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, 27. 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:

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

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

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

2.2 2. zadatak

Prema [2, p. 38] za krivulju $E : y^3 = x^3 - 22x$ je njena pripadna 2-izogena krivulja dana sa $E' : y^3 = x^3 + 4 \cdot 22x = x^3 + 88x$. Za računanje ranga krivulje E promatramo odgovarajuća preslikavanja α i β te određujemo $|Im(\alpha)|$ i $|Im(\beta)|$.
Rješenje za $Im(\alpha)$:

$$E : y^3 = x^3 - 22x \to a = 0, b = -22$$

Prema tome tražimo (M, e, N) takve da jednadžba:

$$b_1 M^4 + b_2 e^4 = N^2$$

ima rješenja, pri čemu vrijedi:

- b_1 djelitelj od 22 koji je kvadratno slobodan
- $b_1 b_2 = -22$
- $(M, e) = 1$, gdje (M, e) označava najvećeg zajedničkog djelitelja od M i e

Naša jednadžba za b_1 i b_2 izgleda simetrično pa je dovoljno provjeravati egzistenciju rješenja za parove djetitelja:

1. $b_1 \in \{1, -22\} \to (M, e, N) = (1, 0, 1)$ za $b_1 = 1$, a za $b_1 = -46$ je rješenje $(M, e, N) = (0, 1, 1)$

2. $b_1 \in \{-2, 11\} \to$ Jednadžba izgleda:

$$-2M^4 + 11e^4 = N^2$$

   I ima rješenje $(M, e, N) = (-1, 1, 3)$

3. $b_1 \in \{2, -11\} \to$ Jednadžba izgleda:

$$-11M^4 + 2e^4 = N^2$$

   U slučaju da je M paran, e mora biti neparan jer $(M, e) = 1$, pa onda slijedi i da

N mora biti paran:

$$M = 2k, N = 2l, \text{ gdje k i l cijeli brojevi}$$

$$2e^4 = 11 \cdot 2^4 k^4 + 2^2 l^2 \to e^4 = 2 \cdot (2^2 k^4 + l^3)$$

Pa imamo da e^4 mora biti paran, a onda i e mora biti djeljiv s 2, a to je kontradikcija jer je i M djeljiv s 2 pa bi imali $2|(M, e)$.
U slučaju da je M neparan, slijedi i da N mora biti neparan. Imamo onda:

$$M^4 \equiv N^2 \equiv 1 (\operatorname{mod} 8) \to 11M^4 \equiv 3 (\operatorname{mod} 8)$$

Pa slijedi da je:

$$2e^4 \equiv 4(\text{mod8}) \to e^4 \equiv 2(\text{mod } 4)$$

Provjeravamo vrijedi li gornja kongruencija za $x \in \{0, 1, 2, 3\}$ i lako se dobije da ona nema riješenja.

4. $b \in \{-1, 22\} \to$ Jednadžba izgleda:

$$-1M^4 + 22e^4 = N^2$$

Postupak je analogan kao u prošlom slučaju, odnosno M i N su iste parnosti: Ako su M i N parni, slijedit će da i e mora biti paran, a to je kontradikcija jer bi bilo da $2|(M, e)$. Ako pak M i N neparni onda ispada: $22e^4 \equiv 2(\text{mod } 8)$ odnosno $11e^4 \equiv 3e^4 \equiv 1(\text{mod } 4)$ za što ispada da nema riješenja uvrštavanjem elemenata iz $\mathbb{Z}_4$.

Zaključujemo da imamo riješenje za 4 različita b_1 pa zaključujemo da $|Im(\alpha)| = 4$ Analogno riješavamo za $Im(\beta)$:

$$b_1' M^4 + b_2' e^4 = N^2$$

. Gdje (M, e, N) tražimo, a b_1' i b_2' su poznati takvi da vrijedi:

- b_1' djelitelj od 88 koji je kvadratno slobodan

- $b'_1 b'_2 = 88$
- $(M, e) = 1$, gdje (M, e) označava najvećeg zajedničkog djelitelja od M i e

Iz uvjeta $b'_1 b'_2 = 88$ slijedi da $b'_1 > 0$, u suprotnom $b'_2 < 0$ također pa jednadžba

$$b'_1 M^4 + b'_2 e^4 = N^2$$

uopće nema realnih riješenja. Pozitivni djelitelji od 88 su: $1, 2, 4, 8, 11, 22, 44, 88$ no brojeve $4, 8, 44$ i 88 isključujemo kao opcije jer nisu kvadratno slobodnu (dijeli ih 4 (kvadrat broja 2)).

1. $b'_1 = 1 \rightarrow$ Jednadžba izgleda:

   $$M^4 + 88e^4 = N^2$$

   Jedno očito riješenje je $(M, e, N) = (1, 0, 1)$

2. $b'_1 = 2 \rightarrow$ Jednadžba izgleda:

   $$2M^4 + 4 \cdot 11e^4 = N^2 \tag{6}$$

   Iz jednadžbe vidimo da $2|N \rightarrow N = 2L$ L cijeli broj :

   $$2M^4 + 4 \cdot 11e^4 = 4L^2 \Leftrightarrow M^4 + 2 \cdot 11e^4 = 2L^2$$

   Sada vidimo da M^4 paran, pa jer M cijeli broj slijedi da i $2|M$, pa postoji $K \in \mathbb{Z}$ takav da $M = 2K$:

   $$2^4K^4 + 2 \cdot 11e^4 = 2L^2 \rightarrow$$
   $$2^3K^4 + 11e^4 = L^2 \tag{7}$$

   Iz zadnje jednadžbe vidimo da L i e moraju biti iste parnosti:
   Ukoliko e i L parni imamo onda $e = 2f, L = 2J$ pa slijedi:

   $$2^3K + 2^4 \cdot 11f = 2^2J \rightarrow 2K^4 + 4 \cdot 11 = J$$

Zadnji oblik je ekvivalentan jednadžbi (6). Zaključujemo da jednadžba nema netrivijalnih rješenja u $\mathbb{Z}$.

3. $b_1' = 11 \rightarrow$ Jednadžba izgleda:

$$11M^4 + 2^3e^4 = N^2$$

Ima ekvivalentni oblik kao (7) pa zaključujemo da nema rješenja.

4. $b_1' = 22 \rightarrow$ Jednadžba izgleda:

$$22M^4 + 4e^4 = N^2$$

Jedno riješenje je dano sa $(0, 1, 2)$.

Vidimo da imamo riješenje za 2 b_1' iz čega slijedi da $|Im(\beta) = 2$.

Nakon ovako iscrpnog računa, konačno zaključujemo da je:

$$2^r = \frac{|Im(\alpha)||Im(\beta)|}{4} = 2 \Rightarrow rank(E(\mathbb{Q})) = 1$$

2.3 3. zadatak

Imamo:

$$
\begin{align}
p(x) &= (x-4)(x-3)(x-2)x(x+1)(x+2)(x+3)(x+4) \tag{8}\\
&= x^8 + x^7 - 29x^6 - 29x^5 + 244x^4 + 244x^3 - 576x^2 - 576x \tag{9}
\end{align}
$$

Znamo da je $\deg r \leq 3$ pa iz toga zaključujemo da su koeficijenti uz x^4, x^5, x^6, x^7, x^8 jedanaki za $p(x)$ i za $(q(x))^2$, osim toga zaključujemo da je $\deg q = 4$. Stavimo da je:

$$q(x) = q_4x^4 + q_3x^3 + q_2x^2 + q_1x + q_0 \tag{10}$$

$$r(x) = r_3x^3 + r_2x^2 + r_1x + r_0 \tag{11}$$

Iz toga imamo:

$$
\begin{gathered}
(q(x))^2 = q_4^2x^8 + 2q_3q_4x^7 + (q_3^2 + 2q_2q_4)x^6 + (2q_2q_3 + 2q_1q_4)x^5 + \\
(q_2^2 + 2q_1q_3 + 2q_0q_4)x^4 + (2q_1q_2 + 2q_0q_3)x^3 + (q_1^2 + 2q_0q_2)x^2 + 2q_0q_1x + q_0^2
\end{gathered} \tag{12}
$$

$$
\begin{aligned}
p(x) = (q(x))^2 - r(x) = q_4^2x^8 + 2q_3q_4x^7 + (q_3^2 + 2q_2q_4)x^6 \\
(q_2^2 + 2q_1q_3 + 2q_0q_4)x^4 + (2q_1q_2 + 2q_0q_3 - r_3)x^3 + \\
(q_1^2 + 2q_0q_2 - r_2)x^2 + (2q_0q_1 - r_1)x + (q_0^2 - r_0)
\end{aligned} \tag{13}
$$

Iz toga slijedi da mora vrijediti:

$$q_4^2 = 1 \rightarrow q_4 = \pm 1 \tag{14}$$

Uzimamo $q_4 = 1$ (da smo uzeli drugačije, dobili bi drugačija rješenja za koeficijente u čijim će se jednadžbama pojavljivati q_4, ali to ne bi utjecalo na točnost rješenja, odnosno, rješenja može biti više). Redom ćemo uvrštavati q_4 da bi dobili q_3, zatim q_3 i q_4 za q_2, a onda q_2, q_3, q_4 za q_1 te na koncu q_1, q_2, q_3, q_4 za q_0.

$$\begin{aligned} 2q_3 = 1 \rightarrow q_3 &= \frac{1}{2} \\ \frac{1}{4} + 2q_2 = -29 \rightarrow q_2 &= \frac{-117}{8} \\ \frac{-117}{8} + 2q_1 = -29 \rightarrow q_1 &= \frac{-115}{16} \\ \left(\frac{-117}{8}\right)^2 + \frac{-115}{16} + 2q_0 = 244 \rightarrow q_0 &= \frac{2387}{128} \end{aligned} \tag{15}$$

Iz (14) i (15) dolazimo do jednadžbi za koeficijente r_0, r_1, r_2, r_3:

$$\begin{aligned} (2q_1q_2 + 2q_0q_3 - r_3) = 244 \rightarrow r_3 &= \frac{-1935}{128} \\ (q_1^2 + 2q_0q_2 - r_2) = -576 \rightarrow r_2 &= \frac{42083}{512} \\ (2q_0q_1 - r_1) = -576 \rightarrow r_2 &= \frac{315319}{1024} \\ (q_0^2 - r_0) = 0 \rightarrow r_0 &= \frac{5697769}{16384} \end{aligned} \tag{16}$$

Pa je riješenje dano sa:

$$q(x) = x^4 + \frac{1}{2}x^3 - \frac{117}{8}x^2 - \frac{115}{16}x + \frac{2387}{128}$$

$$r(x) = -\frac{1935}{128}x^3 + \frac{42083}{512}x^2 + \frac{315319}{1024}x + \frac{5697769}{16384}$$

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.