Uvod u aritmetiku eliptičkih krivulja

Točke konačnog reda. Lutz-Nagell teorem - 8.lekcija

Ako je E bilo koja abelova grupa (s aditivnim zapisom i neutralnim elementom O) i P njen element, onda za niz elemenata

$$P, 2P, 3P, ...$$

mogu nastupiti dvije mogućnosti.
Prva je da su u tom nizu svi elementi različiti. Tada kažemo da je P element **beskonačnog reda**. Uočite da je tada $< P >:= \{..., -2P, -P, O, P, 2P, ...\}$ beskonačna ciklička grupa generirana s P (onosno $-P$), koja je izomorfna grupi $\mathbf{Z}$ (jedan od izomorfizama preslikava P u 1; ima li još koji?).
Druga je da je $mP = O$ za neki $m \in \mathbf{N}$. Tada ako je m najmanji prirodni broj s tim svojstvom kažemo da je P (konačnog) reda m i tada je skup $< P >= \{O, P, 2P, ..., (m-1)P\}$ ciklička grupa m-tog reda (s generatorom P; što možete reći o drugim generatorima?), koja je izomorfna grupi $\mathbf{Z}/m\mathbf{Z}$ (koja se pak može realizirati kao skup $\{0, 1, 2, ..., (m-1)\}$ uz zbrajanje modulo m).
Lako se vidi da elementi kojima red dijeli m (tj. rješenja jednadžbe $mT = O$) čine podgrupu u E. Naime, ako je $mT = O$, onda je i $m(-T) = O$,i ako je $mT_1 = mT_2 = O$, onda je $m(T_1 + T_2) = O$.
Takodjer svi elementi konačnog reda čine podgrupu u E (torzijska podgrupa, oznaka E_{tors}).
Ako je E eliptička krivulja potrebna je dodatna napomena. Na primjer, ako gledamo eliptičke krivulje nad $\mathbf{C}$ i njihove točke nad $\mathbf{C}$, onda ima jedna točka 1. reda - to je O, vidjeli smo da ima 3 točke 2. reda, koje skupa s O čine grupu rješenja jednadžbe $2T = O$, lako se može pokazati da ima 8 točaka 3. reda, koje skupa s O čine grupu rješenja jednadžbe $3T = O$. Jednadžba $4T = O$ ima 16 rješenja: O, 3 točke 2. reda i 12 točaka 4. reda. Općenito, jednadžba $mT = O$ na eliptičkoj krivulji ima m^2 kompleksnih rješenja koje čine grupu izomorfnu $\mathbf{Z}/m\mathbf{Z} \oplus \mathbf{Z}/m\mathbf{Z}$ (direktna suma abelovih grupa).
Na primjer, ako je E zadana standardnom afinom jednadžbom

$$y^2 = x^3 + ax^2 + bx + c \tag{1}$$

gdje je $x^3+ax^2+bx+c = (x-e_1)(x-e_2)(x-e_3)$, onda su $O, (e_1, 0), (e_2, 0), (e_3, 0)$ rješenja jednadžbe $2T = O$. Uočite da je $(e_1, 0) + (e_2, 0) = (e_3, 0)$ i analogno za ostale mogućnosti, odakle se vidi da je ta grupa izomorfna direktnoj sumi grupa drugog reda. Slično, rješenja jednadžbe $3T = O$ su 9 fleksova krivulje itd. Isto vrijedi općenito u karakteristici 0 nad algebarski zatvorenim poljem, a uz neke izuzetke, i u svakoj karakteristici.

Podgrupa racionalnih točaka konačnog reda eliptičke krivulje nad Q.
Nas ovdje zanima **aritmetički**, tj. **diofantski** aspekt problema. Zato u (1) predpostavljamo da je E zadana nad $\mathbf{Q}$, tj. da su a, b, c, d iz (1) racionalni brojevi i da razmatramo samo točke krivulje definirane nad $\mathbf{Q}$, tj. iz $E(\mathbf{Q})$, tj. s racionalnim koordinatama. Tada opet **racionalna** rješenja jednadžbe

$$mT = O$$

čine podgrupu, samo ne mora biti m^2 racionalnih točaka (i u pravilu je tako).
Uvedimo ovakve oznake:
$E[m]$:= podgrupa svih točaka koje su rješenja jednadžbe $mT = O$.
$E[m](\mathbf{Q})$:= podgrupa svih točaka iz $E[m]$ definiranih nad $\mathbf{Q}$.
$E_{\mathrm{tors}}(\mathbf{Q})$:= podgrupa svih $\mathbf{Q}$-racionalnih točaka konačnog reda (torzijska podgrupa).

Primjer 1. (i) Neka je $E : y^2 = x^3 - x$. Tada je $E[2] = E[2](\mathbf{Q}) = \{O, (0,0), (1,0)(-1,0)\}$.
(ii) Neka je $E : y^2 = x^3 + x$. Tada je $E[2] = \{O, (0,0), (i,0)(-i,0)\}$ i $E[2](\mathbf{Q}) = \{O, (0,0)\}$.
Pokušajte u ovim primjerima odgovoriti na pitanje što je $E_{\mathrm{tors}}(\mathbf{Q})$. Je li ta grupa konačna ili beskonačna?

Prirodno pojednostavljenje - eliptičke krivulje definirane nad Z.
Za razmatranje racionalne torzije dovoljno je gledati eliptičke krivulje definirane nad $\mathbf{Z}$. Na primjer

$$E : y^2 = x^3 - \frac{3}{2}x^2 + \frac{11}{16}x - \frac{3}{32}$$

nakon množenja s 64 postaje

$$(8y)^2 = (4x)^3 - 6(4x)^2 + 11(4x) - 6$$

odnosno

$$E' : y'^2 = x'^3 - 6x'^2 + 11x' - 6.$$

Vidimo da je E' definirana nad $\mathbf{Z}$ i da je preslikavanje

$$\phi : E \to E'; \ (x, y) \mapsto (4x, 8y)$$

izomorfizam tih krivulja definiran nad $\mathbf{Q}$. Uočite da pri tom izomorfizmu
(i) $E(\mathbf{Q})$ prelazi u $E'(\mathbf{Q})$
(ii) $E[m](\mathbf{Q})$ prelazi u $E'[m](\mathbf{Q})$, za sve m.
(iii) $E(\mathbf{Q})_{tors}$ prelazi u $E'(\mathbf{Q})_{tors}$.

Tako nešto možemo napraviti općenito, a ne samo u ovom primjeru. Na primjer, ako jednadžbu

$$y^2 = x^3 + \frac{a}{d}x^2 + \frac{b}{d}x + \frac{c}{d}$$

pomnožimo s d^6, dobit ćemo

$$(d^3y)^2 = (d^2x)^3 + ad(d^2x)^2 + bd^3(d^2x) + cd^5$$

, pa je početna krivulja $\mathbf{Q}$-izomorfna krivulji

$$y'^2 = x'^3 + adx'^2 + bd^3x' + cd^5$$

(uz izomorfizam $(x, y) \mapsto (d^2x, d^3y)$).
Zato ćemo, kad nam zatreba smatrati da je Weierstrassov model eliptičke krivulje definiran nad $\mathbf{Z}$, tj. da su koeficijenti a, b, c iz (1) cijeli brojevi.

O torzijskim točkama eliptičke krivulje nad $\mathbf{Q}$ izreć ćemo nekoliko tvrdnja. Najgrublja od njih je sljedeća.

(I) Skup $\mathbf{Q}$-racionalnih točaka konačnog reda eliptičke krivulje nad $\mathbf{Q}$ je konačan.

Za jednu suptilniju tvrdnju potreban je cjelobrojni model.

(II) Neka je E eliptička krivulja s cjelobrojnim koeficijentima. Tada svaka $\mathbf{Q}$-racionalna točka konačnog reda ima cjelobrojne koordinate.

Napomenimo da ovo ne znači da je i svaka točka s cjelobrojnim koordinatama automatski torzijska. Medjutim, ako naidjemo na racionalnu necjelobrojnu točku (na cjelobrojnom W. modelu), onda znamo da je to točka beskonačnog reda.

Primjer 2. (i) Neka je $E : y^2 = x^3 + 3x$ i uočimo njenu točku $P(\frac{1}{4}, \frac{7}{8})$. Ta je točka, prema tvrdniji (II), beskonačnog reda.
(ii) Točka $Q(3,6)$ takodjer je na krivulji i ima cjelobrojne koordinata. Ona nije konačnog reda jer $2Q$ nema cjelobrojne koordinate (pokažite), pa $2Q$ nije konačnog reda (zato nije ni Q).

Još preciznija tvrdnja o torzijskim točkama je Lutz-Nagellov teorem iz 1937. odnosno 1935. godine (prema francuskoj matematičarki Elisabeth Lutz i norveškom matematičaru Trygve Nagell-u). Za tu tvrdnju podsjetimo na pojam diskriminante D polinoma $f(x) := x^3 + ax^2 + bx + c = (x - e_1)(x - e_2)(x - e_3)$, koja je definirana kao

$$D = (e_1 - e_2)^2(e_2 - e_3)^2(e_3 - e_1)^2$$

Izravnim računanjem dobije se

$$D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$$

(uočite posljednja dva pribrojnika - već smo na njih nailazili).

Lutz-Nagell-ov teorem. Neka je E s cjelobrojnim koeficijentima i neka je D diskriminanta od E. Tada svaka $\mathbf{Q}$-racionalna točka konačnog reda ima cjelobrojne koordinate. Ako je $P(x, y)$ takva afina točka, onda je ili $y = 0$ ili je $y^2|D$.

Uočite da je tvrdnja (II) sadržana u teoremu, a da je drugi dio teorema konstruktibilna varijanta tvrdnje (I). Zato je taj teorem dobra osnova algoritma za odredjivanje torzijskih točaka.

Primjer 3. Neka je $E : y^2 = x^3 - x^2 + x$. Tada je $D = -3$ pa su jedine $\mathbf{Q}$-racionalne torzijske točke $O, (0,0)$ i možda neke od onih (x, y) za koje je $y = \pm 1$ ili ± 3. Za $y = \pm 1$ dobijemo $x = 1$ i lako provjerimo da za $P(1,1)$ vrijedi $2P = (0,0)$ pa su $(1, \pm 1)$ takodjer torzijske. Za $y \pm 3$ dolazimo do jednadžbe $x^3 - x^2 + x - 9 = 0$ koja nema cjelobrojnih rješenja. Zato je $E(\mathbf{Q})_{tors} = \{O, (0,0), (1, \pm 1)\}$. Pokažite da je ta grupa izomorfna $\mathbf{Z}/4\mathbf{Z}$.

Zadatak. Odredite racionalne torzijske točke i torzijsku podgrupu krivulja zadanih afinim jednadžbama:

(i) $y^2 = x^3 + 2$,
(ii) $y^2 = x^3 + x$,
(iii) $y^2 = x^3 + 4$,
(iv) $y^2 = x^3 + 4x$,
(v) $y^2 = x^3 - x^2 + \frac{1}{4}$,
(vi) $y^2 = x^3 + 1$,
(vii) $y^2 = x^3 + \frac{9}{4}x^2 - x + 1$,
(viii) $y^2 = x^3 - x$,
(ix) $y^2 = x^3 + 5x^2 + 4x$,
(x) $y^2 = x^3 + 337x^2 + 20736x$,

Iako izgleda da je s L-N teoremom problem torzije riješen, treba napomenuti da ja za velike D problem faktorizacije često vrlo mukotrpan ili praktično nemoguć (to je problem subeksponencijalne, a ne polinomijalne složenosti). Zato se za odredjivanje torzije (do na izomorfizam) često koristi jedan kriterij koji ćemo upoznati kad budemo obradjivali eliptičke krivulje nad konačnim poljem i redukciju eliptičke krivulje. S duge strane, iz L-N teorema, informaciju o torziji dobivamo samo za konkretnu krivulju, a malo toga možemo reći za sve krivulje (ili familije krivulja). Na primjer za familiju krivulja

$$y^2 = x^3 - n^2x,$$

za $n \in \mathbf{N}$ (koja je povezano s problemom kongruentnih brojeva - o tome ćemo više poslije), dobijemo $D = 4n^6$, odakle nije lako izvesti činjenicu da se za sve ove krivulje torzijska podgrupa poklapa s podgrupom $\{O, (0,0), (\pm n, 0)\}$.

Problem mogućih racionalnih torzija (za sve eliptičke krivulje nad $\mathbf{Q}$) riješio je Mazur (1977-1978.).

Mazurov teorem. Neka je P racionalna točka m-tog reda na eliptičkoj krivulji E nad $\mathbf{Q}$. Tada je

$$1 \leq m \leq 10, \text{ ili } m = 12.$$

Moguće torzijske podgrupe su
(I) cikličke grupe reda m za $1 \leq m \leq 10$, ili $m = 12$.
(II) direktni produkt cikličkih grupa reda 2 i reda $2n$ za $1 \leq n \leq 4$.

O svim **Q**-racionalnim točkama govori Mordellov teorem iz 1922. godine. Jednostavnim riječima on tvrdi da se sve racionalne točke mogu povlačenjem tangenata i sekanata dobiti iz konačnog skupa takvih točaka (generatora).

Mordellov teorem. Neka je E eliptička krivulja nad $\mathbf{Q}$. Tada je $E(\mathbf{Q})$ konačno generirana abelova grupa.

Lutz-Nagellov teorem dokazat ćemo u sljedećoj lekciji. Taj je dokaz složen, ali elementaran. U nastavku ćemo dokazati i Mordellov teorem (uz neka ograničenja). Taj je dokaz relativno elementaran, ali još uvijek nije pronadjen algoritam za odredjivanje generatora (iako postoje vrlo uspješne metode). Dokaz Mazurova teorema je vrlo složen i neelementaran (potrebna su duboka znanja iz algebarske geometrije i algebarske teorije brojeva)i nećemo ga dokazivati.