Uvod u aritmetiku eliptičkih krivulja

Slabi Mordell-ov teorem - 11.lekcija

Za dokaz Mordellova teorema preostala nam je tvrdnja (IV), koja se katkad naziva **slabi mordellov teorem.** To je najteži i najvažniji dio teorema. Dakle, treba dokazati:
(IV) Podgrupa $2E(\mathbf{Q})$ ima konačan indeks u grupi $E(\mathbf{Q})$.
Radi jednostavnosti, grupu $E(\mathbf{Q})$ označit ćemo kao Γ. Dakle, treba dokazati da je $\Gamma/2\Gamma$ konačna grupa. Iako bi se dokaz mogao provesti u punoj općenitosti (medjutim, tada bi morali prijeći na razmatranje u poljima algebarskih brojeva), najjednostavniji je dokaz ako su sva tri korijena e_1, e_2, e_3 polinoma f cijeli brojevi. Mi tu nećemo napraviti takvu restrikciju, već ćemo predpostaviti samo da polinom f ima bar jedan racionalan korijen (pa onda i cjelobrojan). Nakon jednostavne zamjene varijabla možemo predpostaviti da je taj korijen jednak 0, pa možemo smatrati da je

$$E : y^2 = x^3 + ax^2 + bx.$$

Uočite da je tada $T(0,0)$ racionalna točka na E i da je $2T = O$. Takodjer, tu je $D = b^2(a^2 - 4b)$ pa treba biti $b \neq 0$ i $a^2 \neq 4b$ (što se vidi i izravno).

Primjer. Neka je $E : y^2 = x^3 - x^2 + x - 1$. Tu je $x = 1$ racionalan korijen od f. Razvojem po $x - 1$ dobijemo $y^2 = (x-1)^3 + 2(x-1)^2 + 2(x-1)$, pa je E izomorfna nad $\mathbf{Q}$ eliptičkoj krivulji $E' : y^2 = x^3 + 2x^2 + 2x$, koja je gornjeg oblika.

Priprema za slabi mordell-ov teorem, homomorfizmi ϕ i ψ.
Put za dokazivanje da je $\Gamma/2\Gamma$ konačna ide posredno preko jedne druge eliptičke krivulje koja je tijesno povezana s E. To je krivulja

$$\bar{E} : y^2 = x^3 + \bar{a}x^2 + \bar{b}x,$$

gdje je $\bar{a} := -2a$ i $\bar{b} = a^2 - 4b$ (uočite da je $\bar{E}$ zaista eliptička krivulja).
Te dvije krivulje su izogene, tj. postoji netrivijalni homomorfizam medju njima. O tome govori:
Teorem 1. (i) Racionalno preslikavanje $\phi : E \to \bar{E}$ zadano lokalno kao

$$\phi(x,y) := (\frac{y^2}{x^2}, \frac{y(x^2-b)}{x^2}),\ za\ (x,y) \neq (0,0)$$

proširuje se do homomorfizma eliptičkih krivulja sa svojstvom $\phi(0,0) = \bar{O}$.
(ii) Racionalno preslikavanje $\psi : \bar{E} \to E$ zadano lokalno kao

$$\psi(\bar{x}, \bar{y}) := (\frac{\bar{y}^2}{4\bar{x}^2} \frac{\bar{y}(\bar{x}^2 - \bar{b})}{8\bar{x}^2}),\ za\ (\bar{x}, \bar{y}) \neq (0,0)$$

proširuje se do homomorfizma eliptičkih krivulja sa svojstvom $\psi(0,0) = O$.
(iii) $(\psi \circ \phi)(P) = 2P$ za sve $P \in E$ i $(\phi \circ \psi)(\bar{P}) = 2\bar{P}$, za sve $\bar{P} \in \bar{E}$.
Dokaz. Da su ϕ i ψ dobro definirani dokazuje se izravno (a može se, kao i za ostale detalje, pogledati [S-T, str. 76-82]). Da se te funkcije proširuju do morfizma za koje je $\phi(O) = \bar{O}$ i $\psi(\bar{O}) = O$ vidjeli smo u ranijem primjeru. Tada možemo primijeniti opći rezultat, dovoljno je napomenuti da su to racionalna preslikavanja koja neutralni element preslikavaju u neutralni, pa su onda to homomorfizmi grupa, a može se lako sve to i izravno dokazati, samo treba strpljenja (vidi [S-T]). Jednako tako, izravno se dokazuje da je kompozicija tih preslikavanja množenje s 2.

Djelovanje od ϕ i ψ na racionalne točke.
Kao i prije, grupu racionalnih točaka na E označimo kao Γ, a analogno tome pripadnu grupu na $\bar{E}$ označimo kao $\bar{\Gamma}$. Na svim točkama i ϕ i ψ su surjekcije, medjutim, općenito to nije istina za racionalne točke. Naravno, ta su preslikavanja definirana nad **Q** pa racionalne točke preslikavaju u racionalne.
Zato je
(a) $\phi(\Gamma)$ je podgrupa od $\bar{\Gamma}$, a mi želimo pokazati da je konačna indeksa.
(b) $\psi(\bar{\Gamma})$ je podgrupa od Γ, a mi želimo pokazati da je konačna indeksa (podsjetimo da je indeks $(A : B)$ podgrupe B abelove grupe A broj elemenata u kvocijentnoj grupi A/B; za nekomutativne je grupe slično, ali to nas tu ne zanima).
Zašto je važno da su gornji indeksi konačni?
Kad bismo to znali, odmah bi $\Gamma/2\Gamma$ bila konačna grupa. Naime, indeksi se ponašaju poput dvostrukih razlomaka (uz neke uvjete), pa je (sjetimo se da je $2\Gamma = \psi(\phi(\Gamma)))$

$$(\Gamma : 2\Gamma) = (\Gamma : \psi(\bar{\Gamma})) \cdot (\psi(\bar{\Gamma}) : \psi(\phi(\Gamma)) \leq (\Gamma : \psi(\bar{\Gamma})) \cdot (\bar{\Gamma} : \phi(\Gamma)) < \infty$$

(izravan dokaz u [S-T], lema na str. 87.).
Opis grupa $\phi(\Gamma)$ i $\psi(\bar{\Gamma})$.
Taj je opis načelno zaista jednostavan. Naime, za $(\bar{x}, \bar{y}) \in \bar{\Gamma}$ različit od $(0,0)$ vrijedi sljedeće:

$(\bar{x}, \bar{y}) \in \phi(\Gamma)$ akko $\bar{x} = w^2$ za neki racionalni w.
Tome treba dodati da je $(0,0) \in \phi(\Gamma)$ akko $\bar{b} = a^2 - 4b$ kvadrat prirodna broja.
Za $\psi(\bar{\Gamma})$ vrijedi potpuno analogna tvrdnja. Naime, ψ se definira potpuno analogno kao ϕ samo što treba komponirati s izomorfizmom $(x, y) \mapsto (\frac{x}{4}, \frac{y}{8})$.
Dokaz tvrdnje. Jedan je smjer očit, zato predpostavimo da je $\bar{x} = w^2$ za racionalan w i $\bar{x} \neq 0$. Tražimo $(x, y) \in \Gamma$ tako da bude $\phi(x, y) = (\bar{x}, \bar{y})$. Kako mora biti $\frac{y^2}{x^2} = w^2$, vidimo da tražimo točku oblika $(x, \pm wx)$. Da bi ta točka bila u Γ mora biti $w^2x^2 = x^3 + ax^2 + bx$, a kako je $x \neq 0$, dobijemo $x^2 + (a - w^2)x + b = 0$, odakle je $x = w^2 - a \pm \frac{\bar{y}}{w}$ (iskoristite jednadžbu od $\bar{E}$).
Sad uočimo točke iz Γ:
(x_1, wx_1) gdje je $2x_1 = w^2 - a + \frac{\bar{y}}{w}$ i
(x_2, wx_2) gdje je $2x_2 = w^2 - a - \frac{\bar{y}}{w}$.
Još treba pokazati da se te točke preslikavaju u $(\bar{x}, \bar{y})$, a dovoljno je za prvu. Očito je $\frac{y_1^2}{x_1^2} = w^2$, dok je $\frac{y_1(x_1^2 - b)}{{x_1}^2} = \frac{wx_1(x_1^2 - x_1x_2)}{{x_1}^2} = w(x_1 - x_2) = \bar{y}$.

Dokaz da je $(\Gamma : \psi(\bar{\Gamma}))$ i $(\bar{\Gamma} : \phi(\Gamma))$ konačno.
Vidjeli smo da te činjenice dokazuju slabi mordellov teorem. Kako su one simetrične, dovoljno je pokazati jednu od njih, na primjer prvu.
Odgovor će biti vrlo jednostavan:$(\Gamma : \psi(\bar{\Gamma})) \leq 2^{k+1}$, gdje je k broj prostih djelitelja od b. Za drugi kvocijent vrijedi analogno, samo s $\bar{b}$ umjesto b.
Za dokaz najprije podsjetimo na grupu $\mathbf{Q}^*$ racionalnih brojeva bez nule i njenu podgrupu $\mathbf{Q}^{*\mathbf{2}}$ koja se sastoji od kvadrata racionalnih bojeva koji nisu nula, te na kvocijentnu grupu $\mathbf{Q}^*/\mathbf{Q}^{*\mathbf{2}}$ kojoj su reprezentanti $-1, 1$ i prirodni brojevi koji u rastavu nemaju viših potencija. Neka tilda označava klase u $\mathbf{Q}^*/\mathbf{Q}^{*2}$. Tada vrijedi $(\tilde{t})^2 = \tilde{1}$ za sve $t \in \mathbf{Q}$.
Definirajmo preslikavanje

$$\alpha : \Gamma \to \mathbf{Q}^*/\mathbf{Q}^{*\mathbf{2}}$$

ovako

$$\alpha(O) = \tilde{1},\ \alpha(0,0) = \tilde{b},\ \alpha(x, y) = \tilde{x}\ za\ x \neq 0.$$

Mi želimo pokazati da je α homomorfizam grupa i dokazati da je jezgra tog homomofizma upravo $\psi(\bar{\Gamma})$. To će biti presudno za dokaz. Napomenimo da za dokaz da je α homomorfizam ne možemo koristiti rezultate algebarske geometrije, jer to nije preslikavanje medju algebarsko-geometrijskim objektima, već to moramo pokazati izravno. Takodjer, napomenimo da je u $\mathbf{Q}^*/\mathbf{Q}^{*2}$)

grupni zakon multiplikativan. Idemo redom.

(1) α je homomorfizam grupa.

Naime $\alpha(-P) = \alpha(x, -y) = \tilde{x} = (\tilde{\frac{1}{x}}) = \alpha(P)^{-1}$. Za preostale dvije točke je očito.

Ostaje pokazati, ako je $P_1 \oplus P_2 \oplus P_3 = O$ onda je $\alpha(P_1)\alpha(P_1)\alpha(P_1) = \tilde{1}$.

To slijedi izravno iz jednadžbe za x koordinate triju točaka presjeka pravca $y = \lambda x + \mu$ i E:

$$x^3 + (a - \lambda^2)x^2 + (b - 2\lambda\mu)x - \mu^2 = 0.$$

Sad iz $x_1x_2x_3 = \mu^2$ izravno slijedi naša tvrdnja za afine točke različite od $(0, 0)$. Ostali se slučajevi lako provjere.

(2). Jezgra od α je $\psi(\bar{\Gamma})$.

To je očito iz karakterizacije $\psi(\bar{\Gamma})$ - sastoji se od svih (x, y) takvih da je x kvadrat racionalna broja, itd.

To govori da α inducira ulaganje $\Gamma/\psi(\bar{\Gamma}) \hookrightarrow \mathbf{Q}^*/\mathbf{Q}^{*2}$.

Ocjena slike od α.

Nećemo odgovoriti točno što je slika od α već samo približno, ali i to će biti dovoljno. Neka su $p_1, p_2, ..., p_k$ prosti brojevi koji dijele b. Tada je $\alpha(\Gamma)$ podgrupa podgrupe od $\mathbf{Q}^*/\mathbf{Q}^{*2}$ koja se sastoji od klasa elemenata oblika $\pm p_1^{\epsilon_1} \cdot p_2^{\epsilon_2} \cdot ... \cdot p_k^{\epsilon_k}$ gdje su ϵ_i jednaki 1 ili 0. Kako ta podgrupa ima 2^{k+1} elemenata, vrijedi $(\Gamma : \psi(\bar{\Gamma})) \leq 2^{k+1}$.

Da bismo ocijenili sliku od α najprije razmotrimo kako izgledaju $(x, y) = (\frac{m}{e^2}, \frac{n}{e^3}) \in \Gamma$, gdje su prikazi maksimalno skraćeni.

Stavljajući to u jednadžbu od E dobijemo (za $(x, y) \neq (0, 0)$)

$$n^2 = m(m^2 + ame^2 + be^4).$$

Zapišimo $m = \pm m'^2 \cdot q_1 \cdot q_2 \cdot ... \cdot q_s$, gdje su q_j različiti prosti brojevi. Tada $q_1 \cdot q_2 \cdot ... \cdot q_s | (m^2 + ame^2 + be^4)$ pa $q_1 \cdot q_2 \cdot ... \cdot q_s | b$ (jer su m i e relativno prosti).

Zato su q_j djelitelji od b pa su neki p_i. To znači da je

$$\alpha(x, y) = \pm \bar{p_1}^{\epsilon_1} \cdot \bar{p_2}^{\epsilon_2} \cdot ... \cdot \bar{p_k}^{\epsilon_k}$$

kako smo i tvrdili.