Uvod u aritmetiku eliptičkih krivulja

Eksplicitna formula za rang - kvazialgoritam 12.lekcija

Napomenimo da smo u posljednje dvije lekcije dokazali da je grupa racionalnih točaka $\Gamma := E(\mathbf{Q})$ konačno generirana. Istina, potpun dokaz smo proveli samo za eliptičke krivulje $\mathbf{Q}$-izomorfne eliptičkim krivuljama

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

iako sve vrijedi općenito (štoviše, analogna tvrdnja vrijedi za svako polje algebarskih brojeva konačna stupnja nad $\mathbf{Q}$ - to se zove Mordell-Weilov teorem; takodjer, analogno vrijedi za višedimenzionalne analogone eliptičkih krivulja - za jakobijane algebarskih krivulja i općenito, za abelove mnogostrukosti).
U dokazu smo koristili visine i ocjenu za broj elemenata u $\Gamma/2\Gamma$. Sad ćemo pokazati da možemo zaboraviti na visine (one su svoju ulogu odigrale) i koncentrirati se samo na kvocijent $\Gamma/2\Gamma$.
Dogovor. Od sad ćemo operaciju zbrajanja na eliptičkoj krivulji označavati jednostavno znakom $+$, a znak $\oplus$ koristit ćemo na standardan način, kao znak za **direktnu sumu**.

Kao prvi korak iskoristimo općepoznatu činjenicu da je svaka konačno generirana abelova grupa izomorfna umnošku slobodne abelove grupe ranga r (direktna suma r kopija grupe cijelih brojeva) i torzijske podgrupe. Za nas to znači:

$$\Gamma \cong \mathbf{Z}^r \oplus \mathbf{Z}/p_1^{n_1}\mathbf{Z} \oplus ... \oplus \mathbf{Z}/p_k^{n_k}\mathbf{Z} \tag{1}$$

gdje je r jednoznačno definiran i zove se **rang** od Γ, a p_j su (ne nužno različiti) prosti brojevi.

Primjer. (i) Neka je $E : y^2 = x^3 - 5x$ i $\Gamma := E(\mathbf{Q})$ njena grupa $\mathbf{Q}$-racionalnih točaka (**Mordell-Weilova grupa**). Pokazat ćemo da je $r = 1$. Takodjer, uz pomoć Lutz-Nagell-ova teorema dobije se da je torzijska podgrupa drugog reda. Zato je $\Gamma \cong \mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$.
Malo podrobnija analiza pokazuje da je Γ generirana točkom $P(-1, 2)$ beskonačna reda i točkom $T(0, 0)$ reda 2. Zato je $\Gamma = \{mP + nT\}$ gdje su $m \in \mathbf{Z}$ i $n = 0$ *ili* 1 jednoznačni.
Uočite razliku izmedju izomorfizma i jednakosti.

(ii) Neka je $E : y^2 = x^3 - x$. Pokazat ćemo da je $r = 0$, a već smo vidjeli da se torzijska podgrupa sastoji samo od točaka 2 reda, tj. $\Gamma_{\text{tors}} = \{O, (0,0), (1,0), (-1,0)\}$. Te su točke organizirane u grupu četvrtog reda izomorfnu direktnoj sumi grupa 2. reda, tj. $\Gamma[2] \cong \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$.

Općenito, za svaku eliptičku krivulju nad $\mathbf{Q}$, grupa racionalnih točaka drugog reda $\Gamma[2]$ ili je trivijalna ili drugog reda ili direktna suma grupa 2. reda. To znači da se u (1) u torzijskom dijelu broj 2 ne pojavljuje, pojavljuje se jednom ili dva puta. Iz Mazurova teorema lako možemo izvesti koji se prosti brojevi i s kojim eksponentima mogu pojavljivati u (1), medjutim to nam nije potrebno.
$\Gamma[2]$ možemo općenito opisati, za grupe iz (1), a ne nužno samo one koje dolaze od eliptičkih krivulja. Naime za $p \neq 2$ množenje s 2 u abelovoj grupi neparnog reda je izomorfizam, a u cikličkoj grupi koja ima red potenciju broja 2 to je homomorfizam s dvočlanom jezgrom, izomorfnom dakle s $\mathbf{Z}/2\mathbf{Z}$. Zato je, za grupe (1),

$$\Gamma[2] \cong (\mathbf{Z}/2\mathbf{Z})^s$$

gdje je s broj indeksa j u (1) za koje je $p_j = 2$.

Iz (1) slijedi izravno (uočite razliku izmedju 2Γ i $\Gamma[2]$)

$$2\Gamma \cong 2\mathbf{Z}^r \oplus 2(\mathbf{Z}/p_1^{n_1}\mathbf{Z}) \oplus ... \oplus 2(\mathbf{Z}/p_k^{n_k}\mathbf{Z}) \tag{2}$$

Zato je

$$\Gamma/2\Gamma \cong (\mathbf{Z}/2\mathbf{Z})^r \oplus (\mathbf{Z}/p_1^{n_1}\mathbf{Z}/2(\mathbf{Z}/p_1^{n_1}\mathbf{Z})) \oplus ... \oplus (\mathbf{Z}/p_k^{n_k}\mathbf{Z}/2(\mathbf{Z}/p_k^{n_k}\mathbf{Z})). \tag{3}$$

Izravno iz definicije se vidi da je $\mathbf{Z}/p_j^{n_j}\mathbf{Z}/2(\mathbf{Z}/p_j^{n_j}\mathbf{Z})$ trivijalna grupa osim u slučaju kad je $p_j = 2$, tada je ta grupa izomorfna cikličkoj grupi 2. reda $\mathbf{Z}/2\mathbf{Z}$ (argument smo već rekli).
Sad dobivamo važnu formulu

$$(\Gamma : 2\Gamma) = 2^r \cdot 2^s$$

gdje je, opet, s broj indeksa j za koje je $p_j = 2$.
Zato vrijedi

$$(\Gamma : 2\Gamma) = 2^r \cdot |\Gamma[2]| \tag{4}$$

To je već dosta dobra eksplicitna formula za rang Kako smo vidjeli gore, s općenito može biti $0, 1$ ili 2, pa $|\Gamma[2]|$ može biti $1, 2$ ili 4. Medjutim ako se ograničimo samo na krivulje

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

onda je $|\Gamma[2]| = 2$ ako $a^2 - 4b$ nije kvadrat, a $|\Gamma[2]| = 4$ ako jest (dok je $|\Gamma[2]| = 1$ za sve ostale eliptičke krivulje nad $\mathbf{Q}$, tj. za one koje nisu $\mathbf{Q}$-izomorfne ovima gore).

Zaključak. Ako bismo u (4) znali odrediti lijevu stranu, znali bismo odrediti i rang. Nažalost, ne postoji algoritam za odredjivanje $(\Gamma : 2\Gamma)$ (bar za sad) i to je jedan od najitrigantnijih problema suvremene matematike.

Kvazialgoritam za odredjivanje ranga za $E : y^2 = x^3 + ax^2 + bx$.
Iz (4) vidimo da je $2^r = \frac{(\Gamma:2\Gamma)}{|\Gamma[2]|}$.
Sjetimo se, da smo za krivulje gornjeg oblika izveli

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

Može se pokazati (pogledajte [S-T, str.91)]da ova nejednakost nije daleko od jednakosti. Naime to je jednakost ako E ima četiri $\mathbf{Q}$-racionalne točke 2. reda (tj. ako je $a^2 - 4b$ puni kvadrat, tj. ako je $|\Gamma[2]| = 4$), a lijeva je strana 2 puta manja od desne inače (tj. ako je $|\Gamma[2]| = 2$). To znači da je

$$2^r = \frac{(\Gamma : \psi(\bar{\Gamma})) \cdot (\bar{\Gamma} : \phi(\Gamma))}{4} = \frac{|\alpha(\Gamma)| \cdot |\bar{\alpha}(\bar{\Gamma})|}{4}$$

gdje je $\alpha : \Gamma \to \mathbf{Q}^*/\mathbf{Q}^{*2}$ homomorfizam grupa definiran prije i sjetimo se da je $\alpha(0, 0) = \tilde{b}$, $\alpha(O) = \tilde{1}$ i za sve ostale točke $\alpha(x, y) = \tilde{x}$,
dok je $\bar{\alpha} : \bar{\Gamma} \to \mathbf{Q}^*/\mathbf{Q}^{*2}$ definiran potpuno analogno, samo što umjesto a, b stavljamo $\bar{a} : -2a$, a umjesto b stavljamo $\bar{b} := a^2 - 4b$.
Dakle, problem bi bio riješen ako bismo znali odredjivati slike od α i $\bar{\alpha}$. Mi ćemo pokazati postupak (ne algoritam), kojim ćemo, ako budemo imali sreće, moći odrediti sliku od α (a za $\bar{\alpha}$ sve je analogno).
Slika od α. Znamo da je $\tilde{1}$ u slici, jer je $\alpha(O) = \tilde{1}$. Sjetimo se da se afine točke $(x, y) \in \Gamma$ mogu predočiti u skraćenom zapisu

$$x = \frac{m}{e^2},\ y = \frac{n}{e^3}$$

uz $e > 0$ (naravno m, n, e su cijeli te m, e relativno prosti ili $m = 0$, i n, e relativno prosti ili $n = 0$).

Slučaj $n = 0$.
Postoje dvije mogućnosti. Prva je da $a^2 - 4b$ nije kvadrat. Tada je $m = 0$ i $\alpha(0, 0) = \tilde{b}$. Naravno, to je novi element slike ako b nije kvadrat, inače je $\tilde{b} = \tilde{1}$.
Druga je, ako je $a^2 - 4b = d^2$ puni kvadrat. Tada su i $(\frac{-a\pm d}{2}, 0) \in \Gamma$ pa su i klase od $(\frac{-a\pm d}{2})$ u slici.
Slučaj $n \neq 0$**, tada je i** $m \neq 0$**.** Tada gledamo u jednadžbu

$$n^2 = m(m^2 + ame^2 + be^4). \tag{5}$$

U toj (diofantskoj) jednadžbi nepoznanice su m, n, e, a rješenja tražimo u cijelim brojevima, ali tako da bude $e > 0$, zatim da m, e te n, e budu relativno prosti (m i n ne moraju biti relativno prosti). Sad definiramo nove veličine b_1, b_2 ovako:
Neka b_1 bude hipotetska najveća zajednička mjera od m i b, ali tako da bude $mb_1 > 0$, i neka bude $b_1b_2 = b$ i $b_1m_1 = m$ (uočite da je $m_1 > 0$).
Ako to stavimo u jednadžbu (1) vidimo da $b_1^2|n^2$, tj. $b_1|n$ pa stavljamo $n = b_1n_1$. Ako sad u toj jednadžbi skratimo s b_1^2 dolazimo do jednadžbe

$$n_1^2 = m_1(b_1m_1^2 + am_1e^2 + b_2e^4), \tag{6}$$

u kojoj su b_2 i m_1 te e i m_1 relativno prosti, pa je desna strana umnožak relativno prostih brojeva, a kako je $m_1 > 0$, vidimo da je svaki od njih puni kvadrat, dakle
$m_1 = M^2$, $b_1m_1^2 + am_1e^2 + b_2e^4 = N^2$, pa nakon eliminacije m_1 dobijemo diofantsku jednadžbu

$$N^2 = b_1M^4 + aM^2e^2 + b_2e^4 \tag{7}$$

u kojoj koeficijenti zadovoljavaju uvjet $b_1b_2 = b$, a nepoznanice su 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
(ovo (2) nije tako presudno za postupak (iako je katkad korisno), na primjer, uz svako rješenje $((M, e, N)$ od (7) i (kM, ke, k^2N) je rješenje, pa uvijek možemo doći do rješenja kod kojega su M i e relativno prosti, ali sad se nećemo upuštati u tu analizu).
Gledamo sve takve mogućnosti za b_1 i b_2, i za svaku takvu jednadžbu gledamo ima li rješenja (M, e, N) ili ne. Ako nema, idemo dalje, a ako ima dobili smo

racionalnu točku $P(x,y)$ gdje je:

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

Tu nam je bitan samo x, točnije bitan je samo b_1 jer je $\alpha(P) = \tilde{x} = \tilde{b_1}$, i tako smo dobili vrijednost u slici od α. Uočite da je ta vrijednost iz slike neovisna o tome koje smo rješenje od (7) našli, jer ona osvisi samo o b_1. Uočite i tako da slika od α ima samo konačno mnogo vrijednosti (to znamo od prije).
Sad se sve ovo ponovi s $\bar{E}$ i $\bar{\alpha}$ i primijenimo formulu $2^r = \frac{|\alpha(\Gamma)|\cdot|\bar{\alpha}(\bar{\Gamma})|}{4}$.
Osnovni problem ovog postupka (a zato to i nije algoritam) što, bar za sad, nema nikakve eksplicitne metode ili algoritma za odlučivanje ima li jednadžba (7) rješenje traženog oblika ili ne, odnosno odredjivanje bar jednog rješenja (ukoliko postoji).
Napomena. U (7) je diofantska jednadžba s trima nepoznanicama i gledamo cjelobrojna rješenja. Medjutim, ako podijelimo s e^4 dobijemo jednadžbu krivulje

$$v^2 = b_1 u^4 + au^2 + b_2$$

i gledamo racionalna rješenja (kao i do sada).
Uvjet $a^2 - 4b_1 b_2 = a^2 - 4b \neq 0$ govori da je pripadna afina krivulja C_0 nesingularna. Medjutim (jedina) beskonačno daleka točka $[0,1,0]$ je singularna (provjerite) i snjom se dobije krivulja C. Opća je činjenica da je C $\mathbf{Q}$-biracionalno izomorfna nesingularnoj krivulji A genusa 1 (koja obavezno ima model u obliku nesigularne projektivne kubične krivulje). Ne samo to već je preslikavanje s A u C morfizam (nad $\mathbf{Q}$) i bijekcija osim u dvjema točkama koje idu u $[0,1,0]$. Ovdje se sve, čak i više, može izravno pokazati (vidi [Silverman, The arithmetic of elliptic curves, Prop.2.5.2]). Naime, eksplicitno se može napisati jednadžba od A kao prostorne krivulje u projektivnom prostoru $\mathbf{P^3(C)}$ (točnije, to je sustav dviju jednadžba) tako da je A bez dviju točaka (definiranih nad $\mathbf{Q}(\sqrt{b_1})$) izomorfna nad $\mathbf{Q}$ s C_0, a te dvije točke odlaze u singularnu točku $[0,1,0]$ od A. Te izuzetne točke su racionalne akko je b_1 puni kvadrat, ali taj nam slučaj nije zanimljiv jer je onda slika od α jednaka $\tilde{1}$ (što nije nova vrijednost - za taj dio pogledajte odgovarajući dio u Washingtonu o "quartic curves"). Ako pak b_1 nije kvadrat, onda su racionalne točke od C_0 i A u bijekciji (ako ih uopće i ima).
Može se pokazati da postoji izomorfizam s koeficijentima iz $\mathbf{Q}$ izmedju A i neke nesingularne kubike. Sad se problem odredjivanja bar jednog cjelobrojnog netrivijalnog rješenja od (7) svodi na problem odredjivanja bar jedne

racionalne točke na toj kubici (ako postoji). Opet smo se vratili na nesingularne kubike (krivulje genusa 1) definirane nad $\mathbf{Q}$ i pitamo se imaju li one $\mathbf{Q}$-racionalnu točku, tj. jesu li to eliptičke krivulje nad $\mathbf{Q}$. Ne postoji algoritam za takvo nešto, a mnogi bi ga htjeli naći.