Teoria liczb
zadanie domowe 2, na 27.04

Rozwiązanie zadania należy spisać i przysłać, można papierowo lub elektronicznie. Zadanie jest na zaliczenie: warto oddawać również częściowo rozwiązane zadanie. Rozwiązanie może (a czasem nawet powinno) korzystać z zadań z ćwiczeń oraz z materiału z wykładu. Dopuszczalne jest konsultowanie się z kolegami, natomiast bardzo proszę oddawać wyłącznie rozwiązania spisane przez siebie i zrozumiane przez siebie (niekoniecznie wymyślone przez siebie).

Zadanie 1. Niech p będzie nieparzystą liczbą pierwszą. Jeśli $p \equiv 3 \pmod 4$ to kładziemy $\alpha = p$, jeśli $p \equiv 1 \pmod 4$ to definiujemy $\alpha := a + bi \in \mathbb{Z}[i]$, gdzie $a, b \in \mathbb{Z}_+$ są takie, że $p = a^2 + b^2$.

(a) Pokaż, że ideał generowany przez α w $\mathbb{Z}[i]$ jest maksymalny. Pokaż, że ciało $\mathbb{Z}[i]/(\alpha)$ zawiera ciało $\mathbb{Z}/(p)$.

(b) Niech $N(\alpha)$ oznacza liczbę elementów ciała $\mathbb{Z}[i]/(\alpha)$. Pokaż, że $N(\alpha) = p$ jeśli $p \equiv 1 \pmod 4$ oraz $N(\alpha) = p^2$ jeśli $p \equiv 3 \pmod 4$. *Wskazówka: $\mathbb{Z}[i]/(\alpha)$ jest przestrzenią wektorową nad $\mathbb{Z}/(p)$.*

(c) Niech element $\beta \in \mathbb{Z}[i]$ będzie niepodzielny przez α. Pokaż, że $\beta^{(N(\alpha)-1)/4} \equiv i^j \pmod \alpha$, gdzie $j \in \{0, 1, 2, 3\}$, zaś i jest pierwiastkiem czwartego stopnia z jedynki.

(d) Pokaż, że następujące warunki są równoważne:

   (a) $\beta^{(N(\alpha)-1)/4} \equiv 1 \pmod \alpha$,

   (b) istnieje $\gamma \in \mathbb{Z}[i]$ taki, że $\gamma^4 \equiv \beta \pmod \alpha$.

   Wskazówka: grupa $(\mathbb{Z}[i]/(\alpha))^*$ ma generator bo to grupa multiplikatywna ciała.