SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Marko Sikirić

BIRCH I SWINNERTON-DYEROVA SLUTNJA

Diplomski rad

Voditelj rada:
prof. dr. sc. Filip Najman

Zagreb, 2016

Ovaj diplomski rad obranjen je dana _____ pred ispitnim povjerenstvom u sastavu:

1. _____, predsjednik
2. _____, član
3. _____, član

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Sadržaj

Uvod

U ovom radu bavit ćemo se Birch i Swinnerton-Dyer slutnjom, koja je jednan od sedam milenijskih problema. To je sedam dalokesežnih problema koje je odabrao The Clay Mathematics Institute (CMI) za čije riješenje je ponuđena nagrada od po milijun dolara. Riječ je o hipotezi iz područja teorije brojeva kojom se opisuje skup racionalnih rješenja jednadžbi kojima se definira eliptična krivulja. Razvili su je početkom 60.-ih godina 20. stoljeća Bryan Birch i Peter Swinnerton-Dyer s pomoću jednog od prvih računala. Njihovi i svi kasniji izračuni tu hipotezu snažno podupiru, no do danas su dokazani tek posebni slučajevi ove slutnje. Ova slutnja ima značajnu važnost, ne samo u teorijskoj matematici, zbog široke primjene eliptičkih krivulja u kriptografiji. Također bi dokaz ove slutnje dao riješenje 2000 godina starog problema kongruentnih brojeva.

Počet ćemo s definicijom i osnovnim svojstvima eliptičkih krivulja. Zatim ćemo definirati i pomnije promotriti ključne pojmove slutnje što su L-funkcije i Tate-Šavarevićeva grupa. Na kraju ćemo dati iskaz slabe i jake verzije Birch i Swinnerton-Dyerove slutnje te napredak, glavne rezultate i posljedice.

Napomenimo još da ovaj rad daje pregled ovog jako širokog i zanimljivog područja današnje matematike i treba služiti kao inspiracija za daljne proučavanje.

Poglavlje 1

Uvodne definicije i teoremi

1.1 Osnovno o eliptičkim krivuljama

Definicija i jednadžbe

Počet ćemo sa definicijom eliptičke krivulje i kratkim objašnjenjem osnovnih pojmova definicije. Valja napomenuti da se eliptička krivulja može definirati na više ekvivalentih načina (vidi [9, str. 45]) no za naše potrebe bit će dovoljna sljedeća definicija.

Definicija 1.1.1. ***Eliptička krivulja*** *nad poljem K (pišemo E/K) je nesingularna projektivna kubna krivulja s barem jednom točkom.*

Kratko pojasnimo gore navedene pojmove. Kubna krivulja je skup točaka iz K^2 koje zadovoljavaju kubnu jednadžbu u dvije varijable koja ima sljedeću formu u afinim koordinatama tj. njena afina jednadžba je oblika:

$$F(x,y) = ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0,$$
$$a, b, c, ..., j \in K$$

Nesingularnost znači da za sve točke $P \in \overline{K}^2$ koje zadovoljavaju jednadžbu krivulje vrijedi da je bar jedna parcijalna derivacija $\frac{\partial F}{\partial x}, \frac{\partial F}{\partial y}$ različita od 0 gdje je $\overline{K}$ algebarsko zatvorenje od K. Kako je eliptička krivulja projektivna potrebno je definirati projektivnu ravninu $\mathbb{P}^2(K)$ nad poljem K:

$$\mathbb{P}^2(K) = \{(X,Y,Z) \in K^3 \mid (X,Y,Z) \neq 0\}/\sim$$

gdje je $(X,Y,Z) \sim (X',Y',Z')$ ako i samo ako postoji $c \neq 0$, $c \in K$ takav da $(X,Y,Z) = (cX', cY', cZ')$. Time dobivamo projektivnu ravninu na K. Primijetimo da ako u gornjoj

afinoj jednadžbi uvedemo substituciju $x = \frac{X}{Z}, y = \frac{Y}{Z}$ dobivamo projektivnu jednadžbu. U slučaju $Z \neq 0$ klasa ekvivalencije ima reprezentant $(x, y, 1)$ pa tu klasu možemo identificirati s (x, y). Za $z = 0$ postoji klasa ekvivalencije koja ima reprezentant $(0, 1, 0)$, tu klasu identificiramo s točkom u beskonačnosti O. Svaka jednadžba eliptičke krivulje se može svesti na *Weierstrassovu formu*

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

te ako je karakteristika od K različita od 2 i 3 gornja jednadžba se može transformirati u *kratku Weierstrassovu formu* oblika

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

Pogledajmo detaljnije tu transformaciju. Krenimo od jednadžbe u *Weierstrassovoj formi*

$$y^2 + a_1xy + a_3y = x^3 + a_2 + a_4x + a_6.$$

Iz ovog izraza supstitucijom $y \mapsto \frac{y - a_1x - a_3}{2}$ dobivamo

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6,$$

gdje je:

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, \\ b_4 &= a_1a_3 + 2a_4, \\ b_6 &= a_3^2 + 4a_6. \end{aligned}$$

Nadalje supstitucijom $x \mapsto \frac{x - 3b_2}{36}, y \mapsto \frac{y}{108}$, dobijemo jednadžbu u kratkoj Weierstrassovoj formi

$$y^2 = x^3 + 27c_4x + 54c_6,$$

gdje je

$$\begin{aligned} c_4 &= b_2^2 - 24b_4, \\ c_6 &= -b_2^2 + 36b_2b_4 - 216b_6. \end{aligned}$$

Primijetimo da smijemo napraviti ove supstitucije samo ako je karakteristika polja različita od 2 i 3. Sada možemo definirati još dvije važne veličine:

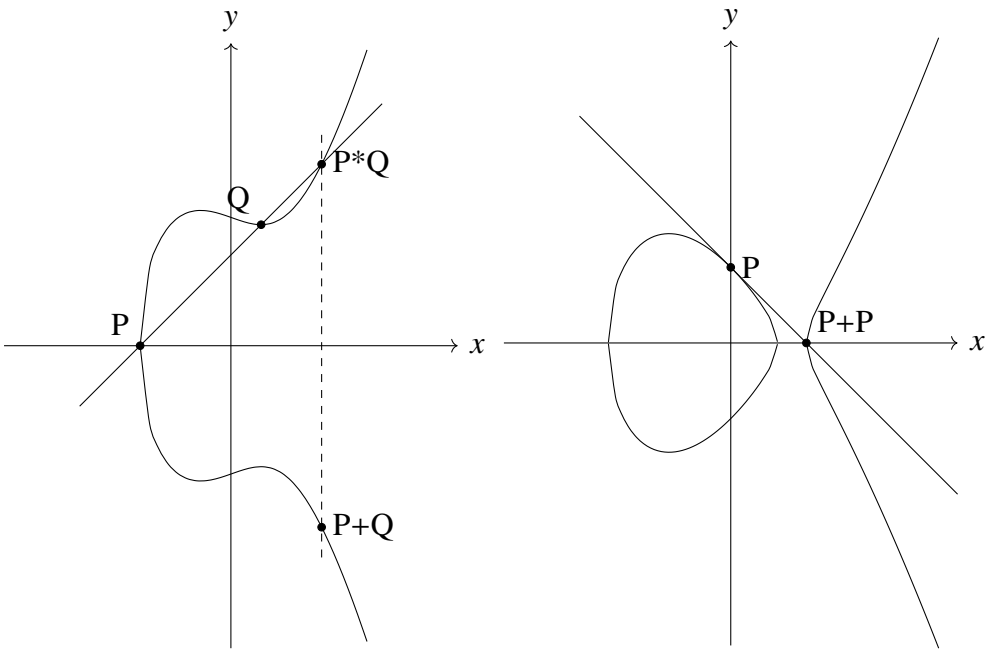
1. diskriminantu $\Delta = \frac{c_4^3 - c_6^2}{1728}$,
2. j-invarijantu $j = \frac{c_4^3}{\Delta}$.

U jednadžbi danoj s $y^2 = x^3 + ax + b$ je $\Delta = -16(4a^3 + 27b^2)$. Sada se uvjet nesingularnosti krivulje svodi na $\Delta \neq 0$.

Eliptičke krivulje kao grupe

Eliptičku krivulju možemo promatrati kao skup točaka koje zadovoljavaju Weierstrassovu jednadžbu s točkom u beskonačnosti. Označimo taj skup s $E(K)$. Jedno od najvažnijih svojstava koje je temelj svih daljnjih razmatranja jest da uz prirodno uvođenje operacije zbrajanja točaka iz $E(K)$ one tvore *Abelovu grupu*. Pogledajmo način zadavanja operacije zbrajanja točaka na eliptičkoj krivulji nad $\mathbb{Q}$. Neka je E zadana *Weierstrassovom jednadžbom*. Vidjeli smo da se E sastoji od $(x, y, z) \in \mathbb{P}^2$ koje zadovoljavaju jednadžbu s točkom u beskonačnosti O.

Neka su $P, Q \in E(\mathbb{Q})$ i $P \neq Q$, povucimo pravac L kroz točke P, Q. Kako su $P, Q \in \mathbb{Q}^2$ L ima racionalni nagib te kako je stupanj eliptičke krivulje 3 taj pravac siječe krivulju u još jednoj točki $R \in E(\mathbb{Q})$. Ukoliko je nagib pravca ∞ tada je $R = O$ te je $P + Q = O$. Ako je $R \neq O$ tada definiramo $P + Q$ kao točku koju dobijemo osnom simetrijom oko $x - osi$. Pogledajmo još slučaj kada je $P = Q$. Sada pravac L dobivamo povlačenjem tangente kroz točku P te L opet siječe E u točki R. Istim postupkom kao u prvom slučaju dobijemo $P + P$. Iz konstrukcije se direktno vidi da je operacija komutativna, točka u beskonačnosti O je neutralni element. Primijetimo da svaki vertikalni pravac prolazi kroz točku u beskonačnosti pa inverznu točku dobijemo simetralnim preslikavanjem oko $x-osi$. Za asocijativnost je dokaz nešto kompliciraniji pa ga u ovom radu nećemo navoditi(vidi [9, str. 27], [11, str. 52] i [7, str. 66]). Na donjim slikam vidimo dva primjera zbrajanja točaka na eliptičkim krivuljama.



$y^2 = x^3 - 3x + 18$ $y^2 = x^3 - 2x + 1$

Navedimo sada algebarske formule operacije zbrajanja točaka na eliptičkoj krivulji.

Propozicija 1.1.2. *Ako su $P = (x_1, y_1)$ i $Q = (x_2, y_2)$ točke na eliptičkoj krivulji $E(\mathbb{Q})$ koja je dana s (1.3), tada vrijede sljedeće formule:*

1. $-O = O$;
2. $-P = (x_1, -y_1)$;
3. $O + P = P$;
4. *ako je* $Q = -P$ *onda je* $Q + P = O$;
5. *ako je* $Q \neq P$, *onda je* $P + Q = (x_3, y_3)$, *gdje je*

$$x_3 = \lambda^2 - x_1 - x_2, y_3 = -y_1 + \lambda(x_1 - x_3),$$
$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & ako\ je x_2 \neq x_1, \\ \dfrac{3x_1^2 + a}{2y_1} & ako\ je x_2 = x_1. \end{cases}$$

Sada se prirodno nameće pitanje kakva je struktura grupe $E(\mathbb{Q})$. Na to pitanje odgovor daje sljedeći važan teorem:

Teorem 1.1.3. *(Mordell-Weil). Neka je K polje algebarskih brojeva. Grupa $E(K)$ je konačno generirana Abelova grupa.*

Ovaj teorem je dokazao Mordell (1922) za $K = \mathbb{Q}$, a Weil (1928) općenito za polja algebarskih brojeva. Direktno iz prethodnog teorema i teorema o klasifikaciji konačno generiranih Abelovih grupa slijedi:

Korolar 1.1.4.

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

Torzijska grupa $E(\mathbb{Q})_{torz}$ sastoji se od svih točaka konačnog reda, odnosno ona je izomorfna produktu cikličkih grupa $\mathbb{Z}_{k_1} \times \cdots \times \mathbb{Z}_{k_m}$. Mazur je 1978. godine dokazao da $E(\mathbb{Q})_{torz}$ može biti izomorfna samo sa sljedećih 15 grupa:

$$\mathbb{Z}_k, \text{ za } k = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12$$
$$\mathbb{Z}_2 \times \mathbb{Z}_k, \text{ za } k = 2, 4, 6, 8.$$

Također za zadanu eliptičku krivulju imamo efikasne algoritme koji računaju torziju. Time je problem strukture torzijske grupe u potpunosti riješen te ostaje problem računanja r, broja nezavisnih točaka beskonačnog reda kojeg nazivamo *rang* od E. Ovaj problem do danas nije riješen i središnji je problem ovog rada. Dakle, ne postoji algoritam koji bi nalazio rang eliptičke krivulje. Napomenimo da postoji postupak traženja *ranga*, ali nije jasno da li postupak staje u konačno koraka.

Izomorfizmi eliptičkih krivulja

Kako smo napomenuli da će nas u ovom radu najviše zanimati grupovna struktura eliptičkih krivulja odnosno *rang* istih često će nas zanimati samo predstavnici izomorfnih krivulja. Pa pogledajmo izomorfizme među krivuljama.

Neka je dana eliptička krivulja u *Weierstrassovoj formi*. Izomorfne krivulje nad $\mathbb{Q}$ dobivamo zamjenom varijabli $x \mapsto u^2x + r, y \mapsto u^3y + su^2x + t$ gdje je $r, s, t \in \mathbb{Q}$ i $u \in \mathbb{Q}^*$. U slučaju *kratke Weierstrassove forme* imamo izomorfizam dan s $x \mapsto u^2x, y \mapsto u^3y, u \in \mathbb{Q}^*$. Valja napomenuti da je j-invarijanta izomorfnih krivuljama uvijek ista. Vrijedi i obrat, tj. dvije eliptičke krivulje su izomorfne nad algebarskim zatvorenjem od $\mathbb{Q}$ ako i samo ako imaju istu j-invarijantu.

Redukcija eliptičke krivulje modulo p

Promotrimo *kratku Weierstrassovu formu*

$$y^2 = x^3 + ax + b, \quad a, b \in \mathbb{Q}, \quad \Delta = 4a^3 + 27b^2 \neq 0$$

Za tako zadanu jednadžbu uvijek možemo izabrati u tako da gore danom zamjenom varijabli dobijemo izomorfnu krivulju u kojoj su $a, b \in \mathbb{Z}$ i $|\Delta|$ je minimalan u odnosu na sve njoj izomorfne krivulje. Takvu jednadžbu krivulje zovemo *minimalna* jednadžba od E.

Definicija 1.1.5. *Neka je zadana eliptička krivulja u minimalnoj kratkoj Weierstrassovoj formi $y^2 = x^3 + ax + b$ te prost broj $p \geq 5$, definiramo reduciranu krivulju modulo p kao $\overline{E} : y^2 = x^3 + \overline{a}x + \overline{b}$ gdje su $\overline{a} = a \pmod p, \overline{b} = b \pmod p$.*

Definicija 1.1.6. *Eliptička krivulja E ima **dobru redukciju** modulo p ako je s $\overline{E}$ dana nesingularna jednadžba. Kažemo da E ima **lošu redukciju** u p ako je s $\overline{E}$ dana singularna jednadžba.*

Da E ima lošu redukciju modulo p vrijedi kada kubni polinom $x^3 + \overline{a}x + \overline{b}$ ima višestruki korijen. Pogledajmo slučajeve loše redukcije:

1. Kažemo da E ima ***aditivnu redukciju*** modulo p ako $E \pmod p$ ima šiljak što vrijedi ako $x^3 + \overline{a}x + \overline{b}$ ima trostruki korijen, odnosno ako $p|4a^3 + 27b^2$ i $p| - 2ab$.

2. E ima ***multiplikativnu redukciju*** modulo p ako $\overline{E}$ ima čvor, što je slučaj kada $x^3 + \overline{a}x + \overline{b}$ ima dvostruki korijen, odnosno ako $p|4a^3 + 27b^2$ i $p \nmid -2ab$. Imamo dva slučaja *multiplikativne redukcije*:

   a) Rascjepiva ako su koeficijenti smjera tangenata u singularnoj točki iz $\mathbb{F}_p$ što vrijedi ako i samo ako je $-2ab$ kvadrat u $\mathbb{F}_p$.

b) Nerascjepiva ako nije rascjepiva.

Da bismo definirali analogne pojmove za $p \in \{2, 3\}$ trebamo raditi sa *Weierstrassovom formom* od E.

Eliptičke krivulje nad konačnim poljima

Definicija 1.1.7. *Ako E ima dobru redukciju modulo p onda je s* $\overline{E}$ *dana eliptička krivulja nad konačnim poljem* $\mathbb{F}_p$ *i pišemo* $E(\mathbb{F}_p)$.

Prisjetimo se da i ovdje vrijedi da je $E(\mathbb{F}_p)$ grupa uz prethodno definiranu operaciju zbrajanja. Nas će opet najviše zanimati struktura grupe i njen red $|E(\mathbb{F}_p)|$. Odmah iz jednadžbe od E vidimo da je $1 \leq |E(\mathbb{F}_p)| \leq 2p + 1$. To slijedi iz činjenice da je $\mathcal{O} \in E(\mathbb{F}_p)$ te da za svaki x postoje najviše dva $y - na$ tako da su kvadrat desne strane jednadžbe. No kako je $\mathbb{F}_p$ konačno generirana samo elementi oblika g^{2n}(g je generator grupe) mogu imati kvadratni korijen. Pa imamo $|E(\mathbb{F}_p)| \approx p + 1$. Još bolju informaciju nam daje sljedeći teorem.

Teorem 1.1.8. *(Hasse).*

$$q + 1 - 2\sqrt{q} \leq |E(\mathbb{F}_q)| \leq q + 1 + 2\sqrt{q}$$

Ovaj teorem je ključan u svim razmatranjima broja točaka na $E(\mathbb{F}_p)$, te se koristi u većini algoritama za nalaženje $|E(\mathbb{F}_p)|$ za dani p. Od tih algoritama spomenimo neke. $|E(\mathbb{F}_p)|$ možemo naći sljedećom formulom:

$$|E(\mathbb{F}_p)| = p + 1 + \sum_{x \in \mathbb{F}_p} \left(\frac{x^3 + ax + b}{p} \right).$$

Traženje reda gornjom formulom je složenosti $O(p\, ln^2 p)$ te je neprimjenjivo za $p > 1000$. Napomenimo ovdje da se u praksi koriste algoritmi sa boljom složenošću kao Shanks-Mestreova medotda složenosti $O(p^{1/4+\epsilon})$ te polinomijalni algoritam kojeg je dao Schoof složenosti $O(ln^8\, q)$.

Poglavlje 2

L-funkcije

L-funkcije eliptičkih krivulja prikupljaju "informacije" o eliptičkim krivuljama nad $\mathbb{F}_p$ za sve proste p te očekujemo da će nam reći nešto o ponašanju krivulje nad $\mathbb{Q}$, točnije o rangu, što nas u ovom radu najviše zanima. Kako je L-funkcija usko vezana za *zeta funkciju*, ona se može definirati preko njenog člana. Pogledajmo *zeta* funkciju za eliptičke krivulje:

$$Z(E(\mathbb{F}_p), T) = exp\left(\sum_{n=1}^{\infty} N_{p^n} \frac{T^n}{n}\right),$$

gdje je N_{p^n} broj točaka od E nad konačnim poljem $\mathbb{F}_{p^n}$, exp je eksponencijalna funkcija s bazom e. Može se dokazati([11, str. 143]) da je ova funkcija racionalna i sljedećeg oblika.

$$Z(E(\mathbb{F}_p), T) = \frac{L_p(T)}{(1-T)(1-pT)},$$

gdje je $L_p(T) = 1 - a_p T + pT^2$, te $a_p = p + 1 - Np$. Primijetimo da je L_p definiran samo u slučaju dobre redukcije E modulo p, za definiciju L-funkcije potrebno je proširiti L_p i u slučaju loše redukcije.

$$L_p(T) = \begin{cases} 1 - T & \text{ako E ima rascjepivu multiplikativnu redukciju u p,} \\ 1 + T & \text{ako E ima nerascjepivu multiplikativnu redukciju u p,} \\ 1 & \text{ako E ima aditivnu redukciju u p.} \end{cases}$$

Za ovako definiran L_p vrijedi relacija

$$L_p(1/p) = \widetilde{N}_p/p,$$

gdje je $\widetilde{N}_p$ broj nesingularnih točaka od E nad $\mathbb{F}_p$. Sada možemo definirati *L-funkciju*

Definicija 2.0.1. ***L-funkcija*** *eliptičke krivulje E nad $\mathbb{Q}$ je Eulerov produkt*

$$L_E(s) = \prod_{p\ prost} L_p(p^{-s})^{-1}$$

Gornji produkt se može napisati i kao red

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

Može se dokazati da ovaj $L_E(s)$ konvergira za sve $Re(s) > \frac{3}{2}$ te vrijedi sljedeći teorem.

Teorem 2.0.2. *Za L-funkciju postoji analitičko proširenje na cijelu kompleksnu ravninu te postoji funkcionalna relacija u vrijednostima funkcije u s i 2-s.*

Dokaz ovog teorema uključuje između ostalog rad Deuringa, Weila, Eichlera, Shimure te Wilesov Teorem o modularnosti. Nas će najviše zanimati slučaj kada je s=1. Još ćemo definirati konduktor od $E/\mathbb{Q}$, za to će nam trebati sljedeća funkcija.

$$f_p = \begin{cases} 0 & \text{ako E ima dobru redukciju u p,} \\ 1 & \text{ako E ima multiplikativnu redukciju u p,} \\ 2+\delta_p & \text{ako E ima aditivnu redukciju u p.} \end{cases}$$

Gdje je δ_p kompliciranije definirati (za više vidi [11, str. 450]). Ali imamo formulu koju je dao Ogg kojom možemo izračunati f_p u svim slučajevima.

$$f_p = ord_p(\Delta) + 1 - m_p,$$

gdje je m_p broj ireducibilnih komponenti na Neronovom modelu od E u p (vidi [11, poglavlje 15]) i Δ minimalna diskriminanta od E.

Definicija 2.0.3. ***Konduktor*** $N_{E/\mathbb{Q}}$ *se definira na sljedeći način:*

$$N_{E/\mathbb{Q}} = \prod_{pprost} p^{f_p}$$

Sada definiramo funkciju $\Lambda(E, s)$ koja nam daje precizniju verziju teorema (2.0.2).

$$\Lambda(E, s) = N_{E/\mathbb{Q}}^{s/2}(2\pi)^{-s}\Gamma(s)L_E(s),$$

gdje je $\Gamma(s) = \int_0^\infty t^{s-1}e^{-t}dt$.

Teorem 2.0.4. *Neka je $E/\mathbb{Q}$ eliptička krivulja. Tada za funkciju $\Lambda(E, s)$ postoji analitičko proširenje na cijelu kompleksnu ravninu i zadovoljena je sljedeća jednadžba*

$$\Lambda(E, s) = w_E\Lambda(E, 2-s) \text{ za neki } w_E = \pm 1.$$

Broj w_E je važan broj čije predznak još određuje da li je red izčezavanja od $L_E(s)$ u $s = 1$ paran ili neparan ali to ćemo detaljni vidjeti kasnije.

Poglavlje 3

Tate-Šafarevičeva grupa

U ovom poglavlju ćemo objasniti konstrukciju gore navedene grupe za koju se nadamo da će nam dati važnu informaciju o rangu.

3.1 p-adski brojevi

Počet ćemo definiranjem osnovnih pojmova potrebnih za konstrukciju navedene grupe.

Definicija 3.1.1. *Neka je K polje. Kažemo da je funkcija* $|\cdot|_v : K \mapsto \mathbb{R}$ ***apsolutna vrijednost*** *ako zadovoljava sljedeća tri uvjeta:*

1. $|x|_v \neq 0, x \in K$, *te* $|x|_v = 0$ *ako i samo ako* $x = 0$,
2. *Za sve* $x, y \in K$ *imamo* $|xy|_v = |x|_v|y|_v$,
3. $|x + y|_v \leq |x|_v + |y|_v \; x, y \in K$.

Pogledajmo sada jedan skup nama korisnih apsolutnih vrijednosti nad $\mathbb{Q}$. Neka je p prost broj. Svaki nenul element a iz $\mathbb{Q}$ možemo prikazati kao $a = p^r \frac{m}{n}$ gdje su $m, n \in \mathbb{Z}$ i $p \nmid n, m$. Definiramo $|a|_p = \frac{1}{p^r}, a \neq 0$ te $|0|_p = 0$. Odmah se vidi da je $|\cdot|_p$ apsolutna vrijednost na $\mathbb{Q}$. Također s apsolutnom vijednosti imamo i metriku d_p na $\mathbb{Q}$ danu s $d_p(a, b) = |a - b|_p$. Primijetimo da su a i b blizu ako je njihova razlika djeljiva s velikom potencijom od p. Ovako definiranim apsolutnim vrijednostima analogno konstrukciji od $\mathbb{R}$ možemo definirati zatvorenje od $\mathbb{Q}$ za svaki prost broj p. Za niz (a_n) kažemo da je ***Cauchyev***(za p-adsku metriku) ako za svaki $\epsilon > 0$ postoji N_ϵ takav da vrijedi $|a_m - a_n|_p < \epsilon$ kada su $m, n > N_\epsilon$. Niz (a_n) konvergira prema a ako za svaki $\epsilon > 0$ postoji N_ϵ takav da je $|a_n - a| < \epsilon$ za sve $n > N_\epsilon$. Neka je R skup svih Cauchyevih nizova u $\mathbb{Q}$(za p-adsku metriku). R je prsten. Neka je I skup svih nizova u R koji konvergiraju k 0. Tada je I ideal u R te $\mathbb{Q}_p$ definiramo kao kvocijentni prsten R/I. Kažemo da je $\mathbb{Q}_p$ *zatvorenje* od $\mathbb{Q}$. Kao što smo napomenuli za

standardnu apsolutnu vrijednost ovim postupkom dobijemo $\mathbb{R}$. Analogno kao za R vrijedi sljedeći teorem.

Teorem 3.1.2. *$\mathbb{Q}_p$ je polje, te je zatvoreno. Odnosno svaki Cauchyev niz u $\mathbb{Q}_p$ ima jedinstven limes u $\mathbb{Q}_p$.*

3.2 Galoisova kohomologija

U ovom poglavlju objasnit ćemo kratko osnovna svojstva kohomologije grupa. Kako su nama potrebne samo grupe H^1 i H^2 zadržat ćemo se samo na njihovim definicijama te osnovnim nama potrebnim rezultatima.

Definicija 3.2.1. *Neka je G konačna grupa, neka je M Abelova grupa. Kažemo da grupa G **(lijevo) djeluje** na M ako postoji preslikavanje $G \times M \mapsto M$ tako da*

1. $\sigma(m + m') = \sigma m + \sigma m', \forall \sigma \in G,\ \forall m, m' \in M,$
2. $(\sigma\tau)(m) = \sigma(\tau m)\ \forall \sigma, \tau \in G,\ \forall m \in M,$
3. $1_G m = m,\ \forall m \in M.$

Zadati djelovanje od G na M je isto kao i zadati homomorfizam $G \mapsto Aut(M)$. *G-modul M* je abelova grupa zajedno s djelovanjem od G na M. Neka su M i N G-moduli. *Homomorfizam G-modula* je homomorfizam $\phi : M \mapsto N$ koji komutira s djelovanjem od G, tj. vrijedi $\phi(\sigma m) = \sigma\phi(m)$ za $\forall \sigma \in G$. Definirajmo sada nama važnu grupu *G-invarijantnih* elemenata, tj. elemenata koje G fiksira.

Definicija 3.2.2. *Nulta kohomološka grupa koju označavamo s $H^0(G, M)$ ili M^G je sljedeći skup:*

$$H^0(G, M) = \{m \in M | \sigma(m) = m, \forall \sigma \in G\}.$$

Neka je dan *egzaktan niz G-modula*

$$0 \longrightarrow P \xrightarrow{\phi} M \xrightarrow{\psi} N \longrightarrow 0,$$

gdje su ϕ i ψ homomorfizmi G-modula takvi da je ϕ injekcija, ψ surjekcija te vrijedi $Img(\phi) = Ker(\psi)$. Može se pokazati da za G-invarijante vrijedi sljedeći egzaktni niz:

$$0 \longrightarrow P^G \xrightarrow{\phi} M^G \xrightarrow{\psi} N^G,$$

ali ne vrijedi da je ψ surjekcija.

Definicija 3.2.3. *Neka je M G-modul. Definiramo grupu 1-kolanaca (s G u M) kao*

$$C^1(G,M) = \{preslikavanja\ \xi : G \mapsto M\}.$$

Grupa 1-kociklusa je dana s

$$Z^1(G,M) = \left\{\xi \in C^1(G,M) \mid \xi(\sigma\tau) = \xi(\sigma) + \sigma\xi(\tau),\ \forall \sigma,\tau \in G\right\}$$

Grupu 1-korubova definiramo s

$$B^1(G,M) = \left\{\xi \in C^1(G,M) \mid postoji\ m \in M\ takav\ da\ \xi(\sigma) = \sigma m - m,\ \forall\ \sigma \in G\right\}$$

Raspisivanjem lijeve i desne strane izraza $\xi(\sigma\tau) = \xi(\sigma)+\sigma\xi(\tau)$ za $\xi \in B^1(G,M)$ odmah vidimo da vrijedi $B^1(G,M) \subset Z^1(G,M)$ te možemo definirati sljedeću važnu grupu.

Definicija 3.2.4. ***Prva kohomološka grupa*** *G-modula M je kvocijentna grupa*

$$H^1(G,M) = \frac{Z^1(G,M)}{B^1(G,M)}$$

Napomena 3.2.5. *Ako je djelovanje od G na M trivijalno tada direktno iz definicije slijedi* $H^0(G,M) = M$ *i* $H^1(G,M) = Hom(G,M)$.

Sada navodimo nama jako korisnu propoziciju.

Propozicija 3.2.6. *Neka je dan egzaktan niz G-modula*

$$0 \longrightarrow P \xrightarrow{\phi} M \xrightarrow{\psi} N \longrightarrow 0$$

tada postoji dugi egzaktni niz

$$0 \to H^0(G,P) \to H^0(G,M) \to H^0(G,N) \xrightarrow{\delta} H^1(G,P) \to H^1(G,M) \to H^1(G,N),$$

gdje δ definiramo na sljedeći način. Neka je $n \in H^0(G,N) = N^G$. Biramo $m \in M$ tako da $\psi(m) = n$ i definiramo kolanac $\xi \in C^1(G,M)$, sa $\xi(\sigma) = \sigma(m) - m$. Pogledajmo

$$\psi(\xi(\sigma)) = \psi(\sigma(m) - m) = \psi(\sigma(m)) - \psi(m) = \sigma(\psi(m)) - n = \sigma(n) - n = n - n = 0.$$

Slijedi $\xi(\sigma) \in Ker(\psi)$, $\forall\sigma \in G$, te iz $Img(\phi) = Ker(\psi)$ imamo $\xi \in Img(\phi)$. Preko inverza od ϕ na $Img(\phi)$ možemo smatrati da je $\xi \in Z^1(G,P)$. Konačno definiramo $\delta(n)$ kao kohomološku klasu od ξ u $H^1(G,P)$.

Napomena 3.2.7. *Primijetimo da rezultati vrijede za konačne grupe G. Također vrijede analogni rezultati i za slučaj kad je G Galoisova grupa, koji ćemo koristiti.*

3.3 Izogenije

Sad ćemo kratko pogledati preslikavanja između eliptičkih krivulja. Kako eliptičke krivulje imaju istaknutu točku O prirodno je gledati preslikavanja koja poštuju to svojstvo. Takva preslikavanja se nazivaju izogenije te ćemo dati kratak pregled osnovnih činjenica.

Definicija 3.3.1. *Neka su E_1 i E_2 eliptičke krivulje.* ***Izogenija*** *iz E_1 u E_2 je morfizam $\phi : E_1 \mapsto E_2$ koji zadovoljava $\phi(O) = O$.*

Lema 3.3.2. *Neka je $m \in \mathbb{Z}$, $m \neq 0$ i K algebarsko zatvoreno polje. Tada vrijedi $[m](E(K)) = E(K)$.*

Također vrijedi da je svaka izogenija homomorfizam grupa. Pogledajmo skup izogenija od E_1 na E_2 u oznaci

$$Hom(E_1, E_2) = \{izogenije\ E_1 \mapsto E_2\},$$

što tvori grupu uz definiranje sume na sljedeći način

$$(\phi + \psi)(P) = \phi(P) + \psi(P).$$

Nadalje za $E_1 = E_2$ gornja grupa gdje operaciju množenja definirano kompozicijom $(\phi\psi)(P) = \phi(\psi(P))$ nam da je prsten u sljedećej oznaci

$$End(E) = Hom(E, E),$$

kojeg zovemo *prsten endomorfizama* od E. Nas će najviše zanimati izogenije *množenje s m* za $m \in \mathbb{Z}$

$$[m] : E \mapsto E \ \text{ gdje je } \ [m](P) = \underbrace{P + P + \ldots + P}_{\text{m puta}}.$$

Primijetimo da za $m < 0$ definiramo $[m](P) = [-m](-P)$. Ovdje ćemo pogledati preslikavanje

$$[] : \mathbb{Z} \mapsto End(E)$$

koje je bijekcija za većinu eliptičkih krivulja, drugim riječima preslikavanje m u *množenje s m* za $m \in \mathbb{Z}$. Za većinu krivulja E nam daje $End(E) \cong \mathbb{Z}$, a ostale su zanimljiv skup krivulja za koje imamo sljedeću definiciju.

Definicija 3.3.3. *Neka je E/K eliptička krivulja nad poljem algebarskih brojeva K. Ako je $End(E) \supsetneq \mathbb{Z}$ kažemo da E ima* ***kompleksno množenje****.*

3.4 Definicija Tate-Šafarevičeve grupe

Kako naslov kaže, ovdje ćemo definirati ključnu grupu za našu slutnju. Pa krenimo od notacije.

$\overline{K}$ je algebarsko zatvorenje od K gdje je K polje algebarskih brojeva. Nama će najčešće biti $K = \mathbb{Q}$.

$E(K)[m]$ je jezgra množenja s m $[m] : E(K) \mapsto E(K)$.

$mE(K)$ je slika od $[m] : E(K) \mapsto E(K)$.

G je Galoisova grupa $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$.

M_K je skup apsolutnih vrijednosti na K, nas će zanimati $M_{\mathbb{Q}}$ što možemo izjednčiti s prostim brojevima za p-adske apsolutne vrijednosti i ∞ za standardnu apsolutnu vrijednost.

Za eliptičku krivulju E, te izogeniju *množenja s m* postoji sljedeći egzaktni niz.

$$0 \longrightarrow E(\overline{\mathbb{Q}})[m] \longrightarrow E(\overline{\mathbb{Q}}) \xrightarrow{[m]} E(\overline{\mathbb{Q}}) \longrightarrow 0.$$

Sada upotrebom propozicije dobijemo dugi egzaktni niz.

$$0 \longrightarrow E(\mathbb{Q})[m] \longrightarrow E(\mathbb{Q}) \xrightarrow{[m]} E(\mathbb{Q}) \xrightarrow{\delta} H^1(G, E(\overline{\mathbb{Q}})[m]) \xrightarrow{\psi} H^1(G, E(\overline{\mathbb{Q}})) \xrightarrow{[m]} H^1(G, E(\overline{\mathbb{Q}})).$$

Sada čitamo iz gornjeg egzaktnog niza $Ker(\delta) = Im([m]) = mE(\mathbb{Q})$ pa po prvom teoremu o izomorfizmu i iz $Im(\psi) = Ker([m]) = H^1(G, E(\mathbb{Q}))$ imamo sljedeći egzaktni niz:

$$0 \longrightarrow \frac{E(\mathbb{Q})}{mE(\mathbb{Q})} \xrightarrow{\delta} H^1(G, E(\overline{\mathbb{Q}})[n]) \longrightarrow H^1(G, E(\overline{\mathbb{Q}}))[n] \longrightarrow 0.$$

Analogno gornjem, dobijemo egzaktan niz za p-adske brojeve

$$0 \longrightarrow \frac{E(\mathbb{Q}_p)}{mE(\mathbb{Q}_p)} \xrightarrow{\delta} H^1(G_p, E(\overline{\mathbb{Q}_p})[n]) \longrightarrow H^1(G_p, E(\overline{\mathbb{Q}_p}))[n] \longrightarrow 0.$$

gdje je $G_p = Gal(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ Pogledajmo sada vezu između ova dva niza. Neka je $\overline{\mathbb{Q}_p}$ neko algebarsko zatvorenje od $\mathbb{Q}_p$. Ulaganje $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ se proširuje na ulaganje $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}_p}$,

$$\begin{array}{ccc} \overline{\mathbb{Q}} & \longrightarrow & \overline{\mathbb{Q}_p} \\ \uparrow & & \uparrow \\ \mathbb{Q} & \longrightarrow & \mathbb{Q}_p \end{array}$$

Djelovanje od G_p na $\overline{\mathbb{Q}} \subset \overline{\mathbb{Q}_p}$ definira homomorfizam $G_p \mapsto G$. Nadalje, svaki 1-kociklus $G \mapsto E\left(\overline{\mathbb{Q}_p}\right)$ definira kompozicijom 1-kociklus $G_p \mapsto E(\mathbb{Q}_p)$. Na ovaj način dobijemo homomorfizam $H^1(G, E(\overline{\mathbb{Q}})) \mapsto H^1(G_p, E(\overline{\mathbb{Q}_p}))$, koji je neovisan o izboru ulaganja $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$. Kako što gore navedeno vrijedi za sve proste p te za standardnu apsolutnu vrijednost gdje ćemo označavati $\mathbb{Q}_\infty = \mathbb{R}$, imamo sljedeći komutativni diagram.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \frac{E(\mathbb{Q})}{mE(\mathbb{Q})} & \longrightarrow & H^1(G, E(\overline{\mathbb{Q}})) & \longrightarrow & H^1(G, E(\overline{\mathbb{Q}}))[m] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \prod\limits_{p \in M_{\mathbb{Q}}} \frac{E(\mathbb{Q}_p)}{mE(\mathbb{Q}_p)} & \longrightarrow & \prod\limits_{p \in M_{\mathbb{Q}}} H^1(G_p, E(\overline{\mathbb{Q}_p})) & \longrightarrow & \prod\limits_{p \in M_{\mathbb{Q}}} H^1(G_p, E(\overline{\mathbb{Q}_p}))[m] & \longrightarrow & 0 \end{array} \tag{3.1}$$

Ovdje ćemo definirati, ne manje važnu Selmerovu grupu, te konačno i Tate-Šafarevićenvu grupu koja će nas dalje zanimati.

Definicija 3.4.1. *Selmerovu grupu $S^{(n)}(E/\mathbb{Q})$ definiramo na sljedeći način:*

$$S^{(n)}(E/\mathbb{Q}) = Ker\left\{H^1(G, E(\overline{\mathbb{Q}})[n]) \longrightarrow \prod_{p \in M_{\mathbb{Q}}} H^1(G_p, E(\mathbb{Q}_p))\right\}.$$

Definicija 3.4.2. *Tate-Šafarevičeva grupa $Ш(E/\mathbb{Q})$ je podgrupa od $H^1(G, E(\mathbb{Q}^{al}))$ definirana s*

$$Ш(E/\mathbb{Q}) = Ker\left\{H^1(G, E(\overline{\mathbb{Q}})) \longrightarrow \prod_{p \in M_{\mathbb{Q}}} H^1(G_p, E(\mathbb{Q}_p))\right\}.$$

Ova zanimljiva grupa je ključna u rješavanju pitanja ranga za eliptičke krivulje. Od posebne važnosti je pitanje konačnosti ove grupe. Uvriježeno je mišljenje da je ova grupa konačna te se očekuje istinitost sljedeće slutnje.

Slutnja 3.4.3. *Tate-Šafarevićeva grupa $Ш(E/\mathbb{Q})$ je konačna za svaku elipitčku krivulju $E/\mathbb{Q}$.*

Istintost ove slutnje bi nam dala algoritam za nalaženje ranga eliptičke krivulje. Jedan korak k rješenju ove slutnje dao je Cassels sljedećim teoremom. Iako se dokaz ove slutnje čini dalekim, ipak su Rubin i Kolyvagin dali važan doprinos riješenju kao što ćemo ubrzo vidjeti. Pogledajmo još jedan zanimljiv rezultat Casselsa koji upućuje na zanimljivu činjenicu o redu grupe za koju ne znamo je li konačna.

Teorem 3.4.4. *Neka je E/K eliptička krivulja nad algebarskim poljem K. Postoji alternirajuće bilinearno sparivanje*

$$\Gamma : Ш(E/K) \times Ш(E/K) \mapsto \mathbb{Q}/\mathbb{Z}$$

čija je jezgra sa svake strane podgrupa djeljivih elemenata od $Ш(E/K)$. Drugim riječima, ako $\Gamma(\alpha, \beta) = 0$ za sve $\beta \in Ш(E/K)$, tada za svaki cijeli broj $N \geq 1$ postoji $\alpha_N \in Ш(E/K)$ takav da vrijedi $N\alpha_N = \alpha$. Posebno vrijedi da je, ako je $Ш(E/K)$ konačna grupa, red grupe kvadrat prirodnog broja.

Pogledat ćemo još i alternativnu definiciju Tate-Šafarevičeve grupe, odnosno njenu geometrijsku interpretaciju.

Definicija 3.4.5. *Neka je $E/\mathbb{Q}$ eliptička krivulja. **(Glavni) homogeni prostor** ili **torzor** od $E/\mathbb{Q}$ je glatka krivulja $C/\mathbb{Q}$ zajedno sa slobodno tranzitivnim grupovnim djelovanjem od E na C nad $\mathbb{Q}$. Drugim riječima, homogeni prostor za $E/\mathbb{Q}$ sastoji se od para (C, μ) gdje je $C/\mathbb{Q}$ glatka krivulja i $\mu : C(\overline{\mathbb{Q}}) \times E(\overline{\mathbb{Q}}) \mapsto C(\overline{\mathbb{Q}})$ je morfizam koji ima sljedeća svojstva*

1. *$\mu(a, O) = a$ za sve $a \in C(\overline{\mathbb{Q}})$,*
2. *$\mu(\mu(a, P), Q) = \mu(q, P + Q)$ za sve $a \in C(\overline{\mathbb{Q}})$ i $P, Q \in E(\overline{\mathbb{Q}})$,*
3. *Za sve $a, b \in C(\overline{\mathbb{Q}})$ postoji jedinstveni $P \in E(\overline{\mathbb{Q}})$ takav da je $\mu(a, P) = b$.*

Ovdje je prirodno pisati $\mu(a, P) = a + P$. Primijetimo da je uvijek jasno o kojo operaciji zbrajanja se radi. Također možemo definirati operaciju oduzimanja kako iz svojstva (3.) imamo za $a, b \in C(\overline{\mathbb{Q}})$ $a - b = P$ gdje je $P \in E(\overline{\mathbb{Q}})$ jedinstven, takav da $a + P = b$.

Definicija 3.4.6. *Dva homogena prostora $C/\mathbb{Q}$ i $C'/\mathbb{Q}$ su ekvivalentna ako postoji izomorfizam $\Phi : C \mapsto C'$ definiran nad $\mathbb{Q}$ koji je kompatibilan s djelovanjem od E na C i na C', tj.*

$$\Phi(a + P) = \Phi(a) + P.$$

Sada imamo definiciju *Weil − Châteletove* grupe $WC(E/\mathbb{Q})$ kao skup klasa ekvivalencije homogenih prostora. Sljedeći teorem nam daje alternativnu definiciju Tate-Šafarevičeve grupe.

Teorem 3.4.7. *Ako je $E/\mathbb{Q}$ eliptička krivulja. Tada postoji bijekcija*

$$WC(E/\mathbb{Q}) \mapsto H^1(G, E(\overline{\mathbb{Q}}))$$

definirana na sljedeći način: Neka je C torzor od E, izaberimo proizvoljnu točku $p_0 \in C(\overline{\mathbb{Q}})$. Preslikavamo

$$[C] \mapsto [\sigma \mapsto p_0^\sigma - p_0]$$

gdje uglatim zagradama označavamo klasu ekvivalencije.

Sada imamo ekvivalentnu definiciju Tate-Šafarevičeve grupe

$$Ш(E/\mathbb{Q}) = Ker\left\{WC(E/\mathbb{Q}) \longrightarrow \prod_{p \in M_{\mathbb{Q}}} WC(E/\mathbb{Q}_p)\right\}$$

Elemente Tate-Šafarevičeve grupe možemo gledati kao torzore od E koji su svugdje lokalno trivijalni.

Poglavlje 4

Birch i Swinnerton-Dyerova slutnja

4.1 Iskaz Birch i Swinnerton-Dyerove slutnje

U ovom poglavlju iskazat ćemo navedenu snažnu slutnju, te vidjeti koliko očekujemo da je snažna veza među dosad definiranim objektima kao što su L-funkcija i rang eliptičke krivulje. Vidjet ćemo koji su dokazi koji ju podupiru i koje su njezine posljedice. Krenimo od prve ideje te pogledajmo razvoj slutnje.

Neka je E eliptička krivulja nad $\mathbb{Q}$. Sjetimo se da je $N_p = |\overline{E}(\mathbb{F}_p)|$, gdje je $\overline{E}$ redukcija od E nad $\mathbb{F}_p$. Jedna ideja je da je $rang(E(\mathbb{Q}))$ vezan za veličinu grupe $\overline{E}(\mathbb{F}_p)$. Za svaki p u kojem E ima dobru redukciju postoji preslikavanje $E(\mathbb{Q}) \mapsto \overline{E}(\mathbb{F}_p)$, ali općenito preslikavanje je daleko od toga da bude injektivno ili surjektivno. Na primjer ako je $E(\mathbb{Q})$ beskonačna, tada i jezgra mora biti beskonačna. No ako je $E(\mathbb{Q})$ konačna ($|E(\mathbb{Q})| \leq 16$) tada je narušena surjektivnost za sve veće p (zato što $|E(\mathbb{F}_p)| \geq p + 1 - 2\sqrt{p}$).

Kasnih 50-ih godina prošlog stoljeća, Birch i Swinnerton-Dyer smatrali su da za veće (većeg ranga) $E(\mathbb{Q})$ su i N_p veći nego obično. Na Cambridgeu su imali pristup jednom od rijetkih računala u to vrijeme, te su mogli testirati tu ideju za velike P (velike koliko je računalo bilo brzo). Neka je

$$f(P) = \prod_{p \leq P} \frac{N_p}{p}$$

Sjetimo se da je $N_p \approx p$. Njihovi izračuni su ih doveli do sljedeće slutnje.

Slutnja 4.1.1. *Za svaku eliptičku krivulju nad $\mathbb{Q}$, postoji konstanta C takva da vrijedi*

$$\lim_{P \to \infty} f(P) = C \log(P)^r$$

gdje je $r = rang(E(\mathbb{Q}))$

Birch i Swinnerton-Dyer su mogli prilično konzistento predvidjeti rang ali su otkrili da $f(P)$ jako oscilira kako se P povećava te da je teško naći C. Te su svoju slutnju izrazili pomoću L-funkcije koja, sjetimo se, također prikuplja "informacije" o $\overline{E}(\mathbb{F}_p)$ za sve p. t Također smo rekli da je L-funkcija definirana na cijeloj kompleksnoj ravnini pa tako i u 1. Izreci mo sada slutnju jednog od milenijskih problema.

Slutnja 4.1.2. *(Birch i Swinnerton-Dyer, slaba verzija). Neka je $E/\mathbb{Q}$ eliptička krivulja. Tada Taylorov razvoj od $L_E(s)$ za s=1 ima sljedeći oblik*

$$L_E(s) = c(s-1)^r + \text{članovi višeg reda}$$

gdje je $c \neq 0$ i $r = rang(E/\mathbb{Q})$.

Posebno vrijedi $L_E(1) = 0 \Leftrightarrow E(\mathbb{Q})$ je beskonačna. Prije nego što pogledamo detaljnije rezultate koji podupiru ovu slutnju i daljni razvoj dat ćemo i jaču verziju koja nam govori kolika je konstanta c u gornjoj jednadžbi. Ta verzija uključuje red Tate-Šafarevičeve grupe te još neke vrijednosti koje ćemo sad kratko definirati. Neka je eliptička krivulja dana u minimalnoj Weierstrassovj formi

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

Sjetimo se da je jednadžba minimalna ako je $|\Delta|$ minimalan za sve izomorfne jednadžbe. Definiramo *invarijantni diferencijal*

$$\omega = \frac{dx}{2y + a_1x + a_3}$$

te definiramo

$$\Omega = \int_{E(\mathbb{R})} |\omega|$$

Nadalje definiramo važnu funkciju *kanonsku visinu* $\hat{h}(\mathbb{Q}) \mapsto \mathbb{R}$. Koja ima važna svojstva i ključna je za dokaz Mordell-Weilovog teorema. Prvo definirajmo *naivnu visinu* $H(\frac{m}{n}) = max\{|m|, |n|\}$ te *logaritamsku visinu* za $P = (x, y) \in E(\mathbb{Q})$ sa $h(P) = lnH(x)$ te $H(\mathcal{O}) = 0$. Definiramo kanonsku visinu s

$$\hat{h} = \lim_{n\to\infty} \frac{h(2^nP)}{4^n}.$$

Još nam je potrebno $Néron - Tateovo$ sparivanje visina točaka $P, Q \in E(\mathbb{Q})$

$$\langle P, Q\rangle = \frac{1}{2}(\hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)).$$

Definicija 4.1.3. *Eliptički regulator od $E(\mathbb{Q})$, u oznaci $R_{E(\mathbb{Q})}$, je definiran na sljedeći način. Biramo točke $P_1, P_2, \ldots, P_r \in E(\mathbb{Q})$ koje generiraju $E(\mathbb{Q})/E(\mathbb{Q})_{tors}$, te je*

$$R_{E(\mathbb{Q})} = det\left(< P_i, P_j >\right)_{1\leq i,j\leq r}.$$

Ako je r=0, definiramo $R(E(\mathbb{Q})) = 1$.

Još je nužno definirati c_p za to se vratimo p-adskim brojevima, te $E(\mathbb{Q}_p)$. Definiramo

$$E_0(\mathbb{Q}_p) = \left\{P \in E(\mathbb{Q}_p) \mid \overline{P}\text{nije singularna točka}\right\}.$$

gdje je $\overline{P}$ slika od P u $E(\mathbb{F}_p)$. Imamo $c_p = |E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)|$ Napomenimo da ako E ima dobru redukciju u p vrijedi $c_p = 1$. Za sve gore definirane vrijednosti imamo algoritme za njihovo računanje te su one dobro poznate za široki skup eliptičkih kriuvlja. Stoga sada možemo iskazati jaču verziju naše slutnje.

Slutnja 4.1.4. *(Birch i Swinnerton-Dyerova slutnja, jača verzija). Neka je $E/\mathbb{Q}$ eliptička krivulja te neka je $r = rang(E(\mathbb{Q}))$. Tada vrijedi*

$$\lim_{s\to 1} \frac{L_E(s)}{(s-1)^r} = \frac{\Omega Ш(E/\mathbb{Q})R_{E(\mathbb{Q})} \prod_p c_p}{|E(\mathbb{Q})_{torz}|^2}.$$

4.2 Napredak i rezultati

Počevši s radom Bircha i Swinnerton-Dyera, jako puno numeričkih rezultata snažno podupire gornje dvije slutnje. Kao što smo rekli, sve vrijednosti jače slutnje možemo izračunati, osim reda grupe $Ш(E/\mathbb{Q})$. Kako ne znamo red grupe, jednadžbu u jačoj verziji koristimo za pretpostavljenu vrijednost za $|Ш|$, koja u svim izračuntaim slučajevima ispadne kvadrat cijelog broja, što se slaže s Casselsovim teoremom. Ovo dodatno podupire slutnju. Osvrnimo se na izogene krivulje koje, kao što smo spomenuli, imaju isti rang. Izogene krivulje također imaju isti broj točaka modulo p za svaki prost p pa slijedi da imaju istu L-funkciju. Zaključujemo da bi, kada bi slutnja vrijedila, izraz

$$\frac{\Omega Ш(E/\mathbb{Q})R(E(\mathbb{Q})) \prod_p c_p}{|E(\mathbb{Q})_{torz}|^2}$$

morao biti invarijanta za izogene krivulje. Cassels je to dokazao uz pretpostavku da je $Ш(E/\mathbb{Q})$ konačna grupa. Zanimljivo je da niti jedna vrijednost ne mora biti ista za izogene krivulje.

Intuitivno se čini da je najpristupačniji dio slutnje 4.1.2 probati dokazati $rang(E(\mathbb{Q})) \geq 1$ povlači $L_E(1) = 0$. To su za eliptičke krivulje s kompleksnim množenjem dokazali Coates i Wiles. Ovdje navodimo pojednostavljenu verziju njihovog teorema.

Teorem 4.2.1. *Neka je E eliptička krivulja definirana nad $\mathbb{Q}$ s kompleksnim množenjem. Ako je $rang(E(\mathbb{Q})) \geq 1$ vrijedi $L_E(1) = 0$.*

Dokaz. Vidi [2]. □

Posebno je ovaj teorem primjenjiv na krivulje $y^2 = x^3 - Dx$ gdje je $D \in \mathbb{Q},\ D \neq 0$, a to su krivulje koje su Birch i Swinnerton-Dyer originalno proučavali. Djelomični obrat ovog teorema dao je Greenberg ovim zanimljivim rezultatom.

Teorem 4.2.2. *Neka je E eliptička krivulja definirana nad $\mathbb{Q}$ s kompleksnim množenjem. Ako $L_E(s)$ ima neparan red nultočke za $s = 1$ onda $rang(E(\mathbb{Q})) \geq 1$ ili je p − primarna podgrupa Tate-Šafarevičeve grupe $Ш(E(\mathbb{Q}))$ beskonačna za sve proste p gdje E ima dobru redukciju (osim eventualno za $p = 2$ ili 3).*

Dokaz. Vidi [4]. □

I ovaj teorem naglašava važnost Tate-Šafarevičeve grupe odnosno pitanja njene konačnosti. Sljedeći važan teorem objavili su Gross i Zagier 1986. godine.

Teorem 4.2.3. *Pretpostavimo da je $L_E(1) = 0$ za eliptičku krivulju $E/\mathbb{Q}$. Tada postoji racionalna točka $P \in E(\mathbb{Q})$ takva da $L'_E(1) = \alpha \cdot \Omega \cdot \langle P, P \rangle$ sa $\alpha \in \mathbb{Q}^\times$. Posebno, vrijedi*

1. *Ako je $L'_E(1) \neq 0$, tada $E(\mathbb{Q})$ sadrži točke beskonačnog reda.*
2. *Ako je $L'_E(1) \neq 0$ i $rang(E(\mathbb{Q})) = 1$ tada vrijedi $L'_E(1) = \alpha\, \Omega\, R_{E/\mathbb{Q}}$ za neki racionalni broj $\alpha \neq 0$.*

Dokaz. Ovdje su Gross i Zagier dokazali vezu između $L'_E(1)$ i kanonske visine točke iz $E(\mathbb{Q})$ zvane *Heegnerova točka*. Za dokaz i detalje vidi [5] □

Rubin ovim snažnim rezultatom daje prvi primjer konačne Tate-Šafarevičeve grupe. Ovdje ćemo navesti samo jedan dio teorema.

Teorem 4.2.4. *Neka je E eliptička krivulja definirana nad $\mathbb{Q}$ poljem K s kompleksnim množenjem. Ako je $L_E(1) \neq 0$ tada je $Ш(E/\mathbb{Q})$ konačna grupa.*

Za potpuni iskaz teorema i dokaz vidi, [10]. Nadalje, Rubin daje ovaj rezultat.

Teorem 4.2.5. *Neka je E eliptička krivulja definirana nad $\mathbb{Q}$ s kompleksnim množenjem. Ako je $rang(E(\mathbb{Q})) \geq 2$ tada red nultočke od $L_E(1)$ veći ili jednak 2.*

Ovaj teorem s (4.2.1) i (4.2.3) ima sljedeći direktni korolar.

Korolar 4.2.6. *Neka je E eliptička krivulja definirana nad $\mathbb{Q}$ s kompleksnim množenjem. Ako je r red nultočke od $L_E(1) \leq 1$, tada je $rang(E(\mathbb{Q}))$ jednak toj vrijednosti r.*

Kolyvagin je proširio ove razultate Rubina na modularne krivulje, te dokazom teorema o modularnosti imamo sljedeći rezultat.

Teorem 4.2.7. *(Gross-Zagier, Kolyvagin) Ako je rang*$(E(\mathbb{Q})) \leq 1$ *tada vrijedi rang*$(E(\mathbb{Q}))$ *je jednak redu nultočke funkcije* $L_E(1)$*.*

Ovo je dosad najači rezultat koji podupire slutnju (4.1.2), drugim riječim gornji teorem kaže da (4.1.2) vrijedi za sve krivulje ranga ≤ 1 . Također imamo da vrijedi

$$L_E(1) \neq 0 \;\Rightarrow\; E(\mathbb{Q}) \; i \; Ш(E) \text{ su konačne grupe.}$$

Pogledajmo nedavno objavljene rezultate vezane za Birch i Swinnerton Dyerovu slutnju. Rad Bhargave, Skinnera i Zhanga iz 2014. godine daje procjenu koliko "mnogo" krivulja zadovoljava našu slutnju. Ovdje ćemo uvesti još jednu visinu da bi mogli točno izeći njihov rezultat. Krenuti ćemo od sljedeće činjenice. Svaka eliptička krivulja $E/\mathbb{Q}$ je izomorfna jedinstvenoj krivulji oblika $E_{A,B} : y^2 = x^3 + Ax + B$ gdje su $A, B \in \mathbb{Z}$ i za sve proste brojeve p vrijedi $p^6 \nmid B$ ako $p^4 \mid A$. Tada definiramo visinu $\hat{H}$ od $E = E_{A,B}$ kao

$$\hat{H}(E_{A,B}) = max\left\{4|A^3|, 27B^2\right\}.$$

Teorem 4.2.8. *Najmanje* $66,48\%$ *eliptičkih krivulja definiranih nad* $\mathbb{Q}$*, kada su poredane po visini* $\hat{H}$*, zadovoljava (4.1.2).*

Teorem 4.2.9. *Najmanje* $66,48\%$ *eliptičkih krivulja definiranih nad* $\mathbb{Q}$*, kada su poredane po visini* $\hat{H}$*, ima konačnu grupu* $Ш(E(\mathbb{Q}))$*.*

Iako ovaj postotak ovisi o odabiru visine ova dva teorema ipak vrijede za većinu krivulja. Važno je napomenuti da autori ustvari dokazuju da je većina krivulja ranga ≤ 1 (vidi [1]), čak se sluti da 100% krivulja ima rang ≤ 1. Te iz (4.2.7) slijedi da takve krivulje zadovoljavaju (4.1.2).

Završit ćemo jednim zanimljivim rezultatom o parnosti ranga. Počnimo s još jednom snažnom slutnjom.

Slutnja 4.2.10. *(Slutnja parnosti). Neka je r rang eliptičke krivulje* E/K*. Tada*

$$(-1)^r = w_E$$

Tim i Vladimir Dokchitser daju mnoge snažne rezultate koji podupiru ovu slutnju. Dokazuju da konačnost Tate-Šafarevičeve grupe povlači slutnju parnosti, te daju formulu za w_E pa time i za parnost ranga. Za više o njihovom radu vidi [3].

4.3 Posljedice

Iako istinitost Birch i Swinnerton-Dyerove slutnje povlači razne rezultate, ovdje ćemo detaljnije promotriti 2000 godina star problem iz teorije brojeva. To je problem kongruentnih brojeva. Pozitivan broj $r \in \mathbb{Q}$ je kongruentan ako postoji pravokutni trokut s racionalnim stranicama koji ima površinu r. Pretpostavimo da je $r \in \mathbb{Q}$ kongruentan broj i $X, Y, Z \in \mathbb{Q}$ stranice pravokutnog trokuta s površinom r. Za svaki takav $r \in \mathbb{Q}$ postoji $s \in \mathbb{Q}$ takav da je $s^2 r$ kvadratno slobodan prirodan broj te pravokutni trokut sa stranicam sX, sY, sZ ima površinu $s^2 r$. Sada možemo bez smanjenja općenitosti pretpostaviti da je $r = n$ kvadratno slobodan prirodan broj. Sljedeća propozicija nam daje važnu karakterizaciju kongruentnih brojeva.

Propozicija 4.3.1. *Neka je n fiksirani kvadratno slobodan prirodan broj. Neka su X, Y, Z racionalni brojevi za koje vrijedi $X < Y < Z$. Postoji bijektivno preslikavanje između pravokutnih trokuta s katetama X i Y, hipotenuzom Z, te površinom n i brojeva x takvih da su x, $x - n$ i $x + n$ redom kvadrati nekih racionalnih brojeva. Preslikavanje je definirano na sljedeći način.*

$$X, Y, Z \mapsto x = (Z/2)^2,$$
$$x \mapsto X = \sqrt{x+n} - \sqrt{x-n},\ Y = \sqrt{x+n} + \sqrt{x-n},\ Z = 2\sqrt{x}$$

Posebno, vrijedi da je n kongruentan broj ako i samo ako postoji x takav da su x, $x - n$ i $x + n$ kvadrati racionalnih brojeva.

Dokaz. Neka je X, Y, Z trojka s traženim svojstvom tj. $X^2 + Y^2 = Z^2$, $\frac{1}{2}XY = n$. Ako zbrojimo ili oduzmemo četiri puta drugu jednadžbu od prve dobijemo $(X \pm Y)^2 = Z^2 \pm 4n$. Ako podijelimo obje strane s 4 dobijemo da $x = (Z/2)^2$ te $x \pm n$ su kvadrati od $(X \pm Y)/2$. Obrnuto lako vidimo da za x takav da su x, $x - n$ i $x + n$ kvadrati racionalnih brojeva, gornjim preslikavanjem dobiveni $X < Y < Z$ zadovoljavaju $XY = 2n$ $X^2 + Y^2 = 4x = Z^2$. Ostaje još dokazati injektivnost, što je trivijalno. □

Sljedeća propozicija nam daje vezu kongruentnih brojeva i eliptičkih krivulja.

Propozicija 4.3.2. *Neka je (x, y) točka s racionalnim koordinatama na krivulji $y^2 = x^3 - n^2 x$. Neka x zadovoljava sljedeća dva uvjeta*

1. *x je kvadrat racionalnog broja,*
2. *nazivnik od x je paran.*

Tada postoji pravokutni trokut s racionalnim stranicama i površinom n koji je vezan s x preslikavanjem iz prethodne propozicije.

Dokaz. Neka je $u = \sqrt{x}$ te $v = y/u$ vrijedi $v^2 = y^2/x = x^2 - n^2$ odnosno $v^2 + n^2 = x^2$. Neka je t nazivnik od u, t je po pretpostavci propozicije paran. Primijetimo da su nazivnici od v^2 i x^2 isti (pošto je n cijeli broj i vrijedi $v^2 + n^2 = x^2$), i taj nazivnik je t^4. t^2v, t^2n, t^2x čine primitivnu pitagorinu trojku, gdje je t^2n paran. Može se pokazati (vidi [8, str. 7] i [6, str. 191]) da postoje $a, b \in \mathbb{Z}$ takvi da $t^2n = 2ab$, $t^2v = a^2 - b^2$, $t^2x = a^2 + b^2$. Sada pravokutni trokut sa stranicama $2a/t$, $2b/t$, $2u$ ima površinu $2ab/t^2$, što smo i željeli. Dalje $X = 2a/t$, $Y = 2b/t$, $Z = 2u$ koji s $x = (Z/2)^2 = u^2$ zadovoljavaju uvjete prethodne propozicije. Ovo dokazuje propoziciju. □

Eliptičku krivulju $y^2 = x^3 - n^2x$ ćemo označavati s E_n. Nadalje se da pokazati da sve točke oblika $2P$, gdje je $P \in E_n$, zadovoljavaju pretpostavke gornje propozicije. Također vrijedi da ako točka na E_n nije reda 2, tada je ona beskonačnog reda. Imamo sljedeću propoziciju.

Propozicija 4.3.3. *Broj n je kongruentan ako i samo ako $E_n(\mathbb{Q})$ ima rang ≥ 1.*

Iz ove propozicije vidimo važnost Birch i Swinnerton-Dyerove slutnje za rješavanje problema kongruentinih brojeva. Nadalje sljedeći nam teorem, kojeg je dokazao Tunnel 1983. godine, daje riješenje problema kongruentnih brojeve pod pretpostavkom da vrijedi Birch i Swinnerton-Dyerova slutnja.

Teorem 4.3.4. *Neka je n kvadratno slobodan i neparan (odnosno, paran) pozitivan cijeli broj, te je n površina pravokutnog trokuta s racionalnim stranicama, tada*

$$\#\left\{x, y, z \in \mathbb{Z} \,|\, n = 2x^2 + y^2 + 32z^2\right\} = \frac{1}{2}\#\left\{x, y, z \in \mathbb{Z} \,|\, n = 2x^2 + y^2 + 8z^2\right\}$$

$$\left(odnosno,\ \#\left\{x, y, z \in \mathbb{Z} \,|\, \frac{n}{2} = 4x^2 + y^2 + 32z^2\right\} = \frac{1}{2}\#\left\{x, y, z \in \mathbb{Z} \,|\, n = 4x^2 + y^2 + 8z^2\right\}\right).$$

Ako slaba Birch i Swinnerton-Dyerova slutnja vrijedi za eliptičke krivulje oblika $E_n = y^2 = x^3 - n^2x$ tada vrijedi obrat, odnosno ove jednadžbe povlače da je n kongruentan broj.

Ovdje valja naglasiti da ovaj teorem ima veliku praktičnu vrijednost za određivanje kongruentnosti nekog broja n, tj. gornji teorem u slučaju istinitosti slabe Birch i Swinnerton-Dyerove slutnje vodi k efektivnom i brzom algoritmu za provjeru kongruentnosti od n.

Pogledajmo još jednu posljedicu. Najvažniji je otvoreni problem eliptičkih krivulja problem nalaženja ranga istih. Pogledajmo jedan postupak za traženje ranga. Počnimo od sljedećeg egzaktnog niza.

$$E(\mathbb{Q}) \xrightarrow{\delta} S^{(m)}(E(\mathbb{Q})) \longrightarrow Ш(E(\mathbb{Q}))[m] \longrightarrow 0,$$

gdje je bar u teoriji konačna Selmerova grupa $S^{(m)}(E(\mathbb{Q}))$ efektivno izračunljiva. Kada bismo bili u stanju izračunti $Ш(E(\mathbb{Q}))[m]$ mogli bismo naći generatore za $E(\mathbb{Q})/mE(\mathbb{Q})$,

te i za $E(\mathbb{Q})$. Nažalost, općeniti postupak za računanje $Ш(E(\mathbb{Q}))[m]$ još se traži. Ali ipak za svaki cijeli $n \geq 1$ kombinacijom raznih oblika gornjeg egzaktnog niza možemo dobiti sljedeći komutativni dijagram.

$$\begin{array}{ccccccc} E(\mathbb{Q}) & \longrightarrow & S^{(m^n)}(E(\mathbb{Q})) & \longrightarrow & Ш(E/\mathbb{Q})[m^n] & \longrightarrow & 0 \\ \downarrow{\scriptstyle \mathrm{id}} & & \downarrow & & \downarrow{\scriptstyle \text{množenje s } m^{n-1}} & & \\ E(\mathbb{Q}) & \longrightarrow & S^{(m)}(E(\mathbb{Q})) & \longrightarrow & Ш(E/\mathbb{Q})[m] & \longrightarrow & 0 \end{array}$$

Sada se srednji stupac bar u teoriji može efektivno izračunati te direktno iz dijagrama imamo sljedeću propoziciju.

Propozicija 4.3.5. *Neka je E eliptička krivulja nad poljem $\mathbb{Q}$. Za sve $m \geq 2$ i $n \geq 1$, neka je $S^{(m,n)}(E(\mathbb{Q}))$ slika $S^{(m^n)}(E(\mathbb{Q}))$ u $S^{(m)}(E(\mathbb{Q}))$. Tada postoji egzaktni niz*

$$0 \longrightarrow E(\mathbb{Q})/mE(\mathbb{Q}) \longrightarrow S^{(m,n)} \longrightarrow m^{n-1}Ш(E(\mathbb{Q}))[m^n] \longrightarrow 0$$

Kako bismo našli generatore za $E(\mathbb{Q})$, imamo sljedeći postupak. Računajmo redom Selmerove grupe

$$S^{(m)}(E(\mathbb{Q})) = S^{(m,1)} \supset S^{(m,2)} \supset S^{(m,3)} \supset \dots$$

i grupe racionalnih točaka

$$T_{(m,1)}(E(\mathbb{Q})) \subset T_{(m,2)}(E(\mathbb{Q})) \subset T_{(m,3)}(E(\mathbb{Q})) \subset \dots$$

gdje je $T_{(m,k)}(E(\mathbb{Q}))$ podgrupa od $S^{(m)}(E(\mathbb{Q}))$ generirana svim točkama $P \in E(\mathbb{Q})$ s visinom $h(P) \leq k$. Nadamo se doći do jednakosti

$$S^{(m,n)}(E(\mathbb{Q})) = T_{(m,k)}(E(\mathbb{Q})).$$

U slučaju kad se to dogodi znamo da $m^{n-1}Ш(E(\mathbb{Q}))[m^n] = 0$ i da točke visine $h(P) \leq k$ generiraju $E(\mathbb{Q})/mE(\mathbb{Q})$ pa onda imamo i generatore za $E(\mathbb{Q})$. Problem ovog postupka je što ako $Ш(E/\mathbb{Q})$ sadrži element koji je djeljiv sa svim potencijama od m, ovaj postupak ne staje. Tu nam nadu daje jača verzija Birch i Swinnerton-Dyerove slutnje (4.1.2) iz koje, ako se pokaže da je istinita, slijedi da $Ш(E/\mathbb{Q})$ mora biti konačna te gornji postupak sigurno staje, što nam daje algoritam za traženje ranga.

Zaključak

Danas je proučavanje eliptičkih krivulja iznimno važno ne samo u teorijskoj matematici, već i zbog široke primjene u kriptografiji, koje će se u buduće samo proširiti. Ovdje se nismo dotakli primjene u rješavanju drugih problema teorije brojeva kao što su dokazivanje prostosti i fakorizacija. Bolje razumijevanje eliptičkih krivulja je od velike važnosti u svim poljima njihove primjene. Birch i Swinnerton-Dyerova slutnja velik je korak k razumijevanju eliptičkih krivulja. Istinost ove slutnje čini sw veoma izglednom, što, kako je napomenuto u radu potvrđuju razni izračuni od tvoraca tvrdnje pa do danas. No njeno rješenje se ne čini tako blizu, te se i tu pokazuje njena dubina. Svakako bi rješenje ove slutnje predstavljalo veliki iskorak u matematici danas.

Bibliografija

[1] Manjul Bhargava, Christopher Skinner i Wei Zhang, *A majority of elliptic curves over $\mathbb{Q}$ satisfy the Birch and Swinnerton-Dyer conjecture*, 2014.

[2] J. Coates i A. Wiles, *On the Conjecture of Birch and Swinnerton-Dyer*, Inventiones mathematicae **39** (1977), 223–252, http://eudml.org/doc/142468.

[3] Tim Dokchitser i Vladimir Dokchitser, *Root numbers and parity of ranks of elliptic curves*, (2009).

[4] Ralph Greenberg, *On the Birch and Swinnerton-Dyer Conjecture.*, Inventiones mathematicae **72** (1983), 241–266, http://eudml.org/doc/143019.

[5] B.H. Gross i D.B. Zagier, *Heegner points and derivatives of L-series.*, Inventiones mathematicae **84** (1986), 225–320, http://eudml.org/doc/143341.

[6] G. H. Hardy i E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford University Press, 1975, ISBN 0198533107.

[7] Dale Husemöller, *Elliptic curves*, Graduate texts in mathematics, Springer, New York, 2004, ISBN 0-387-95490-2.

[8] Neal Koblitz, *Introduction to Elliptic curves and Modular Forms*, Springer New York, 1984, ISBN 0-387-96029-5.

[9] J.S. Milne, *Elliptic Curves*, BookSurge Publishers, 2006, ISBN 1-4196-5257-5.

[10] K. Rubin, *Tate-Shafarevich groups and L-functions of elliptic curves with complex multiplication.*, Inventiones mathematicae **89** (1987), 527–560, http://eudml.org/doc/143493.

[11] J.H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, Springer New York, 2009, ISBN 9780387094946.

Sažetak

U ovom radu smo probali što preciznije objasniti ovu važnu matematičku slutnju. Zbog matematičke dubine najvažniji rezultati su samo iskazani. Ono što smo pokušali vidjeti u radu što točnija definicija glavnih pojmova i njihovo objašnjenje. Na početku rada dajemo općenitu sliku eliptičkih krivulja te njihovih osnovnih svojstava. Te kasnije se trudimo da što preciznije pojasnimo pojmove L-funkcija i Tate-Šafarevičeve grupe, gdje ulazimo kratko u pojašnjeje p-adskih brojeva i Galoisove kohomologije. Na kraju dajemo iskaz Birch i Swinnerton-Dyerove slutnje, te navodimo glavne rezultate i posljedice. Svakako rad treba shvatiti kao uvod u ovo duboko područje matematike.

Summary

In this work we tried, as precise as possible, to define and explain this extraordinary conjecture. The deepest results are just stated. We tried to show, as exactly as possible, the main objects and their explanation. First we showed the main properties of elliptic curves and the mathematical theory around them. Then we define and explain L-functions and the very elusive Tate-Šafarevič group, where we to come to p-adic numbers and briefly touch on the subject of Galois Cohomology. At the end we state the Birch and Swinnerton-Dyer conjecture and try to understand where such a strong idea comes from. We show the main results and some consequences of this conjecture. This work is to be understood as an introduction to this wide and deep mathematical domain.

Životopis

Moje ime je Marko Sikirić, rođen sam 13.01.1984 u Novom Sadu. Tamo sam završio 2 razreda osnovne škole, te se selim s obitelji u Ludwigshafen am Rhein, Republika Njemačka gdje završavam osnovnu školu. 1999 se opet selimo u Zagreb gdje upisujem Tehničku školu Ruđera Boškovića koju završavam 2003. godine. Upisujem se na Fakultet elektrotehnike i računarstva u Zagrebu. Nakon pet godina neuspješnog studiranja na FER-u, prebacujem se na Prirodoslovno-matematčki fakultet, gdje studiram do danas.