

# ELIPTIČKE KRIVULJE U KRIPTOGRAFIJI

## zadaca 4.49

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 124. Izračunajte  $124P$ .
2. Pronađite jednu eliptičku krivulju  $E$  nad  $\mathbb{F}_{19}$  sa svojstvom da je red grupe  $E(\mathbb{F}_{19})$  jednak 23.
3. 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  $P = (68, 51)$ .