ODABRANE TEME IZ TEORIJE BROJEVA: PETA ZADAĆA

1. Sage

a) Odredite Diofantovu trojku (s elementima u $\mathbb{Q}(t)$) koja odgovara točki $3R$.

2. Eliptičke krivulje

a) Neka je $R = \mathbb{F}_p[\epsilon]/(\epsilon^2)$. Pokažite da
$$F(X, Y) = X + Y + \epsilon XY^p$$
definira "ne-komutativnu" formalnu grupu.

b) Neka je R prsten. Pokažite da postoji ne-komutativna formalna grupa definirana nad R ako i samo ako postoji $\epsilon \in R$ i cijeli brojevi $m, n \geq 1$ takvi da je $m\epsilon = \epsilon^n = 0$.

c) Neka je E eliptička krivulja $y^2 = x^3 + Ax$. Neka je $w(z) = \sum A_n z^n$ red potencija definiran na predavanju. Dokažite da je $A_n = 0$ za svaki $n \equiv 3 \pmod 4$.

Rok za predaju zadaće je četvrtak 26.1.