math.e

Hrvatski matematički elektronički časopis

Birch i Swinnerton-Dyerova slutnja

eliptičke krivulje **millenium prize**

Damir Mikoć
Odjel za nastavničke studije u Gospiću, Sveučilište u Zadru

Sažetak

Slutnja Bircha i Swinnertona-Dyera opisuje skup racionalnih točaka na eliptičkoj krivulji. Ona je otvoren problem iz polja teorije brojeva i važi za jedan od najizazovnijih matematičkih problema. Slutnja je izabrana za jedan od sedam Millennium Prize problema, koje je naveo Clay Mathematics Institute i ponudio nagradu od 1.000.000 dolara za dokaz svakog problema. Ime je dobila po matematičarima Bryanu Birchu i Peteru Swinnerton-Dyeru koji su do iskaza slutnje došli tijekom prve polovice 1960-ih na temelju eksperimenata uz pomoć računala. Ukratko, eliptička krivulja E nad $\mathbb{Q}$ ima L-funkciju $L_E(s)$ koja je definirana isključivo u terminima lokalnih podataka (redukcija od E modulo prosti brojevi). BSD slutnja predviđa ponašanje funkcije $L_E(s)$ u točki $s=1$ u terminima globalnih podataka (rang grupe racionalnih točaka).

1 Racionalne točke na krivuljama

Skup rješenja polinomijalne jednadžbe

$$f(x,y)=0$$

definira krivulju C. Ako su koeficijenti polinoma f racionalni brojevi postavlja se pitanje koje su racionalne točke na krivulji, tj. rješenja jednadžbe

$$f(x,y)=0 \text{ gdje su } x,y\in\mathbb{Q}.$$

Skup racionalnih točaka krivulje označavamo s $C(\mathbb{Q})$.

Zanima nas odgovor na pitanje: Koliko je velik $C(\mathbb{Q})$? Je li beskonačan?

činjenica 1. *Glatke projektivne krivulje možemo topološki klasificirati s genusom. Preciznije, neka je C glatka projektivna krivulja i $g=g(C)$ njezin genus.*

$$\begin{aligned} g=0 & \quad C(\mathbb{Q})=\emptyset \text{ ili } C(\mathbb{Q}) \text{ je beskonačan} \\ g>1 & \quad C(\mathbb{Q}) \text{ je konačan (Faltings)} \\ g=1 & \quad \text{nema odgovora} \end{aligned}$$

Teorem 2. *Neka je C glatka projektivna krivulja genusa 0 definirana nad poljem k. Tada je C izomorfna s $\mathbb{P}^1$ nad k ako i samo ako je $C(k) \neq \emptyset$.*

Napomenimo da poljem algebarskih brojeva nazivamo konačno proširenje polja $\mathbb{Q}$.

Teorem 3. *[Faltings, 1983.] Neka je C glatka krivulja genusa $g \geq 2$ nad poljem algebarskih brojeva $\mathbb{K}$. Tada je $C(\mathbb{K})$ konačan.*

Teorem 4. *[Mordell-Weil, Weil 1928., Mordell 1922. za $\mathbb{Q}$] Neka je E eliptička krivulja nad poljem algebarskih brojeva $\mathbb{K}$. Tada je $C(\mathbb{K})$ konačno generirana Abelova grupa.*

[Tm. VIII.4.1, 6]

Diofantske jednadžbe. U vezi gornjeg, diofantske jednadžbe možemo podijeliti u tri klase:

- racionalne,
- eliptičke,
- općeg tipa.

Grubo govoreći one korespondiraju jednadžbama stupnja 2,3 i ≥ 4, respektivno.

Pokazuje se da je problem nalaženja racionalnih rješenja:

- *lagan* za prvu klasu,
- *težak ali napadljiv* za drugu,
- *općenito nemoguć* za treću.

Preciznije:

Racionalne jednadžbe ukoliko imaju jedno, automatski imaju beskonačno mnogo rješenja i postoji formula koja ih sve daje.

Eliptičke jednadžbe mogu imati konačno ili beskonačno mnogo rje\v senja. Međutim, imamo lijepu teoriju koja opisuje strukturu rješenja, te daje način kako provjeriti ima li ih konačno ili beskonačno mnogo \v sto je upravo dano sa slutnjom Birch i Swinnerton-Dyera.

Jednadžbe općeg tipa imaju najviše konačno mnogo rješenja (slutnja Mordell 1917., dokaz Faltings 1984.). Općenito ne postoji algoritam za nalaženje tih rješenja.

2 Eliptičke krivulje

Definicija 5. *Eliptička krivulja nad poljem $\mathbb{K}$ je glatka projektivna krivulja genusa 1 sa specificiranom točkom $\mathcal{O} \in E(\mathbb{K})$.*

Za bilo koju točku $P \in E(\mathbb{K})$ kažemo da je racionalna.

Grupa divizora na krivulji C (vidi [6]), u oznaci $\mathrm{Div}(C)$ je slobodna Abelova grupa generirana s točkama od C. Stoga je divizor $D \in \mathrm{Div}(C)$ formalna suma

$$D = \sum_{P \in C} n_P(P),$$

gdje je $n_P \in \mathbb{Z}$ te je $n_P = 0$ za sve osim konačno mnogo $P \in C$. *Stupanj* od D definira se kao

$$\deg D = \sum_{P \in C} n_P.$$

Za projektivnu krivulju C nad poljem $\mathbb{K}$ s $\mathbb{K}(C)$ označavamo polje racionalnih funkcija na krivulji C, dok s $\mathbb{K}(C)^\times$ pripadnu multiplikativnu grupu, tj. grupu svih nenul elemenata od $\mathbb{K}(C)$ s operacijom množenja (vidi [6]).

Definicija 6. *Neka je C projektivna krivulja. Za $D \in \mathrm{Div}(C)$ definiramo linearni sustav ili Riemann-Rochov prostor*

$$L(D) := \{f \in \mathbb{K}(C)^\times \mid \mathrm{div}(f) + D \geq 0\} \cup \{0\}.$$

Skup $L(D)$ je vektorski potprostor nad K od $K(C)$. Definiramo

$$\ell(D) = \dim L(D).$$

Riemann-Rochov teorem. Jedna posljedica Riemann-Rochovog teorema je:

Korolar 7. *Ako krivulja C ima genus 1 i ako je $\deg(D) > 0$, tada vrijedi*

$$\ell(D) = \deg(D).$$

Neka je $P \in C(K)$. Slijedi da je $\ell(nP) = n$. Iz toga dobijemo rastući niz potprostora

$$L(P) \subset L(2P) \subset L(3P) \subset L(4P) \subset L(5P) \subset L(6P).$$

Kako je $\ell(2P) = 2$ i $K = L(P) \subset L(2P)$ slijedi da postoji funkcija x koja ima pol reda 2 u P i nema niti jedan drugi pol. Analogno postoji funkcija y koja u P ima točno pol reda 3 i nema niti jedan drugi pol.

Kako su funkcije s različitim redom pola u P linearno nezavisne, pomoću x i y možemo dobiti baze za različite prostore $L(nP)$:

$$\begin{aligned} L(P) &= \langle 1 \rangle \\ L(2P) &= \langle 1, x \rangle \\ L(3P) &= \langle 1, x, y \rangle \\ L(4P) &= \langle 1, x, y, x^2 \rangle \\ L(5P) &= \langle 1, x, y, x^2, xy \rangle. \end{aligned}$$

Na isti način u prostoru $L(6P)$ dobijemo 7 funkcija

$$1, x, y, x^2, xy, x^3, y^2.$$

Kako je $\dim L(6P) = 6$ one moraju biti linearno zavisne.

Weierstrassova forma. Iz toga dobijemo da je krivulja C izomorfna glatkoj projektivnoj krivulji oblika

$$E\ :\ y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3,$$

gdje su $a_i \in K$. Ovaj izomorfizam šalje točku $P \mapsto \mathcal{O} = (0:1:0)$, tj. u točku u ∞. Gornju jednadžbu nazivamo *Weierstrassova forma* za eliptičku krivulju E. Afina verzija jednadžbe je

$$E\ :\ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Ako je $\mathrm{char}(K) \neq 2, 3$ zamjenom varijabli možemo eliptičku krivulju zapisati u kratkoj Weierstrassovoj formi

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

Ako je eliptička krivulja dana u kratkoj Weierstrassovoj formi tada se vrijednost

$$\Delta(E) = -16(4a^3 + 27b^2)$$

naziva diskriminanta eliptičke krivulje. Vrijedi da je eliptička krivulja glatka (nesingulara) ako i samo ako je $\Delta(E) \neq 0$.

Grupovni zakon.

Teorem 8. *Neka je $E/\mathbb{K}$ eliptička krivulja. Tada skup točaka $E(\mathbb{K})$ ima strukturu Abelove grupe.*

Po Mordell-Weilovom teoremu i klasifikaciji konačno generiranih Abelovih grupa slijedi

$$E(\mathbb{K}) \simeq T \oplus \mathbb{Z}^r.$$

Ovdje je T je podgrupa elemenata konačnog reda koju zovemo **torzijska podgrupa**, dok je $r \geq 0$ i naziva se **rang** od $E(K)$. Torzijsku podgrupu označavamo s $E(\mathbb{K})_{tors}$.

Rang.

Za konkretnu eliptičku krivulju, torziju je lako izračunati.

O rangu (nad $\mathbb{Q}$) se puno manje zna. Ne zna se niti može li biti proizvoljno velik ili postoji gornja ograda za rang svih eliptičkih krivulja nad $\mathbb{Q}$.

Najveći poznati rang eliptičke krivulje nad $\mathbb{Q}$ je 28 (Elkies 2006).

Želimo smisleno računati prosječni rang. Za to moramo nekako moći brojati eliptičke krivulje E nad $\mathbb{Q}$. U tu svrhu se uvodi funkcija visine $H(E)$ na skupu svih racionalnih eliptičkih krivulja $E/\mathbb{Q}$, koju mi nećemo precizno definirati. Pokazuje se da je za bilo koji $X \in \mathbb{R}$ broj eliptičkih krivulja $E/\mathbb{Q}$ takvih da je $H(E) \leq X$ konačan. Ova činjenica nam omogućava da definiramo prosječni rang kao limes (ako postoji):

$$\lim_{X\to\infty} \frac{\sum_{H(E)\leq X} r(E)}{\sum_{H(E)\leq X}}.$$

Slutnja 9. *[Goldfeld] Prosječni rang eliptičkih krivulja nad $\mathbb{Q}$ je 0.5.*

Teorem 10. *[Bhargava i Shankar (2011).] Prosječni rang eliptičkih krivulja nad $\mathbb{Q}$ je < 0.99 .*

Kongruentni brojevi.

Primjer 11. [9] *Za prirodni broj n kažemo da je **kongruentan** ako postoji pravokutan trokut s racionalnim stranicama i površinom n. Niz kongruentnih prirodnih brojeva počinje s:*

$$5, 6, 7, 13, 14, 15, 20, 21, 22, 23, 24, 28, 29, 30, 31, 34, 37, 38, 39, 41, 45, 46, 47, \ldots$$

Na primjer, 5 je kongruentan broj jer je jednak površini trokuta $(20/3, 3/2, 41/6)$, a 6 je kongruentan broj jer je jednak površini trokuta $(3, 4, 5)$. Broj 3 nije kongruentan.

Veza eliptičkih krivulja s kongruentnim brojevima je u slijedećoj činjenici:

$$n \text{ je kongruentan } \Leftrightarrow \ E \ : \ y^2 = x^3 - n^2 x \ \text{ ima pozitivan rang.}$$

3 Birch i Swinnerton-Dyerova slutnja

Birch i Swinnerton-Dyerova slutnja je dobila ime po matematičarima Bryanu Birchu i Peteru Swinnerton-Dyeru koji su do slutnje došli tijekom prve polovice 1960-ih uz pomoć računala.

Bryan John Birch (rođen 25. rujna 1931.) je britanski matematičar s Matematičkog instituta Sveučilišta u Oxfordu. Doktorirao je na Sveučilištu u Cambridgeu.

Sir Henry Peter Francis Swinnerton-Dyer (2. kolovoza 1927. - 26. prosinca 2018.) bio je engleski matematičar specijaliziran za teoriju brojeva na Sveučilištu u Cambridgeu.

BSD slutnja se odnosi na veličinu ranga. Konkretno ona kaže da je (algebarski) rang jednak analitičkom koji se definira preko tzv. L-funkcija. Osnovna ideja je brojati točke nad konačnim poljima. Za to nam je ključna sljedeća procjena:

Teorem 12. *[Hasse] Neka je E eliptička krivulja nad konačnim poljem $\mathbb{F}_p$. Tada je*

$$| \, p + 1 - \#E(\mathbb{F}_p) \, | \leq 2\sqrt{p}.$$

Neka je $N_p = \#E(\mathbb{F}_p)$ i označimo grešku gornje procjene s a_p

$$a_p = p + 1 - N_p.$$

Definicija 13. *Neka je E eliptička krivulja nad $\mathbb{Q}$. Ako za prost broj p vrijedi $p \nmid \Delta(E)$ kažemo da E ima dobru redukciju u p. U suprotonom kažemo da E ima lošu redukciju u p.*

činjenica 14. *Ako $E/\mathbb{Q}$ ima dobru redukciju u p tada je njena redukcija $E(\mathbb{F}_p)$ eliptička krivulja. U suprotnom je $E(\mathbb{F}_p)$ singularna kubika.*

Neka je C singularna kubika nad poljem $\mathbb{K}$ i neka je karakteristika polja različita od 2 i 3. Tada možemo napraviti zamjenu koordinata

takvu da jednadžba od C ima oblik

$$C \ : \ y^2 = x^3 + ax^2.$$

Ako smo redukcijom modulo p neke eliptičke krivulje $E/\mathbb{Q}$ dobili singularnu kubiku C tada kažemo da

$$E \text{ u } p \text{ ima } \begin{cases} \text{aditivnu redukciju} & \text{ako je } a = 0 \\ \text{rascjepivu multiplikativnu redukciju} & \text{ako je } a \neq 0 \text{ kvadrat u } \mathbb{F}_p \\ \text{nerascjepivu multiplikativnu redukciju} & \text{ako } a \text{ nije kvadrat u } \mathbb{F}_p \end{cases}$$

Zanima nas N_p broj točaka singularne kubike nad $\mathbb{F}_p$ kao i koeficijenti greške $a_p = p - N_p$. Definicija od a_p se razlikuje od one za eliptičke krivulje jer smo eliminirali singularnu točku iz razmatranja. Imamo sljedeću tablicu

Tip redukcije	N_p	a_p
Aditivna	p	0
Rascijepiva multiplikativna	$p-1$	1
Nerascijepiva multiplikativna	$p+1$	-1

Vidimo da se broj točaka singularne kubike nad konačnim poljem automatski dobije iz tipa redukcije. Međutim, broj točaka eliptičke krivulje nad $\mathbb{F}_p$ je mnogo suptilnija stvar.

Redukcija modulo p inducira homomorfizam grupa

$$E(\mathbb{Q}) \longrightarrow E(\mathbb{F}_p).$$

Hasseov teorem nam kaže

$$|E(\mathbb{F}_p)| \approx p + 1$$

iz čega zaključujemo da

$$p \text{ raste } (\text{velik}) \ \Rightarrow |E(\mathbb{F}_p)| \text{ raste } (\text{velik}),$$

bez obzira je li $E(\mathbb{Q})$ konačan ili beskonačan.

Birch i Swinnerton-Dyer su primjetili da ukoliko je $E(\mathbb{Q})$ beskonačan, tada broj točaka u $E(\mathbb{F}_p)$ ima tendenciju biti veći nego što je to uobičajeno.

Ideja je mjeriti prosječnu veličinu od $N_p = |E(\mathbb{F}_p)|$.
Stoga *normaliziramo* promatrajući $\frac{N_p}{p}$ umjesto N_p.

Vrijedi

$$1 + \frac{1}{p} - \frac{2}{\sqrt{p}} \leq \frac{N_p}{p} \leq 1 + \frac{1}{p} + \frac{2}{\sqrt{p}},$$

Dakle $\frac{N_p}{p} \approx 1$ i $\lim\limits_{n \to \infty} \frac{N_p}{p} = 1$.

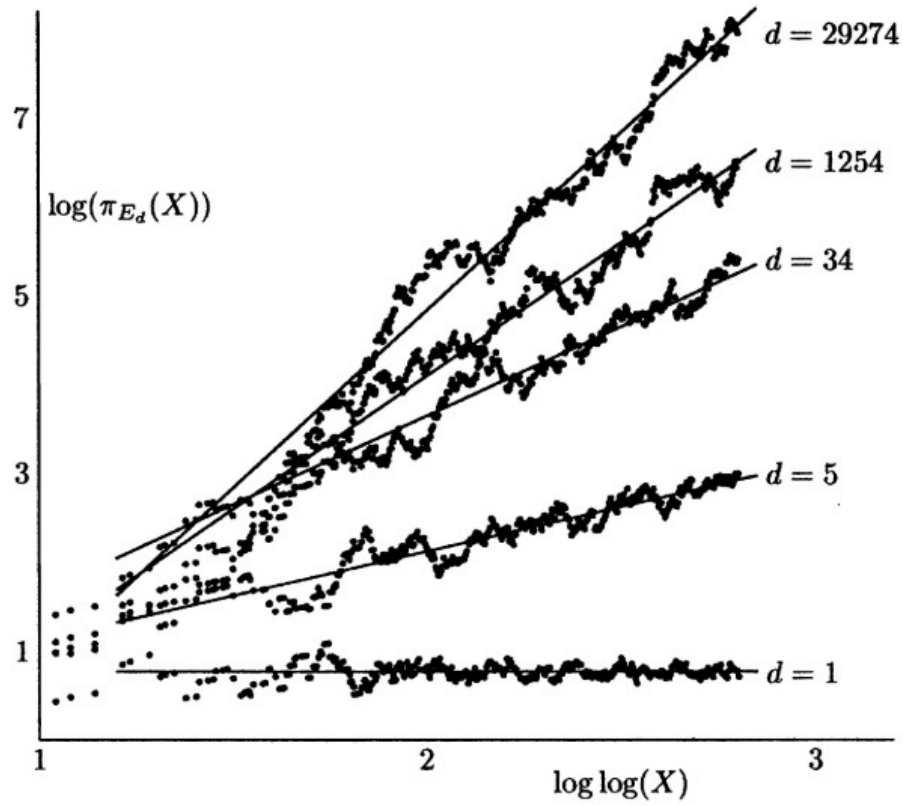
Međutim, ovo vrijedi za bilo koju eliptičku krivulju pa nam to ne daje neku korisnu informaciju.

Birch Swinnerton-Dyer-ova ideja bila je gledati *parcijalne produkte* N_p/p-ova i vidjeti *koliko brzo* oni postaju veliki. Definirajmo funkciju

$$\pi_E(X) := \prod_{p \le X, p \nmid \Delta} \frac{N_p}{p}.$$

Kako bi testirali svoju ideju Birch i Swinnerton-Dyer su 1960. god. računali $\pi_E(X)$ kada X raste za određene eliptičke krivulje E.

BSD eksperiment.



Slika 1: BSD podaci za $y = x^3 - d^2x$

Slika pokazuje ponašanje od $\pi_{E_d}(X)$ za X-eve do 1.5×10^7 za pet različitih krivulja E_d: $y^2 = x^3 - d^2x$ koje redom imaju rang 0, 1, 2, 3 i 4.

Iz slike se uočava približna linearna ovisnost veličine $\log(\pi_E(X))$ o veličini $\log(\log(X))$ tj.

$$\log(\pi_E(X)) \sim \mathrm{rk}(E) \log(\log(X)) + C' \,.$$

Uz $C' = \log(C)$ Birch i Swinerton-Dyer su inicijalno naslutili da

$$\pi_E(X) \sim C \log(X)^{\mathrm{rk}(E)}$$

kada $X \to \infty$ za neku konstantu C koja ovisi samo o E.

Međutim funkcija π_E se ne ponaša jako lijepo i s njom je teško raditi. Stoga su Birch i Swinnerton-Dyer postavili srodnu slutnju koristeći L-funkciju od E umjesto funkcije π_E.

L-funkcije.

L-funkcija od E je Eulerov produkt

$$L_E(s) = \prod_{p|\Delta} (1 - a_p \cdot p^{-s})^{-1} \prod_{p\nmid\Delta} \left(1 - a_p \cdot p^{-s} + p \cdot p^{-2s}\right)^{-1},$$

gdje je $a_p = p + 1 - N_p$ za dobru redukciju, a za lošu redukciju imamo vrijednosi iz tablice 14.

Kako bi vidjeli vezu L_E funkcije s funkcijom π_E, uvrstimo $s = 1$ (iako tu L_E ne konvergira) u produkt i zanemarimo konačno mnogo loših prostih brojeva:

$$\prod_p (1 - a_p p^{-1} + p^{-1})^{-1} = \prod_p \left(\frac{p - a_p + 1}{p}\right)^{-1} = \prod_p \frac{p}{N_p}.$$

Ocjena $|a_p| < 2\sqrt{p}$ (Hasse) povlači da gornji produkt konvergira za $\Re(s) > 3/2$.

Svaki dobar faktor se može razviti u obliku reda

$$(1 - a_p p^{-s} + p^{1-2s})^{-1} = 1 + a_p p^{-s} + a_{p^2} p^{-2s} + a_{p^2} p^{-2s} + \cdots$$

gdje je a_p na lijevoj strani jednak a_p na desnoj (pa to nije loša notacija), te vrijedi

$$a_{p^2} = a_p^2 - p,\ a_{p^3} = a_p^3 - 2a_p p,\ a_{p^4} = a_p^4 + p^2 - 3a_p^2 p^4,\ \ldots\ .$$

Za p-ove loše redukcije stavimo $a_{p^k} = a_p^k$. Tada produkt po svim p-ovima daje izraz

$$L_E(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}.$$

Gore je za $n = \prod_j p_j^{e_j}$

$$a_n = \prod_j a_{p_j^{e_j}}\ .$$

Ovaj red za $L_E(s)$ konvergira za $\Re(s) > 3/2$.

Prirodno je pitati se ima li $L_E(s)$ analitičko produljenje na cijeli $\mathbb{C}$ te zadovoljava li neku funkcijsku jednadžbu, kao što je to slu\v caj s Riemannovom zeta funkcijom (vidi [3]).

Odgovor na to pitanje je pozitivan i dan je s Teoremom modularnosti.

Teorem modularnosti - (ex. Taniyama–Shimurina slutnja).

Kako bi se proučavala analitička svojstva od $L_E(s)$ uvodimo novu funkciju. Neka je $\tau \in \mathbb{H}$, gdje je $\mathbb{H}$ gornja poluravnina i neka je $q = e^{2\pi i \tau}$ $(= e^{2\pi(-y+ix)}$). Definiramo

$$f_E(\tau) = \sum_{n=1}^{\infty} a_n q^n\ .$$

Ovo je funkcija izvodnica koja kodira brojeve točaka na E modulo bilo koji prost broj. Njen red konvergira za $\tau \in \mathbb{H}$ i zadovoljava neka fascinantna svojstva.

Za bilo koji prirodan broj N definiramo podgrupu od $SL_2(\mathbb{Z})$, u oznaci

$\Gamma = \Gamma_0(N)$ na slijedeći način

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}) : c \equiv 0 \pmod{N} \right\}.$$

[1], [Tm. 4.1, 2], [Tm. 14.4, 8].

Teorem 15. *[Teorem modularnosti - Breuil, Conrad, Diamond, Taylor, Wiles] Neka je E eliptička krivulja definirana nad $\mathbb{Q}$. Tada postoji cijeli broj N takav da za svaki $\tau \in \mathbb{H}$ vrijedi [(1)]*

(1) $$f_E\left(\frac{a\tau + b}{c\tau + d}\right) = (cz + d)^2 f_E(\tau) \text{ za sve } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$$

(2) $$f_E(-1/(N\tau)) = \pm N\tau^2 f_E(\tau).$$

Drugim riječima: Holomorfna funkcija $f_E(\tau)$ je primitivna cusp forma težine 2 za $\Gamma_0(N)$.

Ovaj teorem (uz tvrdnje o ponašanju u kaspovima na realnoj osi) kaže da je $f_E(\tau)$ modularna forma (u stvari kusp formna) težine 2 i nivoa N. Najmanji mogući takav N naziva se **konduktor** od E. Prost broj p dijeli N ako i samo ako E ima lošu redukciju u p.

Teorem modularnosti povlači slijedeći rezultat koji je dugo bio poznat kao Hasse-Weilova slutnja. [Kor. 14.5,8], [Tm. 5.4, 5].

Teorem 16. *[Hecke, Wiles, et al.] Neka je E eliptička krivulja, $N = N_E$ njen konduktor.*
Tada funkcija

$$\Lambda_E(s) = \left(\frac{\sqrt{N}}{2\pi}\right)^s \cdot \Gamma(s) \cdot L_E(s)$$

ima analitičko produljenje na cijeli $\mathbb{C}$, te zadovoljava funkcijsku jednadžbu

$$\Lambda_E(2 - s) = \mp \cdot \Lambda_E(s),$$

za sve $s \in \mathbb{C}$. Predznak $\mp$ je suprotan od predznaka u (2) Teorema modularnosti 15.

Analitičko produljenje od $L_E(s)$. Gornji teorem automatski povlači da i funkcija $L_E(s)$ ima analitičko produljenje na cijeli $\mathbb{C}$; uočimo da je $\left(\frac{\sqrt{N}}{2\pi}\right)^s \cdot \Gamma(s)$ različito od 0 za svaki $s \in \mathbb{C}$. Sjetimo se da je funkcija $L_E(s)$ inicijalno definirana redom, konvergirala samo za $\Re(s) > 3/2$.

Kako je $L_E(s)$ analitička funkcija na cijelom $\mathbb{C}$ možemo je razviti u Taylorov red oko $s = 1$, tj.

$$L_E(s) = c_{r_{an}}(s-1)^{r_{an}} + c_{r_{an}+1}(s-1)^{r_{an}+1} + \cdots,$$

tako da je $r_{an} \geq 0$ i $c_{r_{an}} \neq 0$. Nenegativan cijeli broj r_{an} nazivamo analitički rang.

Napomena 17. *Napomenimo da smo skupljali informacije o $E(\mathbb{F}_p)$ preko funkcija izvodnica:*

- $\tilde{L}_E(s)$ *- kodira informacije o $E(\mathbb{F}_p)$ za sve osim konačno mnogo ("loših") prostih brojeva p,*
- $L_E(s)$ *- uključuje informacije o svim prostim brojevima,*
- $\Lambda_E(s)$ *- uključuje informacije "u beskonačnosti". Ovu funkciju često nazivamo normalizirana L-funkcija*

$$\Lambda_E(s) = \left(\sqrt{N}/2\pi\right)^s \cdot \Gamma(s) \cdot L_E(s)\,.$$

BSD I.

Definicija 18. *Red nultočke L-funkcije L_E od eliptičke krivulje $E/\mathbb{Q}$ u točki $s = 1$ naziva se analitički rang od $E/\mathbb{Q}$.*

Slutnja 19.[*Birch-Swinerton-Dyer] Neka je $E/\mathbb{Q}$ eliptička krivulja. Tada su njen algebarski i analitički rang jednaki.*

Teorem 20. *[Gross-Zagier, Kolyvagin] Ako je $\mathrm{rk}_{an}(E/\mathbb{Q}) \leq 1$ tada je*

$$\mathrm{rk}(E/\mathbb{Q}) = \mathrm{rk}_{an}(E/\mathbb{Q}).$$

4 Birch i Swinnerton-Dyerova slutnja II - jača verzija

Slutnja 21. *[Birch i Swinnerton-Dyer]* [7] *Neka je $E/\mathbb{Q}$ eliptička krivulja i neka je $r = \mathrm{rk}(E/\mathbb{Q})$. Tada je*

$$\lim_{s\to 1} \frac{L_E(s)}{(s-1)^r} = \frac{|Ш(E/\mathbb{Q})|\Omega_E R_E \prod_{p|\Delta} c_p}{|E(\mathbb{Q})_{tors}|^2},$$

gdje su nepoznati faktori na desnoj strani brojnika invarijante krivulje i nazivaju se redom: $Ш(E/\mathbb{Q})$ Tate-Šafarevičeva grupa, Ω_E realni period, R_E regulator, a c_p Tamagawini brojevi.

BSD II daje formulu za c_{ran}, tj. za koeficijent vodečeg člana u Taylorovom razvoju funkcije $L_E(s)$ u $s = 1$. Primjetimo da u formuli za c_{ran} sve vrijednosti osim $|Ш(E/\mathbb{Q})|$ dobro razumijemo. Tate-Šafarevičeva grupa je i dalje velika zagonetka. Ne zna se niti je li konačna, iako postoji slutnja da jeste.

Bibliografija

[1] Christophe Breuil, Brian Conrad, Richard Taylor, and Fred Diamond. On the modularity of elliptic curves over Q: Wild 3-adic exercises. Journal of the American Mathematical Society, 14(4):843–939, 2001.

[2] Peter Bruin. Elliptic curves, modularity and the conjecture of Birch and Swinnerton-Dyer, lecture notes. 2016.

[3] Boris Širola. Distribucija prim brojeva i Riemannova zeta-funkcija. Hrvatski matematički elektronički časopis math.e, (13), 2008.

[4] Filip Najman. Eliptičke krivulje nad poljima algebarskih brojeva, skripta. 2013.

[5] Karl Rubin and Alice Silverberg. Ranks of Elliptic Curves. Bulletin (New Series) of the American Mathematical Society, 39(4):455–474, 2002.

[6] Joseph H. Silverman. The Arithmetic of Elliptic Curves, 2nd Edition, volume 106. Springer-Verlag, New York, 2009.

[7] Alice Silverberg. Ranks "cheat sheet". In Women in numbers 2: research directions in number theory, pages 101–110. Contemp. Math., 606, Centre Rech. Math. Proc., Amer. Math. Soc.,Providence, RI, 2013.

[8] Lawrence C. Washington. Elliptic Curves Number Theory and Cryptography Second Edition. Chapman & Hall/CRT, 2008.

[9] Wikipedia contributors. Congruent number — Wikipedia the free encyclopedia, 2019.

ISSN 1334-6083