Eliptičke krivulje

Andrej Dujella, Matija Kazalicki i Filip Najman

Neka je $\mathbb{K}$ proizvoljno polje. *Eliptička krivulja* nad $\mathbb{K}$ je nesingularna projektivna kubna krivulja nad $\mathbb{K}$ s barem jednom $\mathbb{K}$-racionalnom točkom.

Svaka takva krivulja može se biracionalnim transformacijama dovesti u *Weierstrassov oblik*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

gdje su $a_1, \ldots, a_6$ konstante iz $\mathbb{K}$.

Ako karakteristika polja $\mathbb{K}$ nije 2 ili 3, eliptička krivulja se može zapisati u *kratkom Weierstrassovom obliku*

$$y^2 = x^3 + ax + b,$$

gdje su a i b konstante iz $\mathbb{K}$. Sada nesingularnost znači da kubni polinom x^3+ax+b nema višestrukih korijena ili ekvivalentno da je *diskriminanta* $\Delta = -4a^3 - 27b^2 \neq 0$.

Na $E(\mathbb{K})$, skupu $\mathbb{K}$-racionalnih točaka na eliptičkoj krivulji nad $\mathbb{K}$ (afine točke (x, y) koje zadovoljavaju gornje jednadžbe zajedno s točkom u beskonačnosti $\mathcal{O}$), može se na prirodan način uvesti binarna operacija uz koju taj skup postaje Abelova grupa.

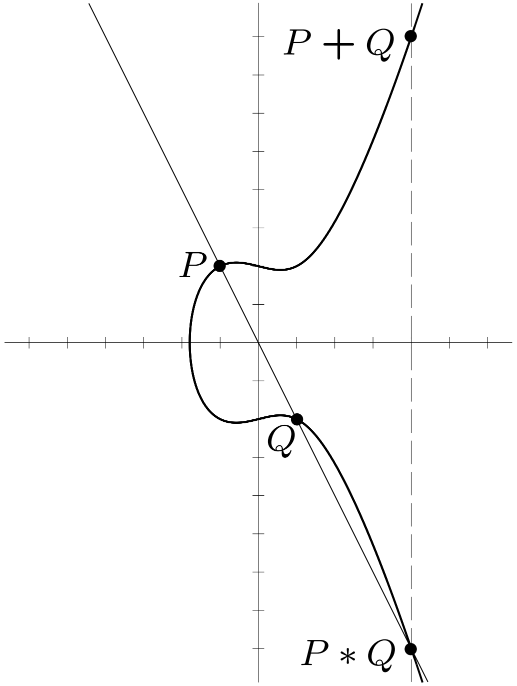
Da bi vizualizirali tu operaciju, uzmimo da je $\mathbb{K} = \mathbb{R}$. Ravninska krivulja $E(\mathbb{R})$ ima jednu ili dvije komponente, u ovisnosti o tome ima li polinom $x^3 + ax + b$ jednu ili tri realne nultočke.

Uvodimo operaciju zbrajanja na skupu $E(\mathbb{R})$.

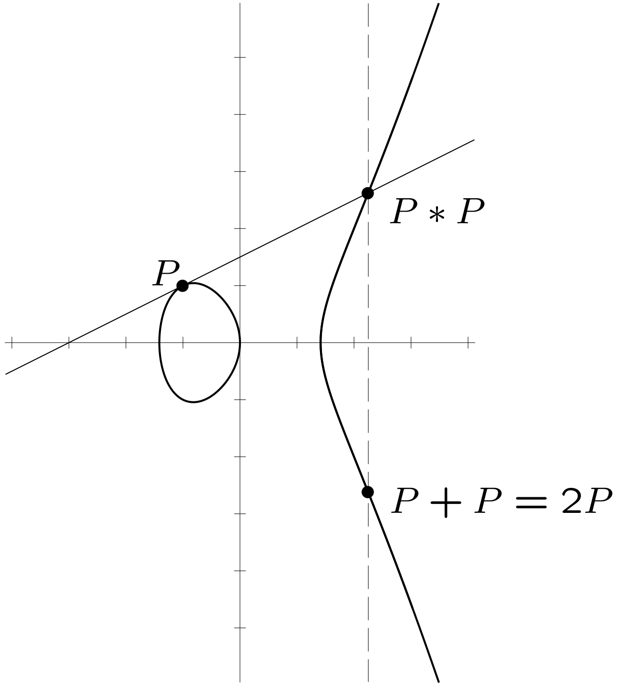
Točka u beskonačnosti $\mathcal{O}$ je neutralni element. Suprotna točka $-P$ je točka s istom x-koordinatom kao P, ali y-koordinatom suprotnog predznaka.

Ako P i Q imaju različite x-koordinate, onda pravac kroz točke P i Q siječe krivulju u točno još jednoj točki, koju označimo s $P * Q$. Definiramo $P + Q$ kao $-(P * Q)$.

Ako je $P = Q$, onda umjesto sekante povlačimo tangentu u točki P.



sekanta



tangenta

Iz ove geometrijske definicije, mogu se dobiti eksplicitne algebarske formule za koordinate zbroja točaka. Te formule imaju smisla nad bilo kojim poljem (uz male modifikacije u slučaju polja karakteristike 2 ili 3) i uz njih eliptička krivulja postaje Abelova grupa.

Neka je $P = (x_1, y_1)$ and $Q = (x_2, y_2)$. Tada:

1) $\mathcal{O} + P = P$;
2) ako je $Q = -P$, onda je $P + Q = \mathcal{O}$;
3) ako je $Q \neq -P$, onda je $P + Q = (x_3, y_3)$,
$x_3 = \lambda^2 - x_1 - x_2$,
$y_3 = -y_1 + \lambda(x_1 - x_3)$,

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, & \text{ako je } x_2 \neq x_1, \\ \frac{3x_1^2 + a}{2y_1}, & \text{ako je } x_2 = x_1. \end{cases}$$

Mordell-Weilov teorem: Neka je E eliptička krivulja nad poljem racionalnih brojeva $\mathbb{Q}$ (ili općenitije nad poljem algebarskih brojeva $\mathbb{K}$). Tada je $E(\mathbb{Q})$ konačno generirana Abelova grupa. Drugim riječima

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{tors}} \times \mathbb{Z}^r.$$

gdje je $E(\mathbb{Q})_{\text{tors}}$ podgrupa elemenata konačnog reda – *torzijska grupa*, dok je $r \geq 0$ *rang* eliptičke krivulje.

Pitanja: Koje su moguće torzijske grupe, koji su mogući rangovi, te koje su moguće kombinacije torzijske grupe i ranga, tj. koje su moguće strukture Mordell-Weilove grupe (nad $\mathbb{Q}$, nad $\mathbb{Q}(t)$, nad $\mathbb{K}$ zadanog stupnja, ...)?

Mazur (1977): Postoji točno 15 mogućih torzijskih grupa $E(\mathbb{Q})_{\text{tors}}$:
$\mathbb{Z}/n\mathbb{Z}$ za $1 \leq n \leq 10$ ili $n = 12$,
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}$ za $1 \leq m \leq 4$.

S druge strane, nije poznato koje vrijednosti za r (rang krivulje) su moguće. Slutnja je da rang može biti proizvoljno velik, ali danas nije poznata niti jedna eliptička krivulja ranga većeg od 28. Rekordnu krivulju ranga 28 pronašao je Elkies 2006. godine.

"Većina" krivulja ima mali rang.
Slutnja: 50% krivulja ima rang 0, a 50% rang 1.
Bhargava & Shankar (2015): - prosječni rang je < 1.

Konstrukcija eliptičkih krivulja velikog ranga (sa zadanom torzijom)

1. Konstrukcija parametarske familije eliptičkih krivulja nad $\mathbb{Q}$ koja sadrži krivulje relativno velikog ranga (tj. eliptičke krivulje nad $\mathbb{Q}(t)$ velikog generičkog ranga).

2. Izbor najboljih kandidata za veliki rang unutar dane familije.

Opća ideja: za očekivati je da će za krivulje velikog ranga broj $|E(\mathbb{F}_p)|$ biti relativno velik za većinu prostih brojeva p.

Precizna tvrdnja: Birch i Swinnerton-Dyerova slutnja.

3. Računanje ranga.

Jedna od metoda za konstrukciju familija relativno velikog ranga koristi Diofantove m-torke.

Definicija: Skup $\{a_1, a_2, \ldots, a_m\}$ of m racionalnih brojeva različitih od nule naziva se *racionalna Diofantova m-torka* ako je $a_i \cdot a_j + 1$ potpun kvadrat za sve $1 \leq i < j \leq n$.

Npr. $\{1, 3, 8, 120\}$ je jedna Diofantova četvorka.

Neka je $\{a, b, c\}$ racionalna Diofantova trojka. Za eliptičku krivulju

$$y^2 = (ax + 1)(bx + 1)(cx + 1)$$

kažemo da je inducirana trojkom $\{a, b, c\}$.

Dujella (2007): Svaka eliptička krivulja s torzijskom grupom $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ je inducirana nekom racionalnom Diofantovom trojkom.

Dujella & Peral (2014): Postoje krivulje ranga 4 nad $\mathbb{Q}(t)$ i ranga 9 nad $\mathbb{Q}$ s torzijskom grupom $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. To su krivulje rekordnog ranga za tu torziju, a inducirane su racionalnim Diofantovim trojkama. Dokaz da je rang nad $\mathbb{Q}(t)$ točno jednak 4 koristi algoritam Gusić & P. Tadić (2012,2015).

Dujella, Kazalicki, Mikić & Szikszai (2015): Postoji beskonačno mnogo racionalnih Diofantovih šestorki.

Neke od podtrojki šestorki iz DKMS daju krivulje rekordnog ranga nad $\mathbb{Q}$ i $\mathbb{Q}(t)$ s torzijskom grupom $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.

Eliptičke krivulje nad kvadratnim poljima

Najman (2010): a) Torzijska grupa eliptičke krivulje nad $\mathbb{Q}(i)$ je izomorfna jednoj od grupa iz Mazurovog teorema ili $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$.
b) Torzijska grupa eliptičke krivulje nad $\mathbb{Q}(\sqrt{-3})$ je izomorfna jednoj od grupa iz Mazurovog teorema ili $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ ili $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.

U pozadini dokaza leže *modularne krivulje* (parametriziraju eliptičke krivulje s nekim propisanim svojstvom).

Postoji točno 26 mogućih torzijskih grupa za eliptičke krivulje nad kvadratnim poljima (Kamienny (1991), Kenku & Momose (1984)).
Krivulje s rekordnim rangom uz zadanu torzijsku grupu: Aguirre, Dujella, Jukić Bokun & Peral (2014), Najman (2014).

Kamienny & Najman (2011): Svaka eliptička krivulja s torzijom $\mathbb{Z}/14\mathbb{Z}$ nad $\mathbb{Q}(\sqrt{-7})$ ima rang 0.
Svaka eliptička krivulja s torzijom $\mathbb{Z}/15\mathbb{Z}$ nad $\mathbb{Q}(\sqrt{5})$ i $\mathbb{Q}(\sqrt{-15})$ ima rang 0.

Mazur & Rubin (2010): Neka je $\mathbb{K}$ polje algebarskih brojeva. Postoji eliptička krivulja E nad $\mathbb{K}$ s rangom 0.

Bosman, Bruin, Dujella & Najman (2014) Nad $\mathbb{Q}(i, \sqrt{5})$ postoji jedinstvena krivulja s torzijom $\mathbb{Z}/15\mathbb{Z}$ i ona ima rang 1.

Bosman, Bruin, Dujella & Najman (2014) Neka je $\mathbb{K}$ kvadratno polje.
$\mathbb{Z}/13\mathbb{Z} \subset E(\mathbb{K}) \Rightarrow E(\mathbb{K})$ ima paran rang.
$\mathbb{Z}/18\mathbb{Z} \subset E(\mathbb{K}) \Rightarrow E(\mathbb{K})$ ima paran rang.

Primjene eliptičkih krivulja

1) Kriptografija javnog ključa

Funkcija $a^x \bmod p$ je "jednosmjerna" – ona se računa lako, ali njezin inverz *diskretni logaritam* teško.

U grupi $E(\mathbb{F}_p)$ je problem diskretnog logaritma još teži nego u grupi F_p^*.

Sigurnost za koju je potreban ključ od 1024 u F_p^*, u $E(\mathbb{F}_p)$ se može postići s ključem od samo 160 bitova.

Jedan od razloga: neefikasnost "index calculus" metode na $E(\mathbb{F}_p)$ – usko povezano s teškoćom konstrukcije eliptičkih krivulja velikog ranga.

2) Faktorizacija

Lenstra (1984): Subeksponencijalni algoritam za faktorizaciju korištenjem eliptičkih krivulja (ECM). Tada je bio najbrži algoritam za faktorizaciju. I danas je najbrži algoritam za micanje "malih" (s manje od 25 znamenaka) faktora iz zadanog složenog broja.

Ideja algoritam je sljedeća: Za zadani složen broj n, promatramo E nad $\mathbb{Z}/n\mathbb{Z}$, te izvršavamo razne "grupovne" operacije u $E(\mathbb{Z}/n\mathbb{Z})$. Ali budući da je n složen, $\mathbb{Z}/n\mathbb{Z}$ nije polje, pa $E(\mathbb{Z}/n\mathbb{Z})$ nije grupa. S "grupovnim" operacijama nešto će poći po zlu – u nekom trenutku ćemo tražiti inverz nekog elementa d koji nije invertibilan u $\mathbb{Z}/n\mathbb{Z}$, pa ćemo Euklidovim algoritmom dobiti netrivijalni faktor nzd(d, n) od n.

Efikasnost algoritma može se poboljšati korištenjem eliptičkih krivulja s velikom torzijskom grupom (veća torzijska grupa od $E(\mathbb{Q})$, povećava vjerojatnost da će broj $|E(\mathbb{F}_p)|$ biti “gladak”, a ako je k neki višekratnik od $|E(\mathbb{F}_p)|$, onda će se kod računanja koordinata točke $[k]P$ pojaviti nazivnik koji neće biti invertibilan):

nad $\mathbb{Q}$: Montgomery (1987), Atkin & Morain (1993);

nad $\mathbb{K}$: Brier & Clavier (2010), Dujella & Najman (2012).