Sveučilište u Zagrebu

Prirodoslovno - matematički fakultet

Matematički odsjek

Eliptičke krivulje u kriptografiji

3. domaća zadaća

Student:
Antonio Kovačić

Nastavnik:
Doc. dr. sc. Filip Najman

Zagreb, 26. svibnja 2014.

Sadržaj

1 Problem

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

$$E : y^2 = x(x+t)(x+t+38)$$

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

2. Odredite rang eliptičke krivulje nad $\mathbb{Q}$ zadane jednadžbom

$$y^2 = x^3 - 22x$$

3. Za polinom

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

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

2 Rješenje

2.1 1. zadatak