

**Kryptografia z elementami algebry**  
*ćwiczenia*

1. Niech  $Y^2 = X^3 + 2X + 7$  będzie krzywą eliptyczną nad  $\mathbf{F}_{11}$ . Wyznacz  $E(\mathbf{F}_{11})$ .
2. Niech  $Y^2 = X^3 + 3X + 2$  będzie krzywą eliptyczną nad  $\mathbf{F}_{13}$ . Sprawdź czy punkty  $P = (5, 5)$ ,  $Q = (3, 7)$ ,  $R = (2, 4)$  należą do  $E(\mathbf{F}_{13})$ .
3. Niech  $Y^2 = X^3 + X + 4$  będzie krzywą eliptyczną nad  $\mathbf{F}_{11}$ . Niech  $P = (2, 5)$ ,  $Q = (3, 10) \in E(\mathbf{F}_{11})$ . Oblicz
  - (a)  $P + Q$
  - (b)  $2Q$
  - (c)  $Q - P$
4. Niech  $Y^2 = X^3 + 4$  będzie krzywą eliptyczną nad  $\mathbf{F}_7$ . Niech  $Q = (0, 5) \in E(\mathbf{F}_7)$ . Wyznacz  $\langle Q \rangle$ .
5. Niech  $Y^2 = X^3 + 2X$  będzie krzywą eliptyczną nad  $\mathbf{F}_{11}$ . Niech  $H = \{\mathcal{O}, (0, 0)\}$ . Sprawdź czy  $H < E(\mathbf{F}_{11})$ .