Modularna metoda za rješavanje diofantskih jednadžbi

Dujella, Marta

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Marta Dujella

MODULARNA METODA ZA RJEŠAVANJE DIOFANTSKIH JEDNADŽBI

Diplomski rad

Voditelj rada:
izv. prof. dr. sc. Filip Najman

Zagreb, Rujan, 2018.

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

Diofantske jednadžbe su polinomijalne jednadžbe nad $\mathbb{Z}$, $\mathbb{Q}$ ili općenitije nad nekim zanimljivim prstenom ili poljem. Još od antike predstavljaju jedno od glavnih područja zanimanja teorije brojeva. Općeniti problem je nalaženje njihovih rješenja. Jedan od najpoznatijih primjera je jednadžba

$$a^n + b^n = c^n,$$

za koju je još 1637. godine Pierre de Fermat tvrdio da nema netrivijalnih rješenja u cijelim brojevima za $n > 2$. Ova tvrdnja je poznata kao posljednji Fermatov teorem. Ovaj problem intrigirao je mnoge matematičare tijekom stoljeća, te potaknuo razvoje mnogih novih grana matematike. Pristup koji je konačno doveo do dokaza je povezivanje ovog problema s eliptičkim krivuljama, koje su jedan od centralnih objekata proučavanja teorije brojeva i algebarske geometrije. Naime, 1980-ih godina je Gerhard Frey predložio da se hipotetskom rješenju (a, b, c) Fermatove jednadžbe pridruži eliptička krivulja

$$E : y^2 = x(x - a^p)(x + b^p),$$

tzv. Freyeva krivulja, te primjetio da bi takva krivulja imala neobična svojstva. Tu se bitnim pokazala veza između eliptičkih krivulja i modularnih formi, funkcijama gornje kompleksne poluravnine s posebnim svojstvima. Naime, tada još samo pretpostavka, a kasnije poznato kao teorem o modularnosti je da je svaka eliptička krivulja nad $\mathbb{Q}$ modularna, tj. da joj možemo pridružiti modularnu formu posebnog oblika. Jean-Pierre Serre i Ken Ribet pokazali su da Freyeva krivulja nije modularna, dakle njeno postojanje bi opovrgnulo tadašnju pretpostavku o modularnosti svih eliptičkih krivulja nad $\mathbb{Q}$. No, 1995. je Andrew Wiles dokazao teorem o modularnosti za polustabilne eliptčke krivulje, posebnu klasu eliptičkih krivulja kojoj pripada Freyeva krivulja, pa time napokon dokazao i posljednji Fermatov teorem.

U ovom radu pokazat ćemo primjenu tih metoda na Fermatovu jednadžbu, kao i još neke diofantske jednadžbe. Pritom se koristimo teoremom o modularnosti, ali i drugim rezultatima o eliptičkim krivuljama i modularnim formama.

U prvom poglavlju definiramo eliptičke krivulje i dajemo pregled osnovnih svojstava. Glavna literatura o ovoj temi bila je [9]. Bavimo se grupovnom strukturom eliptičkih krivulja, te posebno promatramo torzijsku podgrupu. Nadalje, detaljno obrađujemo redukciju

eliptičkih krivulja modulo p, slučajevima dobre i loše redukcije. Također se bavimo izogenijama, preslikavanjima među eliptičkim krivuljama koja čuvaju njihova bitna svojstva.

U drugom poglavlju zanimaju nas modularne forme. Definiramo modularnu grupu i njene kongruencijske podgrupe, te zatim definiramo modularne forme obzirom na njih. Nakon pregleda osnovnih svojstava modularnih formi prelazimo na posebnu vrstu modularnih formi, newforme. Dajemo definiciju newformi i navodimo neka njihova svojstva. Nakon toga iskazujemo Ribetov teorem i teorem o modularnosti koji su ključni za vezu između modularnih formi i eliptičkih krivulja. Osnovna literatura za ovo poglavlje bila je [1].

U trećem poglavlju pokazujemo na primjerima kako se teorem o modularnosti i Ribetov teorem koriste u rješavanju diofantskih jednadžbi. Pritom slijedimo bilješke Samira Sikseka o ovoj temi [7]. Prvi primjer je poznati Fermatov posljednji teorem. Nakon toga prelazimo na jednadžbu

$$x^p + L^r y^p + z^p = 0,$$

koja je sličnog tipa kao Fermatova, ali ipak zahtjevnija. Na primjeru te jednadžbe pokazujemo različite metode pristupa rješavanju. Na kraju pokazujemo još jedan primjer jednadžbe. U rješavanju ovih jednadžbi koristimo svojstva eliptičkih krivulja i newformi iz prethodna dva poglavlja.

Diplomski ispit napravljen je u sklopu aktivnosti Projekta KK.01.1.1.01.0004 - Znanstveni centar izvrsnosti za kvantne i kompleksne sustave te reprezentacije Liejevih algebri.

Poglavlje 1

Eliptičke krivulje

1.1 Osnovno o eliptičkim krivuljama

Weierstrassova jednadžba

Definicija 1.1.1. ***Eliptička krivulja*** *E nad poljem $\mathbb{K}$ je nesingularna projektivna krivulja genusa 1 nad $\mathbb{K}$ s istaknutom točkom.*

Svaka eliptiča krivulja može se uložiti u $\mathbb{P}^2$ kao kubna krivulja sa samo jednom točkom O na pravcu u beskonačnosti. Tada svaka eliptička krivulja ima jednadžbu oblika

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3,$$

gdje su $a_1, ..., a_6 \in \mathbb{K}$. Točka $O = [0 : 1 : 0]$ je bazna točka i zovemo ju točka u beskonačnosti. Takvu jednadžbu zovemo dugom Weierstrassovom formom. Obično ju zapisujemo u nehomogenim koodrinatama ($x = X/Z, y = Y/Z$):

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{1.1}$$

Tada eliptičku krivulju E nad $\mathbb{K}$ možemo shvatiti kao skup svih točaka $(x, y) \in \mathbb{K} \times \mathbb{K}$ koji zadovoljavaju 1.1, zajedno s "točkom u beskonačnosti" $O = [0 : 1 : 0]$.

Nadalje, ako je karakteristika polja $\mathbb{K}$ različita od 2, onda se (nadopunjavanjem na potpuni kvadrat) gornja jednadžba može svesti na oblik

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

gdje je

$$b_2 = a_1^2 + 4a_2, \quad b_4 = a_1a_3 + 2a_4, \quad b_6 = a_3^2 + 4a_6.$$

Definiramo još i $b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$. Ako je pak karakteristika od $\mathbb{K}$ različita i od 3, daljnjim transformacijama možemo dobiti jednadžbu u obliku

$$y^2 = x^3 - 27c_4 - 54c_6,$$

gdje je

$$c_4 = b_2^2 - 24b_4, \quad c_6 = -b_2^3 + 36b_2b_4 - 216b_6.$$

Definiramo bitne veličine pridružene eliptičkoj krivulji E, zadanoj s 1.1:

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6,$$

$$j = c_4^3/\Delta.$$

Definicija 1.1.2. *Veličinu Δ zovemo **diskriminanta**, a j je **j-invarijanta** eliptičke krivulje.*

Ako je $char(\mathbb{K}) \neq 2, 3$, tada E možemo zadati u *kratkoj Weierstrassovoj formi*

$$E : y^2 = x^3 + Ax + B,$$

i tada je diskriminanta dana s $\Delta = -16(4A^3 + 27B^2)$.

Primjer 1.1.3. *Za eliptičku krivulju oblika $E : y^2 = x(x-a)(x-b)$, diskriminanta od E je $\Delta = 16a^2b^2(a+b)^2$, a $c_4 = 16((a-b)^2 - ab)$ i $j(E) = \frac{256((a-b)^2-ab)^3}{a^2b^2(a-b)^2}$.*

Uvjet nesingularnosti od E je ekvivalentan s uvjetom $\Delta \neq 0$. Ako je E dana s $y^2 = f(x)$, gdje je f polinom stupnja tri s koeficijentima u K, tada je E nesingularna ako i samo ako f nema višestrukih korijena.

Izomorfizam između eliptičkih krivulja dan je s

$$x' = u^2x + r, \quad y' = u^3y + su^2x + t,$$

gdje su $r, s, t \in \mathbb{Q}$, a $u \in \mathbb{Q}^*$. Vrijedi:

$$\Delta' = u^{12}\Delta, \quad j' = j.$$

Dakle, izomorfne krivulje imaju istu j-invarijantu. Obrat vrijedi samo nad algebarski zatvorenim poljem (nad $\mathbb{Q}$ ne vrijedi). Dokazi ovih tvrdnji mogu se naći u [9].

Twist eliptičke krivulje E/K je glatka krivulja C'/K koja je izomorfna s E nad $\bar{K}$.

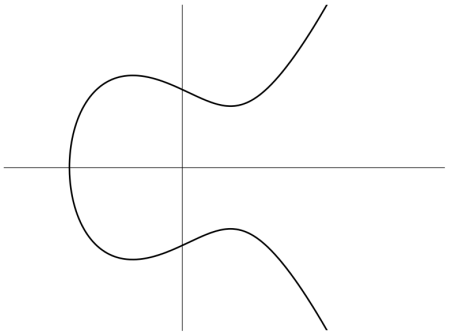
Primjer 1.1.4. *Neka je E/K eliptička krivulja zadana s*

$$y^2 = f(x)$$

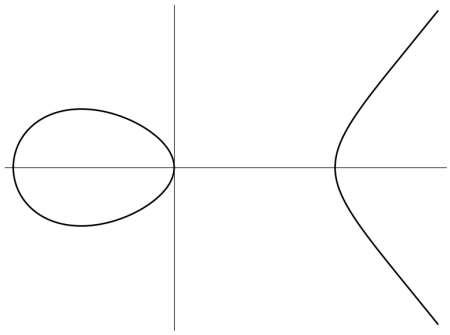
i $K(\sqrt{d})$ kvadratno proširenje od K. Tada je

$$C : dy^2 = f(x)$$

twist od E, izomorfizam nad $\bar{K}$ je $\phi : C \to E$, $\phi(x, y) = (x, y\sqrt{d})$. Kažemo da je C kvadratni twist od E sa d, i označavamo je se E^d.



Slika 1.1: Elitptička krivulja $y^2 = x^3 - x + 1$



Slika 1.2: Elitptička krivulja $y^2 = x^3 - x$

Operacija zbrajanja i grupovna struktura

Bitno svojstvo eliptičkih krivulja je da na točkama eliptičke krivulje možemo definirati operaciju zbrajanja, s kojom one postaju Abelova grupa.

Neka je $E \subset \mathbb{P}^2$ eliptička krivulja nad $\mathbb{K}$ dana Weierstrassovom jednadžbom 1.1. S $E(\mathbb{K})$ ćemo značavati skup točaka $P = (x, y) \in \mathbb{K}^2$ koje zadovoljavaju 1.1, zajedno s točkom u beskonačnosti $\mathcal{O} = [0 : 1 : 0]$. Neka je $l \subset \mathbb{P}^2$ pravac. Jer je jednadžba kojom je E zadana stupnja 3, a pravac l stupnja 1, prema Bezoutovom teoremu (vidi [6]), l sijeće E u 3 točke (brojeći kratnost). Neka su $P, Q \in E(\mathbb{K})$ i neka je l jedinstveni pravac kroz P i Q ako $P \neq Q$, odnosno tangenta na E kroz P ako $P = Q$. Tada l sijeće E u jedinstvenoj trećoj točki R. Neka je l' jedinstveni pravac kroz R i $\mathcal{O}$. Tada l' sijeće E u $\mathcal{O}$, R i jedinstvenoj trečoj točki, i nju uzimamo kao definiciju za $P + Q$.

Uz tako definirano zbrajanje točaka, $(E(K), +)$ postaje Abelova grupa. Doista, iz gornje definicije je jasno da je $P + \mathcal{O} = \mathcal{O} + P = P$, za svaku točku $P \in E(K)$, pa je $\mathcal{O}$ neutralni element. Nadalje, ako je $P \in E(K)$, i l_p pravac kroz P i $\mathcal{O}$, tada l_p siječe E u jedinstvenoj trećoj točki P'. Tada je pravac l iz definicije $P + P'$ upravo l_p, i $R = \mathcal{O}$, pa je l' tangenta na E kroz $\mathcal{O}$. Ona siječe E samo u $\mathcal{O}$, pa je $P + P' = \mathcal{O}$. Komutativnost je jasna iz definicije zbrajanja. Asocijativnost je kompliciranije za dokazati, može se, na primjer, provjeriti direktnim računom iz konkretnih formula za zbrajanje točaka. Formule i dokaz mogu se naći u [9, Poglavlje III.2]

Torzijska grupa

Vrlo bitan teorem o grupovnoj strukturi eliptičkih krivulja je Mordell-Weilov teorem.

Teorem 1.1.5 (Mordell-Weil)**.** *Neka je K polje algebarskih brojeva, i E/K eliptička krivulja. Tada je $E(K)$ konačno generirana Abelova grupa.*

Iz Mordell-Weilovog teorema i strukturnog teorema za konačno generirane Abelove grupe, slijedi da je $E(K)$ oblika

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

$E(K)_{tors}$ je skup svih točaka od $E(K)$ konačnog reda, što je podgrupa od $E(K)$, a r je nenegativni cijeli broj koji zovemo rang od $E(K)$.

Za eliptičku krivulju E nad poljem K, i $n \in \mathbb{N}$ definiramo **m-torziju** od E

$$E[m] = \{P \in E(\bar{K}) : mP = O\}.$$

Sa $E(K)[m]$ označavamo sve točke iz $P \in E(K)$ za koje vrijedi $mP = O$. **Torzijska podgrupa** od E je skup svih točaka od E konačnog reda (što je očito podgrupa od E),

$$E_{tors} = \bigcup_{m=0}^{\infty} E[m].$$

.

Prvo pitanje vezano za torzijsku grupu je pitanje određivanja torzijske grupe za danu krivulju E. Sljedeći teorem daje algoritam za traženje potencijalnih torzijskih točaka na E.

Teorem 1.1.6 (Lutz-Nagell)**.** *Neka je $E/\mathbb{Q}$ eliptička krivulja dana jednadžbom*

$$y^2 = x^3 + ax^2 + bx + c = f(x), \quad a, b, c \in \mathbb{Z}.$$

Ako je $P = (x_0, y_0) \in E(\mathbb{Q})_{tors}$, tada su $x_0, y_0 \in \mathbb{Z}$. Također vrijedi da ili $y_0 = 0$ ili $y_0^2 \mid \Delta_0 = -\Delta/16$.

Dokaz. Dokaz da su x_0 i y_0 iz $\mathbb{Z}$ može se naći u [9]. Dokažimo drugu tvrdnju teorema. Primjetimo da ako je $2P = O$, tada je $P = -P$, odnosno $(x_0, y_0) = (x_0, -y_0)$, pa je $y_0 = 0$. Pretpostavimo da je $y_0 \neq 0$. Tada je $2P \neq O$, pa je $2P = (x_1, y_1)$. Kako je P konačnog reda, i $2P$ je konačnog reda, pa prema prvoj tvrdnji teorema slijeda da su $x_1, y_1 \in \mathbb{Z}$. Iz formula za zbrajanje imamo: $x_1 = \lambda^2 - 2x_0 - a, \lambda = (3x_0^2 + 2ax_0 + b)/2y_0$, iz čega slijedi da je $\lambda \in \mathbb{Z}$. Tada $y_0 \mid 3x_0^2 + 2ax_0 + b = f'(x_0)$. Sada primjenimo prošireni euklidov algoritam na polinome $f(x)$ i $f'(x)^2$, pa dobijemo

$$g_1(x)f(x) + g_2(x)f'(x)^2 = \Delta_0.$$

Uvrštavanjem $x = x_0$ u gornju relaciju, dobivamo da $y_0 \mid f(x_0) = y_0^2$ i $y_0 \mid f'(x_0)$, pa mora biti i $y_0 \mid \Delta_0$. □

Vrlo netrivijalno pitanje jest određivanja svih grupa koje se mogu pojaviti kao torzijske podgrupe eliptičkih krivulja nad nekim poljem K. Odgovor na to pitanje u slučaju $K = \mathbb{Q}$ dao je Mazur 1978. godine.

Teorem 1.1.7 (Mazur)**.** *Neka je $E/\mathbb{Q}$ eliptička krivulja. Tada je torzijska podgrupa $E(\mathbb{Q})_{tors}$ izomorfna jednoj od sljedećih grupa:*

$$\mathbb{Z}/N\mathbb{Z}, \quad za\ 1 \leq N \leq 10\ ili\ N = 12,$$
$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}, \quad za\ 1 \leq N \leq 4.$$

Za svaku od grupa u gornjem teoremu postoje beskonačne familije krivulja sa zadanom torzijskom grupom. U [3] se može naći popis beskonačnih familija za sve grupe iz Mazurovog teorema. Na primjer, eliptičke krivulje s torzijskom grupom $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ imaju, do na izomorfizam, jednadžbe oblika $y^2 = x(x + a)(x + b)$ (za $a, b \neq 0$ i međusobno različiti).

Singularne krivulje

Zanimljivo je promotriti i slučaj kada je E singularna krivulja. Može se pokazati da ako projektivna krivulja stupnja 3 ima singularnu točku, tada ima samo jednu takvu. Pretpostavimo da je E dana Weirstrassovom jednadžbom kao u 1.1, ali da je E singularna. Dakle, E je zadana s

$$f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0.$$

Neka je $P = (x_0, y_0)$ singularna točka na E, dakle

$$\frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = 0.$$

Razvojem f u Taylorov red oko $(x - x_0, y - y_0)$, dobivamo da je

$$f(x - y) - f(x_0, y_0) = f_2(x - x_0, y - y_0) + f_3(x - x_0, y - y_0),$$

gdje su f_2, f_3 homogeni polinomi stupnja 2, odnosno 3. Konkretno, $f_2(x, y) = -(3x_0 + 2a_2)(x - x_0)^2 + a_1(x - x_0)(y - y_0) + (y - y_0)^2$, a $f_3(x, y) = -(x - x_0)^3$. Polinom f_2 se faktorizira u linearne faktore u $\bar{K}$, pa postoje $\alpha, \beta \in \bar{K}$, takvi da je

$$f_2 = ((y - y_0) - \alpha(x - x_0))((y - y_0) - \beta(x - x_0)).$$

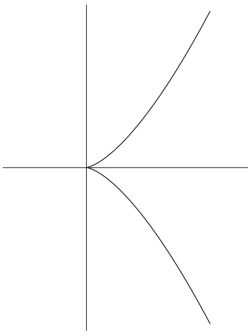
Linearni faktori od f_2 su tangente na E u P. Razlikujemo slučajeve u ovisnosti o tome je li $\alpha = \beta$.
Ako je $\alpha \neq \beta$, tada E ima dvije različite tangente u P, pa kažemo da je P **čvor**. Tangente na E u P su

$$y - y_0 = \alpha(x - x_0) \quad \text{i} \quad y - y_0 = \beta(x - x_0),$$

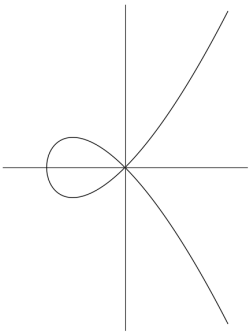
s koeficijentima smjera α i β. često će biti bitno razlikovati slučajeve kada α i β jesu, odnosno nisu iz K.
Ako je $\alpha = \beta$, E ima jednu (duplu) tangetnu

$$y - y_0 = \alpha(x - x_0),$$

sa koeficijentom smjera α. U ovom slučaju kažemo da je P **šiljak**.
Više o algebarskim krivuljama može se naći u [6].



Slika 1.3: Krivulja $y^2 = x^3$ ima šiljak



Slika 1.4: Krivulja $y^2 = x^3 + x^2$ ima čvor

Konkretan kriterij za određivanje tipa singulariteta dan je u sljedećoj propoziciji, čiji dokaz se može naći u [9].

Propozicija 1.1.8. *Neka je E krivulja dana Weirstrassovom jednadžbom, te veličine* Δ *i* c_4 *definirane kao u odjeljku 1.1. Tada vrijedi:*

(i) E je nesingularna ako i samo ako je $\Delta \neq 0$*,*

(ii) E ima čvor ako i samo ako je $\Delta = 0$ *i* $c_4 \neq 0$*,*

(iii) E ima šiljak ako i samo ako je $\Delta = 0$ *i* $c_4 = 0$*.*

Najčešće promatramo slučaj kada je E dana s $y^2 = x^3 + ax^2 + bx + c = g(x)$. Tada je E nesingularna ako i samo ako polinom g nema višestrukih korijena. Dakle, ako je E singularna, tada g ima dvostruki ili trostruki korijen, i singularna točka je oblika $P = (0, x_0)$. Ako g ima trostruki korijen, tada je $g(x) = (x - c)^3$, za neki $c \in K$, i singularna točka je upravo $P = (c, 0)$. Tada je $f_2(x, y) = y^2$, pa E ima jednu tangentu, $y = 0$, u P, to jest P je šiljak. Ako g ima dvostruki korijen, tada je oblika $g(x) = (x-b)(x-c)^2, b \neq c$, i sinuglarna točka je $P = (c, 0)$.Vidimo da je $f_2 = y^2 - (c - b)(x - c)^2 = (y - \alpha(x - x_0))(y + \alpha(x - x_0))$, gdje je $\alpha = \sqrt{c - b}$. Dakle, P je čvor.
Raspisivanjem se vidi da vrijedi i obratno, to jest ako je E oblika $y^2 = g(x)$, tada E ima šiljak, odnosno čvor ako i samo ako g ima trostruku, odnosno dvostruku nultočku.

Definicija 1.1.9. *Neka je E (moguće singularna) krivulja dana Weierstrassovom jednadžbom. S* E_{ns} *označavamo nesingularni dio od E, odnosno skup svih nesingularnih točaka na E. Ako je E definirana nad K, s* $E_{ns}(K)$ *označavamo skup svih nesingularnih točaka od* $E(K)$*.*

Sljedeća propozicija govori o grupovonoj strukturi E_{ns}. Dokaz tvrdnji se može naći u [9].

Propozicija 1.1.10. *Neka je E krivulja nad K dana Weierstrassovom jednadžbom, takva da je* $\Delta = 0$. *Dakle E ima jednu singularnu točku S. Tada na* $E_{ns}(K)$ *možemo definirati operaciju zbrajanja, s kojom* $E_{ns}(K)$ *postaje Abelova grupa.*
Također, imamo klasifikaciju grupe $E_{ns}(K)$, *ovisno o vrsti singulariteta. Ako E ima šiljak, tada je* $E_{ns}(K) \cong (K, +)$. *Ako E ima čvor, neka su* α, β *koeficijenti smjera tangenti u P. Ako su* $\alpha, \beta \in K$, *tada je* $E_{ns}(K) \cong (K^*, \cdot)$. *U suprotnom, neka je* $L = K(\alpha, \beta)$. *Tada je* $E_{ns}(K) \cong \{t \in L^* : N_{L/K}(t) = 1\}$.

1.2 Redukcija modulo p

Neka je p prost broj. $\mathbb{F}_p = \{0, 1, ..., p-1\}$ je polje s operacijama zbrajanja i množenja mod p, i to je polje karakteristike p. Za $a \in \mathbb{Z}$ sa $\bar{a}$ označavamo sliku od a u $\mathbb{F}_p$ pri redukciji modulo p, to jest ostatak od a pri dijeljenju s p. Zanima nas što se događa s eliptičkim krivuljama nad $\mathbb{Q}$ kada koeficijente jednadžbe reduciramo modulo p. Kako ista eliptička krivulja može biti dana različitim jednadžbama, bitno je odabrati dobar model za redukciju.

Neka je eliptička krivulja $E/\mathbb{Q}$ dana (dugom) Weierstrassovom jednadžbom. Zamjenom varijabli možemo dobiti jednadžbu za E tako da je $|\Delta|$ minimalno, te da su svi $a_i \in \mathbb{Z}$. Za takvu jednadžbu kažemo da je (globalna) **minimalna Weierstrassova jednadžba** od E, a njenu diskriminantu zovemo **minimalna diskriminanta** i označavamo s Δ_{min}. Ona ima svojstvo da za svaki prosti broj p vrijedi da je potencija od p koja dijeli diskriminantu najmanja moguća. Za traženje minimalne jednadžbe koristi se Tateov algoritam. Detaljni opis Tateovog algoritma može se naći u [8].

Možemo tražiti i minimalnu jednadžbu za pojedini p. Ako je $\mathrm{ord}_p(\Delta) < 12$ ili $\mathrm{ord}_p(c_4) < 4$, onda je ta jednadžba minimalna za prost broj p. Za $p \neq 2, 3$ vrijedi i obrat.

Pretpostavimo sada da je $E/\mathbb{Q}$ dana minimalnom Weierstrassovom jednadžbom

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

Promatramo krivulju

$$\bar{E} : y^2 + \bar{a}_1xy + \bar{a}_3y = x^3 + \bar{a}_2x^2 + \bar{a}_4x + \bar{a}_6$$

nad $\mathbb{F}_p$. Za $P \in E(\mathbb{Q})$, $P = [X_0 : Y_0 : Z_0]$ vrijedi $\bar{P} = [\bar{X}_0 : \bar{Y}_0 : \bar{Z}_0]$ je na $\bar{E}(\mathbb{F}_p)$. Dakle, *redukcija modulo p*: $P \mapsto \bar{P}$ preslikava $E(\mathbb{Q})$ u $\bar{E}(\mathbb{F}_p)$.

No, krivulja $\bar{E}/\mathbb{F}_p$ nije nužno eliptička krivulja, jer ne mora biti nesingularna. Naime, pri redukciji modulo p može se dogoditi da je $\Delta(\bar{E}) = 0$. To je ekvivalentno s $p \mid \Delta(\bar{E})$. Razlikujemo slučajeve u ovisnosti o tome kakva je krivulja $\bar{E}(\mathbb{F}_p)$.

Ako $p \nmid \Delta(\bar{E})$, tada je $\bar{E}$ nesingularna, pa je $\bar{E}$ eliptička krivulja nad $\mathbb{F}_p$. U tom slučaju kažemo da E ima **dobru redukciju modulo** p. Tada je s $P \mapsto \bar{P}$ definiran homomorfizam grupa $E(\mathbb{Q}) \to \bar{E}(\mathbb{F}_p)$.

U protivnom, $\bar{E}$ je singularna i kažemo da E ima **lošu redukciju modulo** p. Prema raspravi u odjeljku 1.1 o singularnim krivuljama, razlikujemo dva slučaja.

Ako $\bar{E}$ ima šiljak, kažemo da E ima **aditivnu** redukciju modulo p. Prema propoziciji 1.1.8, to je ekvivalentno s time da $p \mid \Delta$ i $p \mid c_4$.
Ako $\bar{E}$ ima čvor, kažemo da E ima **multiplikativnu** redukciju modulo p. Prema propoziciji 1.1.8, ekivalentan uvjet je da $p \mid \Delta$ i $p \nmid c_4$. Ako su koeficijenti smjera tangenti u čvoru iz $\mathbb{F}_p$, tada kažemo da E ima **rascjepivu** multiplikativnu redukciju modulo p. U suprotnom E ima **nerascjepivu** multiplikativnu redukciju modulo p.

Ako E ima multiplikativnu ili dobru redukciju za svaki prosti broj p, kažemo da je E *polustabilna* eliptička krivulja.

Sada možemo definirati još jednu bitnu veličinu vezanu uz E.

Definicija 1.2.1. *Neka je $E/\mathbb{Q}$ eliptička krivulja.* ***Konduktor*** *od E je*

$$N = \prod_{p \text{ prost}} p^{f_p(E)},$$

gdje je

$$f_p(E) = \begin{cases} 0 & \text{ako } E \text{ ima dobru redukciju u } p \\ 1 & \text{ako } E \text{ ima multiplikativnu redukciju u } p \\ 2 & \text{ako } E \text{ ima aditivnu redukciju u } p \text{ i } p \neq 2,3. \end{cases}$$

Za $p = 2, 3$ $f_p(E)$ se definira kompliciranije, ali općenito vrijedi $f_p(E) \geq 2$ ako E ima aditivnu redukciju u p.

U sljedećem primjeru analiziramo redukciju jedne klase eliptičkih krivulja koja će nam biti bitna u kasnijim razmatranjima nekih diofantskih jednadžbi.

Primjer 1.2.2. *Neka je su $a, b \in \mathbb{Z}$ takvi da $a \equiv -1 \pmod 4$ i $b \equiv 0 \pmod{32}$ i $nzd(a, b) = 1$. Promotrimo eliptičku krivulju*

$$E : y^2 = x(x - a)(x - b).$$

Diskriminanta od E je $\Delta = 16a^2b^2(a - b)^2$. Nadalje, s

$$x = 4x_1,\ y = 8y_1 + 4x_1$$

dan je izomorfizam krivulja E i

$$E_1 : y_1^2 + x_1y_1 = x_1^3 - \frac{a + b + 1}{4} + \frac{ab}{16}.$$

Primjetimo, zbog pretpostavka o a i b vrijedi $4 \mid a+b+1$ *i* $16 \mid ab$. *Računamo* $\Delta(E_1) = 2^{-8}a^2b^2(a-b)^2$ *te* $c_4(E_1) = (a-b)^2 - ab$. *Tvrdimo da je ovo minimalni model za E u 2. Za to je dovoljno vidjeti da je* $\mathrm{ord}_2(c_4(E_1)) < 4$. *Pretpostavimo suprotno, tj. da* $16 \mid c_4(E_1) = (a-b)^2 - ab$. *No, kako* $16 \mid ab$, *tada bi slijedilo da* $16 \mid (a-b)^2$, *ali* $(a-b)^2 \equiv 1 \pmod 4$, *pa je to nemoguće. Dakle,* $\mathrm{ord}_2(c_4(E_1)) < 4$, *što pokazuje da je* E_1 *minimalni model za E u 2.*

Dakle, možemo računati redukciju modulo 2 od E. Jer $32 \mid b$, *slijedi da* $2 \mid \frac{ab}{16}$. *Označimo s* $e \in \mathbb{F}_2$ *ostatak pri dijeljenju s 2 od* $\frac{a+b+1}{4}$. *Tada je redukcija modulo 2 od E krivulja*

$$\bar{E} : y^2 + xy = x^3 + ex^2.$$

Kako $2 \nmid c_4$ *(jer* $2 \nmid a$*), vidimo da E ima multiplikativnu redukciju u 2.*

Za bilo koji drugi p je već E minimalni model. Naime, $c_4(E) = 16((a-b)^2 - ab)$. *Ako p dijeli jedan od* $a, b, a-b$, *tada dijeli samo jedan od njih, jer u suprotnom a i b ne bi bili relativno prosti. Dakle, ako E ima potencijalno lošu redukciju u* $p \neq 2$, *tj. ako* $p \mid \Delta(E)$, *onda* $p \mid a$, *bili* $a-b$. *No, tada* $p \nmid c_4(E)$, *pa je* $\mathrm{ord}_p(c_4(E)) = 0$, *iz čega slijedi da je E minimalan model u p.*

Sada primjetimo da polinom $x(x-a)(x-b)$ *ne može imati trostruku nultočku modulo bilo koji prost broj p. Naime, kada bi imao trostruku nultočku, tada bi vrijeli* $0 \equiv a \equiv b \pmod p$, *no tada* $p \mid a, b$, *što je kontradikcija s pretpostavkom da su a i b relativno prosti. Zaključujemo da E ima multiplikativnu ili dobru redukciju u svakom p, tj. E je polustabilna.*

Dakle (globalni) minimalni model za E je E_1 *i* $\Delta_{min}(E) = 2^{-8}a^2b^2(a-b)^2$. *Konduktor N od E je tada produkt svih prostih brojeva koji dijele* $\Delta_{min}(E)$, *tj.*

$$N = \prod_{l \mid ab(a-b)} l.$$

Jedno zanimljivo pitanje je broj (nesingularnih) točaka na $\bar{E}(\mathbb{F}_p)$. Promotrimo prvo slučaj loše redukcije, kada $p \mid \Delta$, to jest kada je $\bar{E}/\mathbb{F}_p$ singularna. Prema propoziciji 1.1.10, imamo opis grupe $E_{ns}(\mathbb{F}_p)$. Ako E ima aditivnu redukciju, onda je $E_{ns}(\mathbb{F}_p) \cong \mathbb{F}_p$, pa $\bar{E}$ u tom slučaju ima p nesingularnih točaka. Ako E ima rascjepivu multiplikativnu redukciju, onda je $E_{ns}(\mathbb{F}_p) \cong \mathbb{F}_p^*$, pa $\bar{E}(\mathbb{F}_p)$ ima $p-1$ nesingularnih točaka. U slučaju da E ima nerascjepivu multiplikativnu redukciju može se pokazati da $\bar{E}$ ima $p+1$ nesingularnih točaka.

Preostaje pitanje što je sa slučajem dobre redukcije, kada je $\bar{E}$ eliptička krivulja nad $\mathbb{F}_p$. Zato ćemo promotriti neka svojstva eliptičkih krivulja nad općenitim konačnim poljima. S $\mathbb{F}_q$ ćemo označavati konačno polje od q elemenata.

Neka je E eliptička krivulja nad konačnim poljem $\mathbb{F}_q$, dana dugom Weierstrassovom jednadžbom. Zanima nas red grupe $E(\mathbb{F}_q)$. Prva gruba ocjena koju možemo dati je

$$\#E(\mathbb{F}_q) \leq 2q + 1.$$

Naime, O je uvijek na E, a za fiksirani x imamo najviše 2 mogućnosti za y. Kako je $x \in \mathbb{F}_q$, imamo najviše q mogućih x, što ukupno daje gornju ocjenu. No, sljedeći teorem daje puno bolju ocjenu na red od $E(\mathbb{F}_q)$. Označimo s

$$a_q(E) = q + 1 - \#E(\mathbb{F})_q.$$

Veličinu $a_p(E)$ nazivamo **Frobeniusov trag**, a poslije ćemo vidjeti kako je ona povezana s nekim drugim važnim objektima.

Teorem 1.2.3 (Hasse)**.** *Neka je E eliptička krivulja nad konačnim poljem $\mathbb{F}_q$. Tada je*

$$|a_p(E)| \leq 2\sqrt{q}.$$

Definirajmo poopćenje Legendreovog simbole $\left(\frac{x}{p}\right)$ za konačno polje $\mathbb{F}_q$:

$$\left(\frac{x}{\mathbb{F}_q}\right) = \begin{cases} 1 & \text{ako } t^2 = x \text{ ima rješenje } t \in \mathbb{F}_q^\times, \\ -1 & \text{ako } t^2 = x \text{ nema rješenje } t \in \mathbb{F}_q, \\ 0 & \text{ako } x = 0. \end{cases}$$

Propozicija 1.2.4. *Neka je E elitpička krivulja na $\mathbb{F}_q$, definirana sa $E : y^2 = x^3 + ax + b$. Tada je broj točaka na $E(\mathbb{F}_q)$ dan s:*

$$\#E(\mathbb{F}_q) = q + 1 + \sum_{x \in \mathbb{F}_q} \left(\frac{x^3 + ax + b}{\mathbb{F}_q}\right).$$

Dakle, $a_q(E) = -\sum_{x \in \mathbb{F}_q} \left(\frac{x^3+ax+b}{\mathbb{F}_q}\right)$.

Propozicija 1.2.5. *Neka je $E/\mathbb{F}_q$ eliptička krivulja ($q \neq 2$) i neka je $d \in \mathbb{F}_q^\times$. Tada je $E^{(d)}$ twist od E sa d. Vrijedi*

$$\#E^{(d)}(\mathbb{F}_q) = q + 1 - \left(\frac{d}{\mathbb{F}_q}\right) a_q(E).$$

Dakle, ako je d kvadrat u $\mathbb{F}_q$, tada je $a_q(E^{(d)}) = a_q(E)$, a u suprotnom je $a_q(E^{(d)}) = -a_q(E)$.

Dokaz. Neka je E zadana s $E : y^2 = x^3+ax+b$. $E^{(d)}$ je twist od E sa d pa je $dy^2 = x^3+ax+b$, odnosno $y^2 = x^3 + d^2ax + d^3b$ jednadžba od $E^{(d)}$. Dovoljno je izračunati

$$\sum_{x \in \mathbb{F}_q} \left(\frac{x^3 + d^2ax + d^3b}{\mathbb{F}_q}\right).$$

Kako je Legendreov simbol multiplikativna funckija imamo

$$\left(\frac{x^3 + d^2ax + d^3b}{\mathbb{F}_q}\right) = \left(\frac{d^3}{\mathbb{F}_q}\right)\left(\frac{(x/d)^3 + a(x/d) + b}{\mathbb{F}_q}\right) = \left(\frac{d}{\mathbb{F}_q}\right)\left(\frac{(x/d)^3 + a(x/d) + b}{\mathbb{F}_q}\right).$$

Lako se vidi da je skup svih $x \in \mathbb{F}_q$ za koje je $(x/d)^3 + a(x/d) + b$ u bijekciji sa skupom $x \in \mathbb{F}_q$ za koje je $x^3 + ax + b$ kvadrat. Kako sumiramo po svim $x \in \mathbb{F}_q$ slijedi tražena jednakost. □

Na kraju ovog poglavlja vratimo se na problem računanja torzijske grupe eliptičke krivulje $E/\mathbb{Q}$.

Propozicija 1.2.6. *Neka je E eliptička krivulja i p prost broj. Ako E ima dobru redukciju modulo p, tada je redukcija modulo p restringirana na torzijsku podgrupu*

$$\rho_p : E(\mathbb{Q})_{tors} \to \bar{E}(\mathbb{F}_p)$$

injektivni homomorfizam.

Dokaz. Kako E ima dobru redukciju modulo p, ρ_p je homomorfizam grupa, pa je dovoljno provjeriti da ima trivijalnu jezgru. Neka je $P \in E(\mathbb{Q})_{tors}$. Ako $P \neq O$, tada je $P = (x_0, y_0)$, pa su po Lutz-Nagellovom teoremu $x_0, y_0 \in \mathbb{Z}$. Tada je $\rho_p(P) = \bar{P} = (\bar{x_0}, \bar{y_0}) \neq O$. Dakle, $\operatorname{Ker}\rho_p = \{O\}$. □

Kako je jezgra preslikavanja $\rho_p : E(\mathbb{Q})_{tors} \to \bar{E}(\mathbb{F}_p)$ trivijalna, $E(\mathbb{Q})_{tors}$ je izomorfna slici tog preslikavanja, a to je podgrupa od $\bar{E}(\mathbb{F}_p)$. Dakle, $\#E(\mathbb{Q}_{tors})$ dijeli $\#\bar{E}(\mathbb{F}_p)$. Ovo svojstvo možemo iskoristiti u traženju $\#E(\mathbb{Q}_{tors})$ tako da uzimanamo različitih vrijednosti od p. Dobivamo da $\#E(\mathbb{Q}_{tors})$ mora dijeliti najveći zajednički djelitelj tako dobivenih $\#\bar{E}(\mathbb{F}_p)$.

1.3 Izogenije

Sljedeće nas zanimaju preslikavanja među eliptičkim krivuljama koja bi čuvala njihovu strukuru (i kao algebarskih krivulja i kao Abelovih grupa).

Za to će nam trebati neki pojmovi iz algebarske geometrije, u čije detaljne definicije nećemo ulaziti u ovom radu, a mogu se naći u [6].

Neka je X projektivna algebarska mnogostrukost. Tada X možemo pridružiti polje racionalnih funkcija $K(X)$, koje je konačno generirano proširenje polja K, i dimenzija mnogostrukosti X je jednaka stupnju transcedencije polja $K(X)$ nad K. Projektivna krivulja je projektivna mnogostrukost dimenzije 1. Morfizam je racionalno preslikavanje projektivnih mnogostrukosti koje je regularno u svakoj točki.

Neka su C_1 i C_2 krivulje nad K i $\phi : C_1 \to C_2$ nekonstantno racionalno preslikavanje. Tada imamo inducirano ulaganje pripadnih polja racionalnih funkcija:

$$\phi^* : K(C_2) \to K(C_2), \quad \phi^* f = f \circ \phi.$$

Tada je $K(C_1)$ konačno dimenzionalno proširenje od $\phi^*(K(C_2))$. Definiramo **stupanj** preslikavanja ϕ, u oznaci $\deg \phi$, kao 0, u slučaju da je ϕ konstantno, odnosno kao $[K(C_1) : \phi^*(K(C_2))]$ inače. Kažemo da je ϕ separabilno ako je proširenje $K(C_1)$ nad $\phi^*(K(C_2))$ separabilno.

Definicija 1.3.1. *Neka su E_1 i E_2 eliptičke krivulje. **Izogenija** s E_1 na E_2 je morfizam $\phi : E_1 \to E_2$ takav da je $\phi(O) = O$.*
*Dvije eliptičke krivulje E_1 i E_2 su **izogene** ako postoji izogenija ϕ s E_1 na E_2 takva da je $\phi(E_1) \neq O$.*

Teorem 1.3.2. *Neka je $\phi : C_1 \to C_2$ morfizam projektivnih algebarskih krivulja. Tada je ϕ ili konstantno ili surjektivno preslikavanje.*

Dokaz gornjeg teorema može se naći u [2]. Iz teorema slijedi da su jedine mogućnosti za sliku izogenije ϕ:

$$\phi(E_1) = O \quad \text{ili} \quad \phi(E_1) = E_2.$$

Prvi slučaj zovemo nul-izogenija, i pišemo $[0](P) = O$, za svaki $P \in E_1$.
Za eliptičke krivulje E_1, E_2 označimo s $\mathrm{Hom}(E_1, E_2)$ skup svih izogenija s E_1 u E_2. Zbroj dvije izogenije $\phi, \psi : E_1 \to E_2$ je definiran s $(\phi + \psi)(P) = \phi(P) + \psi(P)$, $P \in E_1$. Izogenija $\phi + \psi$ je opet morfizam krivulja pa i očito izogenija, dakle, $\phi + \psi \in \mathrm{Hom}(E_1, E_2)$. Za $\phi \in \mathrm{Hom}(E_1, E_2)$ je $-\phi : E_1 \to E_2$, $(-\phi =)(P) = -\phi(P)$ također izogenija i očito $\phi + (-\phi) = [0]$. Dakle, $\mathrm{Hom}(E_1, E_2)$ je grupa.

Ako je $E_1 = E_2$, izogenije možemo i komponirati. Izogeniju $E \to E$ zovemo **endomorfizam** i skup svih endomorfizama od E označavamo s $\mathrm{End}(E) = \mathrm{Hom}(E, E)$. $\mathrm{End}(E)$ je prsten s operacijama zbrajanja i komponiranja.

Primjer 1.3.3. *Za svaki $m \in \mathbb{Z}$ možemo definirati izogeniju množenja s m $[m] : E \to E$. Za $m > 0$ definiramo na prirodan način:*

$$[m]P = \underbrace{P + \cdots + P}_{m \text{ puta}}, \quad P \in E,$$

dok za $m < 0$ definiramo $[m]P = [-m](-P)$. Za $m = 0$ već smo definirali nul-izogeniju.
Da je $[m]$ morfizam slijedi induktivno iz formula za zbrajanje točaka na eliptičkoj krivulji, a očito je $[m]O = O$, pa je $[m]$ izogenija.
Može se pokazati da je, za $m \neq 0$, $[m]$ nekonstantno preslikavanje.
Također, vrijedi da je $\deg[m] = m^2$ i $[m]$ je separabilna izogenija.

Sljedeći teorem pokazuje da su izogenije doista pogodna preslikavanja između eliptičkih krivulja, u smislu da čuvaju i njihovu grupovnu strukturu.

Teorem 1.3.4. *Neka je $\phi : E_1 \to E_2$ izogenija. Tada je*

$$\phi(P + Q) = \phi(P) + \phi(Q), \quad \text{za svake } P, Q \in E_1.$$

Drugim riječima, ϕ je homomorfizam grupa E_1 i E_2.

Korolar 1.3.5. *Ako je $\phi : E_1 \to E_2$ izogenija, tada je* $\operatorname{Ker}\phi = \phi^{-1}(O)$ *konačna grupa, reda najviše* $\deg\phi$.

Za separabilnu izogeniju ϕ vrijedi i više, tada je $\#\operatorname{Ker}\phi = \deg\phi$.
U odjeljku 1.1 definirali smo m-torziju $E[m]$ kao skup svih točaka P na E čiji red dijeli m, to jest $[m]P = O$. U vidu izogenija, jasno je da je $E[m]$ upravo $\operatorname{Ker}[m]$. Stoga iz dosada navedenih činjenica o izogenijama možemo zaključiti da je $\#E[m] = m^2$. Vrijedi i više:

Teorem 1.3.6. *Neka je $m \in \mathbb{N}$. Ako je $char(K) = 0$ ili $char(K) = p > 0$ i $p \nmid m$, tada je*

$$E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

Nadalje, ako je $char(K) = p > 0$, tada je ili $E[p^r] \cong O$, za sve $r \in \mathbb{N}$, ili je $E[p^r] \cong \mathbb{Z}/p^r\mathbb{Z}$, za sve $r \in \mathbb{N}$

U sljedećem primjeru definiramo još jednu važan tip izogenija.

Primjer 1.3.7. *Neka je K polje karakteristike $p > 0$, neka je $q = p^r$, za $r \geq 1$ i E/K eliptička krivulja zadana Weierstrassovom jednadžbom., odnosno s $f(x, y) = 0$. Neka je $E^{(q)}/K$ krivulja zadana potenciranjem koeficijenata od f na q-tu potenciju. Preslikavanje između E i E^q je dano s*

$$\phi_q : E \to E^{(q)}, \quad \phi(x, y) = (x^q, y^q)$$

*i to je morfizam krivulja, koji zovemo **Frobeniusov morfizam**. Za ϕ_q se može pokazati da je neseparabilan morfizam i* $\deg\phi_q = q$.

Kako je E^q zadana Weierstrassovom jednadžbom, bit će eliptička krivulja ako je nesingularna. Koristeći da je preslikavanje $K \to K, a \mapsto a^q$ homomorfizam, dobivamo da je $\Delta(E^{(q)}) = \Delta(E)^q$ i $j(E^{(q)}) = j(E)^q$. Posebno, jer je E nesingularna, slijedi da je i $E^{(q)}$ nesingularna, dakle $E^{(q)}$ je eliptička krivulja nad K.

*Posebno, ako je $K = \mathbb{F}_q$, tada je preslikavanje $K \to K, a \mapsto a^q$ identiteta, pa je $E = E^{(q)}$, tj. preslikavanje ϕ_q je endomorfizam na E. Tada ϕ_l zovemo **Frobeniusov endomorfizam**. Grupa $E(\mathbb{F}_q)$ je točno skup točaka koje ϕ_q fiksira.*

Prisjetimo se da smo definirali Frobeniusov trag $a_q(E) = q + 1 - \#E(\mathbb{F})_q$. Može se pokazati da za Frobeniusov endomorfizam ϕ_q vrijedi

$$\phi_q^2 - [a_q(E)]\phi_q + [q] = 0,$$

što je jednakost u $\mathrm{End}(E)$. Više o Frobeniusovom endomorfizmu može se naći u [9].

Za eliptičku krivulju E/K i $n \in \mathbb{N}$, ako postoji K-racionalna izogenija $\phi : E \to E'$ takva da je $\mathrm{Ker}\,\phi$ ciklička reda n, kažemo da E ima n-izogeniju.

Primjer 1.3.8. *Neka je* $\mathrm{char}(K) \neq 2$ *i* E/K *eliptička krivulja zadana s*

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

$\Delta(E) = 16b^2(a^2 - 4b)$*, pa zahtijevamo* $b \neq 0$ *i* $a^2 - 4b \neq 0$ *kako bi* E *bila nesingularna. Neka je* E' *eliptička krivulja zadana s*

$$E' : y^2 = x^3 - 2ax^2 + (a^2 - 4b)x$$

i neka je zadano preslikavanje $\alpha : E \to E'$*,*

$$\alpha(x, y) = \left(\frac{y^2}{x^2}, \frac{y(x^2 - b)}{x^2}\right).$$

α *je izogenija krivulja* E *i* E'*. Imamo i izogeniju*

$$\hat{\alpha} : E' \to E,\ \hat{\alpha}(x', y') = \left(\frac{y'^2}{4x'^2}, \frac{y'(a^2 - 4b - x'^2)}{8x'^2}\right),$$

te se direktnim uvrštavanjem dobiva da vrijedi $\hat{\alpha} \circ \alpha = [2]$ *na* E *i* $\alpha \circ \hat{\alpha} = [2]$ *na* E'*. Neka je* $P \in \mathrm{Ker}(\alpha)$*. Tada je* $\alpha(P) = O$*, pa je* $[2]P = \hat{\alpha}(\alpha(P)) = \hat{\alpha}(O) = O$*. Dakle,* $P = O$ *ili* $P = (x_0, 0)$*, tj.* $P = (0, 0)$*. Zaključujemo da je* $\mathrm{Ker}(\alpha) = \{O, (0, 0)\}$*, pa je* α *2-izogenija.*

Propozicija 1.3.9. *Neka je* $\phi : E_1 \to E_2$ *izogenija stupnja* m*. Tada postoji jedinstvena izogenija* $\hat{\phi} : E_2 \to E_1$ *takva da vrijedi*

$$\hat{\phi} \circ \phi = [m].$$

$\hat{\phi}$ *zovemo* ***dualna izogenija*** *od* ϕ*.*

Izogenije α i $\hat{\alpha}$ iz prethodnog primjera su primjer dualnih izogenija. Iz prethodne propzicije slijedi da je "biti izogen" relacija ekvivalencije na eliptičkim krivuljama.

Može se pokazati da izogene krivulje imaju isti konduktor.

Ako su $E/\mathbb{F}_q$ i $E'/\mathbb{F}_q$ eliptičke krivulje izogene nad $\mathbb{F}_q$, tada je $\#E(\mathbb{F}_q) = \#E'(\mathbb{F}_q)$. Štoviše, vrijedi i obrat.

Sljedeći teorem govori kada E ne može imati p-izogenije, u slučaju kada je p prost broj. To će nam biti korisno kasnije, u rješavanju diofantskih jednadžbi.

Teorem 1.3.10 (Mazur [5])**.** *Neka je $E/\mathbb{Q}$ eliptička krivulja, p prost broj.*

(i) Ako je $p \geqslant 17$ i $j(E) \notin \mathbb{Z}[\frac{1}{2}]$, tada E nema p-izogenija.

(ii) Ako je $p \geqslant 11$ i E je polustabilna eliptička krivulja, tada E nema p-izogenija.

(iii) Ako je $p \geqslant 5$ i E polustabilna eliptička krivulja takva da je $\#E(\mathbb{Q})[2] = 4$, tada E nema p-izogenija.

Poglavlje 2

Newforme, Ribetov teorem i teorem o modularnosti

U ovom poglavlju dati ćemo kratki pregled osnovnih definicija o modularnim formama, te iskazati bitne teoreme koje ćemo koristiti u zadnjem poglavlju. U ovom radu nećemo ulaziti u detalje ovog vrlo opsežnog područja. Opširnije o ovoj temi te dokazi iskazanih činjenica mogu se naći u [1].

2.1 Modularne forme

Modularna grupa je grupa 2×2 matrica s cjelobrojnim elementima i determinantom 1,

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{Z}, ad - bc = 1 \right\}.$$

Modularna grupa generirana je matricama $\left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$ i $\left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]$.

Svaki element modularne grupe možemo shvatiti kao automorfizam Riemannove sfere $\hat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$, čije je djelovanje dano s

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}(\tau) = \frac{a\tau + b}{c\tau + d}, \quad \tau \in \hat{\mathbb{C}}.$$

Pritom podrazumijevamo da ako je $c \neq 0$, tada se $-d/c$ preslikava u ∞, a ako je $c = 0$, tada se ∞ preslikava u ∞. Svaki par matrica $\pm\gamma \in \mathrm{SL}_2(\mathbb{Z})$ daje istu transformaciju. Grupa transformacija je generirana preslikavanjima pridruženima generatorima modularne grupe, $\tau \mapsto \tau + 1$ i $\tau \mapsto -1/\tau$.

Gornja poluravnina je

$$\mathcal{H} = \{\tau \in \mathbb{C} : \mathrm{Im}(\tau) > 0\}.$$

Modularna grupa djeluje na $\mathcal{H}$, to jest preslikava gornju poluravninu natrag na samu sebe te je $I(\tau) = \tau$ i $(\gamma\gamma')(\tau) = \gamma(\gamma'(\tau))$, za sve $\gamma, \gamma' \in \mathrm{SL}_2(\mathbb{Z})$.

Za meromorfnu funkciju $f : \mathcal{H} \to \mathbb{C}$ kažemo da je **slabo modularna težine** k, gdje je $k \in \mathbb{Z}$, ako je

$$f(\gamma(\tau)) = (c\tau + d)^k f(\tau), \quad \text{za sve } \gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \text{ i } \tau \in \mathcal{H}.$$

Slabu modularnost dovoljno je provjeriti na generatorima modularne grupe, to jest f je slabo modularna težine k ako vrijedi

$$f(\tau + 1) = f(\tau) \text{ i } f(-1/\tau) = \tau^k f(\tau).$$

Primjetimo da kako $c\tau + d$ nema nultočaka niti polova na $\mathcal{H}$, $f(\tau)$ i $f(\gamma(\tau))$ imaju iste nultočke i polove.

Neka je f slabo modularna funkcija. Tada je $f(\tau + 1) = f(\tau)$, tj. f je $\mathbb{Z}$-periodična, pa f možemo pridružiti funkciju $g : D' \to \mathbb{C}$, takvu da je $f(\tau) = g(2\pi i)$, gdje je $D' = \{q \in \mathbb{C} : |q| < 1\} \setminus \{0\}$. Ako je f holomorfna na $\mathcal{H}$, tada se g može razviti u Laurentov red $g(q) = \sum_{n\in\mathbb{Z}} a_n q^n$, $q \in D'$. Kako je $|q| = e^{-2\pi \operatorname{Im}(\tau)}$, slijedi da $q \to 0$ kada $\operatorname{Im}(\tau) \to \infty$. Zato kažemo da je f holomorfna u ∞ ako se g može proširiti do holomorfne funkcije u $q = 0$, to jest Laurentov razvoj od g sadrži samo sumande s $n \in \mathbb{N}$. Tada se f može razviti u Fourierov red

$$f(\tau) = \sum_{n=0}^{\infty} a_n(f) q^n, \quad q = e^{2\pi i \tau}.$$

Da bi holomorfna slabo modularna fukncija bila holomorfna u ∞ dovoljno je vidjeti da $\lim_{\operatorname{Im}(\tau)\to\infty} f(\tau)$ postoji ili da je $f(\tau)$ ograničena kada $\operatorname{Im}(\tau) \to \infty$.

Definicija 2.1.1. *Neka je k cijeli broj. Funkcija $f : \mathcal{H} \to \mathbb{C}$ je **modularna forma težine** k ako je f holomorfna na $\mathcal{H}$, slabo modularna težine k i holomorna u ∞.*
Skup svih modularnih formi označavamo s $\mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z}))$.

$\mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z}))$ je vektorski prostor nad $\mathbb{C}$. Produkt modularnih formi težine k i l je modularna forma težine $k + l$. Zato skup modularnih formi svih težina čini prsten,

$$\mathcal{M}(\mathrm{SL}_2(\mathbb{Z})) = \bigoplus_{k\in\mathbb{Z}} \mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z})).$$

Kusp forma težine k je modularna forma težine k čiji je vodeći koeficijent u Fourierovom razvoju $a_0 = 0$. Skup svih kusp formi težine k označavamo s $\mathcal{S}_k(\mathrm{SL}_2(\mathbb{Z}))$, i to je vektorski potprostor od $\mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z}))$. Vrijedi da je

$$\mathcal{S}(\mathrm{SL}_2(\mathbb{Z})) = \bigoplus_{k\in\mathbb{Z}} \mathcal{S}_k(\mathrm{SL}_2(\mathbb{Z}))$$

ideal u $\mathcal{M}(\mathrm{SL}_2(\mathbb{Z}))$.

Neka je $N \in \mathbb{N}$. **Glavna kongurencijska podgrupa** nivoa N je

$$\Gamma(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \pmod{N} \right\}.$$

Primjerice, $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$. Označimo s $\phi_N : \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, prirodni homomrfizam tih grupa, $\phi_N : \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \mapsto \left[\begin{smallmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{smallmatrix}\right]$, gdje je $\bar{m}$ ostatak od m pri dijeljenju s N. Tada je $\Gamma(N) = \mathrm{Ker}\,\phi_N$, pa je $\Gamma(N)$ normalna podgrupa od $\mathrm{SL}_2(\mathbb{Z})$. Štoviše, to preslikavanje je surjektivno, pa inducira izmorfizam grupa

$$\mathrm{SL}_2(\mathbb{Z})/\Gamma(N) \cong \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}).$$

Kako je grupa $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ konačna, to pokazuje da je $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N)]$ konačno.

Definicija 2.1.2. *Podgrupa Γ od $\mathrm{SL}_2(\mathbb{Z})$ je **kongruencijska podgrupa** ako je $\Gamma(N) \subset \Gamma$ za neki $N \in \mathbb{N}$. Za najmanji takav N kažemo da je **nivo** kongruencijske podgrupe Γ.*

Iz rasprave prije definicije slijedi da svaka kongruencijska podgrupa ima konačan indeks u $\mathrm{SL}_2(\mathbb{Z})$.

Primjer 2.1.3. *Osim $\Gamma(N)$, najvažniji primjeri kongruencijskih podgrupa su*

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N} \right\},$$

$$\text{te } \Gamma_1(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix} \pmod{N} \right\}.$$

Vrijedi

$$\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N) \subset \mathrm{SL}_2(\mathbb{Z}).$$

Štoviše, može se pokazati da je $\Gamma(N) \trianglelefteq \Gamma_1(N)$ i $[\Gamma_1(N) : \Gamma(N)] = N$, te $\Gamma_1(N) \trianglelefteq \Gamma_0(N)$ i $[\Gamma_0(N) : \Gamma(N)_1] = \phi(N)$.

Za $\gamma = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbb{Z})$ i $\tau \in \mathcal{H}$ definiramo **faktor automorfnosti** $j(\gamma, \tau) = c\tau + d$, te operator $[\gamma]_k$ na funkcijama $f : \mathcal{H} \to \mathbb{C}$:

$$(f[\gamma]_k)(\tau) = j(\gamma, \tau)^{-k} f(\gamma(\tau)).$$

Kako je $j(\gamma, \tau)$ uvijek različit od 0 i ∞, slijedi da ako je f meromorfna funkcija, tada je i $f[\gamma]_k$ meromorfna te ima iste nultočke i polove kao f. Kažemo da je meromorfna funkcija $f : \mathcal{H} \to \mathbb{C}$ **slabo modularna težine k u odnosu na** Γ (gdje je Γ kongruencijska podgrupa) ako je

$$f[\gamma]_k = f, \text{ za sve } \gamma \in \Gamma.$$

Dovoljno je provjeriti slabu modularnost na generatorima od Γ. Ako je f slabo modularna u odnosu na Γ, tada je $f[\gamma]_k$ slabo modularna u odnosu na $\gamma^{-1}\Gamma\gamma$.

Svaka kongruencijska podgrupa Γ od $\mathrm{SL}_2(\mathbb{Z})$ sadrži translacijsku matricu $\left[\begin{smallmatrix}1 & h\\ 0 & 1\end{smallmatrix}\right] : \tau \mapsto \tau + h$, za neki minimalni $h \in \mathbb{N}$ (jer $\Gamma(N) \subset \Gamma$, pa je $\left[\begin{smallmatrix}1 & N\\ 0 & 1\end{smallmatrix}\right] \in \Gamma$). Svaka f koja je slabo modularna obzirom na Γ je zato $h\mathbb{Z}$-periodčina, pa postoji funkcija $g : D' \to \mathbb{C}$ takva da je $f(\tau) = g(q_h)$, gdje je $q = e^{2\pi i\tau/h}$. Ako je f holomorfna na $\mathcal{H}$, tada je g holomorfna na D' pa ima Laurentov razvoj. Kažemo da je f holomorfna u ∞ ako se g može proširiti do holomorfne funkcije u 0. Tada f ima Fourierov razvoj

$$f(\tau) = \sum_{n=0}^{\infty} a_n q_h^n, \quad g_h = e^{2\pi i\tau/h}.$$

Klasu ekvivalencije djelovanja grupe Γ na $\mathbb{Q} \cup \infty$ zovemo **kusp** od Γ. Za svaki $s \in \mathbb{Q} \cup \infty$ postoji $\alpha \in \mathrm{SL}_2(\mathbb{Z})$ takav da je $s = \alpha(\infty)$, tj. svi racionalni brojevi su $\mathrm{SL}_2(\mathbb{Z})$-ekvivalentni ∞, pa je ∞ jedini kusp od $\mathrm{SL}_2(\mathbb{Z})$. Za proizvoljnu kongruencijsku grupu Γ Želimo definirati holomorfnost u svim kuspovima od Γ. Neka je f holomorfna na $\mathcal{H}$ i slabo modularna težine k u odnosu na Γ i $s \in \mathbb{Q}$. Tada postoji $\alpha \in \mathrm{SL}_2(\mathbb{Z})$ takav da je $s = \alpha(\infty)$. Funkcija $f[\alpha]_k$ je holomorfna na $\mathcal{H}$ i slabo modularna u odnosu na $\alpha^{-1}\Gamma\alpha$. Kažemo da je f holomorna u s ako je $f[\alpha]_k$ holomorna u ∞. To objašnjava sljedeću definiciju:

Definicija 2.1.4. *Neka je Γ kongruencijska podgrupa od $\mathrm{SL}_2(\mathbb{Z})$ i $k \in \mathbb{Z}$. Funkcija $f : \mathcal{H} \to \mathbb{C}$je **modularna forma težine** k **u odnosu na** Γ ako je holomorfna na $\mathcal{H}$, slabo modularna težine k u odnosu na Γ i $f[\alpha]_k$ je holomorfna u ∞ za sve $\alpha \in \mathrm{SL}_2(\mathbb{Z})$.*
Skup svih modularnih formi težine k u odnosu na Γ označavamo s $\mathcal{M}_k(\Gamma)$.
*Ako je $a_0 = 0$ vodeći član u Fourierovom razvoju od $f[\alpha]_k$ za sve $\alpha \in \mathrm{SL}_2(\mathbb{Z})$, onda kažemo da je f **kusp forma težine** k **u odnosu na** Γ. Skup svih kusp formi težine k u odnosu na Γ označavamo s $\mathcal{S}_k(\Gamma)$.*

Skup $\mathcal{M}_k(\Gamma)$ je vektorski prostor nad $\mathbb{C}$, a $\mathcal{S}_k(\Gamma)$ je njegov vektorski potprostor. Skupovi modolarnih, odnosno kusp formi, svih težina u odnosu na Γ,

$$\mathcal{M}(\Gamma) = \bigoplus_{k\in\mathbb{Z}} \mathcal{M}_k(\Gamma), \quad \mathcal{S}(\Gamma) = \bigoplus_{k\in\mathbb{Z}} \mathcal{S}_k(\Gamma)$$

su prsteni, a $\mathcal{S}(\Gamma)$ je ideal u $\mathcal{M}(\Gamma)$.

2.2 Newforme

Na modularnim formama možemo definirati tzv. Heckeove operatore, $\langle n\rangle$ i T_n, za $n \in \mathbb{N}$, koji imaju dobra svojstva. Definicija Heckeovih operatora može se naći u [1].

Na prostoru $\mathcal{S}_k(\Gamma_1(N))$ može se definirati skalarni produkt i to tako da su svi Heckeovi operatori $\langle n\rangle$ i T_n za $nzd(n,N) = 1$ normalni na tom prostoru. Kako je prostor $\mathcal{S}_k(\Gamma_1(N))$ konačno dimenzionalan i Heckeovi operatori komutiraju, tada po spektralnom teoremu iz linearne algebre postoji ortogonalna baza vektora koji su istovremeno svojstveni vektori za sve $\langle n\rangle$ i T_n za $nzd(n,N) = 1$. Kako su u ovom slučaju vektori zapravo modularne forme, zovemo ih svojstvene forme.

Prostor $\mathcal{S}_k(\Gamma_1(N/d))$ možemo dekomponirati kao ortogonalnu sumu prostora $\mathcal{S}_k(\Gamma_1(N))^{old}$ i $\mathcal{S}_k(\Gamma_1(N))^{new}$. Ovdje nećemo ulaziti u njihovu definiciju, koja se može naći u [1].

Prostori $\mathcal{S}_k(\Gamma_1(N))^{old}$i $\mathcal{S}_k(\Gamma_1(N))^{new}$ imaju ortogonalnu bazu svojstvenih formi za Heckeove operatore $\{T_n, \langle n\rangle : nzd(n,N) = 1\}$.

Definicija 2.2.1. *Newforma nivoa N je normalizirana svojstvena forma za sve Heckeove operatore $T_n, \langle n\rangle$ za sve $n \in \mathbb{N}$ koja pripada prostoru $\mathcal{S}_k(\Gamma_1(N))^{new}$.*

Ovdje nam normaliziranost od f znači da je $a_1 = 1$ u Fourierovom razvoju od f.

Za newforme vrijedi da su njima pridružene svojstvene vrijednosti operatora T_n upravo pripadni Fourierovi koeficijenti, tj. $T_n f = a_n(f)f$, za sve $n \in \mathbb{N}$.

Za fiksni k i N postoji samo konačno mnogo newformi težine k i nivoa N.

Nas će nadalje zanimati newforme težine $k = 2$. Navesti ćemo neka svojstva newformi koja će nam biti korisna u primjeni na rješavanje jednadžbi. Neka je $f \in \mathcal{S}_2(\Gamma_1(N))$ newforma. Modularna forma f je zadana svojim Fourierovim razvojem,

$$f = \sum_{n=1}^{\infty} c_n q^n,\ q = e^{2\pi i\tau}. \tag{2.1}$$

Newformi f pridruženo je polje algebarskih brojeva $K_f = \mathbb{Q}(\{c_n : n \in \mathbb{N}\})$. Svako ulaganje $\sigma : K_f \hookrightarrow \mathbb{C}$ konjugira f djelujući na koeficijente c_n od f, dakle

$$f^\sigma(\tau) = \sum_{n=1}^{\infty} c_n^\sigma q^n.$$

Štoviše, može se pokazati da je f^σ također newforma. Nas će zanimati newforme do na konjugiranje sa σ. Za proste l imamo ocjenu za koeficijente c_l imamo ocjenu:

$$|c_l^\sigma| \leq 2\sqrt{l}, \quad \text{za sva ulaganja } \sigma : K_f \hookrightarrow \mathbb{C}.$$

Također, a_n su algebarski cijeli brojevi. Može se pokazati i da je K_f realno konačno dimenzionalno proširenje od $\mathbb{Q}$.

Kažemo da je newforma f racionalna ako su svi $c_n \in \mathbb{Q}$, inače kažemo da je f iracionalna.

Kako je $\Gamma_1(N) \subset \Gamma_0(N)$, vrijedi $\mathcal{S}_2(\Gamma_0(N)) \subset \mathcal{S}_2(\Gamma_1(N))$. U teoremu o modularnosti biti će nam bitne baš newforme iz $\mathcal{S}_2(\Gamma_1(N))$. Za dimenzije $\mathcal{S}_2(\Gamma_0(N))$ imamo formule u ovisnosti o N (vidi [1]), pa možemo odrediti kada je $\mathcal{S}_2(\Gamma_0(N)) = \{0\}$.

Teorem 2.2.2. *Ne postoje newforme iz $\mathcal{S}_2(\Gamma_0(N))$ na sljedećim nivoima: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 22, 25, 28, 60.*

U programskom paketu `SAGE` [10] implementirani su algoritmi za računanje newformi zadanog nivoa N.

Definicija 2.2.3. *Neka je $E/\mathbb{Q}$ eliptička krivulja s konduktorom N i neka je f newforma na niovu N', sa Fourierovim razvojem*

$$f = q + \sum_{n\geq 2} c_n q^n,$$

te $K_f = \mathbb{Q}(c_2, c_3, ...)$. Kažemo da E proizlazi modulo p iz newforme f, i pišemo $E \sim_p f$, ako postoji prosti ideal $\mathfrak{P} \mid p$ u K_f takav da za skoro sve proste brojeve l vrijedi

$$a_l(E) \equiv c_l \pmod{\mathfrak{P}}$$

Zapravo, možemo biti i precizniji:

Propozicija 2.2.4. *Pretpostavimo da $E \sim_p f$. Tada postoji prosti ideal $\mathfrak{P} \mid p$ u K_f takav da za svaki prosti broj l vrijedi:*

(i) ako $l \nmid pNN'$, tada je $a_l(E) \equiv c_l \pmod{\mathfrak{P}}$,

(ii) ako $l \nmid pN'$ i $l \| N$, tada $l + 1 \equiv \pm c_l \pmod{\mathfrak{P}}$.

Ako je f racionalna newforma, tada f odgovara nekoj eliptičkoj krivulji F. Ako E proizlazi modulo p iz f, tada kažemo i da E proizlazi modulo p iz F. Pišemo: $E \sim_p F$. U tom slučaju imamo poboljšanje gornje propozicije:

Propozicija 2.2.5. *Neka su E, F eliptičke krivulje nad $\mathbb{Q}$ s konduktorima N, N' redom i pretpostavimo da $E \sim_p F$. Tada za svaki prosti broj l vrijedi:*

(i) ako $l \nmid NN'$, tada je $a_l(E) \equiv a_l(F) \pmod{p}$

(ii) ako $l \nmid N'$ i $l \| N$, tada $l + 1 \equiv \pm a_l(F) \pmod{p}$.

Primjetimo da je gornja propozicija doista poboljšanje prethodne: naime, uklonjena je pretpostavka $l \neq p$.
Uvjete na l iz propozicije možemo izreći i na drugi način: $l \nmid NN'$ je ekvivalentno tome da E i F imaju dobru redukciju u l, dok je $l \nmid N'$ i $l \| N$ ekvivaletno tome da F ima dobru redukciju u l, a E ima multiplikativnu redukciju u l.

Ribetov teorem o snižavanju nivoa

Neka je $E/\mathbb{Q}$ eliptička krivulja, te označimo $\Delta = \Delta_{min}(E)$ i N konduktor od E. Sa $ord_p(n)$ označavamo najveću potenciju od p koja dijeli n. Za je p prost broj, neka je:

$$N_p = N/ \prod_{\substack{q||N \\ p|ord_q(\Delta)}} q. \tag{2.2}$$

Navest ćemo pojednostavljeni slučaj Ribetovog teorema o spuštanju nivoa, koji će nam biti bitan u daljnjim razmatranjima.

Teorem 2.2.6 (Ribet)**.** *Neka je $E/\mathbb{Q}$ eliptička krivlja, Δ, N kao gore i $p \geq 5$. Pretpostavimo da je E modularna te da E nema p-izogenija. Neka je N_p definiran kao u 2.2. Tada postoji newforma f na nivou N_p takva da je $E \sim_p f$.*

Primjetimo da Ribetov teorem ne jamči da će f biti racionalna newforma.

Teorem o modularnosti

Teorem 2.2.7 (Teorem o modularnosti)**.** *Neka je E eliptička krivulja nad $\mathbb{Q}$ konduktora N. Tada postoji newforma $f \in \mathcal{S}_2(\Gamma_0(N))$, takva da je*

$$a_p(f) = a_p(E), \quad \textit{za sve proste } p.$$

Za svaki prirodan broj N, newforme nivoa N su u bijekciji s klasama izogenije eliptičkih krivulja konduktora N. Pridruživanje $f \mapsto E_f$ opisao je Shimura. Iz teorema o modularnosti slijedi da je ovo preslikavanje surjektivno.

Teorem o modularnosti prvo je dokazao Andrew Wiles za polustabilan slučaj, to jest kvadratno slobodni N, što je bilo dovoljno za dokaz posljednjeg Fermatovog teorema. Dokaz za ostale slučajeve dovršili su Christophe Breuil, Brian Conrad, Fred Diamond i Richard Taylor. Više o ovom teoremu može se naći u [1], uključujući nekoliko ekvivalentnih formulacija.

Poglavlje 3

Primjene na diofantske jednadžbe

U ovom poglavlju pokazat ćemo kako do sada razvijenu teoriju eliptičkih krivulja i modularnih formi primjeniti na rješavanje nekih konkretnih diofantskih jednadžbi. Od posebnog su nam zanimanja eksponencijalne diofantske jednadžbe, pogotovo one slične Fermatovoj jednadžbi. Pritom će ključnu ulogu igrati teorem o modularnosti te Ribetov teorem iz prethodng poglavlja. U ovom poglavlju oslanjali smo se prvenstveno na bilješke Samira Sikseka [7], u kojima se mogu naći daljnje refernce i drugi primjeri.

Za danu diofantsku jednadžbu pretpostavit ćemo da ima rješenje i pridružiti mu eliptičku krivulju E, koju zovemo *Freyeva krivulja*. Bitna svojstva koja ćemo zahtjevati od Freyeve krivulje E su sljedeća:

- koeficijenti od E ovise (na neki način) o (pretpostavljenom) rješenju dane diofantske jednadžbe
- minimalna diskriminanta od E se može zapisati u obliku $\Delta_{min} = C \cdot D^p$, gdje je D izraz koji ovisi o rješenju diofantske jednadžbe, dok C ne ovisi o rješenju, već samo o samoj diofantskoj jednadžbi.
- E ima multiplikativnu redukciju u prostim dijeliteljima od D.

Tada će konduktor N od E biti djeljiv s onim prostim brojevima koji dijele C i D. U izrazu za N_p (iz Ribetovog teorema) poništit će se prosti dijelitelji od D, pa će N_p ovisiti samo o diofantskoj jednadžbi. Dakle, imat ćemo konačno mogućnosti za N_p, i za svaki N_p samo konačno mnogo newformi f na nivou N_p. Iz teorema modularnosti je tada $E \sim_p f$ za neku od konačno mnogo f. Ovisno o svojstvima newformi na nivou N_p moći ćemo izvesti zaključke o rješenju početne diofantske jednadžbe.

U prvom odjeljku ovog poglavlja pokazat ćemo kako je ova metoda primjenjena na poznatu Fermatovu jednadžbu, što je napokon dovelo do njenog potpunog rješenja. Nakon toga, u sljedećim odjeljcima dajemo pregled još nekih primjera jednadžbi u čijem

rješavanju se koriste metode koje se oslanjaju na teoriju eliptičkih krivulja i modularnih formi.

3.1 Fermatova jednadžba

Poznati posljednji Fermatov teorem glasi

Teorem 3.1.1 (Posljednji Fermatov teorem)**.** *Jednadžba $a^n + b^n = c^n$ nema rješenja za cijele brojeve a, b, c, n takve da je $n > 2$ i $abc \neq 0$.*

Prvi ga je iskazao Fermat 1637. godine, a potpuni dokaz dao je Andrew Wiles 1995., dokazavši teorem o modularnosti za polustabilne eliptičke krivulje u [11].
Dovoljno je pokazati sljedeću verziju:

Teorem 3.1.2. *Neka je $p \geq 5$ prost. Jednadžba*

$$a^p + b^p + c^p = 0 \tag{3.1}$$

nema rješenja za $a, b, c \in \mathbb{Z}$, $abc \neq 0$ i a, b, c u parovima relativno prosti.

Dokaz. Pretpostavimo da je a, b, c rješenje od 3.1 takvo da $abc \neq 0$ i a, b, c su u parovima relativno prosti. Promatranjem jednadžbe modulo 2 vidimo da je točno jedan od a, b, c paran, pa bez smanjena općenitosti možemo pretpostavti da je to b. Tada je $b^p \equiv 0 \pmod 4$, pa je $a^p + c^p \equiv -b^p \equiv 0 \pmod 4$, to jest točno jedan od a^p i c^p je kongruentan 1, a drugi -1. Dakle, možemo pretpostaviti da vrijedi

$$a^p \equiv -1 \pmod 4, \quad b^p \equiv 0 \pmod 2.$$

Ovom rješenju pridružimo Freyevu eliptičku krivulju

$$E : y^2 = x(x - a^p)(x + b^p).$$

Prema pretpostavci $a, b, c \in \mathbb{Z}$ pa je E eliptička krivulja nad $\mathbb{Q}$. Prema teoremu o modularnosti, E je modularna. Prema 1.1.3 i uvažavajući da a i b zadovoljavaju 3.1:

$$\Delta = 16a^{2p}b^{2p}(a^p + b^p)^2 = 16(abc)^{2p}, \quad c_4 = 16(c^{2p} - a^p b^p), \quad j = \frac{256(c^{2p} - a^p b^p)}{(abc)^2 p}.$$

Nadalje, trebamo izračunati minimalnu diskriminantu i konduktor od E. Prisjetimo se da smo u primjeru 1.2.2 našli minimalni model za ovaj oblik jednadžbe (uz upravo iste pretpostavke koje sada imamo na brojeve a^p i b^p) i pokazali da je polustabilna. Dakle,

$$\Delta_{min} = \frac{(abc)^{2p}}{2^8}, \quad N = \prod_{\substack{l \mid abc \\ l \text{ prost}}} l.$$

Dakle, prosti q takvi da $q \parallel N$ su upravo svi prosti djelitelji od abc. Znamo da je 2 jedan od njih jer $2 \mid b$. Za svaki takav $q \neq 2$ je $ord_q(\Delta_{min}) = 2pk$, a $ord_2(\Delta_{min}) = 2pk - 8$, za neki $k \in \mathbb{Z}$, pa (zbog $p \geq 5$) slijedi da $p \mid ord_q(\Delta_{min})$, za svaki $q \mid abc, q \neq 2$. Iz formule 2.2 za N_p slijedi da je $N_p = 2$.

Za primjenu Ribetovog teorema trebamo se uvjeriti da E nema p-izogenija. Vidimo da je E polustabilna. Želimo primjeniti teorem 1.3.10, pa trebamo još provjeriti da je $\#E(\mathbb{Q})[2] = 4$. Doista:

$$P = (x_1, y_1) \in E(\mathbb{Q})[2] \quad \Leftrightarrow \quad y_1 = 0 \quad \Leftrightarrow \quad x_1(x_1 - a^p)(x_1 + b^p) = 0.$$

Prema pretpostavci $a, b \neq 0$, i međusobno različiti, pa imamo 3 različite 2-torzijske točke, uz O, to jest $\#E(\mathbb{Q})[2] = 4$. Sada iz teorema 1.3.10,(*iii*) slijedi da E nema p-izogenija.
Prema teoremu o modularnosti E je modularna, pa prema Ribetovom teoremu tada postoji newforma f nivoa N_p takva da je $E \sim_p f$. No, jer $N_p = 2$, to je u kontradikciji s teoremom 2.2.2 koji kaže da ne postoje newforme nivoa 2. □

3.2 Jednadžba $x^p + L^r y^p + z^p = 0$

Neka je L neparan prost broj. Promotrimo jednadžbu

$$x^p + L^r y^p + z^p = 0, \quad xyz \neq 0, \quad p \geq 5 \text{ prost.} \tag{3.2}$$

Ovo je jednadžba sličnog tipa kao 3.1, a proučavali su je Serre i Kraus.

Pretpostavimo da su x, y, z rješenja gornje jednadžbe takva da su x, y, z u parovima relativno prosti, te da je $0 < r < p$. Sličnim razmatranjem kao kod Fermatove jednadžbe dobijemo da je točno jedan od brojeva $x^p, L^r y^p$, i z^p paran, te da je jedan od preostala dva broja kongruentan -1, a drugi 1 modulo 4. Neka je A, B, C neka permutacija brojeva $x^p, L^r y^p, z^p$, takva da $2 \mid B$ i $A \equiv -1 \pmod 4$. U vezi s ovom jednadžbom promatrat ćemo eliptičku krivulju

$$E : y^2 = x(x - A)(x + B). \tag{3.3}$$

Tada je $\Delta(E) = 16L^{2r}(abc)^{2p}$. Opet imamo krivulju kao u primjeru 1.2.2, pa znamo da je:

$$\Delta_{min} = \frac{L^{2r}(abc)^{2p}}{2^8}, \quad N = \prod_{\substack{l \mid Labc \\ l \text{ prost}}} l.$$

Iz formule 2.2 za N_p vidimo da je $N_p = 2L$ (točno oni prosti faktori od Δ_{min} čije eksponente dijeli p su prosti faktori od abc različiti od 2). Primjetimo da je E polustabilna i $\#E(\mathbb{Q})[2] = 4$ (istom argumentacijom kao u prethodnom odjeljku), pa prema teoremu

1.3.10,(*iii*) E nema p-izogenija. Prema teoremu o modularnosti E je modularna, pa prema Ribetovom teoremu postoji newforma f nivoa $N_p = 2L$ takva da $E \sim_p f$. Usporedimo to s teoremom 2.2.2 pa dolazimo do kontradikicije za $L = 3, 5, 11$.
Za ostale L imamo sljedeći rezultat:

Teorem 3.2.1 (Mazur)**.** *Neka je L neparan prost broj koji nije oblika $2^m \pm 1$. Tada postoji konstanta C_L takva da ako je (x, y, z, p) rješenje jednadžbe 3.2, tada je $p \leq C_L$.*

Dakle, za fiksirani L imamo ogradu na eksponent p. Za dokaz će nam trebati sljedeča propozicija:

Propozicija 3.2.2. *Neka je $E/\mathbb{Q}$ eliptička krivulja s konduktorom N i neka $t \mid \#E(\mathbb{Q})_{tors}$. Neka je f newoforma nivoa N'. Neka je l prost takav da $l \nmid N'$ i $l^2 \nmid N$. Stavimo*

$$S_l = \{a \in \mathbb{Z} : \quad -2\sqrt{l} \leq a \leq 2\sqrt{l}, \quad a \equiv l + 1 \pmod{t}\}.$$

Neka je c_l l-ti koeficijent od f i definiramo

$$B_l'(f) = N_{K/\mathbb{Q}}((l+1)^2 - c_l^2) \prod_{a \in S_l} N_{K/\mathbb{Q}}(a - c_l)$$

i

$$B_l(f) = \begin{cases} B_l'(f) & \text{ako } f \text{ racionalna} \\ l \cdot B_l'(f) & \text{ako } f \text{ iracionalna} \end{cases}.$$

Ako $E \sim_p f$, tada $p \mid B_l(f)$.

Dokaz. Promotrimo prvo slučaj kada je f racionalna. Tada je f pridružena eliptička krivulja F konduktora N, i za svaki $l \nmid N'$ je $c_l = a_l(F)$. Imamo dva slučaja za l: ili $l \nmid N$ ili $l \parallel N$.

Ako $l \nmid N$, tada E ima dobru redukciju u l, pa prema 1.2.6, $\#E(\mathbb{Q})_{tors} \mid \#E(\mathbb{F}_l)$, pa i $t \mid \#E(\mathbb{F}_l)$. Dakle, $a_l(E) = l + 1 - \#E(\mathbb{F}_l) \equiv l + 1 \pmod{t}$. Prema Hasseovoj ogradi $|a_l(E)| \leq 2\sqrt{l}$, dakle $a_l(E) \in S_l$. Prema 2.2.5, $a_l(E) \equiv c_l \pmod{\mathfrak{P}}$, za neki ideal $\mathfrak{P} \mid p$. Iz toga slijedi da $p \mid N_{K/\mathbb{Q}}(a_l(E) - c_l)$.

Ako pak $l \parallel N$, tada po 2.2.5 vrijedi $l + 1 \equiv \pm c_l \pmod{\mathfrak{P}}$, pa $p \mid N_{K/\mathbb{Q}}((l+1)^2 - c_l^2)$. U oba slučaja $p \mid B_l'(f) = B_l(f)$. Ako f nije racionalna postpupamo isto ako $l \neq p$, a ako $l = p$, tada $p \mid B_l(f)$ po definiciji. □

U dokazu također koristimo sljedeču lemu:

Lema 3.2.3. *(i) Neka je k neparan prirodan broj takav da postoje $n, m \in \mathbb{N}$ takvi da je $k^m = 2^n + 1$. Tada postoji $n' \in \mathbb{N}$ takav da je $k = 2^{n'} + 1$.*

(ii) Neka je $n > 1$ prirodan broj. Pretpostavimo da je $2^n - 1 = k^m$, za neke prirodne projeve k i m. Tada je $m = 1$.

Dokaz. (i) Ako je $m = 1$, gotovi smo. Inače imamo:

$$2^n = k^m - 1 = (k-1)(k^{m-1} + \cdots + k + 1).$$

Dakle, $k - 1 \mid 2^n$, iz čega slijedi $k - 1 = 2^{n'}$, za neki cijeli broj $0 \leq n' \leq n$. Kako je k neparan, slijedi da je $n' > 0$. Dakle, $k = 2^{n'} + 1$, za $n' \in \mathbb{N}$.

(ii) Kako je $n > 1$, slijedi da je $2^n - 1 = k^m$ neparan, pa je i k neparan. Pretpostavimo prvo da je m paran. Tada je k^m potpun kvadrat neparnog broja, pa je $k^m = 8t + 1$, za neki $t \in \mathbb{N}$, odnosno $2^n = k^m + 1 = 2(4t + 1)$. Kako je $n > 1$, $4 \mid 2^n$, pa bo slijedilo da $2 \mid 4t + 1$, što je kontradikcija. Dakle, m mora biti neparan. Sada imamo izraz

$$2^n = k^m + 1 = (k+1)(k^{m-1} - k^{m-2} - \cdots - k - 1).$$

Izraz u drugoj zagradi ima m neparnih sumanada, pa kako je m neparan, slijedi da je cijeli izraz neparan. Kako taj izraz dijeli 2^n, mora biti jednak 1, pa je $k + 1 = 2^n = k^m + 1$, tj. $m = 1$.

□

Dokaz teorema 3.2.1. Prvo želimo pokazati da za proste $L \neq 2^m \pm 1$ ne postoje eliptičke krivulje s punom 2-torzijom i konduktorom $2L$. Pretpostavimo da je F eliptička krivulja s konduktorom $2L$ i torzijom $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Postoji model za F oblika

$$y^2 = x(x-a)(x+b), \quad a, b \in \mathbb{Z},$$

koji je minimalan svuda osim u 2. Diskriminanta tog modela je

$$\Delta = 16a^2b^2(a+b)^2.$$

S druge strane, iz konduktora od F znamo da F ima lošu redukciju u 2 i L, pa je diskriminanta oblika $2^u L^v$. Dakle, L dijeli neki od brojeva $a, b, a + b$. Pretpostavimo da L dijeli više od jednog od tih brojeva. Tada L dijeli sva tri, zbog veze među njima. Kako je $c_4 = 16((a+b)^2 - ab)$, tada bi $L \mid c_4$. No, jer F ima konduktor $2L$, F ima multiplikativnu redukciju u L, što znači da $L \mid \Delta$ i $L \nmid c_4$, pa smo dobili kontradikciju. Dakle, L dijeli točno jedan od brojeva $a, b, a + b$. Zbog $\Delta = 2^u L^v$, preostala dva od $a, b, a + b$ su tada potencije od 2. Uvrstimo to u $a + b - (a + b) = 0$, pa dobivamo izraz

$$\pm 2^\alpha \pm 2^\beta \pm 2^\gamma L^\delta = 0,$$

gdje su $\alpha, \beta, \gamma \geq 0$ i $\delta \geq 1$. Iz ovoga izraza želimo dobiti kontradikciju s pretpostavkom da L nije oblika $2^m \pm 1$.

Uzmimo konkretnosti radi da je $a = 2^\alpha,\ b = 2^\beta$ i $a+b = 2^\gamma L^\delta$. Tada gornji izraz postaje

$$2^\alpha + 2^\beta = 2^\gamma L^\delta \tag{3.4}$$

Bez smanjenja općenitosti je $\alpha \leq \beta$. Pretpostavimo prvo da je $\gamma \leq \alpha$. Tada 3.4 postaje $L^\delta = 2^{\alpha-\gamma} + 2^{\beta-\gamma}$. Kako je L neparan, i desna strana mora biti neparna, a to je jedino moguće kada je $\alpha = \gamma < \beta$. Tada je $L^\delta = 2^{\beta-\gamma} + 1$, pa je prema lemi 3.2.3,*(i)*, $L = 2^{n'} + 1$, za neki $n \in \mathbb{N}$, što je kontradikcija. Dakle, preostaje slučaj $\gamma > \alpha$. Tada 3.4 postaje $1 + 2^{\beta-\alpha} = 2^{\gamma-\alpha}L^\delta$. Jer je $\gamma - \alpha > 0$, desna strana jednadžbe je djeljiva s 2, pa mora biti i lijeva strana, što je jedino moguće ako $\alpha = \beta$. No, tada bi bilo $2 = 2^{\gamma-\alpha}L^r$, tj. $L = 1$, što je kontradikcija jer je L prost.

Drugi oblik koji možemo dobiti je

$$2^\beta - 2^\alpha = 2^\gamma L^\delta,$$

na primjer kada je $a = 2^\alpha,\ b = 2^\gamma$ i $a + b = 2^\beta$. Ovdje je jasno $\alpha \leq \beta$. Ako je $\gamma \leq \alpha$, onda kao i u prvom slučaju dobivamo da mora biti $\gamma = \alpha < \beta$, tj. $2^{\beta-\gamma} - 1 = L^\delta$. Jasno $\beta - \gamma > 1$, jer inače $L = 1$. Sada prema 3.2.3,*(ii)* slijedi da je $L = 2^{\beta-\gamma} - 1$, što je kontradikcija s pretpostavkom. Ako je $\gamma > \alpha$, onda se svodi na istu kontradikciju kao u prvom slučaju.

Time je dokazana početna tvrdnja. Preostaje pokazati da iz toga slijedi tvrdnja teorema. Prema raspravi prije teorema, za E kao u 3.3, konduktora $N = \prod_{l|Labc} l$, imamo $E \sim_p f$ za neku newformu f nivoa $N' = 2L$. Za ogradu na p, prema propoziciji 3.2.2, dovoljno je naći l prost, $l \nmid N'$, $l^2 \nmid N$, takav da je $B_l(f) \neq 0$. Tada p mora dijeliti $B_l(f)$, što nam daje gornju ogradu na p.

Ako je f iracionalna, tada postoji beskonačno mnogo prostih l takvih da $c_l \notin \mathbb{Q}$. Za takve l imamo $B'_l(f) \neq 0$, pa i $B_l(f) \neq 0$.

Ako je f racionalna, tada je f pridružena klasa izogenije eliptičkih krivulja s konduktorom $2L$. Pretpostavimo da je $B_l(f) = 0$ za sve osim konačno mnogo l. Tada se može pokazati da $4 \mid F(\mathbb{Q})_{tors}$, za neku krivulju F pridruženu f. Ali, ne postoji takva krivulja s konduktorom $2L$. Dakle, mora biti $B_l(f) \neq 0$ za beskonačno l. □

Radi ilustracije metode, promotrimo slučaj kada $L = 19$. Neka je E kao prije, i znamo da je $E \sim_p f$, gdje je f neka newforma nivoa $N_p = 38$. Računanjem u SAGE-u, dobivamo da na nivou 38 postoje dvije newforme, obje racionalne:

$$f_1 = q - q^2 + q^3 + q^4 - q^6 - q^7 + \dots$$
$$f_2 = q + q^2 - q^3 + q^4 - 4q^5 - q^6 + 3q^7 + \dots$$

Dakle, $E \sim_p f_1$ ili $E \sim_p f_2$. Kao prije, znamo da $\#E(\mathbb{Q})_{tors} = 4$, pa primjenjujemo propoziciju 3.2.2 s $t = 4$. Za $l \nmid abc$, imamo da $p \mid B_l(f)$. Uzimajući $l = 3, 5$, dobivamo $B_3(f_1) = -15$ i $B_5(f_1) = -144$. No, p mora dijeliti $nzd(B_3(f_1), B_5(f_1)) = nzd(-15, -144) = 3$, što je nemoguće za $p \geq 5$. Dakle, $E \nsim_p f_1$, pa bi moralo biti $E \sim_p f_2$.

Računanjem $B_l(f_2)$ za prvih nekoliko dozvoljenih vrijednosti od l, vidimo da $p = 5 \mid B_l(f_2)$ u prvih nekoliko slučajeva. Također, zbog $B_3(f_2) = 15$, to nam je jedino preostalo moguće rješenje. Iz tablica [4] newformi i eliptičkih krivulja možemo naći da je f_2 newforma [4, 38.2.1.b], i njoj je pridružena klasa izogenije eliptičkih krivulja [4, 38.b]. Neka je F krivulja [4, 38.b2],

$$y^2 + xy + y = x^3 + x^2 + 1.$$

Iz tablica vidimo da F ima točku reda 5, pa $5 \mid \#F(\mathbb{F}_l)$, za sve l dobre redukcije, tj. $l \nmid 38$. Dakle, za $l \nmid 38$ imamo $5 \mid (l + 1 - a_l(F))$, pa $5 \mid B_l(f_2)$. Stoga ne možemo eliminirati slučaj $p = 5$ koristeći propoziciju 3.2.2. No, možemo koristiti sljedeći argument. Pretpostavimo $E \sim_p f_2$, tj. $E \sim_p F$. Tada je $a_l(E) \equiv a_l(F) \pmod 5$, za sve osim konačno mnogo prostih l. Za sve osim konačno prostih l je tada $l + 1 - a_l(E) \equiv l + 1 - a_l(F) \equiv 0 \pmod 5$, tj. $5 \mid \#E(\mathbb{F}_l)$. Tada je E izogena nekoj E' krivulji koja ima točku reda 5, pa E' ima 5-izogeniju. Jer je E izogena E' i 5 prost, tada i E ima 5-izogeniju. No, kako je E polustabilna i ima punu 2-torziju, to je kontradikcija s teoremom 1.3.10. Dakle, jednadžba 3.2 nema rješenja za $L = 19$ i $p \geq 5$.

3.3 Krausova metoda

U ovom poglavlju pokazat ćemo metodu koju je razvio Kraus, a često je korisna u svođenju na kontradikciju za fiksni eksponent p.

U prvom primjeru nastavljamo se baviti jednadžbom 3.2 iz prethodnog odjeljka. Preptostavimo da je $(a, b, c) = (x, y, z)$ rješenje dane jednadžbe. Prisjetimo se da je E ovisila o permutaciji brojeva $a^p, L^r b^p, c^p$. Kako ne bi trebali razmatrati svih 6 slučajeva, koristimo sljedeću lemu.

Lema 3.3.1. *Neka su A, B, C cijeli brojevi različiti od nule, koji zadovoljavaju $A+B+C = 0$. Neka je E eliptička krivulja*

$$E : y^2 = x(x - A)(x - B).$$

Tada svaka permutacija od A, B, C daje krivulju koja je ili izomorna E ili je kvadrtani twist od E sa -1.

Prema lemi je eliptička krivlja

$$E' : y^2 = x(x - a^p)(x + c^p)$$

izomorfna E ili je kvadratni twist sa -1 od E. Želimo rješenju jednadžbe pridružiti eliptičku krivulju koja će ovisiti samo o jednoj varijabli. Ako stavimo $\delta = (\frac{c}{a})^p$, tada imamo eliptičku krivulju

$$E_\delta : y^2 = x(x - 1)(x + \delta),$$

koja je kvadratni twist od E' sa a^p. Tada je $a_l(E) = \pm a_l(E_\delta)$ za $l \nmid a$ (prema 1.2.5).

Kao u prethodnom odjeljku, neka je $E \sim_p f$ za neku newformu nivoa $2L$. Označimo sa c_l l-ti koeficijent u Fourierovom razvoju od f.

Lema 3.3.2. *Pretpostavimo da je l prost broj različit od $2, L$ i p.*

(i) Ako $l \mid abc$, tada $p \mid N_{K/\mathbb{Q}}((l+1)^2 - c_l^2)$.

(ii) Ako $l \nmid abc$, tada $p \mid N_{K/\mathbb{Q}}(a_l(E_\delta)^2 - c_l^2)$.

Neka je sada l prost broj oblika $l = np + 1$ za neki $n \in \mathbb{N}$. Promotrimo skup

$$\mu_n(\mathbb{F}_l) = \{\xi \in \mathbb{F}_l : \xi^n = \bar{1}\}.$$

Ovdje $\bar{1}$ označava jedinicu u $\mathbb{F}_l$. Ako $l \nmid abc$, onda je prema malom Fermatovom teoremu $c^{l-1} \equiv 1 \pmod{l}$ i $(a^{-1})^{l-1} \equiv 1 \pmod{l}$, gdje je a^{-1} inverz od a u $\mathbb{F}_l$. Kako je $l - 1 = np$ i $c^p = \delta a^p$, slijedi da je $c^{np} \equiv \delta^n a^{np} \equiv q \pmod{l}$. Množenjem s a^{-np} dobivamo $\delta^n \equiv 1 \pmod{l}$, tj. $\delta \in \mu_n(\mathbb{F}_l)$.

Propozicija 3.3.3. *Neka je $p \geq 5$ fiksni prosti broj, i E eliptička krivulja definirana kao u 3.3. Pretpostavimo da za svaku newformu f nivoa $2L$ postoji cijeli broj n takav da je $l = np + 1$ prost broj, $l \neq L$ i da pritom vrijedi $p \nmid N_{K/\mathbb{Q}}((l+1)^2 - a_l(f)^2)$ te da za sve $\delta \in \mu_n(\mathbb{F}_l), \delta \neq -1$ vrijedi $p \nmid N_{K/\mathbb{Q}}(a_l(E_\delta))^2 - a_l(f)^2$. Tada jednadžba 3.2 nema rješenja.*

Pokazat ćemo još jedan primjer u kojem se koristi ova metoda. Promotrimo jednadžbu

$$a^2 + 7 = b^p, \quad p \geq 11. \tag{3.5}$$

Reduciranjem jednadžbe modulo 4 vidimo da 3.5 nema rješenja za neparne b. Preptostavimo da je a, b rješenje gornje jednadžbe, dakle b paran i $a \equiv \pm 1 \pmod{4}$. Pretpostavimo $a \equiv 1 \pmod{4}$, što nije smanjenje općenitosti, jer je (a, b) rješenje od 3.5 ako i samo ako je i $(-a, b)$ rješenje. Tom rješenju pridružimo jednadžbu

$$E_a : \; y^2 = x^3 + ax^2 + \frac{a^2+7}{4}x. \tag{3.6}$$

Primjetimo $a^2 + 7 \equiv b^p \equiv 0 \pmod{4}$, jer je b paran, pa je $\frac{a^2+7}{4} \in \mathbb{Z}$. Dobijemo da je

$$\Delta = \frac{-7b^p}{2^{12}}, \quad N = 14 \prod_{l \mid b,\ l \nmid 14} l.$$

Prema Ribetovom teoremu i formuli 2.2, slijedi da je $E_a \sim_p f$, za neku newformu f nivoa $N_p = 14$. Ali na nivou 14 postoji samo jedna newforma [4, 14.2.1.a],

$$f = q - q^2 - 2q^3 + q^4 + 2q^6 + q^7 - q^8 + q^9 + \dots$$

Dakle, $E_a \sim f$, odnosno $E_a \sim F$, gdje je F neka krivulja iz klase izogenije pridružene f, konduktora $N' = 14$.

Fiksirajmo sada prosti $p \geq 11$. Izaberimo l prost broj takav da $l \nmid 14$ i da -7 nije kvadratni ostatak modulo l. Dakle, $l \nmid x^2 + 7 = y^p$, pa $l \nmid y$. Slijedi da $l \nmid NN'$. Iz 2.2.5,*(i)* znamo

$$a_p(E) \equiv a_p(F) \pmod{p}.$$

Dakle, ako definiramo skup

$$T(l, p) = \{\alpha \in \mathbb{F}_l \ : \ a_l(E_\alpha) \equiv a_l(F) \pmod{p}\},$$

tada je $a \equiv \alpha \pmod{l}$, za neki $\alpha \in T(l, p)$. Definirajmo još i drugi skup

$$R(l, p) = \{\beta \in \mathbb{F}_l : \beta^2 + 7 \in (\mathbb{F}_l^\times)^p\},$$

pa je $a \equiv \beta \pmod{l}$, za neki $\beta \in \mathbb{F}_l$. Imamo sljedeću lemu:

Lema 3.3.4. *Pretpostavimo da je l prost takav da $l \nmid 14$ te da -7 nije kvadratni ostatak modulo l, te neka su skupovi $T(l, p)$ i $R(l, p)$ definirani kao gore. Ako je $T(l, p) \cap R(l, p) = \emptyset$, tada jednadžba $x^2 + 7 = y^p$ nema rješenja za $p \geq 11$.*

Iz gornje leme može se kompjuterskom provjerom pokazati da jednadžba 3.5 nema rješenja za $11 \leq p \leq 10^8$.

U [7] se može naći još zanimljvih primjera, kao i opis Freyevih krivulja za razne tipove jednadžbi.

Bibliografija

[1] F. Diamond i J. Shurman, *A First Course in Modular Forms*, Springer New York, 2005.

[2] R. Hartshorne, *Algebraic Geometry*, Springer New York, 2013.

[3] D. S. Kubert, *Universal Bounds on the Torsion of Elliptic Curves*, Proceedings of the London Mathematical Society **33** (1976), br. 2, 193–237.

[4] The LMFDB Collaboration, *The L-functions and Modular Forms Database*, `http://www.lmfdb.org`, 2013, [Online; accessed 5 September 2018].

[5] B. Mazur, *Rational Isogenies of Prime Degree.*, Inventiones mathematicae **44** (1978), 129–162.

[6] I.R. Shafarevich i M. Reid, *Basic Algebraic Geometry 1: Varieties in Projective Space*, Springer Berlin Heidelberg, 2013.

[7] Samir Siksek, *The Modular Approach to Diophantine Equations*, `https://homepages.warwick.ac.uk/staff/S.Siksek/sarajevo/notes.pdf`, July 2016.

[8] J.H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer-Verlag, 1994.

[9] ———, *The Arithmetic of Elliptic Curves*, Springer New York, 2009.

[10] The Sage Developers, *SageMath, the Sage Mathematics Software System (Version 8.2)*, 2018, http://www.sagemath.org.

[11] Andrew Wiles, *Modular elliptic curves and Fermat's last theorem*, Annals of mathematics **141** (1995), br. 3, 443–551.

Sažetak

Andrew Wiles dokazao je 1995. godine posljednji Fermatov teorem, koristeći vezu između eliptičkih krivulja i modularnih formi. Zapravo, Wiles je dokazao poseban slučaj teorema o modularnosti. Cilj ovog rada bio je pokazati primjene teorema o modularnosti i teorije eliptičkih krivulja i modularnih formi na diofantske jednadžbe.

U prvom poglavlju dajemo pregled osnovnih pojmova vezanih uz eliptičke krivulje. Posebno se bavimo sa redukcijom eliptičkih krivulja modulo p: opisujemo slučajeve i podslučajeve dobre i loše redukcije te definiramo konduktor eliptičke krivulje. Na primjeru pokazujemo traženje minimalne jednadžbe i konduktora. Nadalje, definiramo izogenije eliptičkih krivulja i dajemo nekoliko bitnih primjera izogenija. Na kraju poglavlja iskazujemo Mazurov teorem o p-izogenijama.

U drugom poglavlju definiramo modularnu grupu i njene kongruencijske podgrupe, a zatim definiramo i modularne forme obzirom na kongruencijske podgrupe. U nastavku definiramo newforme: posebnu klasu modularnih formi, koje su posebno bitne za teorem o modularnosti i dajemo pregled osnovnih svojstava newformi. Na kraju poglavlja iskazujemo Ribetov teorem i teorem o modularnosti, koji daju osnovu za primjenu ove teorije na rješavanje diofantskih jednadžbi.

U posljednjem poglavlju pokazujemo na primjerima kako se teorem o modularnosti i Ribetov teorem mogu primjeniti na rješavanje diofantskih jednadžbi. Prvi primjer je Fermatova jednadžba $a^p + b^p + c^p = 0$, tj. pokazujemo da iz teorema o modularnosti i Ribetovog teorema slijedi posljednji Fermatov teorem. Nakon toga se bavimo jednadžbom $x^p + L^r y^p + z^p = 0$ i na tom primjeru pokazujemo nekoliko metoda koje se mogu primjeniti na takve jednadžbe. Jedan od pristupa je tzv. Krausova metoda, za čiju primjenu dajemo još jedan primjer.

Summary

Andrew Wiles proved Fermat's last theorem in 1995, using the connection between elliptic curves and modular forms. Actually, Wiles proved a special case od the modularity theorem. The goal of this thesis was to demonstrate application of the modularity theorem and theories of elliptic curves and modular forms to Diophantine equations.

In the first chapter we give an overview of basic terms related to elliptic curves. We especially deal with reduction of elliptic curves modulo p: we describe the cases and subcases of good and bad reduction and define the conductor of an elliptic curve. We show an example of finding the minimal equation and conductor. Furthermore, we define isogenies of elliptic curves and give a few important examples of isogenies. The chapter ends with the statement of Mazur's theorem on p-isogenies.

In the second chapter we define the modular group and its congruence subgroups and then also define modular forms with respect to congruence subgroups. Subsequently, we define newforms: a special class of modular forms, which are especially important for the modularity theorem, and we give an overview of basic properties of newforms. In the end of this chapter we state Ribet's theorem and the modularity theorem, which give the basis for application of this theory on solving Diophantine equations.

In the final chapter we demonstrate the application of the modularity and Ribet's theorem to solving Diophantine equations. The first example is Fermat's eqautions $a^p + b^p + c^p = 0$, i.e. we show that Fermat's last theorem follows from modularity theorem and Ribet's theorem. After that we look at the equation $x^p + L^r y^p + z^p = 0$ and in that example we show a few methods that can be applied to such equations. One approach is the so called method of Kraus, and for this method we give one more example.

Životopis

Rođena sam 20.11.1994. u Zagrebu, gdje sam pohađala Osnovnu školu Stenjevec i zatim V. gimnaziju. Za vrijeme srednje škole sudjelovala sam na natjecanjima iz matematike, uključujući dva državna natjecanja. Maturirala sam 2013. godine te iste godine upisala preddiplomski studij na Matematičkom odsjeku Prirodoslovno-matematičkog fakulteta u Zagrebu. Nakon završetka preddiplomskog studija 2016. godine na istom sam fakultetu upisala diplomski studij Teorijska matematika.

Tokom studija držala sam demonstrature iz nekoliko kolegija. Nagrađena sam Rektorovom nagradom Sveučilišta u Zagrebu 2015./2016. godine i nagradom Matematičkog odsjeka Prirodoslovno-matematičkog fakulteta za najbolje studente završnih godina studija 2017./2018. godine. Sudjelovala sam na studentskom natjecanju Vojtech Jarnik 2018. godine. Aktivni sam član udruge Mladi nadareni matematičari "Marin Getaldić".