ELIPTIČKE KRIVULJE U KRIPTOGRAFIJI

4. zadaća

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 102. Izračunajte $102P$.

2. Zadana je eliptička krivulja

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

nad poljem $\mathbb{F}_{191}$. Odredite red grupe $E(\mathbb{F}_{191})$ Shanks-Mestreovom metodom, koristeći točku $P = (15, 23)$.

3. Dokažite da je broj 863 prost pomoću eliptičkih krivulja. Za ovaj zadatak smijete koristiti računalne programe SAGE/PARI.