Uvod u aritmetiku eliptičkih krivulja

Mordell-ov teorem - 10.lekcija

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

Primjer 1. (i) Grupa $\mathbf{Z}$ je konačno generirana. Točnije, ima jedan generator (broj 1 ili -1); kažemo da ima rang 1 (to je slobodna abelova grupa ranga 1).
(ii) Grupa $\mathbf{Z}[i] := \{a + bi : a, b \in \mathbf{Z}\}$ je konačno generirana, točnije to je slobodna abelova grupa ranga 2 (generatori su, na primjer, $1, i$).
(iii) Skup svih cjelobrojnih rješenja pellove jednadžbe $x^2 - 2y^2 = 1$ je abelova grupa G s obzirom na operaciju $*$ definiranu kao

$$(x_1, y_1) * (x_2, y_2) = (x_1x_2 + 2y_1y_2, x_1y_2 + x_2y_1).$$

Uočite da je $e := (1, 0)$ neutralni element i $(x, y)^{-1} = (x, -y)$. Ta je grupa konačno generirana ranga 1, ali nije slobodna, jer ima torzijski element $\epsilon := (-1, 0)$. Rješenje $t := (3, 2)$ ima beskonačan red i vrijedi

$$G = \{e, \epsilon\} \times < t >$$

gdje je $< t >$ ciklička grupa generirana s t (to je direktni produkt ili suma, svejedno, podgrupa), tj. kao apstraktna grupa G je izomorfna grupi $\mathbf{Z} \oplus \mathbf{Z}_2$.
(iv) Abelova grupa $(\mathbf{Q}, +)$ nije konačno generirana.
(v) Abelova grupa $(\mathbf{Q}^*, \cdot)$ nije konačno generirana.
(vi) Abelova grupa $\mathbf{Q}^*/\mathbf{Q}^{*2}$ nije konačno generirana - ta je grupa kao skup u prirodnoj bijekciji sa skupom svih prirodnih kvadratno slobodnih brojeva kojima je dodan broj -1, a skup generatora je skup svih prostih brojeva skupa s -1 (dokažite).

Visina točke eliptičke krivulje.
Tipičan dokaz Mordellova teorema koristi pojam visine (koji izvorno potječe od Fermata). Za racionalan broj

$$x = \frac{m}{n}$$

gdje je gornji zapis maksimalno skračen, definiramo visinu kao

$$H(x) = H(\frac{m}{n}) := \max\{|m|, |n|\}.$$

Ako je $P(x, y)$ afina racionalna točka na eliptičkoj krivulji

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

definiranoj nad $\mathbf{Q}$, onda visinu od P definiramo kao visinu njene prve koordinate, tj.

$$H(P) := H(x).$$

Često se umjesto H koristi logaritamska visina h definirana kao

$$h(P) := logH(P)$$

gdje je log bilo koji logaritam s bazom većom od 1(a u pravilu smatramo da je prirodni).
Još se definira $H(O) = 1$, tj. $h(O) = 0$.

Kako ćemo h primjenjivati na eliptičku krivulju, bit će potrebno proučiti kako se visina ponaša prema operaciji zbrajanja. Radi toga podsjetimo na formule za x koordinatu zbroja. Neka je $P_0(x_0, y_0)$, $P(x, y)$ i $(P + P_0)(w, \omega)$. Tada je, za $P \neq P_0$,

$$w = -x - x_0 - a + \frac{(y - y_0)^2}{(x - x_0)^2} = \frac{Ay + Bx^2 + Cx + D}{Ex^2 + Fx + G} \tag{1}$$

gdje smo najprije sveli na zajednički nazivnik, potom $y^2 - x^3$ u brojniku zamijenili polinomom 2. stupnja u x i, konačno, uredili da koeficijenti $A, B, ..., G$ budu cijeli.
Slično, ako je $2P(u, v)$, onda je, kako smo vidjeli

$$u = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c} \tag{2}$$

Sad se odmah vidi da je za točke P dovoljno velike visine vrijedi $h(y) \approx \frac{3}{2}h(x),\ h(P + P_0) \approx 2h(P),\ h(2P) \approx 4h(P)$. (jer se kvadriranjem racionalna broja njegova visina udvostručuje itd.). Za dokaz Mordellova teorema te ćemo činjenice morati nešto preciznije zapisati ovako:

(I) Za svaki realan broj M je $\{P \in E(\mathbf{Q}) : h(P) \leq M\}$ je konačan.
(II) Za svaku racionalnu točku P_0 postoji konstanta k_0 tako da za svaku racionalnu točku P vrijedi

$$h(P + P_0) \leq 2h(P) + k_0.$$

(III) Postoji konstanta k tako da za svaku racionalnu točku P vrijedi

$$h(2P) \geq 4h(P) - k.$$

Tim trima svojstvima visine treba dodati još jedno, čisto algebarsko
(IV) Podgrupa $2E(\mathbf{Q})$ ima konačan indeks u grupi $E(\mathbf{Q})$, tj. $E(\mathbf{Q})/\mathbf{2E}(\mathbf{Q})$ je konačna grupa.
Pokazat ćemo kako se iz ova četiri svojstva izvodi Mordellov teorem. Prije toga napomenimo da je samo (I) tvrdnja trivijalna (jer uz zadane uvjete ima samo konačno mnogo mogućnosti za brojnike i nazivnike od $x := x(P)$). Medjutim ostale su tvrdnje netrivijalne, (II) i (III) su elementarne, a (IV) vrlo zaguljena. Taj je zahtjev vrlo jak. Na primjer $\mathbf{Q} = \mathbf{2Q}$ pa je kvocijent poput onog iz (IV) trivijalan, tj. jednočlan. Ipak je $(\mathbf{Q}, +)$ daleko od konačne generiranosti. S druge strane, primjer (vi) pokazuje da takav kvocijent ne mora biti konačan.
Sad trenutno možemo zaboraviti eliptičke krivulje i koncentrirati se na bilo koju abelovu grupu Γ.

Teorem 1. Neka je Γ abelova grupa i $h : \Gamma \to [0, \infty >$ funkcija visine koja zadovoljava svojstva (I), (II) i (III), i neka Γ zadovoljava i svojstvo (IV), tj. neka je $\Gamma/2\Gamma$ konačna grupa. Tada je Γ konačno generirana.
Dokaz. Iz svojstva (IV) slijedi da je skup reprezentanata iz Γ s obzirom na 2Γ konačan, recimo da je to skup

$$A = \{Q_1, Q_2, ..., Q_n\}.$$

To znači da je

$$(Q_1 + 2\Gamma) \cup (Q_2 + 2\Gamma) \cup ... \cup (Q_n + 2\Gamma) = \Gamma. \tag{3}$$

Neka su $k_i,\ i = 1, 2, ..., n$ konstante koje postoje prema (II) (za $-Q_i$ umjesto P_0), i neka je k' najveća od tih konstanata. Definirajmo skup B (koji je konačan prema (I)) kao:

$$B := \{R \in \Gamma : h(R) \leq k + k'\}.$$

Tvrdimo: skup $A \cup B$ generira Γ, posebice Γ je konačno generirana.
Da to pokažemo, neka je $P \in \Gamma$ bilo koji element. Tada, prema (3), postoji $Q_{i_1} \in A$ tako da je $P - Q_{i_1} \in 2\Gamma$, što se moze zapisati i kao
$P - Q_{i_1} = 2P_1$, za neki $P_1 \in \Gamma$. Sad možemo nastaviti s P_1 umjesto P itd.
$P_1 - Q_{i_2} = 2P_2$
$P_2 - Q_{i_3} = 2P_3$
. . .
$P_{m-1} - Q_{i_m} = 2P_m$
Ako drugu jednakost pomnožimo s 2, treću s 4, četvrtu s 8 itd., pa zbrojimo, dobijemo

$$P = Q_{i_1} + 2Q_{i_2} + 4Q_{i_3} + ... + 2^{m-1}Q_{i_m} + 2^m P_m \tag{4}$$

Tvrdimo da bez obzira na P, ako je m dovoljno velik onda je $P_m \in B$.
Za to uočimo neki P_j i vidimo (prema (II) i (III) i definiciji od k_i i k':
$4h(P_j) \leq h(2P_j) + k = h(P_{j-1} - Q_{i_j}) + k \leq 2h(P_{j-1}) + k + k'$, pa je $h(P_j) \leq \frac{3}{4}h(P_{j-1}) - \frac{1}{4}(h(P_{j-1} - (k + k'))$.
Sad vidimo, u nizu $P_1, P_2, P_3, ...$, dok god je $h(P_i) \geq k + k'$, sljedeći element ima visinu bar 75 posto manju od $h(P_i)$, pa jednom visina mora pasti ispod $k + k'$. Dokaz je gotov.

Dakle, da bismo dokazali Mordell-ov teorem, **jedino** treba dokazati tvrdnje (II), (III) i (IV).

Skica dokaza tvrdnje (II). Podsjetimo se najprije da u (1) možemo staviti $x = \frac{m}{e^2}$, $y = \frac{n}{e^3}$ i da su ti prikazi maksimalno skraćeni, pa je $|m| \leq H(P)$ i $e^2 \leq H(P)$. Sad (1)postaje

$$w = \frac{Ane + Bm^2 + Cme^2 + De^4}{Em^2 + Fme^2 + Ge^4}.$$

Takodjer tu zamjenu možemo staviti u jednadžbu krivulje, pa dobijemo

$$n^2 = m^3 + ae^2m^2 + be^4m + ce^6.$$

Sad izravnim uvrštavanjem dobijemo $|n| \leq KH(P)^{\frac{3}{2}}$, gdje je $K := \sqrt{1 + |a| + |b| + |c|}$, a nakon toga i
$|Ane + Bm^2 + Cme^2 + De^4| \leq (|AK| + |B| + |C| + |D|)H(P)^2$ i $|Em^2 + Fme^2 + Ge^4| \leq (|E| + |F| + |G|)H(P)^2$.
Zato je $H(P + P_0) := H(w) \leq K_0 H(P)^2$, gdje je K_0 veća od konstanta na desnim stranama (uočite da nam tu nije bilo važno što brojnik i nazivnik od w možda nisu maksimalno skraćeni). Tako smo, nakon logaritmiranja,

dokazali (II) i dobili ocjenu za $k_0 := logK_0$.

Skica dokaza tvrdnje (III).
Tu gledamo (2)i stavljamo $x = \frac{m}{n}$ gdje je taj prikaz maksimalno skraćen. Zato je

$$u = \frac{\Phi(m,n)}{\Psi(m,n)} := \frac{m^4 - 2bm^2n^2 - 8cmn^3 + (b^2 - 4ac)n^4}{4m^3n + 4am^2n^2 + 4bmn^3 + 4cn^4}.$$

Za razliku od (II), sad nam je važno imaju li $\Phi(m,n)$ i $\Psi(m,n)$ zajedničke faktore (jer želimo dobiti ocjenu oblika $H(u) \geq ...$). Tvrdimo da postoji prirodni broj R tako da zajednička mjera od $\Phi(m,n)$ i $\Psi(m,n)$ dijeli R, bez obzira o kojima m, n je riječ (tj. da takvih mjera ima konačno mnogo pa za R možemo staviti njihov višekratnik). Za tren predpostavimo da je tako i sjetimo se da je $H(P) = \max\{|m|, |n|\}$. Tada je
$H(2P) := H(u) \geq \frac{1}{R}\max\{|\Phi(m,n)|, |\Psi(m,n)|\} \geq \frac{1}{2R}(|\Phi(m,n)| + |\Psi(m,n)|)$
$\geq \frac{1}{2R}H(P)^4 \frac{|\Phi(m,n)|+|\Psi(m,n)|}{\max\{|m|^4,|n|^4\}} = \frac{1}{2R}H(P)^4 \frac{|x^4-2bx^2-8cx+b^2-4ac|+|4x^3+4ax^2+4bx+4c|}{\max\{|x|^4,1\}}$
$\geq \frac{C}{2R}H(P)^4$ (pogledajte odgovarajuće mjesto u [S-T]).
Sad se rezultat ostvaruje logaritmiranjem.
Da bi dokaz završili potrebno je dokazati tvrdnju o broju R. Već smo u dokazu Lutz-Nagell-ova teorema (9. lekcija formula (1)) vidjeli da brojnik $g(x)$ i nazivnik $4f(x)$ od (2) generiraju diskriminantu, naime da postoje polinomi h_1, h_2 s cjelobrojnim koeficijentima (stupnja 3 odnosno 2) tako da bude

$$h_1(x)f(x) + h_2(x)g(x) = D \tag{5}$$

(za naše potrebe dovoljno je bilo znati da su f i g relativno prosti, ali iskoristimo ovo od prije). Sad vidimo, ako $d|\Phi(m,n)$ i $d|\Psi(m,n)$, onda $d|4Dn^7$. Medjutim, ako $d|\Phi(m,n)$, onda $d|4n^5\Phi(m,n)$, pa $d|4m^4n^5$, a kako su m, n relativno prosti, sad $d|4Dn^5$. Daljnjim ponavljanjem dobit ćemo, konačno da $d|4D$. Znači, možemo uzeti $R = 4D$.