Zadanie. Niech $a, b \in \mathbb{Z}$ będą liczbami całkowitymi takimi, że $\operatorname{nwd}(a, b) = 1$ oraz $a^2 + b^2 > 1$. Wykaż, że $\mathbb{Z}[X]/(a + bi) \simeq \mathbb{Z}_{a^2+b^2}$.

Rozwiązanie. Niech $I = (a+bi) \triangleleft \mathbb{Z}[X]$. Wtedy $a^2+b^2 = (a-bi)(a+bi) \in I$ oraz $-b + ia = i(a + bi) \in I$. Niech $A, B \in \mathbb{Z}$ będą takie, że $Aa + Bb = 1$. Wtedy

$$c + di = c + d(Aa + Bb)i = c + dA(-b + ai) + dAb + dB(a + bi) - dBa.$$

Zatem, dla dowolnego $c + di \in \mathbb{Z}[i]$ istnieje liczba naturalna $n \in \mathbb{Z}$ taka, że $[c + di] = [n]$. Dodatkowo, biorąc resztę z dzielenia n przez $a^2 + b^2$ można założyć, że $0 \leq n < a^2 + b^2$. Niech $0 \leq n, m < a^2 + b^2$. Załóżmy, że $[n] = [m]$ zatem $(n - m) \in I$. Oznacza to, że $\frac{n-m}{a+bi} = \frac{(n-m)(a-bi)}{a^2+b^2} \in \mathbb{Z}[i]$. Zatem $a^2 + b^2 | (n-m)a$ oraz $a^2+b^2 | (n-m)b$ skąd $a^2+b^2 | \operatorname{nwd}((n-m)a, (n-m)b) = n-m$ co jest możliwe jedynie gdy $n = m$.