ELIPTIČKE KRIVULJE U KRIPTOGRAFIJI
2. Zadaća

Student: Violeta Atanasov

1. Pokažite da je krivulja

$$y^2 = x^3 + 7x^2 + 8x - 16$$

singularna. Odredite joj singularnu točku, te nađite jednu njezinu racionalnu parametrizaciju.

2. Neka je $E/\mathbb{Q}$ eliptička krivulja zadana s

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

Odredite grupovnu strukturu od $E(\mathbb{F}_7)$.

3. Nađite sve točke konačnog reda, te odredite strukturu torzijske grupe za

$$y^2 = x^3 - 3915x + 113670.$$