ELIPTIČKE KRIVULJE U KRIPTOGRAFIJI

zadaća 1.55

1. Eliptičku krivulju nad $\mathbb{Q}$ zadanu jednadžbom

$$y^2 + xy + y = x^3 - x^2 - 4x + 1$$

prikažite u kratkoj Weierstrassovoj formi.

2. Pokažite da je krivulja

$$y^2 = x^3 + 2x^2 - 4x - 8$$

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

3. Odredite j-invarijantu eliptičke krivulje

$$y^2 + xy + y = x^3 - x^2 + 2.$$