Teoria liczb
zadanie domowe 4, na 25.05

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. Rozważmy równanie $y^2 = x(x-1)(x-2)$. Oblicz wszystkie jego rozwiązania w $\mathbb{Z}_5$ i opisz, jaka jest struktura grupy na zbiorze rozwiązań (uzupełnionym o element neutralny) pochodząca ze struktury krzywej eliptycznej.