

Teoria liczb

zadania różne, 27 lutego

Zadanie 1. Nieparzysta liczba pierwsza p zapisuje się jako $a^2 + b^2$ dla pewnych całkowitych a, b . Pokaż, że $p \equiv 1 \pmod{4}$.

Zadanie 2. Pokaż, że równanie $x^2 + y^2 = 4^n$ nie ma rozwiązań w liczbach całkowitych dodatnich x, y, n .

Zadanie 3. Pokaż, że równanie $x^3 + 2y^3 = 7^n$ nie ma rozwiązań w liczbach całkowitych dodatnich x, y, n .

Zadanie 4. Liczba całkowita a jest względnie pierwsza z 105. Pokaż, że $a^{12} \equiv 1 \pmod{105}$. Ile jest liczb względnie pierwszych z 105 w zbiorze $\{0, 1, 2, \dots, 105 - 1\}$?

Zadanie 5 (istnienie generatora). Niech p będzie nieparzystą liczbą pierwszą. W tym zadaniu pokażemy, że grupa mnożeniowa $\mathbb{Z}_p^* = \{1 \pmod{p}, 2 \pmod{p}, \dots, p - 1 \pmod{p}\}$ jest cykliczna rzędu $p - 1$.

- (a) Niech $a, b \in \mathbb{Z}_p^*$ będą elementami rzędu r_1, r_2 . Pokaż, że istnieje liczba całkowita dodatnia k taka, że rząd ab^k to $\text{NWW}(r_1, r_2)$.
- (b) Niech r będzie największym rzędem elementu w \mathbb{Z}_p^* . Pokaż, że każdy element tej grupy ma rząd będący dzielnikiem r .
- (c) Pokaż, że dla każdego d , równanie $x^d - 1 \equiv 0 \pmod{p}$ ma najwyżej d rozwiązań w \mathbb{Z}_p . Wykorzystaj fakt, że jest to ciało. Wywnioskuj, że r powyżej jest równe $p - 1$.

Zadanie 6 (Twierdzenie Wilsona). (a) Niech p będzie liczbą pierwszą. Pokaż, że $(p - 1)! \equiv -1 \pmod{p}$.

- (b) Niech n będzie dowolną liczbą naturalną. Jakie reszty z dzielenia przez n może dać $(n - 1)!$?

Zadanie 7. Niech p będzie nieparzystą liczbą pierwszą, zaś r będzie liczbą całkowitą niepodzielną przez p . Pokaż, że równanie $a^2 \equiv r \pmod{p}$ ma rozwiązanie wtedy i tylko wtedy, gdy $r^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Jeśli te warunki zachodzą, mówimy, że r jest resztą kwadratową modulo p .

Zadanie 8 ($p = 4k + 1 \iff p = a^2 + b^2$). Niech $\mathbb{Z}[i] \subseteq \mathbb{C}$. Z algebry I wiadomo, że jest to dziedzina z jednoznacznością rozkładu. Niech p będzie liczbą pierwszą taką, że $p \equiv 1 \pmod{4}$.

- (a) Pokaż, że -1 jest resztą kwadratową modulo p , powiedzmy $c^2 \equiv -1 \pmod{p}$.
- (b) Z równania $(c + i)(c - i) = kp$, dla $k \in \mathbb{Z}$, wywnioskuj, że element $p \in \mathbb{Z}[i]$ nie jest pierwszy.
- (c) Niech $p = cd$, gdzie $c, d \in \mathbb{Z}[i]$ są nieodwracalne, powiedzmy $c = a + bi$. Pokaż, że $p = a^2 + b^2$.

Zadanie 9 (**). Ustalmy liczbę pierwszą p oraz liczbę całkowitą dodatnią e . Pokaż, że istnieje dokładnie jedno ciało o p^e elementach.