ELIPTIČKE KRIVULJE U KRIPTOGRAFIJI

3. zadaća

1. Nađite racionalan broj t sa svojstvom da za eliptičku krivulju

$$E : y^2 = x(x+t)(x+t+2).$$

vrijedi $E(\mathbb{Q})_{\text{tors}} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

2. Izračunajte rang eliptičke krivulje nad $\mathbb{Q}$ zadane jednadžbom

$$y^2 = x^3 - 50x.$$

3. Neka je E eliptika krivulja

$$E : y^2 = x^3 + x^2 + 1$$

nad $\mathbb{F}_9$. Odredite kojoj je grupi oblika $\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ izomorfna grpa $E(\mathbb{F}_9)$.