Modularne krivulje

Trbović, Antonela

SVEUČILIŠTE U ZAGREBU
PRIRODOSLOVNO–MATEMATIČKI FAKULTET
MATEMATIČKI ODSJEK

Antonela Trbović

MODULARNE KRIVULJE

Diplomski rad

Voditelj rada:
prof. dr. sc. Filip Najman

Zagreb, Srpanj, 2017.

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, tj. polinomijalne jednadžbe, nad $\mathbb{Z}$, $\mathbb{Q}$ ili nekim drugim nama zanimljivim poljima ili prstenima proučavaju se još od stare Grčke. Zanima nas problem određivanja broja rješenja tih jednadžbi. Najpoznatiji takav problem je Fermatov zadnji teorem, koji nam govori kako za $n \geq 3$ ne postoje $a, b, c \in \mathbb{Z}$ takvi da je $abc \neq 0$ i

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

Dokazao ga je Andrew Wiles 1994. godine, za što je 2016. godine dobio Abelovu nagradu, a ključnu ulogu u dokazu imale su eliptičke krivulje. Dokaz je bio posljedica teorema o modularnosti za polustabilne eliptičke krivulje, tj. eliptičke krivulje koje na mjestima loše redukcije imaju multiplikativnu redukciju. Teorem o modularnosti za sve eliptičke krivulje nad $\mathbb{Q}$ su 2001. godine dokazali Cristophe Breuil, Brian Conrad, Fred Diamond i Richard Taylor. U poglavlju 4 naveli smo neke verzije Teorema o modularnosti.

Centralni objekti koje proučavamo u ovom radu su modularne krivulje. Modularnu krivulju definiramo kao kvocijent gornje poluravnine s obzirom na djelovanje neke kongruencijske grupe, odnosno podgrupe modularne grupe $\mathrm{SL}_2(\mathbb{Z})$. U teoriji brojeva važnu ulogu igra činjenica da su modularne krivulje također prostori parametara, tj. svaka točka na modularnoj krivulji parametrizira eliptičku krivulju s nekim dodatnim svojstvom. Ovo svojstvo smo objasnili u teoremu 3.2.2. Jednu od primjena tog teorema možemo pokazati promatramo li eliptičku krivulju E definiranu nad poljem algebarskih brojeva $\mathbb{K}$. Prema Mordell-Weilovom teoremu i strukturnom teoremu o konačno generiranim Abelovim grupama znamo da ona ima oblik $E \cong T \oplus \mathbb{Z}^r$, gdje je T podgrupa elemenata konačnog reda, a $r \geq 0$ neki cijeli broj. Prirodno se postavlja pitanje koje su njene moguće torzijske podgrupe. Odgovor na to pitanje je za eliptičke krivulje nad $\mathbb{K} = \mathbb{Q}$ dao Mazur 1978. godine. Za općenitiji $\mathbb{K}$ možemo promatrati modularnu krivulju čije točke parametriziraju eliptičku krivulju sa željenim torzijskim svojstvom definiranu nad $\mathbb{K}$ i provjeriti koliko takva modularna krivulja ima $\mathbb{K}-$racionalnih točaka. Više o sličnom problemu za kvadratna polja $\mathbb{K}$ možemo naći u [9].

U 1. poglavlju ovog rada definiramo modularnu grupu, matričnu grupu koja djeluje na kompleksnu gornju poluravninu. Definiramo i modularne forme, slabo modularne funkcije koje zadovoljavaju neke uvjete holomorfnosti, te dajemo bitne primjere modularnih formi koji će se pojavljivati kroz cijeli rad.

U 2. poglavlju definiramo kompleksne toruse, kvocijente kompleksne gornje poluravnine s obzirom na rešetku, i eliptičke krivulje te dokazujemo neka njihova osnovna svojstva koja su nam potrebna kako bismo pokazali na koji način možemo uspostaviti bijekciju između ta dva objekta. Također, pokazujemo da postoji korespondencija između kompleksnih torusa i eliptičkih krivulja do na izomorfizam.

U 3. poglavlju definiramo kongruencijske podgrupe od $\mathrm{SL}_2(\mathbb{Z})$ te definiramo modularnu krivulju kao skup svih orbita pri djelovanju neke kongruencijske podgrupe na gornju poluravninu. Zatim u glavnom teoremu ovoga rada pokazujemo da postoji bijekcija između nekih modularnih krivulja i skupa eliptičkih krivulja sa određenim torzijskim svojstvom.

U 4. i zadnjem poglavlju definiramo dobru odnosno lošu redukciju eliptičke krivulje te $L-$funkciju pridruženu eliptičkoj krivulji kako bismo mogli navesti iskaze različitih verzija Teorema o modularnosti.

Poglavlje 1

Modularne forme

U ovom poglavlju definirat ćemo modularnu grupu i objasniti kako ona djeluje na gornju kompleksnu poluravninu. Zatim ćemo definirati slabo modularne funkcije te modularne forme koje osim slabe modularnosti zadovoljavaju i neke uvjete holomorfnosti. Navest ćemo i primjere modularnih formi koji će nam biti korisni za daljnja razmatranja.

Definicija 1.0.1. *Modularna grupa* $\mathrm{SL}_2(\mathbb{Z})$ *je grupa* 2×2 *matrica s cjelobrojnim matričnim elementima i determinantom 1, tj.*

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

Modularna grupa $\mathrm{SL}_2(\mathbb{Z})$ je generirana elementima

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \text{ i } \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

Algebarski i geometrijski dokaz ove tvrdnje te još neka svojstva modularne grupe možemo naći u [1].
Nadalje, označimo s $\hat{\mathbb{C}}$ Riemannovu sferu $\mathbb{C} \cup \{\infty\}$ i definirajmo preslikavanje

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

Ako je $c \neq 0$, tada se $\frac{-d}{c}$ preslikava u ∞, a ∞ se preslikava u $\frac{a}{c}$, a ako je $c = 0$ tada se ∞ preslikava u ∞. Na taj način svaki element modularne grupe možemo shvatiti kao automorfizam Riemannove sfere.

Označimo s $\mathcal{H}$ gornju poluravninu, tj.

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

Jednostavnim računom možemo vidjeti da vrijedi formula

$$\mathrm{Im}(\gamma(\tau)) = \frac{\mathrm{Im}(\tau)}{|c\tau + d|^2}, \quad \text{za sve } \gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}), \tau \in \mathcal{H}\,.$$

Naime,

$$\mathrm{Im}(\gamma(\tau)) = \mathrm{Im}\,\frac{a\tau + b}{c\tau + d} = \mathrm{Im}\,\frac{(a\tau + b)(c\overline{\tau} + d)}{|c\tau + d|^2} = \mathrm{Im}\,\frac{ac|\tau|^2 + ad\tau + bc\overline{\tau} + bd}{|c\tau + d|^2} =$$

$$= \frac{\mathrm{Im}(ad\tau + bc\overline{\tau})}{|c\tau + d|^2} = \frac{(ad - bc)\,\mathrm{Im}(\tau)}{|c\tau + d|^2} = \frac{\mathrm{Im}(\tau)}{|c\tau + d|^2}, \tag{1.1}$$

gdje smo u zadnjoj jednakosti iskoristili da je $\det \gamma = ad - bc = 1$.

Dakle, svaki element modularne grupe preslikava gornju poluravninu u gornju poluravninu. Označimo li s I jediničnu 2×2 matricu a s γ i γ' proizvoljne elemente modularne grupe $\mathrm{SL}_2(\mathbb{Z})$, primjećujemo da vrijedi

$$I(\tau) = \tau, \quad \tau \in \mathcal{H},$$

$$(\gamma\gamma')(\tau) = \gamma(\gamma'(\tau)), \quad \tau \in \mathcal{H},$$

pa je gore definirano preslikavanje $\mathrm{SL}_2(\mathbb{Z}) \times \mathcal{H} \to \mathcal{H}$ djelovanje grupe $\mathrm{SL}_2(\mathbb{Z})$ na skup $\mathcal{H}$.

Prisjetimo se sada nekih osnovnih pojmova iz kompleksne analize koji će nam biti potrebni za definiciju slabo modularnih funkcija, odnosno modularnih formi.

Neka je $f : D \to \mathbb{C}$, $D \subseteq \mathbb{C}$ otvoren, funkcija koja je diferencijabilna u okolini svake točke iz D. Tada za f kažemo da je holomorfna na D.

Nadalje, ako imamo holomorfnu funkciju f na $D \setminus \{p\}$ za koju postoje holomorfna funkcija $g : D \to \mathbb{C}$ takva da $g(p) \neq 0$ te $n \in \mathbb{N}$ takvi da vrijedi

$$f(z) = \frac{g(z)}{(z - p)^n}, \quad z \in D \setminus \{p\},$$

tada kažemo da je točka p pol funkcije f, te za najmanji takav n kažemo da je red pola p.

Ako je f kompleksna funkcija na D koja je holomorfna na cijelom D osim na nekom skupu izoliranih točaka koji su polovi funkcije, tada za nju kažemo da je meromorfna na D. Pojam meromorfne funkcije će nam biti ključan za sljedeću definiciju.

Definicija 1.0.2. *Neka je $k \in \mathbb{Z}$. Kažemo da je meromorfna funkcija $f : \mathcal{H} \to \mathbb{C}$ slabo modularna težine k ako je*

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

Kako bismo dokazali da je meromorfna funkcija f slabo modularna težine k, dovoljno je provjeriti uvjet iz definicije samo za generatore modularne grupe, tj.

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}),$$

Odnosno, dovoljno je provjeriti da vrijedi

$$f(\tau+1) = f(\tau), \;\; f\left(-\frac{1}{\tau}\right) = \tau^k f(\tau), \;\; \tau \in \mathcal{H}\,.$$

Dokaz ove tvrdnje možemo naći u [2, Lema 1.2.2].

Primijetimo, za $\gamma = -I \in \mathrm{SL}_2(\mathbb{Z})$, uvjet iz definicije postaje $f(\tau) = (-1)^k f(\tau)$, iz čega zaključujemo da osim nul-funkcije ne postoje slabo modularne funkcije neparnih težina. Kao jednostavan primjer slabo modularnih funkcija možemo spomenuti konstantne funkcije, koje su slabo modularne težine 0 ili nul-funkciju, koja je slabo modularna svake težine. Nešto složenije primjere ćemo vidjeti kasnije, kod primjera modularnih formi, budući da je slaba modularnost jedan od uvjeta u definiciji modularne forme.

Jedna od motivirajućih ideja za definiciju slabo modularne funkcije f bila je činjenica da $f \circ \gamma$ i f imaju iste nultočke i polove budući da $(c\tau + d)^k$ nema niti nultočaka niti polova.

Modularne forme su slabo modularne funkcije koje su također holomorfne na gornjoj poluravnini $\mathcal{H}$ te holomorfne u ∞. Kako bismo precizno definirali modularnu formu, objasnimo prvo što znači holomorfnost u ∞.

Primijetimo da modularna grupa $\mathrm{SL}_2(\mathbb{Z})$ sadrži translacijsku matricu

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} : \tau \mapsto \tau + 1,$$

što znači da za svaku slabo modularnu funkciju $f : \mathcal{H} \to \mathbb{C}$ vrijedi $f(\tau+1) = f(\tau)$, tj. funkcija f je $\mathbb{Z}-$periodična. Dakle, postoji Fourierov razvoj funkcije f,

$$f(z) = \sum_{n=0}^{\infty} a_n e^{2\pi i n z}.$$

Označimo sa $D = \{q \in \mathbb{C} : |q| < 1\}$ otvoreni kompleksni disk oko 0 radijusa 1 te neka je $D' = D \setminus \{0\}$.

Funkcija $\tau \mapsto e^{2\pi i \tau} =: q$ preslikava $\mathcal{H}$ u D'. Naime, za $\tau \in \mathcal{H}$ imamo

$$e^{2\pi i \tau} = e^{2\pi i(\operatorname{Re}\tau + i \operatorname{Im}\tau)} = e^{2\pi i \operatorname{Re}\tau} e^{-2\pi \operatorname{Im}\tau} = e^{-2\pi \operatorname{Im}\tau}(\cos(\operatorname{Re}\tau) + i \sin(\operatorname{Re}\tau)),$$

pa koristeći činjenicu da je $\operatorname{Im}\tau > 0$ zaključujemo

$$|e^{2\pi i\tau}| = |e^{-2\pi \operatorname{Im}\tau}(\cos(\operatorname{Re}\tau) + i\sin(\operatorname{Re}\tau))| =$$
$$= |e^{-2\pi \operatorname{Im}\tau}| \cdot \sqrt{\cos^2(\operatorname{Re}\tau) + \sin^2(\operatorname{Re}\tau)} = |e^{-2\pi \operatorname{Im}\tau}| = e^{-2\pi \operatorname{Im}\tau} < 1.$$

Dakle, $e^{2\pi i\tau} \in D'$, a budući da $\operatorname{Re}\tau \in \mathbb{R}$ može biti proizvoljan, slijedi da se svaka vrijednost iz D' postiže. Također, za isto preslikavanje vrijedi $\infty \mapsto 0$.

Dakle, na f možemo gledati kao na holomorfnu funkciju na D' u varijabli q.

Kažemo da je funkcija f holomorfna u ∞ ako se može holomorfno proširiti na cijeli D. Prema Riemannovom teoremu o uklonjivim singularitetima [3, Teorem 3.1] to vrijedi kada je $f(q)$ omeđena na nekoj okolini ishodišta, tj. dovoljno je vidjeti da je

$$\lim_{\operatorname{Im}\tau\to\infty} f(\tau) < \infty.$$

Definicija 1.0.3. *Neka je $k \in \mathbb{Z}$. Kažemo da je funkcija $f : \mathcal{H} \to \mathbb{C}$ modularna forma težine k ako vrijedi*

1. *f je holomorfna na $\mathcal{H}$;*
2. *f je slabo modularna težine k;*
3. *f je holomorfna u ∞.*

Skup svih modularnih formi težine k označavamo s $\mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z}))$. Lako se provjeri da je taj skup vektorski prostor nad $\mathbb{C}$. Zadnji uvjet iz definicije modularne forme, odnosno holomorfnost u ∞, čini dimenziju tog vektorskog prostora konačnom. Više o tome možemo naći u [2, Poglavlje 3] ili [6, Poglavlje 2].

Primjer 1.0.4. *Neka je $k \in \mathbb{N}$ i $k > 2$ paran. Definiramo Eisensteinov red težine k sa*

$$G_k(\tau) = {\sum_{(c,d)}}' \frac{1}{(c\tau + d)^k}, \quad \tau \in \mathcal{H},$$

gdje sumiramo po svim $(c, d) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$. Može se pokazati, koristeći da je $k > 2$ i paran, da je gornji red apsolutno konvergentan i konvergira uniformno na kompaktnim podskupovima od $\mathcal{H}$. To znači da je G_k holomorfna na gornjoj poluravnini te da možemo mijenjati poredak sumacije.

Kako bismo pokazali da vrijedi drugi uvjet iz definicije modularne forme, uzmimo $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ i računajmo

$$G_k(\gamma(\tau)) = {\sum_{(c,d)}}' \frac{1}{(c(\gamma(\tau)) + d)^k} = {\sum_{(c',d')}}' \frac{1}{\left(c'\left(\dfrac{a\tau + b}{c\tau + d}\right) + d'\right)^k} =$$

$$= (c\tau + d)^k \sum_{(c',d')}{}' \frac{1}{((c'a + d'c)\tau + c'b + d'd)^k} = (c\tau + d)^k G_k(\tau),$$

gdje zadnja jednakost vrijedi jer postoji bijekcija

$$\mathbb{Z}^2 \setminus \{(0,0)\} \to (\{c'a + d'c : c', d' \in \mathbb{Z}\} \oplus \{c'b + c'd : c', d' \in \mathbb{Z}\}) \setminus \{(0,0)\}.$$

Naime, vrijedi $\mathrm{nzd}(a,c) = \mathrm{nzd}(b,d) = 1$. *U suprotnom bismo imali* $p > 1$ *takav da vrijedi* $p|a, c$ *ili* $p|b, d$. *U oba slučaja imamo*

$$ad - bc = p\left(\frac{ad}{p} - \frac{bc}{p}\right) > 1$$

Izraz u zagradi je cjelobrojan, jer $p|a, c$ *ili* $p|b, d$, *pa dolazimo do kontradikcije s činjenicom da je* $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, *odnosno da je* $ad - bc = 1$.

Sada,

$$(\{c'a + d'c : c', d' \in \mathbb{Z}\} \oplus \{c'b + c'd : c', d' \in \mathbb{Z}\}) \setminus \{(0,0)\} =$$

$$= \{\mathrm{nzd}(a,c)\mathbb{Z} \oplus \mathrm{nzd}(b,d)\mathbb{Z}\} \setminus \{(0,0)\} = \mathbb{Z}^2 \setminus \{(0,0)\}$$

Dakle, G_k *je slabo modularna funkcija težine* k.

Također, može se pokazati da je

$$\lim_{\mathrm{Im}\,\tau \to \infty} G_k(\tau) < \infty,$$

pa je zato zadovoljen i treći uvjet iz definicije modularne forme.

Dakle, Eisensteinov red težine k, $k > 2$ *paran, je modularna forma težine* k.

Sljedeći primjer će nam biti bitan kasnije, jer ćemo pomoću funkcije Δ iz primjera definirati $j-$invarijantu, koja će nam trebati za jednu od verzija teorema o modularnosti.

Primjer 1.0.5. *Definirajmo prvo*

$$g_2(\tau) = 60G_4(\tau), \;\; g_3(\tau) = 140G_6(\tau).$$

Za još jedan primjer modularne forme stavimo

$$\Delta : \mathcal{H} \to \mathbb{C}, \;\; \Delta(\tau) = (g_2(\tau))^3 - 27(g_3(\tau))^2.$$

Gornju funkciju Δ *nazivamo diskriminantom.*

U prethodnom primjeru smo vidjeli da su G_4 *i* G_6 *modularne forme. To znači da su one holomorfne na gornjoj poluravnini pa iz definicije od* Δ *lako zaključujemo da je i ona holomorfna na gornjoj poluravnini.*

Za $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, *koristeći činjenicu da su* G_4 *i* G_6 *modularne forme, pa onda i slabo modularne funkcije težine* 4*, odnosno* 6*, sljedećim računom vidimo da je* Δ *slabo modularna funkcija težine* 12*:*

$$\Delta(\gamma(\tau)) = (g_2(\gamma(\tau)))^3 - 27(g_3(\gamma(\tau)))^2 = (60G_4(\gamma(\tau)))^3 - 27(140G_6(\gamma(\tau)))^2 =$$

$$= (60(c\tau + d)^4 G_4(\tau))^3 - 27(140(c\tau + d)^6 G_6(\tau))^2 =$$

$$= (c\tau + d)^{12}(60G_4(\tau))^3 - 27(140G_6(\tau))^2 = (c\tau + d)^{12}(g_2(\tau))^3 - 27(g_3(\tau))^2 =$$

$$= (c\tau + d)^{12}\Delta(\tau).$$

Nadalje, vrijedi da je $\lim_{\mathrm{Im}\,\tau\to\infty} G_4(\tau) < \infty$*, i* $\lim_{\mathrm{Im}\,\tau\to\infty} G_6(\tau) < \infty$*, pa iz toga zaključujemo da je i* $\lim_{\mathrm{Im}\,\tau\to\infty} \Delta(\tau) < \infty$.

Dakle, Δ *je modularna forma težine* 12.

Skup modularnih formi svih težina,

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

je prsten. Iz ovoga vidimo da imamo li neke primjere modularnih formi, lako množenjem, odnosno zbrajanjem istih, možemo doći do novih modularnih formi. Originalnije primjere te način na koji možemo konstruirati modularne forme možemo naći u [5, Poglavlje 5].

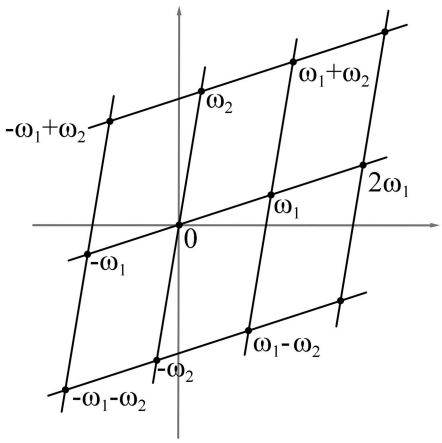
Poglavlje 2

Kompleksni torusi i eliptičke krivulje

U ovom poglavlju definirat ćemo kompleksni torus i eliptičku krivulju. Cilj nam je pokazati na koji način možemo uspostaviti bijekciju između ta dva objekta. Počinjemo s definicijom rešetke i nekim njenim osnovnim svojstvima.

2.1 Kompleksni torusi

Definicija 2.1.1. *Neka je* $\{\omega_1, \omega_2\}$ *baza za* $\mathbb{C}$ *nad* $\mathbb{R}$. *Tada skup* $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$ *zovemo rešetka u* $\mathbb{C}$.



Slika 2.1: Rešetka $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$

Primijetimo da prikaz rešetke nije jedinstven. Npr. $\{\omega_1, \omega_2\} = \{1, i\}$ i $\{\omega_1', \omega_2'\} = \{1, 1+i\}$ su dvije baze od $\mathbb{C}$ nad $\mathbb{R}$ koje određuju istu rešetku.

Bez smanjenja općenitosti možemo uzeti da svaka rešetka $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$ zadovoljava uvjet $\frac{\omega_1}{\omega_2} \in \mathcal{H}$. Naime, ako imamo rešetku $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$ s bazom $\{\omega_1, \omega_2\}$ takvu da $\frac{\omega_1}{\omega_2} \notin \mathcal{H}$, tada baza $\{-\omega_1, \omega_2\}$ određuje istu rešetku, a iz

$$\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = \frac{-1 \cdot \frac{\omega_1}{\omega_2} + 0}{0 \cdot \frac{\omega_1}{\omega_2} + 1} = \frac{-\omega_1}{\omega_2},$$

slično kao u (1.1), zaključujemo da je $\operatorname{Im}(\frac{-\omega_1}{\omega_2}) = -\operatorname{Im}(\frac{\omega_1}{\omega_2})$. Dakle $\frac{-\omega_1}{\omega_2} \in \mathcal{H}$. Čak ni taj uvjet ne određuje jedinstvenu rešetku, no određuje ju do na množenje elementima iz $\mathrm{SL}_2(\mathbb{Z})$, kao što vidimo u sljedećoj lemi.

Lema 2.1.2. *Neka su $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$ i $\Lambda' = \omega_1'\mathbb{Z} \oplus \omega_2'\mathbb{Z}$ dvije rešetke takve da je $\omega_1/\omega_2 \in \mathcal{H}$ i $\omega_1'/\omega_2' \in \mathcal{H}$. Tada je $\Lambda = \Lambda'$ ako i samo ako je*

$$\begin{bmatrix} \omega_1' \\ \omega_2' \end{bmatrix} = \gamma \begin{bmatrix} \omega_1 \\ \omega_2 \end{bmatrix}, \text{ za neki } \gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

Dokaz. Pretpostavimo prvo da je $\Lambda = \Lambda'$, odnosno $\omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z} = \omega_1'\mathbb{Z} \oplus \omega_2'\mathbb{Z}$. Primjećujemo da je $\omega_1, \omega_2 \in \Lambda'$, što znači da ω_1 i ω_2 možemo prikazati kao $\mathbb{Z}-$linearne kombinacije od ω_1' i ω_2'. To možemo zapisati kao

$$\begin{bmatrix} \omega_1 \\ \omega_2 \end{bmatrix} = A \begin{bmatrix} \omega_1' \\ \omega_2' \end{bmatrix}, \text{ za neki } A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\mathbb{Z}).$$

Analogno, budući da je $\omega_1', \omega_2' \in \Lambda$, imamo

$$\begin{bmatrix} \omega_1' \\ \omega_2' \end{bmatrix} = B \begin{bmatrix} \omega_1 \\ \omega_2 \end{bmatrix}, \text{ za neki } B \in M_2(\mathbb{Z}),$$

pa je

$$\begin{bmatrix} \omega_1 \\ \omega_2 \end{bmatrix} = AB \begin{bmatrix} \omega_1 \\ \omega_2 \end{bmatrix}.$$

Budući da su ω_1, ω_2 linearno nezavisni nad $\mathbb{R}$, zaključujemo da je $AB = I$, pa je

$$\det(AB) = \det A \cdot \det B = 1,$$

odnosno $\det A = \det B = \pm 1$. Treba još pokazati da su te determinante jednake 1. No, iz

$$\frac{\omega_1}{\omega_2} = \frac{a\omega_1' + b\omega_2'}{c\omega_1' + d\omega_2'}$$

dijeljenjem brojnika i nazivnika s ω_2' dobijemo

$$\frac{\omega_1}{\omega_2} = \frac{a\frac{\omega_1'}{\omega_2'} + b}{c'\frac{\omega_1'}{\omega_2'} + d},$$

tj. $\frac{\omega_1}{\omega_2} = A\left(\frac{\omega_1'}{\omega_2'}\right)$. Iz pretpostavke $\frac{\omega_1}{\omega_2}, \frac{\omega_1'}{\omega_2'} \in \mathcal{H}$ i formule analogne (1.1) zaključujemo da je $\det A = \det B = 1$.

Obratno, pretpostavimo da vrijedi

$$\begin{bmatrix}\omega_1' \\ \omega_2'\end{bmatrix} = \gamma \begin{bmatrix}\omega_1 \\ \omega_2\end{bmatrix}, \text{ za neki } \gamma = \begin{bmatrix}a & b \\ c & d\end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

Iz toga zaključujemo da je

$$\omega_1' = a\omega_2 + b\omega_1, \;\; \omega_2' = c\omega_1 + d\omega_2.$$

Inkluzija $\Lambda' \subseteq \Lambda$ očito vrijedi, jer su $a, b, c, d \in \mathbb{Z}$, pa je $\omega_1', \omega_2' \in \Lambda$. Kako bismo dokazali obratnu inkluziju, primijetimo da uvjet $ad - bc = 1$ povlači da je

$$\gamma^{-1} = \begin{bmatrix}d & -b \\ -c & a\end{bmatrix}$$

i zapišimo gornju matričnu jednakost u sljedećem obliku:

$$\begin{bmatrix}\omega_1 \\ \omega_2\end{bmatrix} = \gamma^{-1} \begin{bmatrix}\omega_1' \\ \omega_2'\end{bmatrix}, \text{ tj. } \begin{bmatrix}\omega_1 \\ \omega_2\end{bmatrix} = \begin{bmatrix}d & -b \\ -c & a\end{bmatrix} \begin{bmatrix}\omega_1' \\ \omega_2'\end{bmatrix}.$$

Budući da je

$$\omega_1 = d\omega_1' - b\omega_2', \;\; \omega_2 = -c\omega_1' + a\omega_2'$$

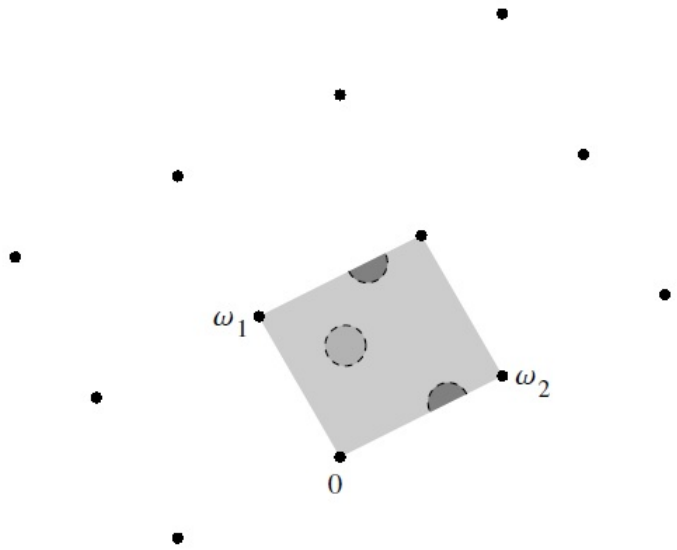
i da su $d, -b, -c, a \in \mathbb{Z}$, slijedi da je $\omega_1, \omega_2 \in \Lambda'$, pa je onda i $\Lambda \subseteq \Lambda'$, čime smo pokazali našu tvrdnju.

□

Definicija 2.1.3. *Za kvocijent kompleksne ravnine i rešetke,*

$$\mathbb{C}/\Lambda = \{z + \Lambda : z \in \mathbb{C}\}$$

kažemo da je kompleksni torus.



Slika 2.2: Geometrijska interpretacija kompleksnog torusa

Algebarski, primjećujemo da je kompleksni torus $\mathbb{C}/\Lambda$ zajedno s operacijom zbrajanja naslijeđenom iz $\mathbb{C}$ Abelova grupa. Geometrijski, kompleksni torus je paralelogram u kompleksnoj ravnini razapet s $\{\omega_1, \omega_2\}$ kojemu poistovjećujemo suprotne stranice. Nadalje, svaki kompleksni torus je Riemannova ploha. Definiciju i više o Riemannovim plohama možemo naći u [4].

Pomoću sljedeće propozicije moći ćemo detaljnije opisati svaki kompleksni torus. Navodimo je bez dokaza, koji se može naći u [2, Poglavlje 1], jer bismo inače morali uvoditi nove pojmove koji nam dalje neće biti od interesa.

Propozicija 2.1.4. *Neka su Λ i Λ' rešetke. Tada postoji holomorfni izomorfizam grupa između kompleksnih torusa $\mathbb{C}/\Lambda$ i $\mathbb{C}/\Lambda'$ ako i samo ako postoji $m \in \mathbb{C}$ takav da je $m\Lambda = \Lambda'$. Izomorfizam je dan sa $\varphi : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$, $\varphi(z + \Lambda_\tau) = mz + \Lambda'$.*

Uzmimo sada proizvoljnu rešetku $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$ takvu da je $\frac{\omega_1}{\omega_2} \in \mathcal{H}$. Označimo $\tau = \frac{\omega_1}{\omega_2}$ i stavimo $\Lambda_\tau = \tau\mathbb{Z} \oplus \mathbb{Z}$. Budući da je $\frac{1}{\omega_2}\Lambda = \Lambda_\tau$, prema prethodnoj propoziciji slijedi da postoji izomorfizam između $\mathbb{C}/\Lambda$ i $\mathbb{C}/\Lambda_\tau$. To znači da je svaki kompleksni torus izomorfan nekom kompleksnom torusu čija je rešetka generirana s $\{\tau, 1\}$.

No, takav τ nije jedinstven. Npr. za rešetku $\Lambda = 2i\mathbb{Z} \oplus 2\mathbb{Z}$ vrijedi da je torus $\mathbb{C}/\Lambda$ izomorfan s $\mathbb{C}/\Lambda_i$, a kako smo ranije vidjeli da vrijedi $\Lambda_i = \Lambda_{i+1}$, također je $\mathbb{C}/\Lambda$ izomorfan s $\mathbb{C}/\Lambda_{i+1}$.

Ako su sada $\tau_1, \tau_2 \in \mathbb{C}$ takvi da je Λ izomorfna s Λ_{τ_1} i s Λ_{τ_2}, iz leme 2.1.2 slijedi da je $\tau_1 = \gamma(\tau_2)$, za neki $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.

Time smo pokazali da svaki kompleksni torus određuje točku $\tau \in \mathcal{H}$ do na djelovanje od $\mathrm{SL}_2(\mathbb{Z})$. Generalizaciju ove tvrdnje ćemo pokazati u poglavlju 3.2.

2.2 Veza između kompleksnog torusa i eliptičke krivulje

Sada ćemo definirati eliptičku krivulju i do kraja ovog poglavlja ćemo dokazati na koji način možemo povezati eliptičke krivulje i već spomenute kompleksne toruse.

Definicija 2.2.1. *Eliptička krivulja nad poljem $\mathbb{K}$ je glatka projektivna krivulja genusa 1 s određenom točkom $\mathcal{O} \in \mathbb{K}$.*

Napomena 2.2.2. *Upravo definirana eliptička krivulja može se nad poljima karakteristike različite od 2 i 3 shvatiti kao skup svih rješenja jednadžbe*

$$y^2 = 4x^3 - a_2x - a_3, \;\; a_2, a_3 \in \mathbb{Z},$$

uz uvjet $a_2^3 - 27a_3^2 \neq 0$, zajedno s "točkom u beskonačnosti" koju označavamo s $\mathcal{O}$.

Promatrajmo sada Weierstrassovu $\wp-$funkciju, $\wp : \mathbb{C} \to \hat{\mathbb{C}}$, danu sa

$$\wp(z) = \frac{1}{z^2} + {\sum_{\omega \in \Lambda}}' \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right), \;\; z \in \mathbb{C}, z \notin \Lambda,$$

gdje sumiramo po svim $\omega \neq 0$. Može se pokazati da je gornja funkcija meromorfna s periodom Λ. Takve funkcije nazivamo eliptičkim funkcijama s obzirom na Λ. Zato je možemo shvatiti i kao funkciju $\mathbb{C}/\Lambda \to \hat{\mathbb{C}}$. Također, svaka eliptička funkcija s obzirom na Λ je racionalna funkcija u ovisnosti o $\wp$ i $\wp'$ [8, Teorem 3.11.1].

Vidimo da funkcija $\wp$ ovisi o rešetki Λ, pa ćemo ponekad, da bismo naglasili o kojoj se rešetki radi, pisati $\wp_\Lambda$.

Sjetimo se, u primjeru 1.0.4 smo definirali Eisensteinov red težine k. No, Eisensteinovi redovi se mogu generalizirati na sljedeći način.

Za rešetku Λ i paran $k > 2$ stavimo

$$G_k(\Lambda) = {\sum_{\omega \in \Lambda}}' \frac{1}{\omega^k}.$$

Primijetimo da je $G_k(\tau)$ od ranije sada jednak $G_k(\Lambda_\tau)$.

Teorem 2.2.3. *Neka je $\wp$ Weierstrassova $\wp$−funkcija s obzirom na rešetku Λ. Tada vrijedi*

1. *Laurentov razvoj od $\wp$ je*

$$\wp(z) = \frac{1}{z^2} + \sum_{\substack{n=2 \\ n \text{ paran}}}^{\infty} (n+1)G_{n+2}(\Lambda)z^n,$$

   za sve z takve da je $0 < |z| < \inf\{|\omega| : \omega \in \Lambda \setminus \{0\}\}$.

2. *Funkcije $\wp$ i $\wp'$ zadovoljavaju jednakost*

$$(\wp'(z))^2 = 4(\wp(z))^3 - g_2(\Lambda)\wp(z) - g_3(\Lambda),$$

   gdje je $g_2(\Lambda) = 60G_4(\Lambda)$ i $g_3(\Lambda) = 140G_6(\Lambda)$.

3. *Neka je $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$ i $\omega_3 = \omega_1 + \omega_2$. Tada se jednadžba koju zadovoljavaju $\wp$ i $\wp'$, $y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$, može zapisati u obliku*

$$y^2 = 4(x - e_1)(x - e_2)(x - e_3),$$

   gdje je $e_i = \wp\left(\frac{\omega_i}{2}\right)$, $i = 1, 2, 3$. Također, e_i, $i = 1, 2, 3$, su međusobno različiti.

Dokaz. Za dokaz prve tvrdnje, nađimo prvo Laurentov razvoj funkcije

$$\zeta(z) = \frac{1}{z} + {\sum_{\omega \in \Lambda}}' \left(\frac{1}{z - \omega} + \frac{1}{\omega} + \frac{z}{\omega^2}\right).$$

Neka je $m = \min\{\omega : \omega \in \Lambda \setminus \{0\}\}$ i označimo sa $D = \{z \in \mathbb{C} : |z| < m\}$ najveću otvorenu kuglu oko 0 koja ne sadrži niti jedan element rešetke Λ osim 0. Primijetimo da se ζ može zapisati i kao

$$\zeta(z) = \frac{1}{z} + {\sum_{\omega \in \Lambda}}' \frac{z^2}{\omega^2(z - \omega)}.$$

Može se pokazati da je red koji se pojavljuje u ζ apsolutno konvergentan za $z \in \mathbb{C} \setminus \Lambda$. Nadalje, za svaki $\omega \in \Lambda \setminus \{0\}$ red

$$\frac{1}{z - \omega} = -\frac{1}{\omega} - \frac{z}{\omega^2} - \frac{z^2}{\omega^3} - \ldots$$

je apsolutno konvergentan za $z \in D$ pa uvrštavanjem tog reda u ζ i mijenjanjem poretka sumacije, što možemo zbog apsolutne konvergencije, dobijemo

$$\zeta(z) = \frac{1}{z} + {\sum_{\omega\in\Lambda}}' \frac{z^2}{\omega^2}\left(-\frac{1}{\omega} - \frac{z}{\omega^2} - \frac{z^2}{\omega^3} - ...\right) =$$

$$= \frac{1}{z} + {\sum_{\omega\in\Lambda}}' \left(-\frac{z^2}{\omega^3} - \frac{z^3}{\omega^4} - \frac{z^4}{\omega^5} - ...\right) =$$

$$= \frac{1}{z} - G_3(\Lambda)z^2 - G_4(\Lambda)z^3 - G_5(\Lambda)z^4 - ...$$

Za neparne k, članovi ω^{-k} i $(-\omega)^{-k}$ u G_k se ponište, dakle vrijedi $G_k = 0$. Sada imamo

$$\zeta(z) = \frac{1}{z} + \sum_{n=2}^{\infty} G_{2n}(\Lambda)z^{2n-1}$$

pa zaključujemo

$$\wp(z) = -\zeta'(z) = \frac{1}{z^2} + \sum_{n=2}^{\infty}(2n-1)G_{2n}(\Lambda)z^{2n-2}$$

te smo time dokazali prvu tvrdnju.

Za dokaz druge tvrdnje, računamo

$$\wp'(z) = \frac{-2}{z^3} + 6g_4(\Lambda)z + 20G_6(\Lambda)z^3 + ...,$$

$$(\wp'(z))^2 = \frac{4}{z^6} - \frac{24G_4(\Lambda)}{z^2} - 80G_6(\Lambda) + z^2\phi_1(z),$$

$$4(\wp(z))^3 = \frac{4}{z^6} + \frac{36G_4(\Lambda)}{z^2} + 60G_6(\Lambda) + z^2\phi_2(z),$$

$$60G_4(\Lambda)\wp(z) = \frac{60G_4(\Lambda)}{z^2} + z^2\phi_3(z),$$

gdje su $\phi_i(z),\ i = 1, 2, 3$, konvergentni redovi potencija na D.

Zadnje 3 jednakosti daju

$$(\wp'(z))^2 - 4(\wp(z))^3 + 60G_4(\Lambda)\wp(z) + 140G_6(\Lambda) = z^2(\phi_1(z) - \phi_2(z) + \phi_3(z)).$$

Kako su $\wp$ i $\wp'$ eliptičke funkcije s obzirom na Λ, funkcija

$$f(z) = (\wp'(z))^2 - 4(\wp(z))^3 + 60G_4(\Lambda)\wp(z) + 140G_6(\Lambda)$$

je također eliptička s obzirom na Λ.

Sada je $f(z) = z^2(\phi_1(z) - \phi_2(z) + \phi_3(z))$ holomorfna i $\Lambda-$periodična, dakle ograničena. Prema Liouvilleovom teoremu f je konstantna funkcija. Točnije, $f = 0$, jer je $\lim_{z\to 0} f(z) = 0$.

Dakle, vrijedi

$$(\wp'(z))^2 - 4(\wp(z))^3 + 60G_4(\Lambda)\wp(z) + 140G_6(\Lambda) = 0,$$

odnosno

$$(\wp'(z))^2 = 4(\wp(z))^3 - g_2(\Lambda)\wp(z) - g_3(\Lambda).$$

Dokažimo sada treći dio teorema. Primijetimo prvo da funkcija $\wp : \mathbb{C}/\Lambda \to \hat{\mathbb{C}}$ ima polove samo u točkama $z \in \Lambda$, što znači da na $\mathbb{C}/\Lambda$ postoji samo jedan pol i on je reda 2. Sumu redova svih polova funkcije zovemo redom te funkcije. Dakle, $\wp$ je reda 2. Također, lako vidimo da je

$$\wp'(z) = -\frac{2}{z^3} - {\sum_{\omega\in\Lambda}}' \frac{2}{(z-\omega)^3}$$

reda 3. Općenito vrijedi da ako je eliptička funkcija reda $N > 0$, tada je N i suma redova svih nultočki te funkcije. Točnije, tvrdnja vrijedi ne samo za nultočke, već i za bilo koju vrijednost funkcije koja se postiže [8, Teorem 3.6.4].

Već smo spomenuli da je funkcija $\wp'$ neparna, a iz toga slijedi da $\wp'$ ima nultočke u točkama reda 2 od $\mathbb{C}/\Lambda$. Naime, ako je točka z reda 2, odnosno $2z \equiv 0 \pmod{\Lambda}$, onda je $z \equiv -z \pmod{\Lambda}$, pa je $\wp'(z) = \wp'(-z) = -\wp'(z)$. Dakle, $\wp'(z) = 0$.

Budući da je $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$, točke reda 2 su oblika $\dfrac{\omega_i}{2},\ i = 1, 2, 3$. Primijetimo da su to jedine nultočke od $\wp'$, budući da je to funkcija reda 3.

Sada iz $(\wp'(z))^2 = 4(\wp(z))^3 - g_2(\Lambda)\wp(z) - g_3(\Lambda)$ vidimo da polinom $p(x) = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$ ima nultočke u $\wp(z)$, za z takve da je $\wp'(z)$, a kako iz prvog dijela dokaza znamo da su $\dfrac{\omega_i}{2},\ i = 1, 2, 3$, takve točke, slijedi da je

$$y^2 = 4(x - e_1)(x - e_2)(x - e_3).$$

Još je preostalo dokazati da su točke $e_i,\ i = 1, 2, 3$, međusobno različite. Definirajmo $f_i(z) = \wp(z) - e_i,\ i = 1, 2, 3$. Primijetimo da f_i i $\wp$ imaju iste polove, pa su funkcije f_i eliptičke reda 2. Dakle, na $\mathbb{C}/\Lambda$, funkcije f_i imaju ili dvije različite nultočke ili jednu nultočku reda 2. No, vrijedi

$$f_i\left(\frac{\omega_i}{2}\right) = f_i'\left(\frac{\omega_i}{2}\right) = 0,$$

pa funkcija f_i nema drugih nultočaka osim $\frac{\omega_i}{2}$. Dakle, $f_i(\frac{\omega_j}{2}) \neq 0$, za $i \neq j$. Sada vidimo da je

$$f_i\left(\frac{\omega_j}{2}\right) = \wp\left(\frac{\omega_j}{2}\right) - e_i = e_j - e_i \neq 0,$$

pa su točke e_i, $i = 1, 2, 3$, međusobno različite. □

U dijelu *2.* prethodnog teorema vidimo da preslikavanje $z \mapsto (\wp_\Lambda(z), \wp'_\Lambda(z))$ preslikava točke $z \in \mathbb{C}/\Lambda$, $z \neq \Lambda$ u točke $(x, y) \in \mathbb{C}^2$ koje zadovoljavaju nesingularnu kubnu jednadžbu $y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$ te je ono bijektivno. Naime, svaka vrijednost $x \in \mathbb{C}$ se postiže dva puta na $\mathbb{C}/\Lambda$, kao što je spomenuto u dokazu prethodnog teorema, tj. $x = \wp_\Lambda(\pm z + \Lambda)$, jer je $\wp_\Lambda$ parna funkcija. Tada je $y = \wp'(\pm z + \Lambda) = \pm\wp'(z + \Lambda)$, gdje druga jednakost vrijedi jer je $\wp'$ neparna funkcija. Za točke $z \in \Lambda$ vrijedi da se preslikavaju u prikladno definiranu točku u beskonačnosti na eliptičkoj krivulji. Tako smo dobili da za svaku rešetku Λ, njoj pridružena Weierstrassova $\wp-$funkcija i njezina derivacija $\wp'$ daju bijekciju između kompleksnog torusa $\mathbb{C}/\Lambda$ i eliptičke krivulje $y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$.

Primjer 2.2.4. *Lako možemo vidjeti [8, Korolar 6.5.3] da vrijedi*

$$g_2\left(e^{\frac{2\pi i}{3}}\right) = 0,\ g_3(i) = 0. \tag{2.1}$$

Sada iz gornjih razmatranja zaključujemo da postoji bijekcija između kompleksnog torusa $\mathbb{C}/\Lambda_{\mu_3}$, gdje smo označili $\mu_3 = e^{\frac{2\pi i}{3}}$, i eliptičke krivulje s jednadžbom $y^2 = 4x^3 - g_3(\mu_3)$.

Također, postoji bijekcija između torusa $\mathbb{C}/\Lambda_i$ i eliptičke krivulje s jednadžbom $y^2 = 4x^3 - g_2(i)x$.

Za sada znamo da između skupa $\mathbb{C}/\Lambda$ i skupa svih rješenja jednadžbe $y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$ postoji bijekcija. No, vrijedi i više. Ta bijekcija preslikava grupovno zbrajanje s torusa $\mathbb{C}/\Lambda$ na eliptičku krivulju $y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$.

U [7, Poglavlje III.2] možemo vidjeti kako je definirano zbrajanje točaka na eliptičkoj krivulji. Ukratko, ako su (x_1, y_1) i (x_2, y_2) dvije točke na eliptičkoj krivulji, one određuju pravac koji siječe krivulju u još jednoj točki, (x_3, y_3). Tada zbroj točaka (x_1, y_1) i (x_2, y_2) definiramo kao točku $(x_3, -y_3)$.

Neka su sada $z_1 + \Lambda$ i $z_2 + \Lambda$ dvije ne-nul točke na $\mathbb{C}/\Lambda$. Točke $(\wp(z_1), \wp'(z_1))$ i $(\wp(z_2), \wp'(z_2))$ na eliptičkoj krivulji određuju tangentu ili sekantu $ax + by + c = 0$. Promotrimo sada funkciju

$$f(z) = a\wp(z) + b\wp'(z) + c.$$

Primijetimo da je f eliptička funkcija s obzirom na Λ. Sada iz [8, Teorem 3.6.7] vidimo da je

$$\sum_{x\in\mathbb{C}/\Lambda} \nu_x(f)x \in \Lambda, \text{ tj. } \sum_{x\in\mathbb{C}/\Lambda} \nu_x(f)x = 0 \text{ u } \mathbb{C}/\Lambda, \tag{2.2}$$

gdje $\nu_z(f)$ označava red od f u točki z, u smislu da je

$$f(z) = (z-x)^{\nu_x(f)}g(z),$$

gdje je $g(z) \neq 0$ holomorfna funkcija na nekoj okolini od x. Primijetimo da je $\nu_z(f) = 0$ za sve $z \in \mathbb{C}/\Lambda$ osim za nultočke i polove.

Kada u funkciji f imamo $b \neq 0$, tada je točka $0+\Lambda$ pol reda 3 za funkciju f, jer je ista točka pol reda 3 za funkciju $\wp'$, te f ima nultočke u točkama $z_1+\Lambda$ i $z_2+\Lambda$. Sada, budući da je $0+\Lambda$ jedini pol funkcije f te je broj nultočki eliptičkih funkcija jednak broju polova (brojeći redove), iz (2.2) zaključujemo da je treća nultočka funkcije f točka $z_3+\Lambda \in \mathbb{C}/\Lambda$ takva da je $z_1+z_2+z_3 \in \Lambda$, tj.

$$z_1+z_2+z_3+\Lambda = 0+\Lambda.$$

Kada je $b=0$, tada je f ima pol reda 2 u $0+\Lambda$ te nultočke u $z_1+\Lambda$ i $z_2+\Lambda$. Kao u prethodnom slučaju, iz (2.2) zaključujemo da je

$$z_1+z_2+\Lambda = 0+\Lambda$$

te ako označimo $z_3 = 0+\Lambda$, opet imamo

$$z_1+z_2+z_3+\Lambda = 0+\Lambda.$$

Ranije smo rekli da se točka $z_3 = 0+\Lambda$ preslikava u točku u beskonačnosti na eliptičkoj krivulji $y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$. U slučaju $b=0$, možemo zamišljati da točka u beskonačnosti leži na pravcu $ax+by+c=0$, koji je vertikalan.

Dakle, ako imamo točke $z_1+\Lambda$ i $z_2+\Lambda$ na $\mathbb{C}/\Lambda$, gdje je $(z_1+\Lambda)+(z_2+\Lambda) = -z_3+\Lambda$, tada vrijedi da su točke $(\wp(z_1),\wp'(z_1))$, $(\wp(z_2),\wp'(z_2))$ i $(\wp(z_3),\wp'(z_3))$ na eliptičkoj krivulji kolinearne. Točka $-z_3+\Lambda$ se preslikava u točku $(\wp(-z_3),\wp'(-z_3)) = (\wp(z_3),-\wp'(z_3))$ na eliptičkoj krivulji.

Time smo pokazali da je bijekcija između $\mathbb{C}/\Lambda$ i eliptičke krivulje $y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$ iz teorema 2.2.3 izomorfizam grupa.

Sjetimo se iz propozicije 2.1.4 da je svaki holomorfni izomorfizam kompleksnih torusa $\mathbb{C}/\Lambda$ i $\mathbb{C}/\Lambda'$ oblika

$$z+\Lambda \mapsto mz+\Lambda',$$

gdje je $\Lambda' = m\Lambda$. Budući da je

$$\wp_\Lambda(z) = m^2\wp_{m\Lambda}(mz),$$

$$\wp'_\Lambda(z) = m^3 \wp'_{m\Lambda}(mz),$$

odgovarajući izomorfizam elptičkih krivulja dan je supstitucijom

$$(x, y) = (m^2 x', m^3 y'),$$

odnosno preslikavanjem

$$(x, y) \mapsto (m^{-2} x, m^{-3} y),$$

te on transformira eliptičku krivulju $y^2 = 4x^3 - g_2 x - g_3$ pridruženu Λ u krivulju $y^2 = 4x^3 - m^{-4} g_2 x - m^{-6} g_3$ pridruženu Λ'.

Sjetimo se sada modularne forme Δ iz primjera 1.0.5.

Propozicija 2.2.5. *Za svaki $\tau \in \mathcal{H}$ vrijedi $\Delta(\tau) \neq 0$.*

Dokaz. Neka je $\tau \in \mathcal{H}$ proizvoljan. U teoremu 2.2.3 smo pokazali da polinom

$$p_\tau(x) = 4x^3 - g_2(\tau)x - g_3(\tau)$$

ima različite nultočke. Primijetimo da je $\Delta(\tau)$ diskriminanta polinoma p_τ do na množenje konstantom. Naime, diskriminanta polinoma oblika $ax^3 + cx + d$ je dana s $-4ac^3 - 27a^2d^2$, pa je diskriminanta polinoma p_τ jednaka

$$16g_2(\tau)^3 - 27 \cdot 16 g_3(\tau)^2 = 16\Delta(\tau).$$

Budući da je diskriminanta polinoma jednaka nuli ako i samo ako postoji neka višestruka nultočka tog polinoma, zaključujemo da je $\Delta(\tau) \neq 0$. □

Definirajmo funkciju

$$j : \mathcal{H} \to \mathbb{C},$$
$$j(\tau) = 1728 \frac{(g_2(\tau))^3}{\Delta(\tau)}.$$

Ovu funkciju zovemo $j-$invarijanta, iz razloga koji će biti objašnjeni na kraju poglavlja.

Iz prethodne propozicije vidimo da je gornja funkcija dobro definirana. Također, može se pokazati da je ona surjektivna [8, Teorem 6.5.5].

Primijetimo da su brojnik i nazivnik $j-$funkcije modularne funkcije iste težine, pa vrijedi

$$j(\gamma(\tau)) = j(\tau),\ \gamma \in \mathrm{SL}_2(\mathbb{Z}),\ \tau \in \mathcal{H}, \tag{2.3}$$

tj. funkcija j je invarijantna na djelovanje grupe $\mathrm{SL}_2(\mathbb{Z})$.

Već smo vidjeli da svakom kompleksnom torusu $\mathbb{C}/\Lambda$ možemo pridružiti eliptičku krivulju

$$y^2 = 4x^3 - a_2(\Lambda)x - a_3(\Lambda).$$

Koristeći prethodnu propoziciju pokazat ćemo da vrijedi i obrat.

Propozicija 2.2.6. *Za svaku eliptičku krivulju*

$$y^2 = 4x^3 - a_2x - a_3,\ \ a_2^3 - 27a_3^2 \neq 0,$$

postoji rešetka Λ *takva da je* $a_2 = g_2(\Lambda)$ *i* $a_3 = g_3(\Lambda)$.

Dokaz. Pretpostavimo prvo da je $a_2 = 0$. Tada zbog $a_2^3 - 27a_3^2 \neq 0$ vrijedi $a_3 \neq 0$. Znamo iz (2.1) da vrijedi $g_2\left(e^{\frac{2\pi i}{3}}\right) = 0$, pa je onda $g_3\left(e^{\frac{2\pi i}{3}}\right) \neq 0$, jer je $\Delta(\tau) = g_2(\tau)^3 - 27g_3(\tau)^2$, a iz propozicije 2.2.5 znamo da je $\Delta(\tau) \neq 0$, za svaki $\tau \in \mathcal{H}$. Dakle, možemo izabrati $\mu \in \mathbb{C} \setminus \{0\}$ takav da je $\mu^{-6}g_3\left(e^{\frac{2\pi i}{3}}\right) = a_3$. Stavimo li $\Lambda = \mu\mathbb{Z} \oplus \mu e^{\frac{2\pi i}{3}}\mathbb{Z}$ imamo da je

$$g_2(\Lambda) = \mu^{-4}g_2\left(e^{\frac{2\pi i}{3}}\right) = 0 = a_2,$$

$$g_3(\Lambda) = \mu^{-6}g_3\left(e^{\frac{2\pi i}{3}}\right) = a_3.$$

Za slučaj kada je $a_3 = 0$ i $a_2 \neq 0$, imamo $g_3(i) = 0$, pa slično zaključujemo $g_2(i) \neq 0$. Sada možemo izabrati $\mu \in \mathbb{C} \setminus \{0\}$ takav da je $\mu^{-4}g_2(i) = a_2$ te za $\Lambda = \mu\mathbb{Z} \oplus \mu i\mathbb{Z}$ vrijedi

$$g_2(\Lambda) = \mu^{-4}g_2(i) = a_2,$$
$$g_3(\Lambda) = \mu^{-6}g_3(i) = 0 = a_3.$$

Neka je sada $a_2, a_3 \neq 0$. Budući da je $j : \mathcal{H} \to \mathbb{C}$ surjekcija, postoji $\tau \in \mathcal{H}$ takav da je

$$j(\tau) = \frac{1728a_2^3}{a_2^3 - 27a_3^2}.$$

Iz definicije funkcije j slijedi

$$\frac{g_2(\tau)^3}{g_2(\tau)^3 - 27g_3(\tau)^2} = \frac{a_2^3}{a_2^3 - 27a_3^2}.$$

Sređivanjem dobijemo

$$\frac{a_2^3}{g_2(\tau)^3} = \frac{a_3^2}{g_3(\tau)^2}. \tag{2.4}$$

Za bilo koji $\omega_2 \in \mathbb{C} \setminus \{0\}$ stavimo $\omega_1 = \tau\omega_2$ i $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$. Tada iz definicija od $g_i(\Lambda)$, $g_i(\tau)$, za $i = 1, 2$, vidimo da je

$$g_2(\Lambda) = \omega_2^{-4}g_2(\tau) \text{ i } g_3(\Lambda) = \omega_2^{-6}g_3(\tau).$$

Primijetimo da bi propozicija bila dokazana kada bismo našli ω_2 takav da je

$$\omega_2^{-4} = \frac{a_2}{g_2(\tau)} \text{ i } \omega_2^{-6} = \frac{a_3}{g_3(\tau)}.$$

Izaberimo ω_2 tako da je zadovoljen prvi uvjet, tj. $\omega_2^{-4} = \frac{a_2}{g_2(\tau)}$. Vidimo da je onda $\omega_2^{-12} = \frac{a_2^3}{g_2(\tau)^3}$. Tada pomoću (2.4) dobijemo da je $\omega_2^{-6} = \pm\frac{a_3}{g_3(\tau)}$. Ako je potrebno, možemo zamijeniti ω_2 s $i\omega_2$, pa će oba uvjeta biti zadovoljena. □

Promatrajmo sada preslikavanje

$$(x, y) \mapsto (m^{-2}x, m^{-3}y)$$

spomenuto ranije, koje transformira eliptičku krivulju $y^2 = 4x^3 - a_2x - a_3$ u $y^2 = 4x^3 - m^{-4}a_2x - m^{-6}a_3$.

Iz gornje propozicije slijedi da za eliptičku krivulju $y^2 = 4x^3 - a_2x - a_3$ postoji rešetka Λ takva da je $a_2 = g_2(\Lambda)$ i $a_3 = g_3(\Lambda)$ te da za eliptičku krivulju $y^2 = 4x^3 - m^{-4}a_2x - m^{-6}a_3$ postoji rešetka Λ' takva da je $m^{-4}a_2 = g_2(\Lambda')$ i $m^{-6}a_3 = g_3(\Lambda')$.

Dakle, vrijedi $g_2(\Lambda) = m^4 g_2(\Lambda')$ i $g_3(\Lambda) = m^6 g_3(\Lambda')$

Sada, uz pomoć razmatranja iznad propozicije 2.2.5, možemo zaključiti da je $\Lambda' = m\Lambda$ i da svako preslikavanje $(x, y) \mapsto (m^{-2}x, m^{-3}y)$ između eliptičkih krivulja dolazi od holomorfnog izomorfizma kompleksnih torusa $z + \Lambda \mapsto mz + \Lambda'$, gdje je $\Lambda' = m\Lambda$.

Dakle, preslikavanje $(x, y) \mapsto (m^{-2}x, m^{-3}y)$ možemo smatrati izomorfizmom između eliptičkih krivulja te od sada poistovjećujemo eliptičke krivulje i kompleksne toruse (do na izomorfizam).

Sjetimo se funkcije

$$j : \mathcal{H} \to \mathbb{C}, \;\; j(\tau) = 1728\frac{(g_2(\tau))^3}{\Delta(\tau)}.$$

Ranije smo zaključili da svaki kompleksni torus do na izomorfizam određuje točku $\tau \in \mathcal{H}$ do na djelovanje od $\mathrm{SL}_2(\mathbb{Z})$. Također, vrijedi (2.3), tj. $j-$funkcija je invarijantna na djelovanje od $\mathrm{SL}_2(\mathbb{Z})$.

Sada zbog gornjih razmatranja o korespondenciji između klasa izmorfizama eliptičkih krivulja i kompleksnih torusa, vidimo da je svakoj klasi eliptičkih krivulja, odnosno kompleksnih torusa, pridružena jedinstvena vrijednost $j-$funkcije.

Poglavlje 3

Modularne krivulje i prostori parametara

U ovom poglavlju ćemo definirati kongruencijske podgrupe, podgrupe modularne grupe $\mathrm{SL}_2(\mathbb{Z})$ s određenim svojstvom, te ćemo pomoću njih definirati modularne krivulje. Zatim ćemo u glavnom teoremu ovoga rada pokazati na koji način svaka točka na modularnoj krivulji parametrizira eliptičku krivulju s nekim dodatnim torzijskim svojstvom.

3.1 Kongruencijske podgrupe

Prvo će nas zanimati neke podgrupe modularne grupe $\mathrm{SL}_2(\mathbb{Z})$.

Definicija 3.1.1. *Neka je $N \in \mathbb{N}$. Glavna kongruencijska podgrupa nivoa N je*

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

Definicija 3.1.2. *Za podgrupu Γ od $\mathrm{SL}_2(\mathbb{Z})$ kažemo da je kongruencijska podgrupa od $\mathrm{SL}_2(\mathbb{Z})$ ako je $\Gamma(N) \leq \Gamma$, za neki $N \in \mathbb{N}$. U tom slučaju kažemo da je Γ kongruencijska podgrupa nivoa N.*

Osim glavne kongruencijske podgrupe, spomenimo još dvije bitne kongruencijske podgrupe koje će nam biti od interesa,

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

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

Lako je vidjeti da vrijedi

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

3.2 Modularne krivulje

Sjetimo se da je svakom kompleksnom torusu pridružena neka rešetka Λ. Također se bez smanjenja općenitosti može uzeti da je $\Lambda = \mathbb{Z} \oplus \tau\mathbb{Z}$, za neki $\tau \in \mathcal{H}$, a na kraju poglavlja 2.1 smo pokazali i da svaka klasa izomorfizama kompleksnih torusa određuje τ na djelovanje grupe $\mathrm{SL}_2(\mathbb{Z})$. Ako za dvije eliptičke krivulje definiramo da su izomorfne ako su njima pridruženi kompleksni torusi izomorfni, pokazali smo da postoji bijekcija između skupa svih eliptičkih krivulja do na izomorfizam i skupa svih orbita $\mathrm{SL}_2(\mathbb{Z}) \setminus \mathcal{H} = \{\mathrm{SL}_2(\mathbb{Z})\tau : \tau \in \mathcal{H}\}$.

Za $\mathrm{SL}_2(\mathbb{Z})\setminus\mathcal{H}$ kažemo da je prostor parametara eliptičkih krivulja. Vidjet ćemo da na sličan način grupe $\Gamma(N), \Gamma_0(N)$ i $\Gamma_1(N)$ generiraju prostor parametara eliptičkih krivulja s nekim svojstvom.

Definicija 3.2.1. *Neka je* Γ *kongruencijska podgrupa od* $\mathrm{SL}_2(\mathbb{Z})$. *Modularna krivulja* $Y(\Gamma)$ *je skup svih orbita pri djelovanju od* Γ *na* $\mathcal{H}$, *tj.*

$$Y(\Gamma) = \Gamma\setminus\mathcal{H} = \{\Gamma\tau : \tau \in \mathcal{H}\}.$$

Modularne krivulje koje su pridružene već spomenutim kongruencijskim podgrupama od $\mathrm{SL}_2(\mathbb{Z})$ označavamo sa

$$Y(N) = \Gamma(N) \setminus \mathcal{H},$$

$$Y_0(N) = \Gamma_0(N) \setminus \mathcal{H},$$

$$Y_1(N) = \Gamma_1(N) \setminus \mathcal{H}.$$

Sada ćemo definirati skupove klasa izomorfizama eliptičkih krivulja s nekim dodatnim svojstvom te ćemo sljedećim teoremom pokazati koja je veza tih skupova s gore definiranim modularnim krivuljama.

Neka je $N \in \mathbb{N}$. Promatrajmo uređene parove (E, C), gdje je E kompleksna eliptička krivulja, a C je ciklička podgrupa od E reda N. Kažemo da su dva takva uređena para ekvivalentna, i pišemo $(E, C) \sim (E', C')$, ako postoji izomorfizam između E i E' koji preslikava C u C'. Primjećujemo da je $\sim$ relacija ekvivalencije i definiramo $S_0(N)$ kao skup svih klasa ekvivalencije te relacije. Elemente skupa $S_0(N)$ označavat ćemo s $[E, C]$.

Slično, za uređene parove (E, Q), gdje je E kompleksna eliptička krivulja, a Q točka na E reda N kažemo da su dva takva para (E, Q) i (E', Q') ekvivalentna, i

pišemo $(E, Q) \sim (E', Q')$, ako postoji izomorfizam između E i E' koji preslikava Q u Q'. To je relacija ekvivalencije i definiramo $S_1(N)$ kao skup svih klasa ekvivalencije te relacije. Elemente skupa $S_1(N)$ označavat ćemo s $[E, Q]$.

Prije definicije skupa $S(N)$, potrebno je definirati još neke pojmove.

Neka je $\mathbb{C}/\Lambda$ kompleksni torus, odnosno eliptička krivulja. Za podgrupu od $\mathbb{C}/\Lambda$ koja sadrži sve točke reda koji dijeli N kažemo da je $N-$torzijska podgrupa i označavamo ju s $E[N]$. Primijetimo da je

$$E[N] = \left\langle \frac{\omega_1}{N} + \Lambda \right\rangle \times \left\langle \frac{\omega_2}{N} + \Lambda \right\rangle.$$

Iz toga lako zaključujemo da je $E[N]$ podgrupa reda N^2, te je

$$E[N] \cong \mathbb{Z}/N\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z}.$$

Sada ćemo definirati Weilovo sparivanje

$$e_N : E[N] \times E[N] \to \mu_N,$$

gdje smo sa μ_N označili grupu $N-$tih korijena iz jedinice.

Neka su $P, Q \in E[N]$, $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$ i $\frac{\omega_1}{\omega_2} \in \mathcal{H}$. Budući da točke $\frac{\omega_1}{N} + \Lambda$ i $\frac{\omega_2}{N} + \Lambda$ generiraju $E[N]$, vrijedi

$$\begin{bmatrix} P \\ Q \end{bmatrix} = \gamma \begin{bmatrix} \frac{\omega_1}{N} + \Lambda \\ \frac{\omega_2}{N} + \Lambda \end{bmatrix},$$

za neki $\gamma \in \mathrm{M}_2(\mathbb{Z}/N\mathbb{Z})$.

Sada definiramo vrijednost Weilovog sparivanja kao

$$e_N(P, Q) = e^{\frac{2\pi i \det \gamma}{N}}.$$

Gornja vrijednost je očito $N-$ti korijen iz jedinice, a koristeći lemu 2.1.2 zaključujemo da je gornja definicija dobra, tj. ona ne ovisi o izboru baze za rešetku Λ.

Može se pokazati da vrijednosti Weilovog sparivanja ostaju očuvane pri izomorfizmu kompleksnih torusa, odnosno eliptičkih krivulja. Više o Weilovom sparivanju i svojstvima možemo naći u [7, Poglavlje III.8].

Definirajmo sada skup $S(N)$.

Za uređene parove $(E, (P, Q))$, gdje je E kompleksna eliptička krivulja, a (P, Q) je par točaka na E koji generira $N-$torzijsku podgrupu od E s Weilovim sparivanjem $e_N(P, Q) = e^{\frac{2\pi i}{N}}$, kažemo da su dva takva para $(E, (P, Q))$ i $(E', (P', Q'))$ ekvivalentna, i pišemo $(E, (P, Q)) \sim (E', (P', Q'))$, ako postoji izomorfizam između E i E' koji preslikava P u P' te Q u Q'. To je relacija ekvivalencije i definiramo $S(N)$ kao skup svih klasa ekvivalencije te relacije. Elemente skupa $S(N)$ označavat ćemo s $[E, (P, Q)]$.

Teorem 3.2.2. *Neka je $N \in \mathbb{N}$.*

1. *Prostor parametara za $\Gamma_0(N)$ je*

$$S_0(N) = \left\{ \left[E_\tau, \left\langle \frac{1}{N} + \Lambda_\tau \right\rangle \right] : \tau \in \mathcal{H} \right\}.$$

Dvije točke $\left[E_\tau, \left\langle \frac{1}{N} + \Lambda_\tau \right\rangle\right]$ i $\left[E_{\tau'}, \left\langle \frac{1}{N} + \Lambda_{\tau'} \right\rangle\right]$ su jednake ako i samo ako je $\Gamma_0(N)\tau = \Gamma_0(N)\tau'$. Dakle, postoji bijekcija

$$\psi_0 : S_0(N) \xrightarrow{\sim} Y_0(N), \quad \left[\mathbb{C}/\Lambda_\tau, \left\langle \frac{1}{N} + \Lambda_\tau \right\rangle \right] \mapsto \Gamma_0(N)\tau.$$

2. *Prostor parametara za $\Gamma_1(N)$ je*

$$S_1(N) = \left\{ \left[E_\tau, \frac{1}{N} + \Lambda_\tau \right] : \tau \in \mathcal{H} \right\}.$$

Dvije točke $\left[E_\tau, \frac{1}{N} + \Lambda_\tau\right]$ i $\left[E_{\tau'}, \frac{1}{N} + \Lambda_{\tau'}\right]$ su jednake ako i samo ako je $\Gamma_1(N)\tau = \Gamma_1(N)\tau'$. Dakle, postoji bijekcija

$$\psi_1 : S_1(N) \xrightarrow{\sim} Y_1(N), \quad \left[\mathbb{C}/\Lambda_\tau, \frac{1}{N} + \Lambda_\tau \right] \mapsto \Gamma_1(N)\tau.$$

3. *Prostor parametara za $\Gamma(N)$ je*

$$S(N) = \left\{ \left[\mathbb{C}/\Lambda_\tau, \left(\frac{\tau}{N} + \Lambda_\tau, \frac{1}{N} + \Lambda_\tau \right) \right] : \tau \in \mathcal{H} \right\}.$$

Dvije točke $\left[\mathbb{C}/\Lambda_\tau, \left(\frac{\tau}{N} + \Lambda_\tau, \frac{1}{N} + \Lambda_\tau\right)\right]$ i $\left[\mathbb{C}/\Lambda_{\tau'}, \left(\frac{\tau'}{N} + \Lambda_{\tau'}, \frac{1}{N} + \Lambda_{\tau'}\right)\right]$ su jednake ako i samo ako je $\Gamma(N)\tau = \Gamma(N)\tau'$. Dakle, postoji bijekcija

$$\psi : S(N) \xrightarrow{\sim} Y(N), \quad \left[\mathbb{C}/\Lambda_\tau, \left(\frac{\tau}{N} + \Lambda_\tau, \frac{1}{N} + \Lambda_\tau \right) \right] \mapsto \Gamma(N)\tau.$$

Dokaz. Pokažimo prvo *2.* Uzmimo neki element $[E, Q] \in S_1(N)$. Znamo od ranije da je $E = \mathbb{C}/\Lambda_{\tau'}$, za neki $\tau' \in \mathcal{H}$. Budući da je točka Q reda N, ona je oblika

$$Q = \frac{c\tau' + d}{N} + \Lambda_{\tau'}, \text{ za neke } c, d \in \mathbb{Z}.$$

Naime, $NQ = c\tau' + d + \Lambda_{\tau'}$, a vrijedi $c\tau' + d \in \Lambda_{\tau'}$. Budući da je red od Q točno N, vrijedi $\mathrm{nzd}(c, d, N) = 1$. Dakle, postoje $a, b, k \in \mathbb{Z}$ takvi da je $ad - bc - kN = 1$. Iz te relacije vidimo da je

$$ad - bc = 1 + kN \equiv 1 \pmod{N},$$

pa zaključujemo da se matrica $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\mathbb{Z})$ reducira modulo N u $\gamma \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$.

Mijenjamo li elemente c i d iz gornje matrice modulo N, to ne utječe na točku Q. Naime, za $r, s \in \mathbb{Z}$ vrijedi

$$\frac{(c+rN)\tau' + (d+sN)}{N} + \Lambda_{\tau'} = \frac{c\tau'+d}{N} + r\tau' + s + \Lambda_{\tau'} =$$

$$= \frac{c\tau'+d}{N} + \Lambda_{\tau'} = Q.$$

Nadalje, isto možemo učiniti i s elementima a i b, te zbog relacije $ad - bc - kN = 1$ determinanta gornje matrice ostaje jednaka 1. Dakle, budući da postoji surjekcija iz $\mathrm{SL}_2(\mathbb{Z})$ u $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, možemo uzeti da je $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.

Neka je sada $\tau = \gamma(\tau') = \dfrac{a\tau'+b}{c\tau'+d}$ i označimo $m = c\tau' + d$. Tada je $m\tau = a\tau' + b$ te vrijedi

$$m\Lambda_\tau = m(\tau\mathbb{Z} \oplus \mathbb{Z}) = m\tau\mathbb{Z} \oplus m\mathbb{Z} = (a\tau'+b)\mathbb{Z} \oplus (c\tau'+d)\mathbb{Z} = \tau'\mathbb{Z} \oplus \mathbb{Z} = \Lambda_{\tau'},$$

gdje predzadnja jednakost slijedi iz leme 2.1.2. Sada iz propozicije 2.1.4 zaključujemo da su kompleksni torusi $\mathbb{C}/\Lambda_\tau$ i $\mathbb{C}/\Lambda_{\tau'} = E$ izomorfni, s izomorfizmom $z + \Lambda_\tau \mapsto mz + \Lambda_{\tau'}$. Također, vrijedi

$$m\left(\frac{1}{N} + \Lambda_\tau\right) = \frac{c\tau'+d}{N} + \Lambda_{\tau'} = Q,$$

pa je $[E, Q] = \left[\mathbb{C}/\Lambda_\tau, \dfrac{1}{N} + \Lambda_\tau\right]$, gdje je $\tau \in \mathcal{H}$, te smo time pokazali da je

$$S_1(N) = \left\{ \left[E_\tau, \frac{1}{N} + \Lambda_\tau\right] : \tau \in \mathcal{H} \right\}.$$

Za dokaz druge tvrdnje iz *2.* pretpostavimo da je

$$\left[E_\tau, \frac{1}{N} + \Lambda_\tau\right] = \left[E_{\tau'}, \frac{1}{N} + \Lambda_{\tau'}\right],$$

za neke $\tau, \tau' \in \mathcal{H}$. Želimo pokazati da je $\Gamma_1(N)\tau = \Gamma_1(N)\tau'$. Iz pretpostavke i propozicije 2.1.4 slijedi da postoji neki $m \in \mathbb{C}$ takav da je

$$m\Lambda_\tau = \Lambda_{\tau'},$$

$$m\left(\frac{1}{N}+\Lambda_\tau\right)=\frac{1}{N}+\Lambda_{\tau'}. \tag{3.1}$$

Iz $m\Lambda_\tau=\Lambda_{\tau'}$ i leme 2.1.2 zaključujemo da je

$$\begin{bmatrix}m\tau\\ m\end{bmatrix}=\gamma\begin{bmatrix}\tau'\\ 1\end{bmatrix},\ \text{za neki } \gamma=\begin{bmatrix}a & b\\ c & d\end{bmatrix}\in \mathrm{SL}_2(\mathbb{Z}), \tag{3.2}$$

pa je onda $m=c\tau'+d$. Sada (3.1) postaje

$$\frac{c\tau'+d}{N}+\Lambda_{\tau'}=\frac{1}{N}+\Lambda_{\tau'},$$

što znači da je $(c,d)\equiv(0,1)\pmod N$. Iz tog uvjeta i činjenice da je $\gamma\in\mathrm{SL}_2(\mathbb{Z})$, tj. $ad-bc=1$, slijedi da je $a\equiv 1\pmod N$, pa je $\gamma\in\Gamma_1(N)$. Iz (3.2) imamo $m\tau=a\tau'+b$, tj. $\tau=\gamma(\tau')$.

Dokažimo sada da je $\Gamma_1(N)\tau=\Gamma_1(N)\tau'$. Neka je $\beta(\tau)$ proizvoljan element iz $\Gamma_1(N)\tau$, gdje je $\beta\in\Gamma_1(N)$. Sada je $\beta(\tau)=\beta(\gamma(\tau'))=\beta\gamma(\tau')$, gdje zadnja jednakost vrijedi jer se radi o djelovanju grupe $\Gamma_1(N)$ na skup $\mathcal{H}$, a budući da je $\beta\gamma\in\Gamma_1(N)$, vrijedi da je $\beta(\tau)\in\Gamma_1(N)\tau'$. Obratna inkluzija se dokazuje sasvim analogno uz činjenicu $\gamma^{-1}(\tau)=\tau'$.

Kako bismo dokazali obrat, pretpostavimo da za neke $\tau,\tau'\in\mathcal{H}$ vrijedi $\Gamma_1(N)\tau=\Gamma_1(N)\tau'$. Želimo pokazati da su točke $\left[E_\tau,\frac{1}{N}+\Lambda_\tau\right]$ i $\left[E_{\tau'},\frac{1}{N}+\Lambda_{\tau'}\right]$ jednake. Budući da je $\Gamma_1(N)\tau=\Gamma_1(N)\tau'$, vrijedi $\tau=\gamma(\tau')$, za neki $\gamma=\begin{bmatrix}a & b\\ c & d\end{bmatrix}\in\Gamma_1(N)$. Ako opet označimo $m=c\tau'+d$, kao ranije imamo

$$m\Lambda_\tau=\Lambda_{\tau'},$$

$$m\left(\frac{1}{N}+\Lambda_\tau\right)=\frac{c\tau'+d}{N}+\Lambda_{\tau'}.$$

Primijetimo da činjenica $\tau=\gamma(\tau'),\ \gamma\in\Gamma_1(N)$ povlači da je $(c,d)\equiv(0,1)\pmod N$. Već smo vidjeli zašto možemo modificirati c i d modulo N, pa zato imamo

$$m\left(\frac{1}{N}+\Lambda_\tau\right)=\frac{c\tau'+d}{N}+\Lambda_{\tau'}=\frac{1}{N}+\Lambda_{\tau'}.$$

Dakle,

$$\left[E_\tau,\frac{1}{N}+\Lambda_\tau\right]=\left[E_{\tau'},\frac{1}{N}+\Lambda_{\tau'}\right]$$

te postoji bijekcija

$$\psi_1 : S_1(N) \xrightarrow{\sim} Y_1(N), \quad \left[\mathbb{C}/\Lambda_\tau, \frac{1}{N} + \Lambda_\tau\right] \mapsto \Gamma_1(N)\tau.$$

Za dokaz od *1.* uzmimo neki element $[E, C] \in S_0(N)$. Znamo od ranije da je $E = \mathbb{C}/\Lambda_{\tau'}$, za neki $\tau' \in \mathcal{H}$. Budući da je po definiciji C ciklička grupa od E reda N, vrijedi da je $C = \langle Q \rangle$, gdje je Q neka točka na E reda N. Dakle, Q je oblika

$$Q = \frac{c\tau' + d}{N} + \Lambda_{\tau'}, \text{ za neke } c, d \in \mathbb{Z}.$$

Sasvim analogno kao u dokazu od *2.* zaključujemo da postoji $\tau \in \mathcal{H}$ i izomorfizam između E i $\mathbb{C}/\Lambda_\tau$ koji prevodi točku Q u točku $\frac{1}{N} + \Lambda_\tau$, pa je

$$[E, C] = \left[\mathbb{C}/\Lambda_\tau, \left\langle \frac{1}{N} + \Lambda_\tau \right\rangle\right]$$

te smo time pokazali da je

$$S_0(N) = \left\{ \left[E_\tau, \left\langle \frac{1}{N} + \Lambda_\tau \right\rangle\right] : \tau \in \mathcal{H} \right\}.$$

Za dokaz druge tvrdnje iz *1.* pretpostavimo da je

$$\left[E_\tau, \left\langle \frac{1}{N} + \Lambda_\tau \right\rangle\right] = \left[E_{\tau'}, \left\langle \frac{1}{N} + \Lambda_{\tau'} \right\rangle\right],$$

za neke $\tau, \tau' \in \mathcal{H}$. Želimo pokazati da je $\Gamma_0(N)\tau = \Gamma_0(N)\tau'$. Iz pretpostavke i propozicije 2.1.4 slijedi da postoji neki $m \in \mathbb{C}$ takav da je

$$m\Lambda_\tau = \Lambda_{\tau'},$$

$$m\left(\frac{1}{N} + \Lambda_\tau\right) = \frac{n}{N} + \Lambda_{\tau'}, \tag{3.3}$$

gdje je $n \in \mathbb{N}$ i $(n, N) = 1$, jer izomorfizam mora preslikavati generator od $\left\langle \frac{1}{N} + \Lambda_\tau \right\rangle$ u neki generator od $\left\langle \frac{1}{N} + \Lambda_{\tau'} \right\rangle$. Iz $m\Lambda_\tau = \Lambda_{\tau'}$ i leme 2.1.2 zaključujemo da je

$$\begin{bmatrix} m\tau \\ m \end{bmatrix} = \gamma \begin{bmatrix} \tau' \\ 1 \end{bmatrix}, \text{ za neki } \gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}), \tag{3.4}$$

pa je onda $m = c\tau' + d$. Sada (3.3) postaje

$$\frac{c\tau' + d}{N} + \Lambda_{\tau'} = \frac{n}{N} + \Lambda_{\tau'},$$

što znači da je $(c, d) \equiv (0, n) \pmod N$, pa slijedi da je $\gamma \in \Gamma_0(N)$. Iz (3.4) imamo $m\tau = a\tau' + b$, tj. $\tau = \gamma(\tau')$.

Dokažimo sada da je $\Gamma_0(N)\tau = \Gamma_0(N)\tau'$. Neka je $\beta(\tau)$ proizvoljan element iz $\Gamma_0(N)\tau$, gdje je $\beta \in \Gamma_0(N)$. Sada je $\beta(\tau) = \beta(\gamma(\tau')) = \beta\gamma(\tau')$, a budući da je $\beta\gamma \in \Gamma_0(N)$, vrijedi da je $\beta(\tau) \in \Gamma_0(N)\tau'$. Obratna inkluzija se dokazuje sasvim analogno uz činjenicu $\gamma^{-1}(\tau) = \tau'$.

Obratno, pretpostavimo da za neke $\tau, \tau' \in \mathcal{H}$ vrijedi $\Gamma_0(N)\tau = \Gamma_0(N)\tau'$. Želimo pokazati da su točke $\left[E_\tau, \left\langle \frac{1}{N} + \Lambda_\tau \right\rangle\right]$ i $\left[E_{\tau'}, \left\langle \frac{1}{N} + \Lambda_{\tau'} \right\rangle\right]$ jednake. Budući da je $\Gamma_0(N)\tau = \Gamma_0(N)\tau'$, vrijedi $\tau = \gamma(\tau')$, za neki $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(N)$. Ako opet označimo $m = c\tau' + d$, imamo

$$m\Lambda_\tau = \Lambda_{\tau'},$$
$$m\left(\frac{1}{N} + \Lambda_\tau\right) = \frac{c\tau' + d}{N} + \Lambda_{\tau'}.$$

Primijetimo da činjenica $\tau = \gamma(\tau')$, $\gamma \in \Gamma_0(N)$ povlači da je $c \equiv 0 \pmod N$. Zato imamo

$$m\left(\frac{1}{N} + \Lambda_\tau\right) = \frac{c\tau' + d}{N} + \Lambda_{\tau'} = \frac{d}{N} + \Lambda_{\tau'}.$$

Znamo da je $m\Lambda_\tau = \Lambda_{\tau'}$, pa je $z + \Lambda_\tau \mapsto mz + \Lambda'$ izomorfizam. Dakle, točka $\frac{1}{N} + \Lambda_\tau$ reda N se mora preslikati u točku reda N. Zaključujemo da je $\frac{d}{N} + \Lambda_{\tau'}$ reda N te je

$$\left\langle \frac{d}{N} + \Lambda_{\tau'} \right\rangle = \left\langle \frac{1}{N} + \Lambda_{\tau'} \right\rangle$$

Dakle,

$$\left[E_\tau, \left\langle \frac{1}{N} + \Lambda_\tau \right\rangle\right] = \left[E_{\tau'}, \left\langle \frac{1}{N} + \Lambda_{\tau'} \right\rangle\right]$$

te postoji bijekcija

$$\psi_0 : S_0(N) \xrightarrow{\sim} Y_0(N), \quad \left[\mathbb{C}/\Lambda_\tau, \left\langle \frac{1}{N} + \Lambda_\tau \right\rangle\right] \mapsto \Gamma_0(N)\tau.$$

Za dokaz od *3.* uzmimo neki element $[E, (P, Q)] \in S(N)$. Znamo da je $E = \mathbb{C}/\Lambda_{\tau'}$, za neki $\tau' \in \mathcal{H}$. Budući da su točke P i Q reda N, kao ranije zaključujemo da su one oblika

$$P = \frac{c_1\tau' + d_1}{N} + \Lambda_{\tau'}, \text{ za neke } c_1, d_1 \in \mathbb{Z},$$

$$Q = \frac{c_2\tau' + d_2}{N} + \Lambda_{\tau'}, \text{ za neke } c_2, d_2 \in \mathbb{Z}.$$

Definirajmo sada

$$\tau = \frac{c_1\tau' + d_1}{c_2\tau' + d_2}$$

te

$$m = c_2\tau' + d_2.$$

Pokazat ćemo da je

$$[E, (P, Q)] = \left[\mathbb{C}/\Lambda_\tau, \left(\frac{\tau}{N} + \Lambda_\tau, \frac{1}{N} + \Lambda_\tau\right)\right].$$

Prvo primijetimo da je $m\Lambda_\tau = \Lambda_{\tau'}$. Naime,

$$m\Lambda_\tau = m(\tau\mathbb{Z} \oplus \mathbb{Z}) = m\tau\mathbb{Z} \oplus m\mathbb{Z} = (c_1\tau' + d_1)\mathbb{Z} \oplus (c_2\tau' + d_2)\mathbb{Z}.$$

Prema lemi 2.1.2 to će biti jednako $\Lambda_{\tau'}$ ako i samo ako je $\begin{bmatrix} c_1 & d_1 \\ c_1 & d_2 \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. No, iz definicije od $S(N)$ znamo da je $e_N(P, Q) = e^{\frac{2\pi i}{N}}$, što iz definicije Weilovog sparivanja znači da je $\det\gamma = 1$, gdje je $\gamma \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ takva da vrijedi

$$\begin{bmatrix} P \\ Q \end{bmatrix} = \gamma \begin{bmatrix} \frac{\tau'}{N} + \Lambda_{\tau'} \\ \frac{1}{N} + \Lambda_{\tau'} \end{bmatrix}.$$

Sada je iz definicije od P i Q jasno da je $\gamma = \begin{bmatrix} c_1 & d_1 \\ c_1 & d_2 \end{bmatrix}$ pa zaključujemo da je $m\Lambda_\tau = \Lambda_{\tau'}$.

Nadalje, vrijedi

$$m\left(\frac{\tau}{N} + \Lambda_\tau\right) = \frac{c_1\tau' + d_1}{N} + \Lambda_{\tau'} = P,$$
$$m\left(\frac{1}{N} + \Lambda_\tau\right) = \frac{c_2\tau' + d_2}{N} + \Lambda_{\tau'} = Q,$$

pa je prva tvrdnja dokazana.

Za dokaz druge tvrdnje iz *3.* pretpostavimo da je

$$\left[\mathbb{C}/\Lambda_\tau, \left(\frac{\tau}{N} + \Lambda_\tau, \frac{1}{N} + \Lambda_\tau\right)\right] = \left[\mathbb{C}/\Lambda_{\tau'}, \left(\frac{\tau'}{N} + \Lambda_{\tau'}, \frac{1}{N} + \Lambda_{\tau'}\right)\right]$$

za neke $\tau, \tau' \in \mathcal{H}$. Želimo pokazati da je $\Gamma(N)\tau = \Gamma(N)\tau'$. Iz pretpostavke i propozicije 2.1.4 slijedi da postoji neki $m \in \mathbb{C}$ takav da je

$$m\Lambda_\tau = \Lambda_{\tau'},$$

$$m\left(\frac{\tau}{N}+\Lambda_\tau\right)=\frac{\tau'}{N}+\Lambda_{\tau'}, \tag{3.5}$$

$$m\left(\frac{1}{N}+\Lambda_\tau\right)=\frac{1}{N}+\Lambda_{\tau'}. \tag{3.6}$$

Iz $m\Lambda_\tau=\Lambda_{\tau'}$ i leme 2.1.2 zaključujemo da je

$$\begin{bmatrix} m\tau \\ m \end{bmatrix}=\gamma\begin{bmatrix} \tau' \\ 1 \end{bmatrix},\ \text{za neki } \gamma=\begin{bmatrix} a & b \\ c & d \end{bmatrix}\in \mathrm{SL}_2(\mathbb{Z}), \tag{3.7}$$

pa je onda $m=c\tau'+d$. Sada (3.5) i (3.6) postaju

$$\frac{m\tau}{N}+\Lambda_{\tau'}=\frac{a\tau'+b}{N}+\Lambda_{\tau'}=\frac{\tau'}{N}+\Lambda_{\tau'},$$

$$\frac{c\tau'+d}{N}+\Lambda_{\tau'}=\frac{1}{N}+\Lambda_{\tau'},$$

što znači da je $(a,b)\equiv(1,0)\pmod N$ i $(c,d)\equiv(0,1)\pmod N$. Dakle, $\gamma\in\Gamma(N)$. Iz (3.7) imamo $m\tau=a\tau'+b$, tj. $\tau=\gamma(\tau')$.

Dokažimo sada da je $\Gamma(N)\tau=\Gamma(N)\tau'$. Neka je $\beta(\tau)$ proizvoljan element iz $\Gamma(N)\tau$, gdje je $\beta\in\Gamma(N)$. Sada je $\beta(\tau)=\beta(\gamma(\tau'))=\beta\gamma(\tau')$, a budući da je $\beta\gamma\in\Gamma(N)$, vrijedi da je $\beta(\tau)\in\Gamma(N)\tau'$. Obratna inkluzija se dokazuje sasvim analogno uz činjenicu $\gamma^{-1}(\tau)=\tau'$.

Obratno, pretpostavimo da za neke $\tau,\tau'\in\mathcal{H}$ vrijedi $\Gamma(N)\tau=\Gamma(N)\tau'$. Želimo pokazati da su točke $\left[\mathbb{C}/\Lambda_\tau,\left(\frac{\tau}{N}+\Lambda_\tau,\frac{1}{N}+\Lambda_\tau\right)\right]$ i $\left[\mathbb{C}/\Lambda_{\tau'},\left(\frac{\tau'}{N}+\Lambda_{\tau'},\frac{1}{N}+\Lambda_{\tau'}\right)\right]$ jednake. Budući da je $\Gamma(N)\tau=\Gamma(N)\tau'$, vrijedi $\tau=\gamma(\tau')$, za neki $\gamma=\begin{bmatrix} a & b \\ c & d \end{bmatrix}\in\Gamma(N)$. Ako opet označimo $m=c\tau'+d$, kao ranije imamo

$$m\Lambda_\tau=\Lambda_{\tau'},$$

$$m\left(\frac{\tau}{N}+\Lambda_\tau\right)=\frac{(c\tau'+d)\tau}{N}+\Lambda_{\tau'}=\frac{a\tau'+b}{N}+\Lambda_{\tau'},$$

$$m\left(\frac{1}{N}+\Lambda_\tau\right)=\frac{c\tau'+d}{N}+\Lambda_{\tau'}.$$

Primijetimo da činjenica $\tau=\gamma(\tau'),\ \gamma\in\Gamma(N)$ povlači da je $(a,b)\equiv(1,0)\pmod N$ i $(c,d)\equiv(0,1)\pmod N$. Zato imamo

$$m\left(\frac{\tau}{N}+\Lambda_\tau\right)=\frac{a\tau'+b}{N}+\Lambda_{\tau'}=\frac{\tau'}{N}+\Lambda_{\tau'},$$

$$m\left(\frac{1}{N}+\Lambda_\tau\right)=\frac{c\tau'+d}{N}+\Lambda_{\tau'}=\frac{1}{N}+\Lambda_{\tau'}.$$

Dakle,

$$\left[\mathbb{C}/\Lambda_\tau,\left(\frac{\tau}{N}+\Lambda_\tau,\frac{1}{N}+\Lambda_\tau\right)\right]=\left[\mathbb{C}/\Lambda_{\tau'},\left(\frac{\tau'}{N}+\Lambda_{\tau'},\frac{1}{N}+\Lambda_{\tau'}\right)\right]$$

te postoji bijekcija

$$\psi : S(N)\xrightarrow{\sim} Y(N),\quad \left[\mathbb{C}/\Lambda_\tau,\left(\frac{\tau}{N}+\Lambda_\tau,\frac{1}{N}+\Lambda_\tau\right)\right]\mapsto \Gamma(N)\tau.$$

□

Uzmemo li $N = 1$, tvrdnja prethodnog teorema kaže da klase izomorfizama eliptičkih krivulja parametriziraju modularnu krivulju

$$Y_0(1)=Y_1(1)=Y(1)=\mathrm{SL}_2(\mathbb{Z})\backslash\,\mathcal{H},$$

odnosno, svaka eliptička krivulja do na izomorfizam određuje točku $\tau\in\mathcal{H}$ do na djelovanje od $\mathrm{SL}_2(\mathbb{Z})$. To je zapravo tvrdnja koju smo pokazali ranije, na kraju poglavlja 2.1.

Poglavlje 4

Teorem o modularnosti

Cilj ovog poglavlja je dati dva različita iskaza teorema o modularnosti. Prvo ćemo definirati dobru, odnosno lošu redukciju eliptičke krivulje te $L-$funkciju pridruženu eliptičkoj krivulji. Pomoću tih definicija ćemo dati prvi iskaz teorema o modularnosti. Zatim ćemo iskoristiti rezultate te terminologiju iz prva 3 poglavlja ovoga rada kako bismo dali i drugi iskaz teorema. Neke činjenice ćemo navoditi bez dokaza te s manje preciznosti nego što smo to činili do sada.

Neka je E eliptička krivulja u smislu napomene 2.2.2, dakle

$$y^2 = 4x^3 - a_2x - a_3, \;\; a_2, a_3 \in \mathbb{Z}, \;\; a_2^3 - 27a_3^2 \neq 0.$$

Lako se vidi da se ona može zapisati u obliku

$$y^2 = x^3 + ax + b, \;\; a, b \in \mathbb{Z}.$$

Označimo

$$\Delta_0(E) = -16(4a^3 + 27b^2).$$

Broj $\Delta_0(E)$ se naziva diskriminanta pridružena eliptičkoj krivulji E.

Sjetimo se modularne forme Δ iz primjera 1.0.5. U dokazu propozicije 2.2.5 smo zaključili da je Δ zapravo diskriminanta pridružena eliptičkoj krivulji do na množenje konstantom, što i opravdava naziv modularne forme Δ.

Definicija 4.0.3. *Neka je E eliptička krivulja dana s $y^2 = x^3 + ax + b, \;\; a, b \in \mathbb{Z}$. Kažemo da je E minimalni model ako je $|\Delta_0(E)| = \min\{|\Delta_0(E')| : E' \text{ je izomorfna s } E\}$.*

Može se pokazati da za svaku klasu izomorfizama eliptičkih krivulja postoji minimalan model.

Neka je sada eliptička krivulja zadana minimalnim modelom

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

gdje je $f(x) = x^3 + ax + b$.

Ako $p \nmid \Delta_0(E)$, može se pokazati da je redukcijom modulo p definirana eliptička krivulja nad poljem $\mathbb{F}_p$, te kažemo da E ima dobru redukciju modulo p. U protivnom, kažemo da E ima lošu redukciju modulo p.

Kod prostih brojeva s lošom redukcijom, kubni polinom f ima višestruki korijen modulo p. Ako polinom ima trostruki korijen, kažemo da E ima aditivnu redukciju, a ako polinom ima dvostruki korijen, onda kažemo da E ima multiplikativnu redukciju.

Nadalje, razlikujemo rascjepivu i nerascjepivu multiplikativnu redukciju. Multiplikativna redukcija je rascjepiva ako su koeficijenti smjera tangenata u singularnoj točki iz $\mathbb{F}_p$, a nerascjepiva inače.

Iz činjenice da diskriminanta eliptičke krivulje ima samo konačno mnogo prostih faktora, zaključujemo da svaka eliptička krivulja ima lošu redukciju u samo konačno mnogo prostih brojeva p.

Spomenimo i još jedan bitan rezultat kojeg ćemo trebati u sljedećoj definiciji, a koji nam govori kako je gornja ograda na broj točaka na eliptičkoj krivulji definiranoj nad konačnim poljem konačna.

Teorem 4.0.4. *Neka je E eliptička krivulja definirana nad konačnim poljem $\mathbb{F}_p$. Tada je*

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

To nas dovodi do sljedeće definicije $L-$funkcije pridružene eliptičkoj krivulji, koja će biti ključna za jedan od iskaza teorema o modularnosti.

Definicija 4.0.5. *Neka je E eliptička krivulja u minimalnom modelu i neka je $\Delta_0(E)$ diskriminanta pridružena E. Definiramo a_p na sljedeći način:*

$$a_p = \begin{cases} p+1-|E(\mathbb{F}_p)|, & \text{ako } p \nmid \Delta_0(E) \\ 1, & \text{ako } E \text{ ima rascjepivu multiplikativnu redukciju u } p \\ -1, & \text{ako } E \text{ ima nerascjepivu multiplikativnu redukciju u } p \\ 0, & \text{ako } E \text{ ima aditivnu redukciju u } p. \end{cases}$$

$L-$funkcija eliptičke krivulje je dana sa

$$L_E(s) = \prod_{p \nmid \Delta_0(E)} \frac{1}{1 - a_p \cdot p^{-s} + p^{1-2s}} \cdot \prod_{p \mid \Delta_0(E)} \frac{1}{1 - a_p \cdot p^{-s}}.$$

Gore definirana $L-$funkcija može se zapisati i u obliku

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

Teorem 4.0.6 (**Teorem o modularnosti**). *Neka je E eliptička krivulja definirana nad $\mathbb{Q}$. Tada su koeficijenti a_n iz*

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

jednaki koeficijentima u Fourierovom razvoju neke modularne forme f, tj. vrijedi

$$f = \sum_{n=1}^{\infty} a_n q^n.$$

Prije iskaza još jedne verzije teorema o modularnosti, sjetimo se da smo na samom kraju poglavlja 2.2 pokazali da je za svaku eliptičku krivulju E do na izomorfizam jedinstveno određena vrijednost $j-$invarijante. Tu vrijednost možemo označiti sa $j(E)$.

Još spomenimo da skupovi $Y_0(N)$, $Y_1(N)$ i $Y(N)$ definirani u poglavlju 3 nisu kompaktni. Da bismo ih kompaktificirali, definiramo

$$X(\Gamma) = \Gamma \backslash \mathcal{H}^*,$$

gdje je Γ neka kongruencijska grupa, a $\mathcal{H}^* = \mathcal{H} \cup \{\infty\} \cup \mathbb{Q}$. Dakle, $X(\Gamma)$ je jednak uniji od $Y(\Gamma)$ te konačnog skupa orbita elemenata od $\mathbb{Q} \cup \{\infty\}$ koji se zovu kuspovi.

Označimo

$$X(N) = \Gamma(N) \setminus \mathcal{H}^*,$$
$$X_0(N) = \Gamma_0(N) \setminus \mathcal{H}^*,$$
$$X_1(N) = \Gamma_1(N) \setminus \mathcal{H}^*.$$

Može se pokazati da $X(N), X_0(N)$ i $X_1(N)$ imaju strukturu kompaktne Riemannove plohe. Više o ovome možemo naći u [2, Poglavlje 2].

Teorem 4.0.7 (**Teorem o modularnosti**). *Neka je E kompleksna eliptička krivulja takva da je $j(E) \in \mathbb{Q}$. Tada za neki $N \in \mathbb{N}$ postoji surjektivna holomorfna funkcija kompaktnih Riemannovih ploha s modularne krivulje $X_0(N)$ na eliptičku krivulju E, tj. $X_0(N) \to E$.*

Gornja verzija teorema o modularnosti nam govori da su eliptičke krivulje s racionalnim vrijednostima $j-$invarijante "slike" modularnih krivulja.

Postoje i jače verzije teorema o modularnosti, u kojima modularnu krivulju $X_0(N)$ zamjenjuju neki drugi objekti, kao što su npr. njezin Jacobijan, a polje racionalnih brojeva zamjenjuje $\mathbb{C}$. Mnoge od tih verzija možemo naći u [2].

Bibliografija

[1] K. Conrad, $SL_2(\mathbb{Z})$, dostupno na http://www.math.uconn.edu/ kconrad/blurbs/grouptheory/SL(2,Z).pdf (ožujak 2017.).

[2] F. Diamond, J. Shurman, *A First Course in Modular Forms*, Springer-Verlag New York, 2005.

[3] S. Lang, *Complex Analysis*, Springer; 4th edition, 2003.

[4] R. Miranda, *Algebraic Curves and Riemann Surfaces*, American Mathematical Society, 1995.

[5] R. A. Rankin, *Modular Forms and Functions*, Cambridge University Press, 2010.

[6] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Iwanami Shoten and Princeton University Press, 1973.

[7] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag New York, 2009.

[8] J. Singerman, *Complex Functions: An Algebraic and Geometric Viewpoint*, Cambridge University Press; 1 edition, 1987.

[9] A. Trbović, *Torzijske grupe eliptičkih krivulja nad kvadratnim poljima*, rad za Rektorovu nagradu, dostupno na http://www.unizg.hr/rektorova/upload_2016/elipticke_krivulje.pdf (svibanj 2017.).

Sažetak

Centralni objekti koje proučavamo u ovom radu su modularne krivulje. Modularnu krivulju definiramo kao kvocijent gornje poluravnine s obzirom na djelovanje neke kongruencijske grupe, odnosno podgrupe modularne grupe $\mathrm{SL}_2(\mathbb{Z})$. U teoriji brojeva važnu ulogu igra činjenica da su modularne krivulje također prostori parametara, tj. svaka točka na modularnoj krivulji parametrizira eliptičku krivulju s nekim dodatnim svojstvom. Objasniti ovu činjenicu bio je glavni cilj ovoga rada, a to smo učinili u teoremu 3.2.2.

Kako bismo došli do definicije modularne krivulje, prvo smo definirali modularne forme, slabo modularne funkcije koje zadovoljavaju neke uvjete holomorfnosti, koje i same mogu biti zanimljiv predmet proučavanja, te smo naveli neke osnovne primjere kao što su Eisensteinovi redovi i diskriminanta, koji su se pojavljivali kroz cijeli rad. Zatim smo definirali kompleksne toruse i eliptičke krivulje te pokazali na koji način možemo uspostaviti bijekciju između ta dva objekta. Pokazali smo i da postoji korespondencija između kompleksnih torusa i eliptičkih krivulja do na izomorfizam. Nadalje, definirali smo kongruencijske podgrupe od $\mathrm{SL}_2(\mathbb{Z})$, a s time smo došli i do definicije modularne krivulje, skupa svih orbita pri djelovanju neke kongruencijske podgrupe na gornju poluravninu. Zatim smo u glavnom teoremu ovoga rada pokazali da postoji bijekcija između nekih modularnih krivulja i skupa eliptičkih krivulja sa određenim torzijskim svojstvom. Naposlijetku smo definirali dobru i lošu redukciju eliptičke krivulje te $L-$funkciju pridruženu eliptičkoj krivulji. Naveli smo i dvije različite verzije iskaza Teorema o modularnosti.

Summary

The central objects of this thesis are modular curves. We define a modular curve as the quotient of the complex upper half plane with respect to a congruence subgroup, i.e. a subgroup of the modular group $\mathrm{SL}_2(\mathbb{Z})$. In number theory, the fact that modular curves are also moduli spaces, i.e. every point on a modular curve parameterizes an elliptic curve with the associated torsion data, is very important. The main goal of this thesis was to prove this fact, which we did in the theorem 3.2.2.

Before the definition of a modular curve, we first defined modular forms, weakly modular functions that satisfy some holomorphy conditions, that are also interesting subjects of study in themselves, and we gave some basic examples, as Eisenstein series and the discriminant function, which we encounter throughout the entire thesis. Furthermore, we defined complex tori and elliptic curves and showed that there exists a bijection between these two objects. Also, we proved that there exists a correspondence between complex tori and elliptic curves up to isomorphism. After the definition of a congruence subgroup od $\mathrm{SL}_2(\mathbb{Z})$ we defined a modular curve, a set of all orbits under the action of some congruence subgroup on the complex upper half plane. In the main theorem of this thesis we proved that there exists a bijection between modular curves and the set of elliptic curves with the associated torsion data. In the end, we defined good and bad reductions of elliptic curves and the $L-$function associated to an elliptic curve. We also state two different versions of The Modularity Theorem.

Životopis

Antonela Trbović rođena je 20. listopada 1993. godine u Rijeci, gdje polazi osnovnu školu Srdoči te Gimnaziju Andrije Mohorovičića. Na Matematičkom odsjeku Prirodoslovno-matematičkog fakulteta Sveučilišta u Zagrebu 2012. godine upisuje Preddiplomski sveučilišni studij matematike te 2015. godine Diplomski sveučilišni studij Teorijska matematika.

Akademske godine 2014./2015. drži demonstrature iz kolegija Diferencijalni račun funkcija više varijabli, a 2015./2016. iz kolegija Teorija skupova.

Akademske godine 2014./2015. te 2016./2017. dobiva nagradu Matematičkog odsjeka Prirodoslovno-matematičkog fakulteta za najbolje studente završnih godina studija, a godine 2015./2016. dobiva Rektorovu nagradu Sveučilišta u Zagrebu za individualni znanstveni rad Torzijske grupe eliptičkih krivulja nad kvadratnim poljima.

U srpnju 2016. godine u Sarajevu polazi dvotjednu ljetnu školu te konferenciju Building Bridges: Automorphic Forms and Related Topics.