

6. Prawo wzajemności reszt kwadratowych

Przypomnienie: symbol Legendre'a $\left(\frac{d}{p}\right)$ jest równy $+1$, jeśli kongruencja $x^2 \equiv d \pmod{p}$ ma rozwiązanie (chyba że $p|d$, wówczas kładziemy $\left(\frac{d}{p}\right) = 0$), a -1 gdy nie ma. (p jest tu – jak niemal wszędzie na tej liście – nieparzystą liczbą pierwszą, zaś d liczbą całkowitą.)

Prawo wzajemności reszt kwadratowych mówi, że dla nieparzystych liczb pierwszych p, q zachodzi

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

czyli $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ jeśli p lub q jest postaci $4k+1$, a $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$ jeśli p i q są postaci $4k+3$. Wraz z dodatkowymi wzorami

$$(D) \quad \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \quad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}, \quad \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$$

pozwala ono dość efektywnie wyliczać symbole Legendre'a.

1. Czy kongruencja $3x^2 - 2x \equiv 7 \pmod{23}$ ma rozwiązanie? A kongruencja $7x^2 + 6x \equiv 2 \pmod{37}$?
2. Uzasadnij, że nieparzysty czynnik pierwszy liczby postaci $n^2 - 5$ przystaje do ± 1 modulo 5 (lub jest równy 5).
3. Wykaż, że jeśli a jest niezerową liczbą całkowitą, zaś p, q nieparzystymi liczbami pierwszymi nie dzielącymi a , oraz $p \equiv q \pmod{4|a|}$, to $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$.
4. Niech p będzie nieparzystą liczbą pierwszą. Uzasadnij, że jeśli $p \mid x^2 - 2$, to $p \equiv \pm 1 \pmod{8}$. Podobnie przeanalizuj czynniki pierwsze p liczb postaci $x^2 + 2$, $x^2 + 1$, $x^4 + 1$ – jakie może być $p \pmod{8}$ w każdym z tych przypadków?
5. Używając poprzedniego zadania wykaż, że istnieje nieskończenie wiele liczb pierwszych postaci (oddzielnie) $8n+1$, $8n+3$, $8n+5$, $8n+7$.
[Wsk. Naśladuj Euklidesa, który pokazał, że istnieje nieskończenie wiele liczb pierwszych.]
6. Wykaż, że jeśli p i $q = 4p+1$ są obie pierwsze, to
 - a) 2 nie jest kwadratem modulo q ;
 - b) 2 jest pierwiastkiem pierwotnym modulo q ;
 - c) $q \mid 2^{2p} + 1$.
7. ($n > 0$) Udowodnij, że $2^{2^n} + 1$ jest liczbą pierwszą $\iff 2^{2^n} + 1 \mid 3^{2^{2^n-1}} + 1$.
8. Dane są takie liczby całkowite a i b , że $a \neq 0$ oraz liczba $3 + a + b^2$ jest podzielna przez $6a$. Wykazać, że liczba a jest ujemna.

[Wsk. nie wprost: pokaż, że jeśli $a > 0$, to $3 + b^2$ ma czynnik pierwszy $p \equiv 2 \pmod{3}$, co daje sprzeczność z prawem wzajemności.]

Symbol Jacobiego

Praktyczne wyliczanie symbolu Legendre'a przy użyciu (W) i (D) ma jeden nieprzyjemny aspekt: wymaga rozkładania liczb na czynniki pierwsze. Aby tego nie robić używamy *symbolu Jacobiego*. Dla nieparzystej dodatniej liczby całkowitej n o rozkładzie na czynniki pierwsze $\prod_i p_i^{\alpha_i}$ kładziemy mianowicie

$$\left(\frac{d}{n}\right) = \prod_i \left(\frac{d}{p_i}\right)^{\alpha_i}.$$

9. Zauważ, że jeśli $a \equiv d \pmod{n}$, to $\left(\frac{a}{n}\right) = \left(\frac{d}{n}\right)$. Zauważ, że $\left(\frac{d}{mn}\right) = \left(\frac{d}{m}\right) \left(\frac{d}{n}\right)$.
 - a) Uzasadnij, że symbol Jacobiego spełnia wzory (D).
 - b) Udowodnij, że dla dowolnych nieparzystych dodatnich względnie pierwszych liczb p, q symbol Jacobiego spełnia (W).
10. Oblicz $\left(\frac{97}{101}\right)$, $\left(\frac{3083}{3911}\right)$.
11. Uzasadnij, że jeśli d jest kwadratem mod n , to $\left(\frac{d}{n}\right) = 1$. Podaj przykład pokazujący, że odwrotna implikacja nie zachodzi.