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

Prema [2, p. 28] je opći oblik krivulje s torzijskom podgrupom $\mathbb{Z}_2 \times \mathbb{Z}_4$ oblika:

$$y^2 = x(x + r^2)(x + s^2), \quad r, s \in \mathbb{Q} \tag{1}$$

Prema tome slijedi:

$$t = s^2 \tag{2}$$

$$t + 38 = r^2 \tag{3}$$

Iz čega slijedi da:

$$r^2 - s^2 = 38 \tag{4}$$

No ne postoje $(r, s) \in \mathbb{Z}^2$ koji zadovoljavaju (4). Zaključujemo da je $(r, s) \in (\mathbb{Q}\backslash\mathbb{Z})^2$, a onda i $t \in \mathbb{Q}\backslash\mathbb{Z}$. Pokušajmo vidjeti postoji li $a \in \mathbb{Z}$ tako da za t vrijedi:

$$t = \left(a + \frac{1}{2}\right)^2, \qquad t + 38 = \left(a + \frac{3}{2}\right)^2 \tag{5}$$

Iz (5) se lako dobije $a = 18$, pa je $s = \frac{37}{2}$, a $r = \frac{39}{2}$. Iz čega slijedi da je $\mathbb{Z}_2 \times \mathbb{Z}_4$ podgrupa od $E(\mathbb{Q})_{\text{tors}}$. Još je ostalo provjeriti da $E(\mathbb{Q})_{\text{tors}} \neq \mathbb{Z}_2 \times \mathbb{Z}_8$ jer imaju isti oblik, no prema:

$$\text{Za } E : y^2 = x(x + r^2)(x + s^2), E(\mathbb{Q})_{\text{tors}} \text{ izomorfna s } \mathbb{Z}_2 \times \mathbb{Z}_8 \text{ akko}$$

$$rs, rs + r^2, rs + s^2 \text{ kvadrati u } \mathbb{Q}$$

No $\frac{37 \cdot 39}{4} = \frac{1443}{4}$ nije kvadrat u $\mathbb{Q}$, pa slijedi tražena tvrdnja za $t = \frac{1369}{4}$.

Literatura

[1] A. Dujella. *Uvod u teoriju brojeva.* http://web.math.pmf.unizg.hr/~duje/utb/utblink.pdf.

[2] A. Dujella. *Eliptičke krivulje u kriptografiji.* http://web.math.pmf.unizg.hr/~duje/elkript/elkripto2.pdf, 2013.