\left(\frac{3}{13}\right) = -1.$$

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 $r_2, r_4, \ldots, r_{\frac{p-1}{2}\cdot 2}$

Rozwiązanie.

(a) Najmniejsze reszty $r_2, \ldots, r_{10}$ wynoszą odpowiednio 2, 4, -5, -3, -1. Zatem są trzy elementy ujemne i nie ma elementów o równych wartościach bezwzględnych.

(b) Jak można zauważyć już z przypadku powyżej, ujemne najmniejsze reszty r_{2a} otrzymamy dla takich a, dla których $p - 2a = |2a - p| < 2a$, czyli $4a > p = 8k + s$. Rozpatrzmy tutaj dwa przypadki:

(a) $s = 1, 3$. W tym przypadku nierówność $4a > p$ sprowadza się do $a \geq 2k + 1$. Ponadto $a \leq \frac{p-1}{2} = 4k + \frac{s-1}{2}$. Moc zbioru takich liczb to $2k + \frac{s-1}{2}$.

(b) $s = 5, 7$. Tutaj nierówność to $a \geq 2k + 2$, więc moc zbioru takich liczb to $2k + \frac{s-1}{2} - 1$.

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 $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.

Rozwiązanie.
(a) Równość $r_{ak} = -r_{al}$ implikuje, że $a(k+l) \equiv r_{ak} + r_{al} = 0 \pmod{p}$. Z założenia p nie dzieli a, więc p dzieli $k+l$. Sprzeczność, bo $2 \leq k+l \leq 2 \cdot \frac{p-1}{2}$. Przypadek $r_{ak} = r_{al}$ eliminujemy podobnie.
(b) Dla każdego a najmniejsza reszta r_a spełnia $|r_a| \leq \frac{p-1}{2}$. Faktycznie, jeśli nie, to zachodziłoby $|r_a - p| < |r_a|$ lub $|r_a + p| < |r_a|$. Zatem lewy zbiór w podpunktu (b) zawiera się w prawym. Na mocy podpunktu (a), oba zbiory mają tę samą moc (po lewej stronie żadne dwa elementy nie są równe), zatem są równe.
(c) Mamy

$$\begin{aligned} a \cdot (2a) \cdot \ldots \cdot \left(\frac{p-1}{2} \cdot a\right) \equiv & (\pm|r_a|) \cdot (\pm|r_{2a}|) \cdot \ldots \cdot \left(\pm r_{\frac{p-1}{2}a}\right) = \\ & (-1)^{\mathrm{N}(a)} |r_a| \cdot |r_{2a}| \cdot \ldots \cdot |r_{\frac{p-1}{2}a}| = (-1)^{\mathrm{N}(a)} \cdot 1 \cdot 2 \cdot \ldots \cdot \frac{p-1}{2} \pmod{p}. \end{aligned}$$

W ostatniej równości użyliśmy podpunktu (b). Skracając obie strony kongruencji przez $(\frac{p-1}{2})!$, która jest względnie pierwsza z p, otrzymujemy $a^{\frac{p-1}{2}} \equiv (-1)^{\mathrm{N}(a)} \pmod{p}$, a stąd $\left(\frac{a}{p}\right) = (-1)^{\mathrm{N}(a)}$.
(d) Używając zadania 3. sprawdzamy, że $\mathrm{N}(2)$ jest parzyste dokładnie, gdy $p \equiv 1, 7 \pmod{8}$. W wyrażeniu $p^2 - 1 = (p-1)(p+1)$ mamy iloczyn dwóch kolejnych liczb parzystych. Jedna z nich jest podzielna przez 2, ale nie przez 4. Wobec tego całe wyrażenie jest podzielne przez 16 dokładnie gdy jeden z czynników jest podzielny przez 8. To zachodzi, gdy $p \equiv 1, 7 \pmod{8}$. Wreszcie, $(-1)^{(p^2-1)/8}$ jest równe 1 dokładnie gdy 16 dzieli $p^2 - 1$. Łącząc te trzy obserwacje, otrzymujemy $(-1)^{\mathrm{N}(2)} = (-1)^{(p^2-1)/8}$. Zatem $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.

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

Rozwiązanie.

Dla każdego k z postulatu Bertranda wynika, że istnieje liczba pierwsza w przedziale $[10^k, 2 \cdot 10^k]$. Ma ona pierwszą cyfrę 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 $n \leq 50$.*

Rozwiązanie.

Na początek sprawdzamy bezpośrednio, że teza zachodzi dla liczb $n \leq 30$. Dalej zakładamy, że $n \geq 31$.

Niech $n = 2m + 1$, wtedy $m \geq 15$. Z postulatu Bertranda, istnieje liczba pierwsza p w przedziale $[m - 3 + 1, 2m - 6]$. Liczba $2m - 6$ nie jest pierwsza, więc $p \leq 2m - 7$.

Mamy $n - p \leq m + 3$. Z indukcji, istnieje zapis liczby $n - p = \sum_{i=1}^{s} q_i$, gdzie q_i są różnymi liczbami pierwszymi, z których każda spełnia $q_i \leq \max(11, n - p - 7) \leq m - 4 < p$. Suma $n = p + \sum_{i=1}^{s} q_i$ pokazuje, że n zapisuje się jako suma różnych liczb pierwszych, z których każda jest mniejsza niż $\max(11, n - 7) = n - 7 = 2m - 6$. To pokazuje, że krok indukcyjny jest wykonany. Przypadek kroku dla $n = 2m$ jest podobny i pomijamy go tu.

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

Rozwiązanie.

(Rozwiązanie na wykładzie 23 marca.)