Teoria liczb
zadanie domowe 5, na 15.06

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 $f(x) = x(x-1)(x-2)$ i niech E będzie krzywą eliptyczną o równaniu Weierstrassa $y^2 = f(x)$. Niech $\mathbb{Z}[i]$ będzie pierścieniem liczb Gaussa i niech $A = \mathbb{Z}[i]/(5)$ będzie pierścieniem ilorazowym.

(a) Ile elementów ma A?

(b) Ile elementów ma zbiór $E(A)$?
Nie jest to konieczne, ale opcjonalnie bardzo pomocne tutaj jest zrozumienie, jakim pierścieniem jest A i/lub chińskie twierdzenie o resztach.

Uwaga: w rozwiązaniu można korzystać z rozwiązania zadania domowego nr 4.