ELIPTIČKE KRIVULJE U KRIPTOGRAFIJI
1. Zadaća

Student: Violeta Atanasov

Neka je E eliptička krivulja zadana s

$$E : y^2 = x^3 + 625x + 46875.$$

1. Nađite njen minimalni model i odredite sve proste brojeve u kojima ima lošu redukciju. (5 bodova)

2. Za najmanji neparni prosti broj p u kojemu E ima lošu redukciju, odredite tip loše redukcije (aditivna, podijeljena multiplikativna ili nepodijeljena multiplikativna). (5 bodova)

3. Neka je E_1 elipticka krivulja zadana s

$$y^2 = x^3 + 4x + 24.$$

Jesu li E i E_1 izomorfne nad $\mathbb{Q}$ i jesu li izomorfne nad $\mathbb{C}$? Dokažite! (5 bodova)