1. Pierścień Gaussa

1. Udowodnij, że każdy element pierwszy pierścienia Gaussa $\mathbf{Z}[i]$ dzieli pewną liczbę pierwszą całkowitą.
2. Sprawdź, że jeśli interpretować liczbę $a+bi$ jako punkt płaszczyzny (a, b), to mnożenie przez i odpowiada obrotowi przeciwzegarowemu o $\pi/2$.
   a) Uzasadnij, że każdy element pierwszy pierścienia $\mathbf{Z}[i]$ jest stowarzyszony z jedynym elementem postaci $a + bi$ spełniającym $a > 0$ i $b \geq 0$.
   b) Uzasadnij, że czynniki pierwsze w $\mathbf{Z}[i]$ liczby pierwszej $p \equiv 1 \bmod 4$ nie są ze sobą stowarzyszone.
3. Uzasadnij, że liczba pierwsza $p \equiv 1 \bmod 4$ ma dokładnie 8 przedstawień w postaci $a^2 + b^2$.
4. Niech $n = p_1^{\alpha_1} \dots p_k^{\alpha_k} q_1^{\beta_1} \dots q_m^{\beta_m} 2^\gamma$ będzie rozkładem (z $\mathbf{Z}$) na czynniki pierwsze, gdzie $p_i \equiv 1 \bmod 4$, $q_j \equiv 3 \bmod 4$. W terminach tego rozkładu określ liczbę przedstawień n w postaci $a^2 + b^2$.
5. Które liczby całkowite przedstawiają się jednoznacznie (z dokładnością do kolejności składników) jako sumy kwadratów dwóch liczb względnie pierwszych?
6. Udowodnij, że liczba przedstawień n w postaci sumy dwóch kwadratów jest równa $4(d_1(n) - d_3(n))$, gdzie $d_1(n)$ to liczba dzielników n które są postaci $4k + 1$, zaś $d_3(n)$ to liczba dzielników n które są postaci $4k + 3$.
7. Rozwiąż w $\mathbf{Z}$: $y^3 = x^2 + 1$.
8. Udowodnij, że $(p - 1)! \equiv -1 \bmod p$ rozkładając wielomian $x^{p-1} - 1$ na czynniki liniowe $\bmod p$.
   (Znasz wszystkie pierwiastki tego wielomianu.)
9. Niech $p = 4k + 3$ będzie liczbą pierwszą. Oblicz $\prod_{n=1}^{p}(n^2 + 1)$ modulo p.
   (Wsk. użyj elementu i, takiego że $i^2 = -1$.)
10. Uzasadnij, że liczba postaci $4^n(8k + 7)$ nie da się przedstawić w postaci sumy trzech kwadratów.

Zadania do domu

11. Skonstruuj okrąg przechodzący przez dokładnie n punktów kratowych.
12. (Chińskie twierdzenie o resztach) Niech $n_1, \dots, n_k$ będą liczbami naturalnymi parami względnie pierwszymi, zaś $r_1, \dots, r_k$ dowolnymi liczbami naturalnymi. Udowodnij, że istnieje liczba naturalna m, taka że
$$m \equiv r_i \bmod n_i, \qquad i = 1, \dots, k$$
13. Udowodnij, że dla dowolnego naturalnego n istnieje takie naturalne N, że żadna z liczb $N+1, \dots, N+n$ nie rozkłada się na sumę kwadratów liczb całkowitych. (Wsk. użyj chińskiego twierdzenia o resztach).
14. Odcinek o długości 2014 na płaszczyźnie jest równoległy do osi OX i nie zawiera punktów kratowych. Czy można tak poruszać tym odcinkiem, by w żadnym momencie nie zawierał punktów kratowych, a po zakończeniu ruchu był równoległy do osi OY? (Wsk. użyj poprzedniego zadania)