ELIPTIČKE KRIVULJE U KRIPTOGRAFIJI

zadaća 1.27

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

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

prikažite u kratkoj Weierstrassovoj formi.

2. Pokažite da je krivulja

$$y^2 = x^3 - 7x^2 - 17x - 9$$

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

3. Odredite j-invarijantu eliptičke krivulje

$$y^2 + xy + y = x^3 - x^2 + 25x + 1.$$