

# ELIPTIČKE KRIVULJE U KRIPTOGRAFIJI

## zadaca 3.29

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

$$E : y^2 = x(x+t)(x+t+114).$$

vrijedi  $E(\mathbb{Q})_{\text{tors}} = \mathbb{Z}_2 \times \mathbb{Z}_4$ .

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

$$y^2 = x^3 + 35x.$$

3. Za polinom

$$p(x) = (x-3)(x-2)(x-1)x(x+1)(x+3)(x+4)(x+5),$$

odredite polinome  $q(x), r(x) \in \mathbb{Q}[x]$  takve da vrijedi  $p(x) = (q(x))^2 - r(x)$  i  $\deg r \leq 3$ .