Uvod u aritmetiku eliptičkih krivulja

Odredjivanje ranga - 13. lekcija

Ponovimo već poznato. Neka je:
$E : y^2 = x^3 + ax^2 + bx$, $\bar{E} : y^2 = x^3 + \bar{a}x^2 + \bar{b}x$, gdje je $\bar{a} : -2a$ i $\bar{b} := a^2 - 4b$.
Označimo:
$\Gamma := E(\mathbf{Q})$, $\bar{\Gamma} := \bar{E}(\mathbf{Q})$,
$\alpha : \Gamma \to \mathbf{Q}^*/\mathbf{Q}^{*2}$ homomorfizam grupa definiran kao
$\alpha(0,0) = \tilde{b}$,
$\alpha(O) = \tilde{1}$
$\alpha(x,y) = \tilde{x}$, za sve ostale točke
dok je $\bar{\alpha} : \bar{\Gamma} \to \mathbf{Q}^*/\mathbf{Q}^{*2}$ definiran potpuno analogno, samo što umjesto a, b stavljamo $\bar{a}$, a umjesto b stavljamo $\bar{b}$. Tilda označava klasu racionalnog broja različitog od nule u $\mathbf{Q}^*/\mathbf{Q}^{*2}$.
Tada je

$$2^r = \frac{|\alpha(\Gamma)| \cdot |\bar{\alpha}(\bar{\Gamma})|}{4} \tag{1}$$

Kvazialgoritam za odredjivanje slike od α (i analogno za $\bar{\alpha}$) .

(I) $\tilde{1}$ i $\tilde{b}$ uvijek su slici (s tim da su jednaki ako je b kvadrat).
Dodatak: ako je $a^2 - 4b = d^2$ puni kvadrat, onda su i klase od $\frac{-a \pm d}{2}$ u slici.
(II) (netrivijalni dio) Za svaku mogućnost $b_1 b_2 = b$ gledamo diofantsku jednadžbu

$$N^2 = b_1 M^4 + aM^2 e^2 + b_2 e^4 \tag{2}$$

s nepoznanicama M, e, N. Rješenja tražimo u cijelim brojevima, ali tako da bude:
(1) $e > 0$
(2) M i e, N i e, b_1 i e, b_2 i M, te M i N su relativno prosti
Ako nema takvog rješenja (M, e, N), biramo drugi par b_1, b_2, a ako ima dobili smo racionalnu točku $P(x, y)$ gdje je:

$$x = \frac{b_1 M^2}{e^2},\ y = \frac{b_1 MN}{e^3}$$

i $\alpha(P) = \tilde{x} = \tilde{b_1}$, i tako smo dobili vrijednost u slici od α (ta vrijednost osvisi samo o b_1, a ne o rješenju (M, e, N)).

Napomena. U [S-T] (I) je djelomično uključeno u (II) jer se dopušta $e = 0$ i $N = 0$, a mi ćemo u (II) priznavati samo rješenja kojima su sve koordinate različite od nule. Takodjer, u (II) ne treba gledati $b_1 = 1$, jer, ako i bude dobrog rješenja, u slici će dati $\tilde{1}$.

Primjeri.

Primjer 1. $E : y^2 = x^3 - x$.
Tu je $a = 0,\ b = -1$, pa je $\bar{a} = 0,\ \bar{b} = 4$, pa je $\bar{E} : y^2 = x^3 + 4x$.
Odredjujemo sliku od α.
Mogućnosti za b_1 jesu ± 1. Kako su obje u (I) ne treba gledati (II) i imamo dva elementa u slici (jer -1 nije kvadrat). Dodatak u (I) daje $d = 2$, zato treba razmotriti $\frac{\pm 2}{2} = \pm 1$, pa ne dobivamo ni jednu novu vrijednost u slici od α. Zaključujemo:
$|\alpha(\Gamma)| = 2$.
Sad odredjujemo sliku od $\bar{\alpha}$.
(I) Daje samo $\tilde{1}$ jer je 4 kvadrat, a dodatak ne nastupa.
(II). Mogućnosti za b_1 jesu $\pm 1, \pm 2, \pm 4$. Brojeve 1 i 4 možemo odbaciti jer su kvadrati i već su u (I), pa ostaju samo $-1, 2, -2, -4$ (i odgovarajuće vrijednosti $-4, 2, -2, -1$ za b_2), pa su pripadne diofantske jednadžbe
(i) $N^2 = -M^4 - 4e^4$
(ii) $N^2 = 2M^4 + 2e^4$
(iii) $N^2 = -2M^4 - 2e^4$
(iv) (i) $N^2 = -4M^4 - e^4$
Vidimo da ni (i) ni (iii) ni (iv) nemaju rješenja (ne dopuštamo nule), pa ostaje (ii) koja ima očito rješenje $(M, e, N) = (1, 1, 2)$ Zaključujemo da je $|\bar{\alpha}(\bar{\Gamma})| = 2$.
Uvrštavajući u (1) dobijemo $2^r = \frac{2 \cdot 2}{4} = 1$, tj. $r = 0$.
Napomene. 1. Rješenje $(1, 1, 2)$ dolazi od točke $(2, 4)$ iz $\bar{\Gamma}$.
(2.) Usput smo dokazali i da $\bar{E}$ ima rang 0.
(3.) Zaključujemo da su racionalne točke na E i $\bar{E}$ torzijske, pa ih eksplicitno možemo odrediti. Pomoću Lutz-Nagell-ova teorema dobije se
$E(\mathbf{Q}) \cong \mathbf{Z}/2\mathbf{Z} \otimes \mathbf{Z}/2\mathbf{Z}$, i $\bar{E}(\mathbf{Q}) \cong \mathbf{Z}/4\mathbf{Z}$, što su neizomorfne grupe. E i $\bar{E}$ su $\mathbf{Q}$-izogene, a rang je invarijanta $\mathbf{Q}$-izogenije, dok torzijska podgrupa nije (izogene krivulje mogu čak imati različito mnogo torzijskih točaka - što tu nije slučaj).
(4.) Jednadžbe (i) i (iv) pripadaju vrijednostima $-1, -4$ od b_1, koji su u istim klasama od $\mathbf{Q}^*/\mathbf{Q}^{*2}$. Tu ni jedna od pripadnih diofantskih jednadžba nije imala rješenje. Općenito može se dogoditi da jedna od njih nema, a druga

ima rješenje koje zadovoljava sve uvjete (pa unaprijed ni jednu ne možemo odbaciti; ako jedna ima rješenje drugu ne moramo gledati, ali ako jedna nema treba provjeriti i drugu). Na primjer, za $y^2 = x^3 - 52x$ i vrijednosti $b_1 = -1, -4$, pripadne su jednadžbe (i) $N^2 = -M^4 + 52e^4$ i (ii) $N^2 = -4M^4 + 13e^4$. Ako sad u (i) uzmemo u obzir uvjet $(M, b_2) = (M, 52) = 1$, dopuštamo samo neparne M, pa nakon redukcije modulo 4 dobijemo jednadžbu $N^2 = -M^4$, koja nema rješenja, pa ni (i) nema dobrog rješenja. Sad bi bilo pogrješno zaključiti da klasa od -1 nije u slici od α. Naime, (ii) ima očito dobro rješenje $(M, e, N) = (1, 1, 3)$. Uočite, takodjer da (i) ima rješenje $(2, 1, 6)$ (koje ne zadovoljava dodatne uvjete iz kvazialgoritma).

Primjer 2. $E : y^2 = x^3 + x$.
Tu je $a = 0,\ b = 1$, pa je $\bar{a} = 0,\ \bar{b} = -4$, pa je $\bar{E} : y^2 = x^3 - 4x$.
Odredjujemo sliku od α.
Tu je $|\alpha(\Gamma)| = 1$.
Jedinu vrijednost - $\tilde{1}$ - dobijemo iz (I), drugih novih nema. Ostaje provjeriti (II) za $b_1 = -1$ čemu korespondira diofantska jednadžba

$$N^2 = -M^4 - e^4.$$

Ta jednadžba nema rješenja. Naime, radimo samo s prirodnim M i e.
Odredimo sliku od $\bar{\alpha}$.
(I) daje $\pm\tilde{1}$ jer -4 nije kvadrat, a dodatak za $d = 4$ daje ± 2, ukupno 4 vrijednosti.
(II). Mogućnosti za b_1 jesu $\pm 1, \pm 2, \pm 4$ i sve su bile u (I). Zaključujemo da je $|\bar{\alpha}(\bar{\Gamma})| = 4$.
Uvrštavajući u (1) dobijemo $2^r = \frac{1 \cdot 4}{4} = 1$, tj. $r = 0$.
Napomena. Opet zaključujemo da su racionalne točke na E i $\bar{E}$ torzijske, pa ih eksplicitno možemo odrediti. Pomoću Lutz-Nagell-ova teorema dobije se
$E(\mathbf{Q}) \cong \mathbf{Z}/2\mathbf{Z}$, i $\bar{E}(\mathbf{Q}) \cong \mathbf{Z}/2\mathbf{Z} \otimes \mathbf{Z}/2\mathbf{Z}$, pa su torzije različitih kardinalnosti. Nas ovdje više zanima E za koju smo dobili da ima samo dvije racionalne točke: O i $(0, 0)$.
Posebice, diofantska jednadžba $N^2 = M^4 + e^4$ (inače dobivena za $b_1 = 1$) ne može imati rješenje (osim trivijalnih koja uključuju nule), jer bi inače eliptička krivulja E imala racionalnu točku različitu od $(0, 0)$. To je dokaz poznate Fermatove tvrdnje (jedine iz teorije brojeva za koju je Fermat dao dokaz).

Primjer 3. $E : y^2 = x^3 - 5x$.
Tu je $a = 0,\ b = -5$, pa je $\bar{a} = 0,\ \bar{b} = 20$, pa je $\bar{E} : y^2 = x^3 + 20x$.
Odredjujemo sliku od α.
(I) Daje $\tilde{1}, \tilde{-5}$ jer -5 nije kvadrat, a dodatak ne nastupa.
(II) Mogućnosti za b_1 jesu $\pm 1, \pm 5$. Kako su 1 i -5 u (I) ostaju $-1, 5$ i pripadne diofantske jednadžbe
(i) $N^2 = -M^4 + 5e^4$
(ii) $N^2 = 5M^4 - e^4$.
Obje imaju očita rješenja $(M, e, N) = (1, 1, 2)$. Zaključujemo:
$|\alpha(\Gamma)| = 4$.
Sad odredjujemo sliku od $\bar{\alpha}$.
(I) Daje $\tilde{1}$ i $\tilde{5}$ jer je 20 u istoj klasi kao i 5, a dodatak ne nastupa.
(II). Mogućnosti za b_1 jesu $\pm 1, \pm 2, \pm 4, \pm 5, \pm 10, \pm 20$. Brojeve 1 i 5 možemo odbaciti jer su u (I), potom i $4, 20$ jer su u njihovim klasama, zatim uočimo da su $-1, -4$ i $-5, -20$ u istim klasama. Konačno ostaju $-1, -4, \pm 2, -5, -20, \pm 10$, pa su pripadne diofantske jednadžbe
(i) $N^2 = -M^4 - 20e^4$
(i)' $N^2 = -4M^4 - 5e^4$
(ii) $N^2 = 2M^4 + 10e^4$
(iii) $N^2 = -2M^4 - 10e^4$
(iv) $N^2 = -5M^4 - 4e^4$
(iv)' $N^2 = -20M^4 - 4e^4$
(v) $N^2 = 10M^4 + 2e^4$
(vi) $N^2 = -10M^4 - 2e^4$
Tu smo stavili (i),(i)' te (iii),(iii)' jer su $-1, -4$ te $-5, -20$ u istim klasama. Medjutim, s njima neće biti problema. Naime, odmah odbacujemo (i),(i)' (iii), (iii)', (iv) i (vi) zbog oba minusa (a tu ne dopuštamo nule), ostaje (ii) i (v). Tvrdimo da ni one nemaju dobra rješenja.
U (ii) možemo predpostaviti da M nije djeljiv s 5, pa jednadžba nema rješenja modulo 5. Sad vidimo da ni (v) nema rješenja, jer je $\tilde{5}$ u slici, a $\tilde{2}$ nije, pa nije ni $\tilde{1}0$ (zbog grupne strukture).
Zaključujemo da je $|\bar{\alpha}(\bar{\Gamma})| = 2$.
Uvrštavajući u (1) dobijemo $2^r = \frac{4 \cdot 2}{4} = 2$, pa je $r = 1$.

Često imamo sreću s konkretnim krivuljama, medjutim još smo uvijek nemoćni s familijama, pa čak i s onim najjednostavnijim - parametriziranim prostim brojevima.

Primjer 4. Familija krivulja $E_p : y^2 = x^3 + px$, za proste p.
Tu je $a = 0$, $b = p$, pa je $\bar{E}_p : y^2 = x^3 - 4px$. Odredjivanje slike od α je jednostavno. U (I) dobijemo $\tilde{1}$ i $\tilde{p}$, dok su u (II) preostale mogućnosti za b_1 brojevi $-1, -p$, pa su i vrijednosti b_2 negativne. Tako je $|\alpha(\Gamma)| = 2$.
Kod $\bar{E}_p$ nastaju problemi. U (I) dobijemo $\tilde{1}$ i $\tilde{-p}$. U (II) su mogućnosti $\pm 1, \pm 2, \pm 4, \pm p, \pm 2p, \pm 4p$. Odbacujemo $1, 4, -p, -4p$, jer već postoje u (I), zatim uočavamo da su u istoj klasi $-1, -4$, te $p, 4p$ pa ostaju $-1, -4, \pm 2, p, 4p \pm 2p$. Ima osam jednadžba koje treba razriješiti:
(i) $N^2 = -M^4 + 4pe^4$
(i)' $N^2 = -4M^4 + pe^4$
(ii) $N^2 = 2M^4 - 2pe^4$
(iii) $N^2 = -2M^4 + 2pe^4$
(iv) $N^2 = pM^4 - 4e^4$
(iv)' $N^2 = 4pM^4 - e^4$
(v) $N^2 = 2pM^4 - 2e^4$
(vi) $N^2 = -2pM^4 + 2e^4$
Odmah vidimo samo to da u isto vrijeme (ii) i (vi) te (iii) i (v) imaju ili nemaju rješenje, takodjer da (i) nema rješenje modulo 4 (uz legitimni uvjet da je M neparan), i slično da (iv)' nema rješenja uz legitimni uvjet da je e neparan, pa ostaje gledati samo (i)', (ii), (iii),(iv). Medjutim to je lako reći, ali teško provesti. Vidimo da uz dvije moguńosti iz (I) ima najviše 8 elemenata u slici od $\bar{\alpha}$ (jer svaki od (ii), (iii) daju 0 ili 2), Tako za r ostaju mogućnosti $0, 1$ ili 2 i pokazuje se da sve mogućnosti nastupaju. Izgleda da dosta toga ovisi o ostatcima prostog broja p modulo 16.
Znade se sljedeće:
(A) Ako je $p \equiv 7, 11$ modulo 16 onda je $r = 0$.
(B) Ako je $p \equiv 3, 5, 13, 15$ modulo 16 onda je **slutnja** da je $r = 1$.
(C) Ako je $p \equiv 1, 9$ modulo 16 onda je **slutnja** da je $r = 0$ ili $r = 2$. Kad je jedno, a kad drugo izgleda da se ne može opisati kongruencijama.
Na primjer, kako je $p = 17 \equiv 1$ modulo 16, slutnja predvidja da je $r = 0$ ili $r = 2$. Kako smo vidjeli α ima 2 vrijednosti, a $\bar{\alpha}$ takodjer 2 u dijelu (I). U (II) dobijemo
(i)' $N^2 = -4M^4 + 17e^4$
(ii) $N^2 = 2M^4 - 34e^4$
(iii) $N^2 = -2M^4 + 34e^4$
(iv) $N^2 = 17M^4 - 4e^4$
jer, kako smo vidjeli, ostale ne treba gledati, ali treba znati da (ii) i (iii) vrijede dvostruko. To dvostruko je ništa, a ni (i)' niti (iv) nemaju rješenja,

iako to nije lako pokazati. Na primjer, (iv) ima rješenje po svakom modulu i nad $\mathbf{R}$, a ipak se pokazuje da (iv) nema rješenja (to je primjer jednadžbe koja pokazuje da u ovakvim okolnostima općenito ne vrijedi lokalno-globalni princip Minkowski-Hasse). Zaključujemo da je $r = 0$, u skladu sa slutnjom. Situacija kad dobivena diofantska jednadžba ima rješenje po svakom modulu i nad $\mathbf{R}$, povezan je s tzv. Selmerovom grupom. Takva jednadžba može, ali ne mora imati cjelobrojno rješenje, i za sad nema algoritma koji odgovara na to pitanje, dok je reduciranje problema na takve jednadžbe algoritamsko.

Zadatak. Odredite rang sljedećih krivulja.
(i) $y^2 = x^3 + 2x$
(ii) $y^2 = x^3 + 3x$
(iii) $y^2 = x^3 + 5x$
(iv) $y^2 = x^3 + 13x$
(v) $y^2 = x^3 + 73x$.

Evo i primjera u kojemu nije $a = 0$.
Primjer 5. Neka je $E : y^2 = x^3 + x^2 + x$. Tada je $a = b = 1$, pa je $\bar{a} = -2$ i $\bar{b} = -3$, dakle $\bar{E} :: y^2 = x^3 - 2x^2 - 3x$.
Slika od ϕ je trivijalna, jer (I) daje samo klasu od 1; naime $b = 1$, a dodatak ne nastupa. U (II) ostaje samo $b_1 = -1$ s pripadnom jednadžbom

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

Kako je $-M^4 + M^2e^2 - e^4 = -(M^2 - e^2)^2 - M^2e^2 < 0$, jednadžba nema rješenja.
Kod $\bar{E}$ u (I) dobijemo 4 vrijednosti: najprije $1, -3$, a u dodatku $-1, 3$ (uočite da je $x^3 - 2x^2 - 3x = x(x + 1)(x - 3)$). Kako su to sve moguće vrijednosti za b_1 u (II), to je sve. Sad je $2^r = \frac{1 \cdot 4}{4} = 1$, pa je $r = 0$.