

ELIPTIČKE KRIVULJE U KRIPTOGRAFIJI

zadaca 4.30

1. Zadana je točka $P = (0, 2)$ na eliptičkoj krivulji $y^2 = x^3 + 2x + 4$ nad poljem \mathbb{F}_{211} .
Odredite NAF prikaz broja 105. Izračunajte $105P$.
2. Zadana je eliptička krivulja

$$E : y^2 = x^3 + x + 4$$

nad poljem \mathbb{F}_{191} . Odredite red grupe $E(\mathbb{F}_{191})$ Shanks-Mestreovom metodom, koristeći točku $P = (22, 13)$.