Teorem o modularnosti

Novak, Ivan

Sveučilište u Zagrebu
Prirodoslovno-matematički fakultet
Matematički odsjek

Ivan Novak

Teorem o modularnosti

Diplomski rad

Voditelj rada:
prof. dr. sc. Filip Najman

Zagreb, srpanj 2023.

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

Tema ovog rada je teorem o modularnosti. Taj teorem govori da je svakoj eliptičkoj krivulji definiranoj nad $\mathbb{Q}$ pridružena modularna forma iz određenog prostora.

Eliptičke krivulje su glatke projektivne algebarske krivulje genusa 1 zajedno s istaknutom točkom. Na skupu racionalnih točaka eliptičke krivulje možemo definirati zbrajanje, te je time dana struktura komutativne grupe. Mordell-Weilov teorem kaže da je ta grupa konačno generirana. Teorija eliptičkih krivulja je bogata i razgranata, te postoji puno zanimljivih otvorenih pitanja o strukturi grupe racionalnih točaka.

Modularne forme su holomorfne funkcije na gornjoj poluravnini koje zadovoljavaju određeno svojstvo simetrije pod djelovanjem modularne grupe $\mathrm{SL}_2(\mathbb{Z})$ ili njenih podgrupa.

Poseban slučaj teorema o modularnosti za semistabilne eliptičke krivulje dokazao je Andrew Wiles 1995. To je bio značajan rezultat jer je pomoću njega dovršen dokaz velikog Fermatovog teorema, koji kaže da jednadžba $x^n + y^n = z^n$ nema netrivijalnih cjelobrojnih rješenja za $n \geq 3$. Teorem o modularnosti je u potpunosti dokazan 2001. od strane Breuila, Conrada, Diamonda i Taylora.

U prvom poglavlju definiramo modularne forme za kongruencijske podgrupe od $\mathrm{SL}_2(\mathbb{Z})$ i promatramo neka njihova osnovna svojstva. Definiramo i Eisensteinove redove, koji su najjednostavniji primjeri modularnih formi.

U drugom poglavlju definiramo eliptičke krivulje nad poljem $\mathbb{C}$ kao kompleksne toruse, odnosno kvocijente $\mathbb{C}/L$, gdje je L rešetka. Nakon toga definiramo modularne krivulje kao Riemannove plohe. Modularne krivulje su važne jer parametriziraju određene klase eliptičkih krivulja zajedno s još nekim podacima o njihovoj torziji.

U trećem poglavlju citiramo rezultate iz teorije kompaktnih Riemannovih ploha iz kojih slijede formule za dimenzije prostora modularnih formi za neku kongruencijsku podgrupu. Ti prostori su konačnodimenzionalni. Posebno, za cijelu modularnu grupu $\mathrm{SL}_2(\mathbb{Z})$, svaka modularna forma težine k je homogeni polinom stupnja k u Eisensteinovim redovima E_4 i E_6.

U četvrtom poglavlju definiramo Heckeove operatore. Heckeovi operatori su familija operatora na prostoru modularnih formi za grupe $\Gamma_1(N)$, koji međusobno komutiraju i koji čuvaju cusp forme. Nadalje, uz Peterssonov skalarni produkt, ti operatori su normalni. Zbog toga prostor cusp formi $\mathcal{S}_k(\Gamma_1(N))$ posjeduje bazu koja se sastoji od modularnih formi koje su svojstveni vektori za sve Heckeove operatore.

Nakon toga uvodimo L-funkcije pridružene modularnim formama te L-funkcije pridružene eliptičkim krivuljama, te iskazujemo verziju teorema o

modularnosti koja kaže da svakoj eliptičkoj krivulji nad $\mathbb{Q}$ s konduktorom N možemo pridružiti modularnu formu s određenim svojstvima za grupu $\Gamma_0(N)$ tako da se pripadne L-funkcije poklapaju. Jedna od posljedica teorema o modularnosti je da se L-funkcije eliptičkih krivulja mogu analitički proširiti na cijeli $\mathbb{C}$. Zbog toga onda ima smisla promatrati red poništavanja njihovih L-funkcija u točki 1. Slavna slutnja Bircha i Swinnerton-Dyera kaže da je rang grupe racionalnih točaka eliptičke krivulje jednak redu poništavanja njene L-funkcije u točki 1, pa zbog teorema o modularnosti ova slutnja ima smisla.

U petom poglavlju pokazujemo kako se modularnost eliptičkih krivulja može primijeniti na diofantske jednadžbe. Posebno, dajemo skicu dokaza velikog Fermatovog teorema, u kojem je teorem o modularnosti ključan i povijesno najteži korak.

1 Modularne forme

1.1 Djelovanje modularne grupe na gornju poluravninu

Definicija 1.1. *Modularna grupa* $\mathrm{SL}_2(\mathbb{Z})$ je grupa svih 2×2 matrica s cjelobrojnim koeficijentima i determinantom 1.

Definicija 1.2. Gornja poluravnina $\mathcal{H}$ je skup svih kompleksnih brojeva s pozitivnim imaginarnim dijelom,

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

Modularna grupa djeluje na $\mathcal{H}$ linearnim razlomljenim transformacijama. Za $\gamma = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbb{Z})$ i $h \in \mathcal{H}$, definiramo

$$\gamma(z) := \frac{az + b}{cz + d}.$$

Lako se vidi da je to djelovanje grupe, odnosno da je $(\gamma\delta)(\tau) = \gamma(\delta(\tau))$ za sve $\gamma, \delta \in \mathrm{SL}_2(\mathbb{Z})$, te $I(\tau) = \tau$. Nadalje, uz iste oznake, direktnim raspisom se dokazuje da vrijedi

$$\mathrm{Im}(\gamma(\tau)) = \mathrm{Im}(\tau)|c\tau + d|^{-2}, \tag{1}$$

pa je $\mathrm{Im}(\gamma(\tau)) > 0$ čim je $\mathrm{Im}(\tau) > 0$.

Neka je $S := \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]$, $T := \left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$.

Propozicija 1.3. *Matrice S i T generiraju* $\mathrm{SL}_2(\mathbb{Z})$.

Dokaz. Neka je $\alpha = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ bilo koja matrica iz $\mathrm{SL}_2(\mathbb{Z})$. Dovoljno je dokazati da postoji matrica $\gamma \in \langle S, T\rangle$ takva da je $\alpha\gamma = I$.

Direktnim računom može se provjeriti da za svaki $n \in \mathbb{Z}$ vrijedi

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n = \begin{bmatrix} a & an + b \\ c & cn + d \end{bmatrix},$$

pa prikladnim izborom n možemo doći do neke matrice $\alpha\gamma$ s donjim redom (c, d'), gdje je $|d'| \leq |c/2|$ ili $c = 0$. Množenje zdesna matricom S prebacuje donji red (c, d) u $(d, -c)$. Ponavljanjem množenja s T^n za prikladni n i potom množenja s S, vidimo da se donji lijevi element matrice strogo smanjuje, osim ako je već bio jednak 0. U svakom slučaju, nakon primjene dovoljno koraka ovog algoritma, dobivamo da postoji matrica $\delta \in \langle S, T\rangle$ takva da je donji redak od $\alpha\delta$ jednak $(0, u)$ za neki u.

Međutim, zbog uvjeta da je determinanta jednaka 1, slijedi da je $u \in \{1, -1\}$. Ako je potrebno, množenjem s $S^2 = -I$ možemo postići da je $u = 1$.

Sada smo došli do matrice oblika $\left[\begin{smallmatrix} 1 & m \\ 0 & 1 \end{smallmatrix}\right]$ za neki $m \in \mathbb{Z}$. Množenjem zdesna s T^{-m} dobivamo matricu I, pa je tvrdnja dokazana. □

Navedimo još kako generatori S i T djeluju na $\mathcal{H}$:

$$T(\tau) = \tau + 1,$$
$$S(\tau) = \frac{-1}{\tau}.$$

1.2 Kongruencijske podgrupe

Sada definiramo neke važne podgrupe modularne grupe.

Definicija 1.4. Neka je N prirodan broj. *Glavna kongruencijska podgrupa razine N* je

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

Napomena 1.5. Kako je $\Gamma(N)$ zapravo jezgra homomorfizma redukcije modulo N, $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, dobivamo da je $\Gamma(N)$ normalna u $\mathrm{SL}_2(\mathbb{Z})$, te imamo izomorfizam

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

Posebno, $\Gamma(N)$ je konačnog indeksa u $\mathrm{SL}_2(\mathbb{Z})$.

Indeks se može lagano izračunati, tako da prebrojimo matrice u $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Kao prvo, za prost broj p, imamo $|\,\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})| = (p^2-1)(p^2-p)$, jer za prvi stupac možemo uzeti bilo što osim nul-stupca, a za drugi bilo koji stupac koji nije zavisan s prvim.

Za svaki $e \geq 1$, svaku matricu iz $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ možemo na $(p^{e-1})^4$ načina podići do matrice iz $\mathrm{GL}_2(\mathbb{Z}/p^e\mathbb{Z})$, pa je $|\,\mathrm{GL}_2(\mathbb{Z}/p^e\mathbb{Z})| = p^{4e-4}(p^2-1)(p^2-p)$. Kako je $\mathrm{SL}_2(\mathbb{Z}/p^e\mathbb{Z})$ jezgra epimorfizma $\det : \mathrm{GL}_2(\mathbb{Z}/p^e\mathbb{Z}) \to (\mathbb{Z}/p^e\mathbb{Z})^\times$, onda je

$$|\,\mathrm{SL}_2(\mathbb{Z}/p^e\mathbb{Z})| = \frac{p^{4e-4}(p^2-1)(p^2-p)}{p^{e-1}(p-1)} = p^{3e}\left(1 - \frac{1}{p^2}\right).$$

Po Kineskom teoremu o ostacima sada lako zaključujemo da za prirodan broj N vrijedi

$$|\,\mathrm{SL}_2(\mathbb{Z}/\mathbb{N}\mathbb{Z})| = N^3 \prod_{p|N} \left(1 - \frac{1}{p^2}\right).$$

Definicija 1.6. Neka je N prirodan broj. Za podgrupu Γ od $\mathrm{SL}_2(\mathbb{Z})$ kažemo da je *kongruencijska podgrupa razine* N ako je $\Gamma(N) \subset \Gamma$.

Napomena 1.7. Kako za svaku kongruencijsku podgrupu Γ razine N vrijedi $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma] \leq [\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N)]$, zaključujemo da su sve kongruencijske podgrupe konačnog indeksa u $\mathrm{SL}_2(\mathbb{Z})$. Nadalje, vidimo da kongruencijska podgrupa razine N sadrži matricu $\alpha_n = \left[\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right]$ koja na $\tau \in \mathcal{H}$ djeluje kao translacija za n, odnosno $\alpha_n(\tau) = \tau + n$.

Primjer 1.8. Osim glavne kongruencijske podgrupe, dvije važne kongruencijske podgrupe su

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

te

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

gdje oznaka $*$ znači da pripadni unos može poprimiti bilo koju vrijednost. Vrijedi

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

Imamo epimorfizam $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto b$ iz $\Gamma_1(N)$ u $\mathbb{Z}/N\mathbb{Z}$ s jezgrom $\Gamma_0(N)$, pa je $\Gamma(N) \triangleleft \Gamma_1(N)$ i $[\Gamma_1(N) : \Gamma(N)] = N$.
Slično, imamo epimorfizam $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto d$ iz $\Gamma_0(N)$ u $(\mathbb{Z}/N\mathbb{Z})^\times$ s jezgrom $\Gamma_1(N)$, pa je $\Gamma_1(N) \triangleleft \Gamma_0(N)$ i $[\Gamma_0(N) : \Gamma_1(N)] = \varphi(N)$.
Posebno, za $N = 2$ vrijedi

$$[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(2)] = \frac{2^3 \left(1 - \frac{1}{2^2}\right)}{2\varphi(2)} = 3.$$

Reprezentanti za $\mathrm{SL}_2(\mathbb{Z})/\Gamma_0(2)$ su

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 \\ -1 & -1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}.$$

Napomenimo da $\Gamma_0(N)$ općenito nije normalna u $\mathrm{SL}_2(\mathbb{Z})$.

Sada definiramo djelovanje $\mathrm{SL}_2(\mathbb{Z})$ na projektivnom pravcu $\mathbb{P}^1(\mathbb{Q}) := \mathbb{Q} \cup \{\infty\}$. Za racionalan broj q i $\gamma = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbb{Z})$, definiramo

$$\gamma(q) = \begin{cases} \frac{aq+b}{cq+d}, & \text{ako je } cq + d \neq 0; \\ \infty, & \text{ako je } cq + d = 0, \end{cases}$$

te definiramo

$$\gamma(\infty) = \begin{cases} \frac{a}{c}, & \text{ako je } c \neq 0; \\ \infty, & \text{ako je } c = 0. \end{cases}$$

Ovo djelovanje zapravo simulira formalni račun s ∞. Kao i prije, lako se uvjeriti da to stvarno jest djelovanje.

Djelovanje $\mathrm{SL}_2(\mathbb{Z})$ na $\mathbb{P}^1(\mathbb{Q})$ je tranzitivno jer za svaki racionalan broj $\frac{a}{c}$ postoje $b, d \in \mathbb{Z}$ takvi da je $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbb{Z})$, pa je svaki racionalan broj u orbiti od ∞. To nije nužno slučaj za inducirano djelovanje neke podgrupe od $\mathrm{SL}_2(\mathbb{Z})$ na $\mathbb{P}^1(\mathbb{Q})$.

Definicija 1.9. Neka je Γ kongruencijska podgrupa od $\mathrm{SL}_2(\mathbb{Z})$. Promotrimo inducirano djelovanje Γ na $\mathbb{P}^1(\mathbb{Q})$. Orbitu pri tom djelovanju zovemo *cusp* od Γ.

Napomena 1.10. Kako je Γ konačnog indeksa u $\mathrm{SL}_2(\mathbb{Z})$, slijedi da je broj cuspova konačan, te manji ili jednak indeksu od Γ. Posebno, $\mathrm{SL}_2(\mathbb{Z})$ ima samo jedan cusp, jer je djelovanje na $\mathbb{P}^1(\mathbb{Q})$ tranzitivno.

1.3 Definicija modularnih formi

Prisjetimo se, kompleksna funkcija definirana na otvorenom skupu $D \subset \mathbb{C}$ je meromorfna ako je holomorfna osim na izoliranom skupu točaka, u kojima ima polove.

Definicija 1.11. Neka je k cijeli broj. Za meromorfnu funkciju $f : \mathcal{H} \to \mathbb{C}$ kažemo da je *slabo modularna težine* k ako za svaki $\tau \in \mathcal{H}$ i svaki $\gamma = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbb{Z})$ vrijedi

$$f(\gamma(\tau)) = (c\tau + d)^k f(\tau).$$

Napomena 1.12. Primijetimo da je svaka slabo modularna funkcija 1-periodična, odnosno

$$f(\tau + 1) = f(\tau).$$

To slijedi direktno uvrštavanjem matrice T umjesto γ u gornju definiciju.

Primjer 1.13. Dokažimo da je nul-funkcija jedina slabo modularna funkcija težine k za neparan k. Naime, za svaku takvu f vrijedi

$$f\left(\frac{-1}{\tau}\right) = \tau^k f(\tau).$$

Međutim, uvrštavanjem $\frac{-1}{\tau}$ umjesto τ u tu jednakost, dobivamo

$$f(\tau) = \left(\frac{-1}{\tau}\right)^k f\left(\frac{-1}{\tau}\right) = (-1)^k f(\tau) = -f(\tau),$$

odnosno $f(\tau) = 0$.

Sa D ćemo označavati jedinični disk, odnosno $D := \{z \in \mathbb{C} : |z| < 1\}$, a sa D' punktirani jedinični disk, odnosno $D' := D \setminus \{0\}$.

Iz sljedeće leme slijedi da svaka modularna forma ima Fourierov razvoj.

Lema 1.14. *Neka je $f : \mathcal{H} \to \mathbb{C}$ holomorfna 1-periodična funkcija. Tada postoji holomorfna funkcija $g : D' \to \mathbb{C}$ takva da je*

$$f(\tau) = g(e^{2\pi i\tau}), \text{ za svaki } \tau \in \mathcal{H}.$$

Dokaz. Prisjetimo se da eksponencijalno preslikavanje $\tau \mapsto e^{2\pi i\tau}$ preslikava $\mathcal{H}$ u D'.

Ideja je jasna, želimo definirati $g(q) := f\left(\frac{\log(q)}{2\pi i}\right)$ za $q \in D'$. Međutim, logaritam nije definiran na cijelom punktiranom disku, pa za svaku točku $q \in D'$ izaberemo jedan logaritam koji je definiran na njenoj okolini. Definicija ne ovisi o izboru tog logaritma jer je f 1-periodična, a dva izbora logaritma se razlikuju za višekratnik od $2\pi i$. Dakle, g je ipak dobro definirana.

Holomorfnost od g slijedi iz toga što je holomorfnost lokalno svojstvo, a svaki logaritam je holomorfan na svom području definicije. □

Uzimanjem Laurentovog razvoja pripadne g oko 0 odmah dobivamo sljedeću propoziciju.

Propozicija 1.15. *Ako je $f : \mathcal{H} \to \mathbb{C}$ holomorfna funkcija koja je 1-periodična, onda postoji niz koeficijenata $(a_n)_{n\in\mathbb{Z}}$ takav da za svaki $\tau \in \mathcal{H}$ vrijedi*

$$f(\tau) = \sum_{n\in\mathbb{Z}} a_n q^n, \text{ gdje je } q = e^{2\pi i\tau}. \tag{2}$$

Razvoj (2) *zovemo* Fourierov razvoj od f, *a koeficijente $(a_n)_{n\in\mathbb{Z}}$ zovemo* Fourierovi koeficijenti od f.

Napomena 1.16. Postojanje Fourierovog razvoja mogli smo opravdati i teorijom Fourierovih redova za funkcije realne varijable. Naime, za fiksan $y > 0$, promotrimo funkciju $f_y(x) := f(x + iy)$. Ta funkcija je neprekidna i 1-periodična, pa po teoriji Fourierovih redova ima Fourierov razvoj

$$f_y(x) = \sum_{n\in\mathbb{Z}} a_n(y)e^{2\pi inx}.$$

Nadalje, znamo i formulu za koeficijente

$$a_n(y) = \int_0^1 f(x + iy)e^{-2\pi inx}dx = e^{-2\pi ny}\int_{iy}^{1+iy} f(z)e^{-2\pi inz}dz.$$

Uzmimo sada neki drugi $y' > 0$ i promotrimo integral 1-periodične funkcije $f(z)e^{-2\pi inz}$ po kvadratu s vrhovima $yi, 1+yi, 1+y'i, y'i$ u smjeru suprotnom od kazaljke na satu. Taj integral je jednak 0 zbog holomorfnosti funkcije, a integrali po vertikalnim stranicama se pokrate zbog 1-periodičnosti, pa dobivamo relaciju

$$\int_{iy}^{1+iy} f(z)e^{-2\pi inz}dz = \int_{iy'}^{1+iy'} f(z)e^{-2\pi inz}dz,$$

iz čega direktno slijedi relacija

$$\frac{a_n(y)}{e^{-2\pi ny}} = \frac{a_n(y')}{e^{-2\pi ny'}}.$$

Iz toga odmah slijedi da je $a_n(y) = c_n \cdot e^{-2\pi iny}$ za neku konstantu c_n, pa je

$$f(x+iy) = \sum_{n\geq 0} c_n e^{2\pi in(x+iy)}.$$

Sada definiramo jedan bitan pojam koji govori o ponašanju holomorfne funkcije na $\mathcal{H}$ u beskonačnosti.

Definicija 1.17. Neka je f holomorfna 1-periodična funkcija. Kažemo da je *f holomorfna u beskonačnosti* ako u njenom Fourierovom razvoju

$$f(\tau) = \sum_{n\in\mathbb{Z}} a_n q^n,\ q = e^{2\pi i\tau}$$

vrijedi $a_n = 0$ za svaki $n < 0$.

Napomena 1.18. Neka je $g : D' \to \mathbb{C}$ funkcija takva da je $g(q) = f(\tau)$. Tada je uvjet holomorfnosti u beskonačnosti ekvivalentan uvjetu da je g holomorfna u 0, odnosno da ju je moguće dodefinirati do holomorfne funkcije na cijelom D.

Još jedan ekvivalentan uvjet, koji i objašnjava naziv pojma, je u sljedećoj propoziciji. Ova propozicija je korisna jer pokazuje da za provjeru uvjeta holomorfnosti u beskonačnosti nije potrebno razvijati funkciju u Fourierov red, već samo promotriti ponašanje $f(\tau)$ za τ koji su daleko od x-osi.

Propozicija 1.19. *Neka je f holomorfna 1-periodična funkcija. Tada je f holomorfna u beskonačnosti ako i samo ako za svaki niz $(z_n)_n \subset \mathcal{H}$ takav da $\mathrm{Im}(z_n) \to +\infty$ vrijedi da je niz $(f(z_n))_n$ ograničen.*

Napomena 1.20. Ovo možemo kraće izreći tako da kažemo da je $f(\tau)$ ograničeno kako $\mathrm{Im}\,\tau \to +\infty$.

Dokaz. Neka je $(z_n)_n$ niz u $\mathcal{H}$, te neka je $q_n = \exp(2\pi i z_n)$ pripadni niz u D'. Tada $\mathrm{Im}(z_n) \to +\infty$ ako i samo ako $q_n \to 0$.

Pretpostavimo da je g holomorfna u 0. Onda je ograničena na nekoj okolini nule, a kako svi osim konačno q_n leže u toj okolini, slijedi da je niz $(q_n)_n$ ograničen. Obratno, ako pretpostavimo da g nije holomorfna u 0, onda možemo naći niz $(q_n)_n$ koji konvergira u 0 a takav da je $(f(q_n))_n$ neograničen. □

Sada smo spremni definirati modularne forme.

Definicija 1.21. Za funkciju $f : \mathcal{H} \to \mathbb{C}$ kažemo da je *modularna forma težine* k ako zadovoljava sljedeće uvjete:

(1) f je slabo modularna težine k,

(2) f je holomorfna,

(3) f je holomorfna u beskonačnosti.

Skup svih modularnih formi težine k označavamo s $\mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z}))$. Ako vrijedi i

(4) $a_0 = 0$ u Fourierovom razvoju od f,

kažemo da je f *cusp forma*. Skup svih cusp formi težine k označavamo s $\mathcal{S}_k(\mathrm{SL}_2(\mathbb{Z}))$.

Napomena 1.22. Da bi funkcija bila modularna forma, mora zadovoljavati tri uvjeta: uvjet transformacije, uvjet holomorfnosti i uvjet rasta u beskonačnosti.

Napomena 1.23. Primijetimo da je linearna kombinacija modularnih formi težine k također modularna forma težine k, odnosno da je $\mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z}))$ vektorski prostor. Isto vrijedi i za $\mathcal{S}_k(\mathrm{SL}_2(\mathbb{Z}))$.

Slijedi da je vektorski prostor

$$\mathcal{M}(\mathrm{SL}_2(\mathbb{Z})) := \bigoplus_k \mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z})),$$

graduirana $\mathbb{C}$-algebra, jer je umnožak modularne forme težine k i modularne forme težine j modularna forma težine $k + j$.

Vratimo se uvjetu slabe modularnosti. Za matricu $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, definiramo njen faktor automorfnosti $j(\gamma, \tau) \in \mathbb{C}$ za $\tau \in \mathcal{H}$ sa

$$j(\gamma, \tau) = c\tau + d,$$

te za cijeli broj k definiramo operator težine k $[\gamma]_k$ na funkcijama $f : \mathcal{H} \to \mathbb{C}$ sa

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

Sad možemo drugačije sročiti uvjet slabe modularnosti. Meromorfna funkcija $f : \mathcal{H} \to \mathbb{C}$ je slabo modularna težine k ako je

$$f[\gamma]_k = f$$

za sve $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.

Lema 1.24. *Za sve $\gamma, \gamma' \in \mathrm{SL}_2(\mathbb{Z})$ i $\tau \in \mathcal{H}$ vrijedi*

(a) $j(\gamma\gamma', \tau) = j(\gamma, \gamma'(\tau))j(\gamma', \tau)$,

(b) $(\gamma\gamma')(\tau) = \gamma(\gamma'(\tau))$,

(c) $[\gamma\gamma']_k = [\gamma]_k[\gamma']_k$,

(d) $\mathrm{Im}(\gamma(\tau)) = \frac{\mathrm{Im}(\tau)}{|j(\gamma,\tau)|^2}$.

(e) $(\gamma(\tau))' = \frac{1}{j(\gamma,\tau)^2}$.

Sve tvrdnje se dokazuju direktnim raspisivanjem, dokaz se može naći u [1, 1.2.]. Primijetimo da tvrdnja (c) zapravo kaže da $\mathrm{SL}_2(\mathbb{Z})$ preko operatora $[\gamma]_k$ djeluje zdesna na skup svih funkcija $\mathcal{H} \to \mathbb{C}$.

Bitna posljedica tvrdnje (c) je i da je uvjet slabe modularnosti dovoljno provjeriti samo na generatorima grupe. Eksplicitnije, meromorfna funkcija f je slabo modularna težine k ako i samo ako vrijedi

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

Sada ćemo poopćiti definiciju modularne forme na općenitu kongruencijsku podgrupu Γ. Uvjet holomorfnosti ostaje isti.

Uvjet transformacije ćemo poopćiti tako što ćemo zahtijevati invarijantnost na Γ, odnosno $f[\gamma]_k = f$ za sve $\gamma \in \Gamma$.

Uvjet ponašanja u beskonačnosti je nešto kompliciraniji. Kao prvo, nije odmah jasno da imamo Fourierov razvoj. Ovdje se koristi uvjet da je Γ kongruencijska podgrupa razine N za neki prirodan broj N, pa je $\left[\begin{smallmatrix} 1 & N \\ 0 & 1 \end{smallmatrix}\right] \in \Gamma$. Ako je f Γ-invarijantna, slijedi $f(\tau+N) = f(\tau)$, pa je f N-periodična. Slijedi da za holomorfnu Γ-invarijantnu funkciju f postoji Fourierov red

$$f(\tau) = \sum_{n \geq 0} a_n q_N^n,$$

gdje je $q_N = e^{2\pi i\tau/N}$.

Sada kad imamo Fourierov razvoj, mogli bismo zahtijevati da je f holomorfna u beskonačnosti, isto kao i kod definicije modularne forme za $\mathrm{SL}_2(\mathbb{Z})$. Međutim, zahtijevat ćemo nešto jači uvjet. Želimo da f bude holomorfna u svim cuspovima. Treba nam još jedna jednostavna lema.

Lema 1.25. *Neka je* Γ *kongruencijska podgrupa od* $\mathrm{SL}_2(\mathbb{Z})$ *i* $\alpha \in \mathrm{SL}_2(\mathbb{Z})$. *Tada je i* $\alpha^{-1}\Gamma\alpha$ *kongruencijska podgrupa od* $\mathrm{SL}_2(\mathbb{Z})$.

Dokaz. Vrijedi $\Gamma(N) \leq \Gamma$, pa je $\alpha^{-1}\Gamma(N)\alpha \leq \alpha^{-1}\Gamma\alpha$, ali $\Gamma(N)$ je normalna pa je $\Gamma(N) \leq \alpha^{-1}\Gamma\alpha$. □

Definicija 1.26. Neka je Γ kongruencijska podgrupa od $\mathrm{SL}_2(\mathbb{Z})$, i neka je k cijeli broj. Funkcija $f : \mathcal{H} \to \mathbb{C}$ je *modularna forma težine* k *za* Γ ako zadovoljava sljedeće uvjete:

(1) $f[\gamma]_k = f$ za sve $\gamma \in \Gamma$,

(2) f je holomorfna,

(3) $f[\alpha]_k$ je holomorfna u beskonačnosti za sve $\alpha \in \mathrm{SL}_2(\mathbb{Z})$.

Skup svih modularnih forma težine k za Γ označavamo s $\mathcal{M}_k(\Gamma)$.

Napomena 1.27. Kao i ranije, uvjet (1) je dovoljno provjeriti na generatorima od Γ.

Uvjet (3) zovemo holomorfnost u cuspovima. Taj uvjet ima smisla jer za svaki $\alpha \in \mathrm{SL}_2(\mathbb{Z})$ vrijedi da je $f[\alpha]_k$ invarijantna za $\alpha^{-1}\Gamma\alpha$ kad god je f Γ-invarijantna, pa je i $f[\alpha]_k$ periodična zbog leme 1.25.

Uvjet (3) je zapravo dovoljno provjeriti samo za reprezentante od $\Gamma\backslash \mathrm{SL}_2(\mathbb{Z})$, odnosno za konačno mnogo matrica.

Sljedeća propozicija daje praktično koristan uvjet jači od uvjeta (3).

Propozicija 1.28. *Neka je* Γ *kongruencijska podgrupa od* $\mathrm{SL}_2(\mathbb{Z})$ *razine* N, *i neka je* $q_N = e^{2\pi i\tau/N}$ *za* $\tau \in \mathcal{H}$. *Pretpostavimo da* $f : \mathcal{H} \to \mathbb{C}$ *zadovoljava uvjete* (1) *i* (2) *iz definicije* 1.26 *te vrijedi:*

(3') f *je holomorfna u beskonačnosti, i postoje konstante* $C, r \geq 0$ *takve da u njenom Fourierovom razvoju* $f(\tau) = \sum_{n\geq 0} a_n q_N^n$ *koeficijenti* $(a_n)_{n>0}$ *zadovoljavaju*

$$|a_n| \leq Cn^r.$$

Tada f *zadovoljava i uvjet* (3) *iz definicije* 1.26.

Skica dokaza. Prvo primijetimo da za $\tau = x + iy$ vrijedi ocjena

$$|f(\tau)| \leq |a_0| + C \sum_{n=1}^{\infty} n^r e^{-2\pi n y/N}.$$

Ocjenjivanjem sume integralom, za funkciju $g(t) := t^r e^{-2\pi t y/N}$, dobivamo

$$|f(\tau)| \leq C_0 + C \left(\int_0^{+\infty} g(t)dt + 1/y^r \right),$$

gdje su C_0 i C neke pozitivne konstante. Integral funkcije g konvergira i ne ovisi o y pa dobivamo ogradu

$$|f(\tau)| \leq C_0 + C/y^r$$

za neke konstante C_0, C (koje nisu nužno iste kao konstante otprije).

Neka je sada $\alpha \in \mathrm{SL}_2(\mathbb{Z})$. Promotrimo funkciju $f[\alpha]_k$. Ona ima razvoj u Fourierov red

$$(f[\alpha]_k)(\tau) = \sum_{n \in \mathbb{Z}} a'_n q_N^n.$$

Treba dokazati da su koeficijenti a'_n za $n < 0$ jednaki 0. To je ekvivalentno s time da je

$$\lim_{q_N \to 0} (f[\alpha]_k)(\tau) \cdot q_N = 0.$$

Ako je $\alpha = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, onda je lijeva strana jednaka

$$f\left(\frac{a\tau + b}{c\tau + d}\right) (c\tau + d)^{-k} q_N,$$

što je po dokazanoj ogradi omeđeno odozgo s

$$(C_0 + C/\operatorname{Im}(\alpha(\tau))^r)(c\tau + d)^{-k} q_N,$$

što teži u 0 kako $q_N \to 0$ jer desni faktor eksponencijalno opada, a lijevi raste najviše polinomijalno. Ovdje se koristi tvrdnja da je $\operatorname{Im}(\alpha(\tau)) = \frac{\operatorname{Im}(\tau)}{|j(\alpha,\tau)|^2}$. □

Sada definiramo cusp forme za kongruencijske podgrupe.

Definicija 1.29. Neka je Γ kongruencijska podgrupa od $\mathrm{SL}_2(\mathbb{Z})$ razine N. Za $f \in \mathcal{M}_k(\Gamma)$ kažemo da je *cusp forma* ako za svaki $\alpha \in \mathrm{SL}_2(\mathbb{Z})$ funkcija $f[\alpha]_k$ ima nultočku u beskonačnosti, odnosno ako joj je koeficijent a_0 u Fourierovom razvoju

$$a_0 + a_1 q_N + a_2 q_N^2 + \ldots$$

jednak 0.

Napomena 1.30. Ono što ovim uvjetom želimo osigurati je da je f "ima nultočku" u svim cuspovima, a ne samo u cuspu ∞.

1.4 Bitni primjeri modularnih formi

Sada smo spremni dati primjere modularnih formi.

Definicija 1.31. Neka je $k > 2$ paran prirodan broj. Definiramo *Eisensteinov red težine* k kao funkciju $G_k : \mathcal{H} \to \mathbb{C}$ definiranu s

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

gdje je suma po svim parovima $(c, d) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$.

Napomena 1.32. Može se dokazati da ovaj red konvergira apsolutno i uniformno na kompaktnim podskupovima od $\mathcal{H}$, iz čega slijedi da je njime definirana holomorfna funkcija.

Točnije, konvergencija je apsolutna i uniformna na skupovima oblika

$$\{\tau \in \mathcal{H} : |\operatorname{Re}\tau| \leq A, |\operatorname{Im}\tau| \geq B\}.$$

Zbog toga se red može derivirati član po član.

Tvrdimo da je G_k modularna forma težine k. Iz računa iz prethodne napomene slijedi da je G_k holomorfna na $\mathcal{H}$ te holomorfna u beskonačnosti. Preostaje provjeriti uvjet slabe modularnosti.

Neka je $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z})$.

Imamo

$$\begin{aligned} G_k(\gamma(\tau)) &= \sum_{(u,v)\in L'} \frac{1}{\left(u \cdot \frac{a\tau+b}{c\tau+d} + v\right)^k} \\ &= (c\tau + d)^k \sum_{(u,v)\in L'} \frac{1}{(au + cv)\tau + (bu + dv))^k}. \end{aligned}$$

Primijetimo da je $(u, v) \mapsto (au+cv, bu+dv)$ linearna funkcija na $\mathbb{Z}^2$, dobivena djelovanjem matrice γ. Kako γ ima cjelobrojni inverz, slijedi da je to bijekcija na $\mathbb{Z}^2$, a kako šalje $(0, 0)$ u $(0, 0)$, zaključujemo da je i bijekcija na L'.

Zbog apsolutne konvergencije možemo promijeniti redoslijed sumacije pa je

$$\sum_{(u,v)\in L'} \frac{1}{((au + cv)\tau + (bu + dv))^k} = \sum_{(u,v)\in L'} \frac{1}{(u\tau + v)^k} = G_k(\tau),$$

i time je slaba modularnost dokazana.

Sljedeći je cilj odrediti Fourierov razvoj od G_k. Za to trebamo jedan trigonometrijski identitet.

Lema 1.33. *Za $\tau \in \mathcal{H}$, vrijedi*

$$\frac{1}{\tau} + \sum_{d=1}^{\infty} \left(\frac{1}{\tau - d} + \frac{1}{\tau + d} \right) = \pi \operatorname{ctg} \pi\tau = \pi i - 2\pi i \sum_{m=0}^{\infty} q^m, \tag{3}$$

gdje je $q = e^{2\pi i \tau}$.

Dokaz. Jednakost srednjeg i desnog izraza slijedi direktno iz $\operatorname{ctg}(\pi\tau) = \frac{i(q+1)}{1-q}$ i jednakosti $\frac{1}{1-q} = \sum_{m=0}^{\infty} q^m$.

Za dokaz druge jednakosti koristimo produktnu formulu za sinus,

$$\pi\tau \prod_{n=1}^{\infty} (1 - \tau^2/n^2) = \sin(\pi\tau).$$

Tvrdnja sada slijedi uzimanjem logaritma na obje strane i deriviranjem. □

Uzmimo sada $k \geq 2$ te derivirajmo $k-1$ puta lijevu i desnu stranu u (3). Zbog lokalno uniformne konvergencije možemo derivirati član po član. Dobivamo sljedeći identitet za sve $\tau \in \mathcal{H}$ i $q = e^{2\pi i \tau}$:

$$\sum_{d \in \mathbb{Z}} \frac{1}{(\tau + d)^k} = \frac{(-2\pi i)^k}{(k-1)!} \sum_{m=1}^{\infty} m^{k-1} q^m. \tag{4}$$

Za paran $k \geq 4$ možemo sumirati inačice jednakosti (4) za $c\tau$ umjesto τ i dobivamo:

$$\begin{aligned} \sum_{(c,d) \in L'} \frac{1}{(c\tau + d)^k} &= \sum_{d \in \mathbb{Z} \setminus \{0\}} \frac{1}{d^2} + 2 \cdot \frac{(2\pi i)^k}{(k-1)!} \sum_{c=1}^{\infty} \sum_{m=1}^{\infty} m^{k-1} q^{cm} \\ &= 2\zeta(k) + 2 \cdot \frac{(2\pi i)^k}{(k-1)!} \sum_{m=1}^{\infty} \sigma_{k-1}(n) q^n, \end{aligned}$$

gdje je $\zeta(k) = \sum_{n=1}^{\infty} n^{-k}$ Riemannova zeta funkcija, a $\sigma_{k-1}(n)$ zbroj svih $(k-1)$-tih potencija djelitelja od n. Primijetimo da Fourierovi koeficijenti imaju interpretaciju u smislu teorije brojeva.

Sa E_k ćemo označavati *normalizirane* Eisensteinove redove,

$$E_k(\tau) := \frac{G_k(\tau)}{2\zeta(k)} = 1 - \frac{2k}{B_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n, \tag{5}$$

gdje su $(B_k)_k$ Bernoullijevi brojevi. Oni su definirani kao koeficijenti u razvoju $\frac{t}{e^t-1}$ u formalni red:

$$\frac{t}{e^t-1} = \sum_{k=0}^{\infty} B_k \frac{t^k}{k!}.$$

Može se dokazati da je

$$2\zeta(k) = -\frac{(2\pi i)^k}{k!} B_k,$$

iz čega slijedi jednakost (5). Primijetimo da redovi E_k imaju racionalne koeficijente.

Sada dajemo prvi primjer cusp forme. Označimo $g_2(\tau) := 60G_4(\tau)$, $g_3(\tau) := 140G_6(\tau)$. Definiramo *diskriminantu*

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

Tada je Δ modularna forma težine 12. Direktnim računanjem Fourierovih koeficijenata dobivamo da u Fourierovom razvoju od Δ vrijedi $a_0 = 0$, $a_1 = (2\pi)^{12}$. Zaključujemo da je Δ cusp forma različita od 0.

Može se dokazati i da Δ nema nultočaka na $\mathcal{H}$. Iz toga slijedi da je funkcija

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

holomorfna na $\mathcal{H}$. Funkciju j zovemo *modularna invarijanta* ili j-invarijanta. Primijetimo da je j invarijantna na $\mathrm{SL}_2(\mathbb{Z})$ (tj. slabo modularna težine 0).

S obzirom da g_2 nema nultočku u ∞, a Δ ima jednostruku nultočku, zaključujemo da j ima jednostruki singularitet u ∞.

Lema 1.34. *Modularna invarijanta $j : \mathcal{H} \to \mathbb{C}$ je surjekcija.*

Skica dokaza. Pretpostavimo suprotno, da postoji $c \in \mathbb{C}$ takav da je $j(\tau) \neq c$ za svaki $\tau \in \mathcal{H}$. Tada prema principu argumenta za svaku petlju γ u $\mathcal{H}$ vrijedi

$$\frac{1}{2\pi i}\int_\gamma \frac{j'(\tau)}{j(\tau)-c} = 0,$$

jer $j(\tau) - c$ nema ni nultočki ni polova unutar $\mathcal{H}$.

Posebno, to vrijedi i za γ sastavljenu od dijela jedinične kružnice od $\frac{-1+\sqrt{3}i}{2}$ do $\frac{1+\sqrt{3}i}{2}$, dva vertikalna segmenta od tih točaka do iste visine h veće od 1, te segmenta koji spaja $\frac{-1}{2} + hi$ sa $\frac{1}{2} + hi$.

Zbog 1-periodičnosti od j se integrali po vertikalnim dijelovima poništavaju. Zbog invarijantnosti j na djelovanje $\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ se poništavaju integrali po lukovima od $\frac{-1+\sqrt{3}i}{2}$ do i te od i do $\frac{1+\sqrt{3}i}{2}$, pa preostaje integral po horizontalnom segmentu od $\frac{-1}{2}+hi$ do $\frac{1}{2}+hi$, koji onda mora biti jednak 0.

Sada napravimo zamjenu varijabli $q = e^{2\pi i\tau}$ i to postaje integral po kružnici radijusa $e^{-2\pi h}$. Nakon zamjene varijabli, funkcija koju integriramo je

$$\frac{-\frac{1}{q^2}+h'(q)}{\frac{1}{q}+h(q)-c},$$

gdje je $j(\tau) = \frac{1}{q} + h(q)$, gdje je h holomorfna funkcija (znamo da j ima jednostruki pol u ∞).

Prema teoremu o reziduumima, uzevši u obzir da nazivnik nikad nije jednak 0 zbog pretpostavke, integral te funkcije po kružnici oko 0 je jednak -1, što je kontradikcija. □

2 Eliptičke krivulje nad kompleksnim brojevima i modularne krivulje

2.1 Kompleksni torusi

Definicija 2.1. *Rešetka u* $\mathbb{C}$ je skup

$$\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 = \{m\omega_1 + n\omega_2 \mid m, n \in \mathbb{Z}\},$$

gdje su $\omega_1, \omega_2 \in \mathbb{C}$ nezavisni nad $\mathbb{R}$.

Napomena 2.2. Primijetimo da nije smanjenje općenitosti zahtijevati da je $\omega_1/\omega_2 \in \mathcal{H}$. Nadalje, uz tu konvenciju vrijedi $\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 = \mathbb{Z}\omega_1' + \mathbb{Z}\omega_2'$ ako i samo ako je

$$(\omega_1, \omega_2) = \begin{bmatrix} a & b \\ c & d \end{bmatrix} (\omega_1', \omega_2')$$

za neku $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbb{Z})$.

Definicija 2.3. Neka su $\omega_1, \omega_2 \in \mathbb{C}$ linearno nezavisni nad $\mathbb{R}$. *Fundamentalni paralelogram od* ω_1, ω_2 je skup

$$\{a\omega_1 + b\omega_2 : a, b \in [0, 1)\}.$$

Fundamentalni paralelogram je zapravo fundamentalna domena djelovanja rešetke na $\mathbb{C}$.

Definicija 2.4. Neka je L rešetka u $\mathbb{C}$. Kompleksni torus je kvocijent $\mathbb{C}/L$.

Topološki, kompleksni torus možemo zamišljati kao fundamentalni paralelogram kojem smo zalijepili nasuprotne stranice. Algebarski, to je komutativna grupa sa zbrajanjem modulo L.

Kompleksni torus ima i strukturu Riemannove plohe, što je pojam koji ćemo sada definirati.

Definicija 2.5. Riemannova ploha je topološki prostor X koji je Hausdorffov i koji zadovoljava drugi aksiom prebrojivosti, zajedno sa maksimalnim (u smislu inkluzije) kompleksnim atlasom.

Kompleksni atlas na X je familija homeomorfizama $\{\phi_\alpha : U_\alpha \to V_\alpha\}$ iz otvorenih podskupova U_α od X u otvorene podskupove V_α od $\mathbb{C}$, tako da su za sve α, β funkcije $\phi_\alpha \circ \phi_\beta^{-1} : \phi_\beta(U_\beta \cap U_\alpha) \to \mathbb{C}$ holomorfne, te je $\bigcup U_\alpha = X$. Homeomorfizme ϕ_α zovemo karte ili lokalne koordinate.

Topologija kompleksnog torusa je kvocijentna topologija od euklidske topologije na $\mathbb{C}$, a karte uzmemo tako da za svaku otvorenu kuglu K u $\mathbb{C}$ koja ne sadrži dvije točke iz jedne klase ekvivalencije $\mathbb{C}/L$ definiramo $\phi_K^{-1} : K \to \pi(K)$ da bude projekcija $x \to x + L$.

Sada želimo definirati morfizme između kompleksnih torusa. S jedne strane, želimo očuvati grupovnu strukturu, a s druge strane želimo i da se struktura Riemannove plohe čuva.

Za funkciju $h : X \to Y$ između Riemannovih ploha s atlasima $\{f_\alpha\}$ i $\{g_\beta\}$ kažemo da je holomorfna ako su sve funkcije $f_\alpha \circ h \circ g_\beta^{-1}$ holomorfne. Slično definiramo meromorfne funkcije između Riemannovih ploha.

Za kompleksne toruse, to znači da se holomorfna funkcija $h : \mathbb{C}/L \to \mathbb{C}$ može poistovjetiti s L-periodičnom funkcijom iz $\mathbb{C}$ u $\mathbb{C}$.

Napomenimo da se svi rezultati kompleksne analize koji su lokalnog tipa prenose na Riemannove plohe, jer se svaka Riemannova ploha lokalno ponaša kao $\mathbb{C}$. Detalji se mogu naći u [5].

Želimo da morfizmi između kompleksnih torusa budu holomorfne funkcije. To je veliki zahtjev, što se vidi iz sljedeće propozicije.

Propozicija 2.6. *Pretpostavimo da je $\varphi : \mathbb{C}/L_1 \to \mathbb{C}/L_2$ holomorfna funkcija između kompleksnih torusa. Onda postoje kompleksni brojevi m, b takvi da je $\varphi(z+L_1) = mz+b+L_2$ te je $mL_1 \subset L_2$. To preslikavanje je invertibilno ako i samo ako je $mL_1 = L_2$.*

Dokaz se može naći u [1, 1.3.2]. Ideja dokaza je podići funkciju φ do holomorfne funkcije $\overline{\varphi} : \mathbb{C} \to \mathbb{C}$, te za $\lambda \in L_1$ promotriti funkciju $\overline{\varphi}(z + \lambda) - \overline{\varphi}(z)$. Slika te funkcije je sadržana u L_2, pa ta funkcija mora biti konstanta, pa je njena derivacija 0. Onda je derivacija od $\overline{\varphi}$ L_1-periodična, pa je ograničena. Po Liouvilleovom teoremu, ona mora biti konstantna. Iz toga lako slijedi tvrdnja.

Primijetimo da ako na φ iz propozicije dodamo uvjet da je $\varphi(0+L_1) = 0+L_2$, što trebamo zahtijevati ako želimo da se čuva grupovna struktura, onda je φ homomorfizam grupa $\mathbb{C}/L_1$ i $\mathbb{C}/L_2$. Nadalje, svi holomorfni homomorfizmi su zapravo množenja s nekim kompleksnim brojem.

Definicija 2.7. Izogenija je ne-nul holomorfni homomorfizam između kompleksnih torusa.

Primjer 2.8. Neka je $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ rešetka u $\mathbb{C}$ i neka je N prirodan broj. Tada je $NL \subset L$, pa je preslikavanje $z + L \mapsto Nz + L$ izogenija iz $\mathbb{C}/L$ u $\mathbb{C}/L$.

Jezgra te izogenije se sastoji od svih točaka oblika

$$\frac{a\omega_1 + b\omega_2}{N} + L,$$

gdje su $a, b \in \mathbb{Z}$. Odmah se vidi da je jezgra izomorfna sa $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$.

Napomena 2.9. Neka je $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ rešetka. Neka je $\tau = \frac{\omega_2}{\omega_1} \in H$ i sa L' označimo rešetku $\mathbb{Z} + \mathbb{Z}\tau$. Tada su $\mathbb{C}/L$ i $\mathbb{C}/L'$ izomorfni, gdje je izomorfizam dijeljenje s ω_1. Zaključujemo da je svaki kompleksan torus izomorfan torusu oblika $\mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau)$ za neki $\tau \in \mathcal{H}$. Taj τ nije jedinstven, ali ako je τ' neki drugi element $\mathcal{H}$ s tim svojstvom, onda su τ i τ' u istoj orbiti djelovanja $\mathrm{SL}_2(\mathbb{Z})$.

Na ovaj način smo dobili korespondenciju:

$$\{ \text{ kompleksni torusi } \}/\sim \longleftrightarrow \ \mathrm{SL}_2(\mathbb{Z})\text{-orbite od } \mathcal{H}.$$

Sada nas zanima kako izgledaju meromorfne funkcije iz kompleksnog torusa u $\mathbb{C}$.

Neka je L rešetka i $\mathbb{C}/L$ pripadni kompleksni torus. Svaka meromorfna funkcija $\mathbb{C}/L \to \mathbb{C}$ može se poistovjetiti sa L-periodičnom meromorfnom funkcijom $\mathbb{C} \to \mathbb{C}$.

Onda je jasno da su jedine holomorfne funkcije iz $\mathbb{C}/L$ u $\mathbb{C}$ konstantne, jer je svaka L-periodična funkcija ograničena, jer je ograničena na pripadnom fundamentalnom paralelogramu.

Slično, ali malo kompliciranije, se može dokazati da svaka nekonstantna meromorfna funkcija iz $\mathbb{C}/L$ u $\mathbb{C}$ mora imati barem dva pola. Naime, zbroj reziduuma mora biti jednak 0, što se vidi integriranjem po rubu fundamentalnog paralelograma (integrali po nasuprotnim stranicama se ponište zbog periodičnosti).

Sada definiramo važnu meromorfnu funkciju preko koje ćemo dati potpuni opis meromorfnih funkcija na $\mathbb{C}/L$.

Definicija 2.10. Neka je L rešetka. Weierstrassova $\wp$ funkcija je funkcija $\mathbb{C} \to \mathbb{C}$ definirana s

$$\wp(z) = \frac{1}{z^2} + \sum_{w \in L'} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2} \right).$$

Ovdje L' označava $L \setminus \{0\}$.

Primijetimo da $\wp$ ovisi o rešetci L, te bi pravilnije bilo pisati $\wp_L$, no pisat ćemo $\wp$ jer ćemo se baviti jednom fiksnom rešetkom.

Može se pokazati da red koji definira $\wp$ konvergira apsolutno i lokalno uniformno oko svake točke koja nije u rešetci. Naime, svaki sumand je reda veličine $|w|^{-3}$.

Primijetimo da $\wp$ ima dvostruki pol u točkama rešetke, te je holomorfna u svim ostalim točkama. Ono što nije očito je da je $\wp$ L-periodična.

Da bismo to vidjeli, promotrimo derivaciju $\wp'$. Možemo derivirati član po član zbog apsolutne i lokalno uniformne konvergencije, i dobivamo

$$\wp'(z) = \frac{-2}{z^3} - \sum_{w \in L'} \frac{-2}{(z-w)^3} = \sum_{w \in L} \frac{-2}{(z-w)^3}.$$

Vidimo da je $\wp'$ očito L-periodična.

Zaključujemo da je za svaki $w \in L'$ funkcija $\wp(z+w) - \wp(z)$ konstantna. Uvrštavanjem $z = -w/2$ i korištenjem činjenice da je $\wp$ parna slijedi da je ta konstanta jednaka 0, pa je periodičnost od $\wp$ dokazana.

Već smo komentirali da svaka nekonstantna meromorfna funkcija na $\mathbb{C}/L$ mora imati barem dva pola unutar fundamentalnog paralelograma, pa je $\wp$ na neki način najjednostavniji mogući primjer takve funkcije.

Može se pokazati da se svaka meromorfna funkcija na kompleksnom torusu može izgraditi od $\wp$ i $\wp'$. Preciznije, vrijedi sljedeća tvrdnja.

Propozicija 2.11. *Neka je L rešetka. Polje meromorfnih funkcija $\mathbb{C}/L \to \mathbb{C}$ je jednako $\mathbb{C}(\wp, \wp')$, odnosno svaka meromorfna funkcija na $\mathbb{C}/L$ je racionalna funkcija od $\wp$ i $\wp'$.*

Dokaz se može naći u [3, Section 1.5]. Dokaz je konstruktivne prirode. Ideja je za danu parnu meromorfnu funkciju napraviti popis njenih polova i nultočaka pazeći na njihove kratnosti, i konstruirati racionalnu funkciju u $\wp$ koja ima iste polove i nultočke, pa njihov omjer mora biti konstantna funkcija.

Možemo iskoristiti činjenicu da ne postoji nenul holomorfna funkcija na $\mathbb{C}/L$ da bismo dobili algebarsku relaciju između $\wp$ i $\wp'$.
Prvo odredimo Laurentov razvoj od $\wp$ oko nule.

Za z koji je bliže ishodištu nego svaki $w \in L'$ imamo

$$\begin{aligned}
\wp(z) &= \frac{1}{z^2} + \sum_{w \in L'} \frac{1}{(z-w)^2} - \frac{1}{w^2} \\
&= \frac{1}{z^2} + \sum_{w \in L'} \frac{1}{w^2}(2 \cdot \frac{z}{w} + 3 \cdot \frac{z^2}{w^2} + 4 \cdot \frac{z^3}{w^3}) \\
&= \frac{1}{z^2} + \sum_{k=1}^{\infty} z^k \sum_{w \in L'} \frac{k+1}{w^{k+2}} \\
&= \frac{1}{z^2} + 3G_4(L)z^2 + 5G_6(L)z^4 + \ldots,
\end{aligned}$$

uz napomenu da je zamjena sumacije opravdana apsolutnom konvergencijom redova $\sum_{w \in L'} \frac{1}{w^s}$ za $s > 2$. Ovdje je $G_k(L)$ definirano s

$$\sum_{w \in L'} \frac{1}{w^k}.$$

Napomena 2.12. Primijetimo da je oznaka ista kao za Eisensteinove redove. Definiciju Eisensteinovih redova možemo proširiti na rešetke, tako da staru oznaku $G_2(\tau)$ poistovjetimo s novom oznakom $G_2(L)$ za $L = \mathbb{Z} + \mathbb{Z}\tau$.

Sada lako dobivamo Laurentov razvoj za $\wp'$, i potenciranjem tih razvoja jednostavnim računom dobivamo sljedeće:

$$\wp'(z)^2 = \frac{4}{z^6} - 24G_4(L)\frac{1}{z^2} + \text{holomorfni dio}$$
$$\wp(z)^3 = \frac{1}{z^6} + 9G_4(L)\frac{1}{z^2} + \text{holomorfni dio},$$

pa $\wp'(z)^2 - 4\wp(z)^3$ ima razvoj oblika $\frac{c}{z^2} +$ holomorfni dio. Da bismo se riješili tog člana, moramo oduzeti $c\wp(z)$, i dobivamo da postoji konstanta c takva da je $\wp'(z)^2 - 4\wp(z)^3 - c\wp(z)$ holomorfna, pa je nužno konstantna.

Zaključujemo da postoji polinom trećeg stupnja f takav da je

$$\wp'(z)^2 = f(\wp(z)).$$

Ako pažljivije raspisujemo, možemo i točno odrediti koeficijente:

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

gdje je $g_2(L) = 60G_4(L)$, $g_3(L) = 140G_6(L)$.

Ako bismo pak slijedili algoritam iz propozicije 2.11, dobili bismo ovu jednadžbu za $\wp'(z)^2$:

$$\wp'(z)^2 = 4\left(\wp(z) - \wp\left(\omega_1/2\right)\right)\left(\wp(z) - \wp\left(\omega_2/2\right)\right)\left(\wp(z) - \wp((\omega_1+\omega_2)/2)\right),$$

gdje su ω_1, ω_2 takvi da je $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$.

Može se pokazati da su vrijednosti od $\wp$ u točkama $\frac{\omega_1}{2}$, $\frac{\omega_2}{2}$, $\frac{\omega_1+\omega_2}{2}$ različite, pa je krivulja definirana jednadžbom

$$y^2 = 4x^3 - g_2(L)x - g_3(L) \tag{6}$$

nesingularna, odnosno dobili smo eliptičku krivulju nad $\mathbb{C}$ u Weierstrassovoj formi. Neka je E krivulja zadana s (6). Tada imamo preslikavanje s torusa $\mathbb{C}/L$ na E:

$$z + L \mapsto \begin{cases} (\wp(z), \wp'(z)), & z \neq 0, \\ \mathcal{O}, & z = 0, \end{cases}$$

gdje je $\mathcal{O}$ točka u beskonačnosti. To preslikavanje je bijektivno, i analitičko (ako i eliptičku krivulju shvatimo kao Riemannovu plohu).

Bijektivnost slijedi iz svojstva $\wp$ da za svaki $c \in \mathbb{C}$ funkcija $\wp(z) - c$ ima dvije nultočke brojeći kratnost. Analitičnost slijedi iz toga da je preslikavanje lokalno zadano analitičkim funkcijama. Detaljnije objašnjenje može se naći u [3, Section 1.5].

Dakle, svakom kompleksnom torusu možemo pridružiti eliptičku krivulju nad $\mathbb{C}$. Tvrdimo da je to preslikavanje esencijalno surjektivno.

Propozicija 2.13. *Neka je E eliptička krivulja nad $\mathbb{C}$ zadana s*

$$y^2 = 4x^3 - a_2x - a_3,$$

gdje su $a_2, a_3 \in \mathbb{C}$ takvi da je krivulja nesingularna. Tada postoji rešetka L takva da je $a_2 = g_2(L)$ i $a_3 = g_3(L)$.

Dokaz. Pretpostavimo prvo da je $a_2 \neq 0$ i $a_3 \neq 0$.
Kako je j-invarijanta surjekcija $\mathcal{H} \to \mathbb{C}$, postoji $\tau \in \mathcal{H}$ takav da je

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

Iz ovoga slijedi

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

Naša tražena rešetka će biti oblika ωL, tj. $\mathbb{Z}\omega + \mathbb{Z}\tau\omega$ za neki ω koji ćemo tek izabrati.

Kako vrijedi $g_2(\omega L) = \omega^{-4} g_2(L)$ i $g_3(\omega L) = \omega^{-6} g_3(L)$, onda možemo pronaći ω takav da je $a_2 = g_2(\omega L)$ i onda će biti $a_3^2 = g_3(\omega L)^2$, pa smo pogodili sa $g_3(\omega L)$ do na predznak.

Ako je predznak krivi, zamijenimo ω sa $i\omega$ i onda je predznak točan, a $g_2(i\omega L) = g_2(\omega L)$, pa smo našli traženu rešetku.

U slučaju kad je $a_2 = 0$, onda rešetka $\mathbb{Z}m + \mathbb{Z}m\mu_3$ zadovoljava uvjete za neki $m \in \mathbb{C} \setminus \{0\}$, gdje je μ_3 treći korijen iz jedinice. To vrijedi jer je $g_2(\mu_3) = 0$ i $g_3(\mu_3) \neq 0$.

Slično, u slučaju kad je $a_3 = 0$, onda možemo uzeti rešetku $\mathbb{Z}m + \mathbb{Z}mi$ za neki $m \neq 0$, jer je $g_3(i) = 0$ i $g_2(i) \neq 0$. □

Napomena 2.14. Primijetimo da sada možemo definirati operaciju zbrajanja na eliptičkoj krivulji preko operacije zbrajanja na torusu. Naime, ako je E eliptička krivulja i $\wp$ Weierstrassova funkcija pripadne rešetke, možemo za $P = (\wp(z), \wp'(z))$, $Q = (\wp(w), \wp'(w))$ definirati

$$P + Q := (\wp(z + w), \wp'(z + w)),$$

uz (smislenu) konvenciju da je točka u beskonačnosti $\mathcal{O}$ jednaka $(\wp(0), \wp'(0))$.

Nadalje, ova definicija zbrajanja je ekvivalentna geometrijskoj definiciji zbrajanja točaka. Ovo se može naći u [9, Chapter 6].

2.2 Modularne krivulje

Već smo ustanovili da kompleksne toruse do na izomorfizam možemo poistovjetiti sa skupom orbita $\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}$. Ali isto tako znamo da možemo poistovjetiti kompleksne toruse i eliptičke krivulje. Zaključujemo da skup orbita $\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}$ zapravo parametrizira sve eliptičke krivulje. Taj skup orbita ćemo zvati modularna krivulja za grupu $\mathrm{SL}_2(\mathbb{Z})$. Općenitije, imamo sljedeću definiciju.

Definicija 2.15. Neka je $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ kongruencijska podgrupa. Definiramo modularnu krivulju $Y(\Gamma)$ za Γ kao skup orbita djelovanja Γ na $\mathcal{H}$,

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

Posebno, za grupe $\Gamma_0(N), \Gamma_1(N), \Gamma(N)$ ćemo pripadne modularne krivulje označavati s $Y_0(N), Y_1(N), Y(N)$ redom.

Kao što smo već rekli, $\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}$ će parametrizirati sve eliptičke krivulje do na izomorfizam. Druge modularne krivulje će parametrizirati eliptičke krivulje zajedno s nekom dodatnom informacijom.

Definicija 2.16. Neka je N prirodan broj.

(a) Pojačana eliptička krivulja za $\Gamma_0(N)$ je uređeni par (E, C), gdje je E kompleksna eliptička krivulja, a C njena ciklička podgrupa reda N. Parovi (E, C) i (E', C') su ekvivalentni, u oznaci $(E, C) \sim (E', C')$ ako postoji izomorfizam $E \to E'$ koji šalje C u C'. Skup klasa ekvivalencije

$$\{\text{pojačane eliptičke krivulje za } \Gamma_0(N)\}/\sim$$

označavamo sa $S_0(N)$ i zovemo prostor parametara za $\Gamma_0(N)$. Klasu ekvivalencije od (E, C) označavamo s $[E, C]$.

(b) Pojačana eliptička krivulja za $\Gamma_1(N)$ je uređeni par (E, Q), gdje je E kompleksna eliptička krivulja, a Q točka na E reda N. Parovi (E, Q) i (E', Q') su ekvivalentni, u oznaci $(E, Q) \sim (E', Q')$ ako postoji izomorfizam $E \to E'$ koji šalje Q u Q'. Skup klasa ekvivalencije

$$\{\text{pojačane eliptičke krivulje za } \Gamma_1(N)\}/\sim$$

označavamo sa $S_1(N)$ i zovemo prostor parametara za $\Gamma_1(N)$. Klasu ekvivalencije od (E, Q) označavamo s $[E, Q]$.

Ova definicija je malo misteriozna, ali sljedeći teorem pokazuje da ima smisla. Ideja je da uz ovu definiciju $Y_0(N)$ i $Y_1(N)$ parametriziraju $S_0(N)$ i $S_1(N)$.

Za $\tau \in \mathcal{H}$, sa L_τ označimo rešetku $\mathbb{Z}\tau + \mathbb{Z}$ i sa E_τ pripadnu eliptičku krivulju.

Teorem 2.17. *Neka je N prirodan broj.*

(a) *Prostor parametara za $\Gamma_0(N)$ je*

$$S_0(N) = \{[E_\tau, \langle 1/N + L_\tau\rangle : \tau \in \mathcal{H}\}.$$

Dvije točke $[E_\tau, \langle 1/N + L_\tau\rangle]$ i $[E_{\tau'}, \langle 1/N + L_{\tau'}\rangle]$ su jednake ako i samo ako su orbite $\Gamma_0(N)\tau$ i $\Gamma_0(N)\tau'$ jednake. Dakle, postoji bijekcija

$$\psi_0 : S_0(N) \xrightarrow{\sim} Y_0(N), \quad [E_\tau, \langle 1/N + L_\tau\rangle] \mapsto \Gamma_0(N)\tau.$$

(b) *Prostor parametara za $\Gamma_1(N)$ je*

$$S_1(N) = \{[E_\tau, 1/N + L_\tau] : \tau \in \mathcal{H}\}.$$

Dvije točke $[E_\tau, 1/N + L_\tau]$ i $[E_{\tau'}, 1/N + L_{\tau'}]$ su jednake ako i samo ako su orbite $\Gamma_1(N)\tau$ i $\Gamma_1(N)\tau'$ jednake. Dakle, postoji bijekcija

$$\psi_1 : S_1(N) \xrightarrow{\sim} Y_1(N), \quad [E_\tau, 1/N + L_\tau] \mapsto \Gamma_1(N)\tau.$$

Dokaz. Dokazat ćemo tvrdnju (a). Tvrdnja (b) je slična, i dokaz se može naći u [1, 1.5.1].

Uzmimo neki par (E, C), gdje je C ciklička reda n. Onda je E izomorfna s E_τ za neki $\tau \in \mathcal{H}$, a grupa C se pod tim izomorfizmom slika u grupu generiranu s $\frac{c\tau+d}{N}$ za neke $c, d \in \mathbb{Z}$ sa $\gcd(c, d, N) = 1$, s tim da su c i d samo zadani modulo N. Sada trebamo sljedeću jednostavnu lemu iz elementarne teorije brojeva.

Lema 2.18. *Neka su c, d, N relativno prosti cijeli brojevi. Tada postoji cijeli broj u takav da su $c + uN$ i d relativno prosti.*

Dokaz. Uzmimo prost broj p koji dijeli d. Onda $p \nmid c$ ili $p \nmid c + N$. Neka je $u_p = 1$ ako $p \nmid c + N$ i $u_p = 0$ inače. Uzmimo, po Kineskom teoremu o ostacima, broj u takav da je $u \equiv u_p \pmod{p}$ za svaki p koji dijeli d. Tada je $c + uN$ po konstrukciji relativno prost s d. □

Zamijenimo onda ako je potrebno c i d s brojevima $c + uN$ i d iz leme, i možemo pretpostaviti da su c i d relativno prosti. Onda postoje cijeli brojevi a, b takvi da je $\gamma := \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbb{Z})$.

Dakle, imamo par $(\mathbb{Z}\tau + \mathbb{Z}, \langle \frac{c\tau+d}{N}\rangle)$.

Međutim, $\mathbb{Z}\tau + \mathbb{Z} = \mathbb{Z}(a\tau + b) + \mathbb{Z}(c\tau + d)$. Onda promotrimo izomorfizam množenja sa $\frac{1}{c\tau+d}$ u torus $\mathbb{C}/(\mathbb{Z}(\gamma(\tau)) + \mathbb{Z})$. On šalje $\frac{c\tau+d}{N}$ u $\frac{1}{N}$, pa imamo

$$\left(\mathbb{C}/(\mathbb{Z}\tau + \mathbb{Z}), \left\langle \frac{c\tau + d}{N} \right\rangle\right) \sim \left(\mathbb{C}/(\mathbb{Z}(\gamma(\tau)) + \mathbb{Z}), \langle 1/N\rangle\right).$$

Pretpostavimo sada da je $[\mathbb{C}/L_\tau, \langle 1/N\rangle] = [\mathbb{C}/L_{\tau'}, \langle 1/N\rangle]$. Treba dokazati da su τ i τ' u istoj orbiti pod djelovanjem $\Gamma_0(N)$.

Znamo da postoji kompleksan broj m takav da je $m(\mathbb{C}/L_\tau) = \mathbb{C}/L_{\tau'}$ odnosno $mL_\tau = L_{\tau'}$, te je $m\langle 1/N + L_\tau\rangle = \langle 1/N + L_{\tau'}\rangle$.

Onda je $\mathbb{Z}m\tau + \mathbb{Z}m = \mathbb{Z}\tau' + \mathbb{Z}$, pa postoji $\left[\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbb{Z})$ takva da je $m\tau = a\tau' + b$ i $m = c\tau' + d$. Treba dokazati da je $\left[\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right] \in \Gamma_0(N)$, tj. da je $c \equiv 0 \pmod N$.

Iz drugog uvjeta slijedi da je $m\frac{1}{N} + L'_\tau = \frac{u}{N} + L'_\tau$ za neki u relativno prost s N.

Ali ako uvrstimo $m = c\tau' + d$ dobivamo

$$\frac{c\tau' + d - u}{N} \in L_{\tau'},$$

odnosno N dijeli c i N dijeli $d - u$, pa je tvrdnja dokazana.

□

Za $N = 1$, dobivamo da su sve eliptičke krivulje parametrizirane s $Y_0(1) = Y(\mathrm{SL}_2(\mathbb{Z})) = \mathrm{SL}_2(\mathbb{Z})\backslash\ \mathcal{H}$, kao što smo i ranije objasnili.

Modularne krivulje se također mogu shvatiti kao Riemannove plohe. Detaljna konstrukcija je dana u drugom poglavlju [1].

Topologija je kvocijentna topologija inducirana surjekcijom $\pi : \mathcal{H} \to Y(\Gamma)$,

$$\pi(\tau) = \Gamma\tau.$$

Ovime je povezanost naslijeđena. Može se pokazati i da je $Y(\Gamma)$ Hausdorffov.

Za kompleksnu strukturu oko točaka koje imaju trivijalan stabilizator lokalne koordinate su samo lokalni inverzi kanonske surjekcije π.

Za točke s netrivijalnim stabilizatorom vrijedi da je stabilizator konačan i ciklički, te su lokalne koordinate kompliciranije. Točke s netrivijalnim stabilizatorom zovu se *eliptičke točke*.

Riemannove plohe $Y(\Gamma)$ nisu kompaktne, ali ih možemo kompaktificirati dodavanjem konačno mnogo točaka. Prisjetimo se da smo djelovanje od $\mathrm{SL}_2(\mathbb{Z})$ definirali i na $\mathbb{P}_1(\mathbb{Q})$. Onda dakle imamo djelovanje na $\mathcal{H}\cup\mathbb{P}_1(\mathbb{Q})$, pa za kongruencijsku podgrupu Γ definiramo $X(\Gamma)$ kao skup orbita tog proširenog djelovanja,

$$X(\Gamma) := \Gamma\backslash(\mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})).$$

Točke oblika Γs za $s \in \mathbb{P}^1(\mathbb{Q})$ zovemo cuspovi za modularnu krivulju $X(\Gamma)$.

Na $\mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$ definiramo topologiju kojoj su baza svi otvoreni skupovi u $\mathcal{H}$, sve otvorene kružnice koje dodiruju x-os u racionalnim točkama, zajedno

s tim točkama, te svi skupovi oblika $\{\mathrm{Im}(\tau) > A\}$ za $A > 0$, zajedno s točkom ∞.

Onda na $X(\Gamma)$ definiramo topologiju kao kvocijentnu topologiju upravo definirane topologije, u odnosu na kanonsku projekciju π.

To čini $X(\Gamma)$ kompaktnim, povezanim i Hausdorffovim topološkim prostorom. Ako dodefiniramo kompleksnu strukturu sa $Y(\Gamma)$ na $X(\Gamma)$, dobivamo da je $X(\Gamma)$ kompaktna Riemannova ploha.

Sa $X(N), X_0(N)$ i $X_1(N)$ ćemo označavati $X(\Gamma(N)), X(\Gamma_0(N))$ i $X(\Gamma_1(N))$. Sada smo spremni izreći prvu verziju teorema o modularnosti.

Teorem 2.19 (Teorem o modularnosti, geometrijska verzija)**.** *Neka je E kompleksna eliptička krivulja čija je j-invarijanta racionalna. Tada za neki prirodan broj N postoji surjektivna holomorfna funkcija između Riemannovih ploha s modularne krivulje $X_0(N)$ na eliptičku krivulju E,*

$$X_0(N) \longrightarrow E.$$

Ta funkcija zove se modularna parametrizacija od E.

Napomena 2.20. Modularne krivulje možemo definirati i algebarski. Naime, svaka kompaktna Riemannova ploha se može interpretirati kao algebarska krivulja nad $\mathbb{C}$ i obratno. Konkretan slučaj te korespondencije smo već vidjeli kad smo objasnili vezu između kompleksnih torusa i eliptičkih krivulja nad $\mathbb{C}$. Također, moguće je dati definiciju modularnih krivulja preko funktora. Prednost takvih definicija je što se mogu poopćiti na sva polja, a ne samo na potpolja od $\mathbb{C}$.

Više o ovim pristupima može se naći u [4].

Primjer 2.21. Pokažimo kako možemo eksplicitno doći do jednadžbe za $X_1(11)$. Znamo da $X_1(11)$ parametrizira (do na cuspove) sve parove (E, P) gdje je E eliptička krivulja, a P točka reda 11 na E.

Svaku eliptičku krivulju možemo prikazati, prema [2, 1.5], u takozvanoj Tateovoj normalnoj formi:

$$y^2 + (1-c)xy - by = x^3 - bx^2,$$

tako da je naša izabrana točka, u ovom slučaju ona reda 11, jednaka $(0, 0)$.

Ove koordinate su zgodne jer u njima možemo jednostavno izračunati višekratnike točaka. Točnije, $P = (0, 0)$ je reda 11 ako i samo ako je $6P = -5P$.

Iz formula za zbrajanje dobivamo

$$6P = \left(\frac{(c-b)(c^3+bc-b^2)}{(c-b+c^2)^2}, \frac{c(c-b)^2(bc^2-c^2+3bc-2b^2)}{(c-b+c^2)^3} \right),$$
$$-5P = \left(\frac{-bc(b-c-c^2)}{(b-c)^2}, \frac{b^2(b-c-c^2)^2}{(b-c)^3} \right).$$

Dakle, P je reda 11 ako i samo ako se x-koordinate i y-koordinate poklapaju.

Iz toga dobivamo algebarsku jednadžbu za b i c, koja je onda model za krivulju $X_1(11)$. Primijetimo da je $X_1(11)$ zapravo definirana nad $\mathbb{Q}$.

Zapravo je jedan od modela za $X_1(11)$ sljedeći ([10]):

$$y^2 + y = x^3 - x.$$

Ovo je eliptička krivulja. Može se pokazati da ima samo 5 racionalnih točaka. Ali $X_1(11)$ ima 5 racionalnih cuspova, odnosno ni jedna od točaka ne odgovara eliptičkoj krivulji. Iz toga slijedi da ne postoji eliptička krivulja nad $\mathbb{Q}$ koja ima racionalnu točku reda 11.

3 Struktura prostora modularnih formi

U ovom poglavlju ćemo citirati rezultate koji opisuju strukturu prostora $\mathcal{M}_k(\Gamma)$ za kongruencijsku podgrupu $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$.

3.1 Dimenzija prostora

Modularne krivulje $X(\Gamma)$ su kompaktne Riemannove plohe. Svaka kompaktna Riemannova ploha je homeomorfna nekoj sferi s g rupa, i taj broj g zovemo *genus*.

Neka je $f : X \to Y$ nekonstantno holomorfno preslikavanje kompaktnih Riemannovih ploha. Tada je f surjekcija, jer je $f(X)$ otvoren po teoremu o otvorenom preslikavanju iz kompleksne analize, i zatvoren kao slika kompakta pod neprekidnom funkcijom.

Nadalje, postoji prirodan broj d, koji zovemo stupanj od f, takav da za svaki $y \in Y$ vrijedi

$$\sum_{x \in f^{-1}(\{y\})} e_x = d,$$

gdje je e_x kratnost nultočke funkcije $z \mapsto f(z) - y$ u točki x. Broj e_x zovemo indeks grananja od f u x.

Također, ako su nam dane kompaktne Riemannove plohe X i Y s genusima g_X i g_Y te preslikavanje f stupnja d sa X u Y, tada vrijedi Riemann-Hurwitzova formula:

$$2g_X - 2 = d(2g_Y - 2) + \sum_{x \in X}(e_x - 1).$$

Iz ove formule posebno slijedi da ne postoje nekonstantna holomorfna preslikavanja iz Riemannove plohe manjeg genusa u Riemannovu plohu većeg genusa.

U situaciji koja nas interesira, primijetimo da ako su Γ_1 i Γ_2 kongruencijske podgrupe takve da je $\Gamma_1 \subset \Gamma_2$, tada postoji prirodna projekcija $\pi : X(\Gamma_1) \to X(\Gamma_2)$,

$$\pi(\Gamma_1\tau) := \Gamma_2\tau.$$

To je nekonstantno holomorfno preslikavanje. Stupanj mu je jednak indeksu $[\{\pm I\}\Gamma_2 : \{\pm I\}\Gamma_1]$. Naime, svaka točka $\Gamma_2\tau$ koja nije eliptička niti cusp je pogođena točno sa svim $\Gamma_1\alpha$ za koje je $\alpha\tau^{-1} \in \{\pm I\}\Gamma_2$.

Posebno, za $\Gamma_2 = \mathrm{SL}_2(\mathbb{Z})$, stupanj preslikavanja projekcije $\pi : X(\Gamma) \to X(1)$ je jednostavno odrediti.

Nadalje, genus od $X(1)$ je jednak 0. To slijedi iz toga što je j-invarijanta holomorfna bijekcija s $X(1)$ u $\mathbb{P}^1(\mathbb{C})$. Dokazali smo da je surjekcija gledana

kao funkcija $\mathcal{H} \to \mathbb{C}$ s jednostrukim polom u ∞, ali vrijednosti j-invarijante u nekoj točki su određene orbitom te točke pod djelovanjem $\mathrm{SL}_2(\mathbb{Z})$. Nadalje, za svaki $c \in \mathbb{C}$ smo u dokazu leme 1.34 izračunali integral

$$\frac{1}{2\pi i} \int_\gamma \frac{j'(\tau)d\tau}{j(\tau) - c}$$

po krivulji γ i dobili da je jednak ± 1 (ovisno o orijentaciji integrala), pa je svaka vrijednost c pogođena jednom.

Dakle, da bismo odredili genus od općenite $X(\Gamma)$, potrebno je analizirati grananje projekcije u svakoj točki i iskoristiti Riemann-Hurwitzovu formulu. Grananja nema u neeliptičkim točkama, pa nas samo zanimaju praslike eliptičkih točaka u $X(1)$ pod projekcijom.

Označimo s y_2, y_3 i y_∞ točke $\mathrm{SL}_2(\mathbb{Z})i, \mathrm{SL}_2(\mathbb{Z})\omega_3$ i $\mathrm{SL}_2(\mathbb{Z})\infty$, gdje je $\omega_3 = \frac{1+\sqrt{3}i}{2}$. To su eliptičke točke i cusp od $X(1)$. Tada vrijedi sljedeći teorem.

Teorem 3.1. *Neka je Γ kongruencijska podgrupa od $\mathrm{SL}_2(\mathbb{Z})$. Neka je $\pi : X(\Gamma) \to X(1)$ prirodna projekcija i neka je d njen stupanj. Nadalje, označimo s $\epsilon_2, \epsilon_3, \epsilon_\infty$ redom broj eliptičkih točaka u praslikama od y_2, y_3 te broj cuspova od Γ. Tada je genus od $X(\Gamma)$ jednak*

$$g = 1 + \frac{d}{12} - \frac{\epsilon_2}{4} - \frac{\epsilon_3}{3} - \frac{\epsilon_\infty}{2}.$$

Dokaz. [1, 3.1.1]. □

Uz pomoć Riemann-Rochovog teorema za Riemannove mnogostrukosti, pomoću genusa se može izraziti dimenzija prostora $\mathcal{M}_k(\Gamma)$ i $\mathcal{S}_k(\Gamma)$. Teorem iskazujemo samo za parne k, za neparne k se formule za dimenzije mogu naći u [1, Section 3.6].

Teorem 3.2 (Formule za dimenzije)**.** *Neka je k paran cijeli broj. Neka je Γ kongruencijska podgrupa od $\mathrm{SL}_2(\mathbb{Z})$, g genus od $X(\Gamma)$, i neka su $\epsilon_2, \epsilon_3, \epsilon_\infty$ redom broj eliptičkih točaka u praslici od y_2, y_3 te broj cuspova. Tada vrijedi:*

$$\dim(\mathcal{M}_k(\Gamma)) = \begin{cases} (k-1)(g-1) + \left\lfloor \frac{k}{4} \right\rfloor \epsilon_2 + \left\lfloor \frac{k}{3} \right\rfloor \epsilon_3 + \frac{k}{2}\epsilon_\infty & \text{ako je } k \geq 2, \\ 1 & \text{ako je } k = 0, \\ 0 & \text{ako je } k < 0. \end{cases}$$

Nadalje, vrijedi:

$$\dim(\mathcal{S}_k(\Gamma)) = \begin{cases} (k-1)(g-1) + \left\lfloor \frac{k}{4} \right\rfloor \epsilon_2 + \left\lfloor \frac{k}{3} \right\rfloor \epsilon_3 + \left(\frac{k}{2} - 1\right) \epsilon_\infty & \text{ako je } k \geq 4, \\ g & \text{ako je } k = 2, \\ 0 & \text{ako je } k \leq 0. \end{cases}$$

Ako specijaliziramo teorem na $\mathrm{SL}_2(\mathbb{Z})$, dobivamo sljedeći eksplicitan opis prstena $\mathcal{M}(\mathrm{SL}_2(\mathbb{Z}))$.

Teorem 3.3. *Vrijedi $\mathcal{M}_0(\mathrm{SL}_2(\mathbb{Z})) = \mathbb{C}$. Za paran ne-nul cijeli broj $k < 4$ je $\mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z})) = \{0\}$. Za paran cijeli broj $k \geq 4$, vrijedi*

$$\mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z})) = \mathcal{S}_k(\mathrm{SL}_2(\mathbb{Z})) \oplus \mathbb{C}E_k,$$

gdje je E_k normalizirani Eisensteinov red, te je

$$\dim \mathcal{S}_k(\mathrm{SL}_2(\mathbb{Z})) = \begin{cases} \left\lfloor \frac{k}{12} \right\rfloor - 1 & za\ k \equiv 2 \pmod{12}, \\ \left\lfloor \frac{k}{12} \right\rfloor & za\ k \not\equiv 2 \pmod{12}. \end{cases}$$

Graduirani prsten svih modularnih formi $\mathcal{M}(\mathrm{SL}_2(\mathbb{Z}))$ je $\mathbb{C}[E_4, E_6]$, a ideal svih cusp formi je glavni ideal generiran diskriminantom Δ.

Dokazi teorema nalaze se u [1, Section 3.5].

Primjer 3.4. Iz ovog teorema slijede neke neočekivane multiplikativne relacije između različitih Eisensteinovih redova, koje onda daju neobične identitete između aritmetičkih funkcija σ_k.

Na primjer, prostor $\mathcal{M}_8(\mathrm{SL}_2(\mathbb{Z}))$ je jednodimenzionalan, pa je $E_8 = E_4^2$.

Raspisivanjem koeficijenata Fourierovih redova, dobivamo:

$$E_4(\tau)^2 = \left(1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) q^n\right)^2$$

$$E_8(\tau) = 1 + 480 \sum_{n=1}^{\infty} \sigma_7(n) q^n,$$

odnosno

$$\sigma_7(n) = \sigma_3(n) + 120 \sum_{k=1}^{n-1} \sigma_3(k)\sigma_3(n-k).$$

Primjer 3.5. Neka je p prost broj. Odredimo genus g od $X_0(p)$. Kao prvo, iz formula iz primjera 1.8 možemo vidjeti da je indeks $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(p)]$ jednak $p + 1$. Prvo ćemo pronaći skup reprezentanata desnih klasa.

Za $j \in \{0, 1, \ldots, p-1\}$, neka je $\alpha_j = \left[\begin{smallmatrix} 1 & 0 \\ j & 1 \end{smallmatrix}\right]$, te neka je $\alpha_\infty = \left[\begin{smallmatrix} 1 & -1 \\ 1 & 0 \end{smallmatrix}\right]$.

Tvrdimo da nikoje dvije od ovih $p + 1$ matrica nisu u istoj klasi. Pretpostavimo da je

$$\begin{bmatrix} a & b \\ pc & d \end{bmatrix} \begin{bmatrix} 1 & 0 \\ j & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ k & 1 \end{bmatrix}.$$

Onda je $d = 1$ gledanjem donjeg desnog unosa, i $pc + j = k$ gledanjem donjeg lijevog unosa, ali onda $p \mid k - j$, odnosno $k = j$ pa nikoje dvije od matrica α_i nisu u istoj klasi za $i \in \{0, 1, \ldots, p-1\}$. Slično se lako provjeri da α_∞ nije u istoj klasi kao α_i, pa je ovo stvarno skup reprezentanata.

Dokažimo sada da $\Gamma_0(p)$ ima točno dva cuspa. Odredimo prvo orbitu točke ∞. Neka je $\frac{u}{v} \in \mathbb{Q}$ takav da za neku matricu vrijedi

$$\begin{bmatrix} a & b \\ pc & d \end{bmatrix} \begin{pmatrix} u \\ \overline{v} \end{pmatrix} = \infty.$$

Tada dobivamo $pcu = -dv$, pa slijedi da $p \mid v$. Obratno, za svaki racionalan broj oblika $\frac{u}{pv}$ možemo pronaći matricu $\left[\begin{smallmatrix} a & b \\ pc & d \end{smallmatrix}\right]$ koja $\frac{u}{pv}$ šalje u ∞. Dakle, orbitu od ∞ čine svi racionalni brojevi x takvi da je $\nu_p(x) < 0$.

Dokažimo da svi ostali racionalni brojevi čine jednu orbitu. Dovoljno je za svaki $\frac{u}{v} \in \mathbb{Q}$ takav da $p \nmid v$ pronaći matricu $\left[\begin{smallmatrix} a & b \\ pc & d \end{smallmatrix}\right] \in \Gamma_0(p)$ takvu da je

$$\begin{bmatrix} a & b \\ pc & d \end{bmatrix} (1) = \frac{u}{v}.$$

To se svodi na sustav jednadžbi

$$\begin{aligned} ad - pbc &= 1, \\ v(a+b) &= u(pc+d). \end{aligned}$$

Stavimo $b = u - a$, $d = v - pc$, tako da drugi uvjet bude zadovoljen, a prvi uvjet postaje

$$av - pcu = 1.$$

Kako su v i pu relativno prosti, po Bezoutovoj lemi možemo pronaći a i c s traženim svojstvom. Dakle, broj cuspova je točno 2.

Da bismo odredili eliptičke točke u praslici od $z \in \{i, \omega_3\}$, trebamo promotriti za koje točke oblika $\alpha_j(i)$ postoji netrivijalna $\gamma \in \Gamma_0(p)$ takva da je $\gamma\alpha_j(z) = \alpha_j(z)$.

Pokazuje se da se u oba slučaja to svodi na kvadratnu jednadžbu modulo p. Točnije, broj eliptičkih točaka u praslici od i je $1+\phi_p(-1)$, a broj eliptičkih točaka u praslici od ω_3 je $1 + \phi_p(-3)$, gdje je ϕ_p Legendreov simbol modulo p. Obje ove vrijednosti samo ovise o p modulo 12.

Konačno, dobivamo da je genus jednak

$$1+\frac{p+1}{12}-\frac{(1+\varphi_p(-1))}{4}-\frac{(1+\varphi_p(-3))}{3}-1 = \begin{cases} \left\lfloor \frac{p+1}{12} \right\rfloor - 1 & p \equiv 1 \pmod{12}, \\ \left\lfloor \frac{p+1}{12} \right\rfloor & \text{inače.} \end{cases}$$

Posebno, po teoremu 3.2 zaključujemo da su prostori $\mathcal{S}_2(\Gamma_0(p))$ trivijalni za svaki prost broj $p \leq 13$ osim $p = 11$.

Postoji i elementarni pristup računanju dimenzija, koji je manje efikasan. Pristup je preuzet iz [6, Chapter VII]. Primijenit ćemo ga na $\mathrm{SL}_2(\mathbb{Z})$.

Fundamentalna domena djelovanja $\mathrm{SL}_2(\mathbb{Z})$ na $\mathcal{H}$ je skup

$$\mathcal{D} = \{\tau \in \mathcal{H} : \mathrm{Re}(\tau) \in [-1/2, 1/2], |\tau| \geq 1\}.$$

Za holomorfnu funkciju f i kompleksan broj z, sa $\nu_z(f)$ označimo red poništavanja od f u z. Za modularnu formu f, sa $\nu_\infty(f)$ označimo red poništavanja u beskonačnosti, odnosno najmanji $n \geq 0$ takav da je $a_{n+1}(f) \neq 0$.

Propozicija 3.6 (Formula valencije)**.** *Neka je $f \in \mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z}))$, gdje je k paran prirodan broj. Tada vrijedi*

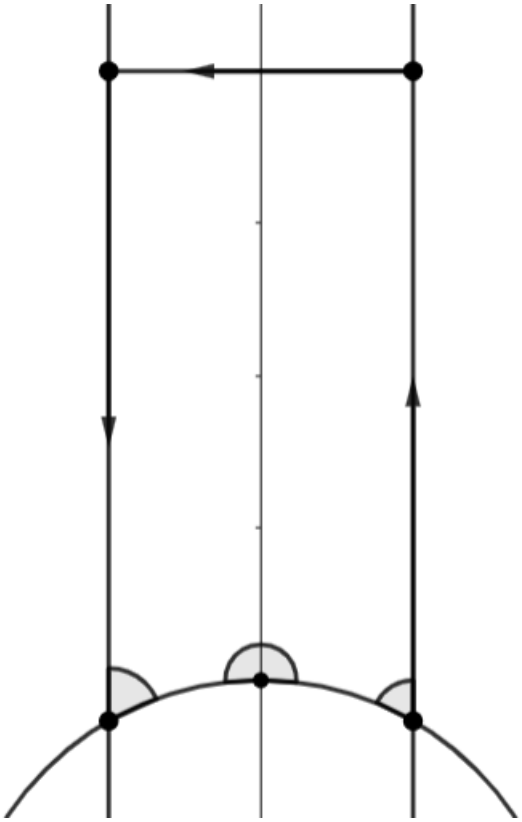
$$\nu_\infty(f) + \frac{1}{2}\nu_i(f) + \frac{1}{3}\nu_{\omega_3}(f) + \sum_{\substack{z \in \mathcal{D} \\ z \neq i, \omega_3}} \nu_z(f) = \frac{k}{12}.$$

Skica dokaza. Ideja je integrirati logaritamsku derivaciju od f po rubu fundamentalne domene. Pretpostavimo radi jednostavnosti da f nema nultočka ni polova na rubu fundamentalne domene, osim možda u $i, \omega_3, \omega_3 - 1$.

Konkretno, neka je $M > 1$ takav da f nema nultočka ni polova na skupu $\{z \in \mathcal{D} : \mathrm{Im}(z) > M\}$ osim eventualno u ∞.

Promotrimo integral po krivulji γ kao na Slici 1 logaritamske derivacije od f, odnosno

$$\int_\gamma \frac{f'(z)}{f(z)} dz.$$



Slika 1: krivulja po kojoj integriramo

Kružnica na slici je jedinična kružnica, a označene točke su

$$\omega_3 - 1,\ i,\ \omega_3,\ \frac{1}{2} + Mi,\ -\frac{1}{2} + Mi.$$

Krivulja se sastoji od horizontalne dužine koja spaja $\frac{1}{2} + Mi$ i $\frac{-1}{2} + Mi$, dviju vertikalnih dužina, te dijelova kružnice, s time da zaobilazimo točke $\omega_3 - 1, i, \omega_3$ malim kružnim lukovima.

Integral po cijeloj γ je prema principu argumenta jednak

$$2\pi i \sum_{\substack{z \in \mathcal{D} \\ z \neq i, \omega_3}} \nu_z(f).$$

Integral po horizontalnoj dužini zamjenom varijabli možemo svesti na integral (u negativnom smjeru) po q po kružnici oko točke 0 od Fourierovog razvoja od f'/f, koji je po teoremu o reziduumima jednak $-2\pi i \nu_\infty(f)$.

Integrali po vertikalnim segmentima se skrate jer je f'/f periodična s periodom 1.

Preostaje integral po kružnim dijelovima. Za integrale po malim krugovima koristimo sljedeću lemu.

Lema 3.7. *Neka je f holomorfna funkcija na nekoj okolini točke $z_0 \in \mathbb{C}$, te pretpostavimo da u z_0 ima najviše jednostruki pol. Neka je $(\varepsilon_n)_n$ niz pozitivnih realnih brojeva koji teži u 0, i neka je α_n niz realnih brojeva koji teži u α. Označimo sa γ_n kružni luk oko z_0 radijusa ε_n sa središnjim kutem α_n. Tada je*

$$\lim_{n\to\infty} \int_{\gamma_n} f(z)dz = \alpha i \operatorname{Res}_{z_0}(f).$$

Dokaz. Za n dovoljno velik, f ima Laurentov razvoj $a_{-1}(z-z_0)^{-1} + g(z)$, gdje je g holomorfna oko z_0.

Parametriziramo luk γ_n sa $z(t) = z_0 + \varepsilon_n e^{it}$, $t \in [\alpha_0, \alpha_0 + \alpha_n]$.

Nakon te zamjene varijabli se lako vidi da je integral po γ_n oblika

$$\int_{\alpha_0}^{\alpha_0+\alpha_n} ia_{-1} + \varepsilon_n \mathcal{O}(1)dt.$$

Drugi pribrojnik teži u 0 kako $n \to \infty$, a prvi teži u $\alpha i a_{-1}$, pa je lema dokazana. □

Iz leme i iz principa argumenta direktno slijedi da integrali od f'/f po malim kružnicama koje zaobilaze $\omega_3 - 1, i, \omega_3$ konvergiraju u

$$-2 \cdot \frac{1}{6}\nu_{\omega_3}(f) - \frac{1}{2}\nu_i(f).$$

Još je potrebno dokazati da integral po dijelu jedinične kružnice teži u $\frac{k}{12}$.

Ideja je da matrica S koja šalje z u $\frac{-1}{z}$ preslikava jedan od preostalih lukova na drugi, a zbog modularnosti znamo kako se f transformira pod djelovanjem S. Raspis tog dijela dokaza se može pronaći u [6, Chapter VII]. □

Ovaj pristup bi se mogao primijeniti i na ostale kongruencijske podgrupe, no tada bismo morali eksplicitno znati kako izgledaju fundamentalne domene i što se događa s cuspovima, što nije često slučaj.

Objasnimo sada kako iz formule valencija slijedi teorem 3.3.

Za paran $k \geq 0$, za svaku nenul modularnu formu $f \in \mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z}))$ vrijedi

$$\nu_\infty(f) + \frac{1}{2}\nu_i(f) + \frac{1}{3}\nu_{\omega_3}(f) + \sum_{\substack{z\in\mathcal{D}\\ z\neq i,\omega_3}} \nu_z(f) = \frac{k}{12}.$$

Za $k = 0$, ako pretpostavimo da postoji nekonstantna modularna forma težine 0, ona po formuli nigdje nema nultočku što je nemoguće, uz isti argument kao za kompleksne toruse. Naime, modularna forma težine 0 je isto što i holomorfna funkcija na kompaktnoj Riemannovoj plohi $X(1)$, pa možemo primijeniti Liouvilleov teorem. Dakle, $\{1\}$ je baza za $\mathcal{M}_0(\mathrm{SL}_2(\mathbb{Z}))$.

Za $k = 2$ primijetimo da ne možemo napisati $1/6$ u obliku s lijeve strane, pa je $\mathcal{M}_2(\mathrm{SL}_2(\mathbb{Z})) = \{0\}$.

Za $k = 4$ vidimo da svaka nenul modularna forma težine 4 mora imati jednostruku nultočku u ω_3 i nemati drugih nultočaka. Posebno, Eisensteinov red G_4 ima jednostruku nultočku u ω_3 i nema drugih nultočaka. Iz toga odmah vidimo da je svaka modularna forma težine 4 oblika $c \cdot G_4$ za neku konstantu c, jer za svaku takvu f je f/G_4 holomorfna modularna forma težine 0 bez nultočki.

Za $k = 6$ analogno zaključujemo i dobijemo da G_6 ima jednostruku nultočku u i te nema drugih nultočaka. Analogno je također svaka modularna forma težine 6 oblika $c \cdot G_6$ za neku konstantu c.

Onda promotrimo diskriminantu $\Delta = (g_2(\tau))^3 - 27(g_3(\tau))^2$, gdje je $g_2(\tau) = 60G_4(\tau)$, $g_3(\tau) = 140G_6(\tau)$.

Ona je cusp forma težine 12, pa iz formule valencija vidimo da nema drugih nultočaka osim ∞, te u ∞ ima jednostruku nultočku. Primijetimo da onda imamo bijekciju iz $\mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z}))$ u $\mathcal{S}_{k+12}(\mathrm{SL}_2(\mathbb{Z}))$ definiranu s $f \mapsto \Delta f$.

To je bijekcija jer ako je f cusp forma, onda je f/Δ holomorfna na $\mathcal{H}$ jer Δ tamo nema nultočaka, ali i holomorfna u ∞ jer je

$$\nu_\infty(f/\Delta) = \nu_\infty(f) - \nu_\infty(\Delta) \geq 0.$$

Dokažimo još da je skup $B = \{G_4^i G_6^j : 4i + 6j = k\}$ baza za $\mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z}))$.

Kao prvo, linearna nezavisnost slijedi direktno iz toga što svaka modularna forma iz B ima drugačiji red poništavanja u ω_3. Taj red je za $G_4^i G_6^j$ jednak i.

Nadalje, dokažimo da je ovo skup izvodnica. Za $k = 4$ i $k = 6$ smo to već dokazali, a za ostale k ćemo to dokazati matematičkom indukcijom.

Za $k \geq 8$, uzmimo $f \in \mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z}))$ i promotrimo $f - \lambda g$ za bilo koji $g \in B$, gdje je $\lambda \in \mathbb{C}$ takav da je $f - \lambda g$ cusp forma. Onda je $\frac{f-\lambda}{\Delta}$ forma težine $k-12$, a po pretpostavci indukcije svaka takva forma je polinom u G_4 i G_6, pa je i $f - \lambda g$ polinom u G_4 i G_6, te tvrdnja slijedi.

4 Heckeovi operatori i L-funkcije

4.1 Heckeovi operatori

Cilj ovog poglavlja je definirati Heckeove operatore, posebnu klasu linearnih operatora na vektorskim prostorima cusp formi $\mathcal{S}_k(\Gamma_1(N))$. Definirat ćemo i skalarni produkt uz koji su ti operatori normalni, te komutiraju. Iz toga slijedi da postoji baza za $\mathcal{S}_k(\Gamma_1(N))$ koja se sastoji od svojstvenih vektora za sve Heckeove operatore.

Sa $\mathrm{GL}_2(\mathbb{Q})^+$ ćemo označavati skup svih racionalnih 2×2 matrica s pozitivnom determinantom.

Neka su Γ_1 i Γ_2 kongruencijske podgrupe od $\mathrm{SL}_2(\mathbb{Z})$. Za $\alpha \in \mathrm{GL}_2(\mathbb{Q})^+$, definiramo dvostruki koset

$$\Gamma_1 \alpha \Gamma_2 := \{\gamma_1 \alpha \gamma_2 : \gamma_1 \in \Gamma_1, \gamma_2 \in \Gamma_2\}.$$

Grupa Γ_1 djeluje množenjem slijeva na dvostruki koset $\Gamma_1 \alpha \Gamma_2$. Dokažimo da tih orbita ima konačno mnogo.

Lema 4.1. *Neka je Γ kongruencijska podgrupa od $\mathrm{SL}_2(\mathbb{Z})$ i $\alpha \in \mathrm{GL}_2(\mathbb{Q})^+$. Tada je $\alpha^{-1}\Gamma\alpha \cap \mathrm{SL}_2(\mathbb{Z})$ također kongruencijska podgrupa od $\mathrm{SL}_2(\mathbb{Z})$.*

Dokaz. Prema definiciji kongruencijske podgrupe, postoji prirodan broj M takav da je $\Gamma(M) \leq \Gamma$, te možemo pretpostaviti da je M takav da su $M\alpha$ i $M\alpha^{-1}$ cjelobrojne matrice.

Tvrdimo da je $\Gamma(M^3) \leq \alpha^{-1}\Gamma\alpha \cap \mathrm{SL}_2(\mathbb{Z})$.

Naime, svaka matrica γ iz $\Gamma(M^3)$ je oblika $I + M^3\beta$, gdje je β cjelobrojna 2×2 matrica. Onda je $\alpha\gamma\alpha^{-1} = I + \alpha M^3 \beta \alpha^{-1} = I + M\alpha\beta(M\alpha)^{-1}$, što se nalazi u $\Gamma(M)$, pa onda i u Γ. Dakle, tvrdnja je dokazana.

□

Lema 4.2. *Neka su Γ_1 i Γ_2 kongruencijske podgrupe od $\mathrm{SL}_2(\mathbb{Z})$, te neka je $\alpha \in \mathrm{GL}_2(\mathbb{Q})^+$. Neka je $\Gamma_3 = \alpha^{-1}\Gamma_1\alpha \cap \Gamma_2$.*

Promotrimo preslikavanje iz Γ_2 u $\Gamma_1\alpha\Gamma_2$ zadano s $\gamma \mapsto \alpha\gamma$. To preslikavanje inducira prirodnu bijekciju iz skupa desnih klasa $\Gamma_3\backslash\Gamma_2$ u prostor orbita $\Gamma_1\backslash\Gamma_1\alpha\Gamma_2$. Drugim riječima, $\{\gamma_{2,j}\}_j$ je skup reprezentanata za $\Gamma_3\backslash\Gamma_2$ ako i samo ako je $\{\alpha\gamma_{2,j}\}_j$ skup reprezentanata za orbite $\Gamma_1\backslash\Gamma_1\alpha\Gamma_2$.

Dokaz. Promotrimo preslikavanje iz Γ_2 u prostor orbita $\Gamma_1\backslash\Gamma_1\alpha\Gamma_2$ definirano s $\gamma_2 \mapsto \Gamma_1\alpha\gamma_2$.

To preslikavanje je očito surjektivno, a dva elementa γ_2 i γ_2' se šalju u istu orbitu ako i samo ako je $\Gamma_1\alpha\gamma_2 = \Gamma_1\alpha\gamma_2'$, što je ekvivalentno s

$$\gamma_2'\gamma_2^{-1} \in \alpha^{-1}\Gamma_1\alpha,$$

a kako su $\gamma_2, \gamma_2' \in \Gamma_2$, to je ekvivalentno s $\gamma_2'\gamma_2^{-1} \in \Gamma_3$.

Dakle, spomenuto preslikavanje inducira bijekciju sa skupa desnih klasa $\Gamma_3\backslash\Gamma_2$ u skup orbita, pa tvrdnja slijedi.

□

Iz ove leme direktno slijedi da je prostor orbita $\Gamma_1\backslash\Gamma_1\alpha\Gamma_2$ konačan, jer je za svake dvije kongruencijske podgrupe G_1 i G_2 indeks $[G_1 : G_1 \cap G_2]$ konačan.

Sada smo spremni definirati operatore dvostrukog koseta.

Prvo ćemo proširiti definiciju operatora $[\gamma]_k$, koji su do sad bili definirani za $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, na grupu $\mathrm{GL}_2(\mathbb{Q})^+$. Za $\gamma \in \mathrm{GL}_2(Q)^+$, definiramo operator težine k na skupu funkcija $\{f : \mathcal{H} \to \mathbb{C}\}$ sa

$$(f[\gamma]_k)(\tau) := (\det\gamma)^{k-1} j(\gamma,\tau)^{-k} f(\gamma(\tau)).$$

Direktnim računom se provjeri da se svojstvo (c) iz Leme 1.24 prenosi na ovako definirane operatore težine k.

Definicija 4.3. Neka su Γ_1 i Γ_2 kongruencijske podgrupe od $\mathrm{SL}_2(\mathbb{Z})$ i neka je $\alpha \in \mathrm{GL}_2(\mathbb{Q})^+$. Definiramo *operator težine* k $[\Gamma_1\alpha\Gamma_2]_k$ iz prostora $\mathcal{M}_k(\Gamma_1)$ u prostor $\mathcal{M}_k(\Gamma_2)$ s

$$(f[\Gamma_1\alpha\Gamma_2]_k)(\tau) := \sum_j (f[\beta_j]_k)(\tau),$$

gdje suma ide po nekom skupu reprezentanata $\{\beta_j\}_j$ za skup orbita $\Gamma_1\backslash\Gamma_1\alpha\Gamma_1$.

Provjerimo da definicija ne ovisi o izboru reprezentanata. Za to je dovoljno dokazati da ako je $f \in \mathcal{M}_k(\Gamma_1)$ i vrijedi $\Gamma_1\alpha\gamma_2 = \Gamma_1\alpha\gamma_2'$ za neke $\gamma_2, \gamma_2' \in \Gamma_2$, onda je $f[\alpha\gamma_2]_k = f[\alpha\gamma_2']_k$.

Označimo s Γ_3 grupu $\alpha^{-1}\Gamma_1\alpha \cap \mathrm{SL}_2(\mathbb{Z})$. Tada se direktno vidi da je $f[\alpha]_k \in \mathcal{M}_k(\Gamma_3)$, a iz uvjeta slijedi i da je $\gamma_2'\gamma_2^{-1} \in \Gamma_3$, pa je $f[\alpha]_k[\gamma_2]_k = f[\alpha]_k[\gamma_2']_k$, i tvrdnja slijedi.

Nadalje, treba vidjeti da je $f[\Gamma_1\alpha\Gamma_2]_k$ invarijantna na djelovanje Γ_2. Neka je $\gamma_2 \in \Gamma_2$. Tada je $(f[\Gamma_1\alpha\Gamma_2]_k)[\gamma_2]_k = \sum_j f[\beta_j\gamma_2]_k$.

Međutim, ako je $\{\beta_j\}_j$ skup reprezentanata za $\Gamma_1\backslash\Gamma_1\alpha\Gamma_2$, onda je i $\{\beta_j\gamma_2\}_j$ skup reprezentanata, pa je invarijantnost dokazana.

Nadalje, treba provjeriti holomorfnost u cuspovima. To slijedi iz činjenice da je svaka $f[\beta]_k$ holomorfna u beskonačnosti za svaki $\beta \in \mathrm{GL}_2(\mathbb{Q})^+$, a zbroj funkcija holomorfnih u beskonačnosti je holomorfan u beskonačnosti (s time da je period za Fourierov razvoj možda drugačiji).

Također, može se dokazati da ako je f cusp forma, tada je i $f[\Gamma_1\alpha\Gamma_2]_k$ cusp forma, pa ima smisla restrikcija $[\Gamma_1\alpha\Gamma_2]_k : \mathcal{S}_k(\Gamma_1) \to \mathcal{S}_k(\Gamma_2)$.

Promotrimo sada neke posebne slučajeve operatora dvostrukih koseta.

(a) $\Gamma_1 \supset \Gamma_2$. Uzmimo $\alpha = I$, tada postoji samo jedna orbita, i vrijedi $f[\Gamma_1 I \Gamma_2]_k = f$, odnosno dobivamo operator inkluzije $\mathcal{M}_k(\Gamma_1) \to \mathcal{M}_k(\Gamma_2)$.

(b) $\alpha^{-1}\Gamma_1\alpha = \Gamma_2$. Tada je $\{\alpha\}$ jednočlani skup reprezentanata, i vrijedi $f[\Gamma_1\alpha\Gamma_2]_k = f[\alpha]_k$. Ovo je izomorfizam $\mathcal{M}_k(\Gamma_1) \to \mathcal{M}_k(\Gamma_2)$.

(c) $\Gamma_1 \subset \Gamma_2$. Ponovno uzmimo $\alpha = I$ i neka su $\{\gamma_{2,j}\}_j$ reprezentanti desnih klasa za $\Gamma_1\backslash\Gamma_2$. Tada je $f[\Gamma_1\alpha\Gamma_2]_k = \sum_j f[\gamma_{2,j}]_k$ (do na konstantu) projekcija $\mathcal{M}_k(\Gamma_1) \to \mathcal{M}_k(\Gamma_2)$.

Naime, za $f \in \mathcal{M}_k(\Gamma_2)$ vrijedi $f[\Gamma_1\alpha\Gamma_2]_k = [\Gamma_2 : \Gamma_1]f$.

Sada smo spremni definirati Heckeove operatore.

Neka je sada $\Gamma_1 = \Gamma_2 = \Gamma_1(N)$, i uzmimo bilo koji $\alpha \in \Gamma_0(N)$.

Tada je operator $[\Gamma_1(N)\alpha\Gamma_1(N)]_k$ jednak $[\alpha]_k$. Nadalje, prisjetimo se da postoji izomorfizam $\Gamma_0(N)/\Gamma_1(N) \to (\mathbb{Z}/N\mathbb{Z})^\times$, koji šalje matricu $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(N)$ u $d \in (\mathbb{Z}/N\mathbb{Z})^\times$, pa je operator $[\alpha]_k$ jedinstveno određen donjim desnim elementom matrice α. Dakle, za $d \in \mathbb{Z}$ relativno prost sa n, možemo definirati operator

$$\langle d\rangle : \mathcal{M}_k(\Gamma_1(N)) \to \mathcal{M}_k(\Gamma_1(N)),\ \langle d\rangle f = f[\alpha]_k,$$

gdje je α bilo koja matrica iz $\Gamma_0(N)$ čiji je donji desni element kongruentan s d modulo N. Operator $\langle d\rangle$ zovemo *dijamantni operator*. Dijamantni operatori su prvi tip Heckeovih operatora.

Za drugi tip Heckeovih operatora, neka je p uzmimo ponovno $\Gamma_1 = \Gamma_2 = \Gamma_1(N)$, te neka je p prost broj. Uzmimo matricu

$$\alpha_p = \begin{bmatrix} 1 & 0 \\ 0 & p \end{bmatrix},$$

i definiramo operator $T_p : \mathcal{M}_k(\Gamma_1(N)) \to \mathcal{M}_k(\Gamma_1(N))$ sa

$$T_p f := f[\Gamma_1(N)\alpha_p\Gamma_1(N)]_k.$$

Sljedeća propozicija daje nešto eksplicitniji opis Heckeovih operatora (odnosno daje eksplicitan opis reprezentanata dvostrukih koseta za α_p).

Propozicija 4.4. *Neka je N prirodan broj, te p prost broj. Heckeov operator $T_p : \mathcal{M}_k(\Gamma_1(N)) \to \mathcal{M}_k(\Gamma_1(N))$ je dan s*

$$T_p f = \begin{cases} \sum_{j=0}^{p-1} f[\left[\begin{smallmatrix} 1 & j \\ 0 & p \end{smallmatrix}\right]]_k & \text{ako } p \mid N, \\ \sum_{j=0}^{p-1} f[\left[\begin{smallmatrix} 1 & j \\ 0 & p \end{smallmatrix}\right]]_k + f[\left[\begin{smallmatrix} m & n \\ N & p \end{smallmatrix}\right]\left[\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right]]_k & \text{ako } p \nmid N, \end{cases}$$

gdje su m, n cijeli brojevi za koje je $mp - nN = 1$.

Dokaz. [1, 5.2.1] □

Modularne forme f iz $\mathcal{M}_k(\Gamma_1(N))$ su 1-periodične, pa imaju Fourierov razvoj

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

Za prirodan broj N, označimo s $\mathbb{1}_N$ trivijalni karakter mod N, odnosno $\mathbb{1}_N(k) = 0$ ako $\gcd(N, k) > 1$ i $\mathbb{1}_N(k) = 1$ inače.

Sljedeća propozicija govori o Fourierovom razvoju od $T_p f$.

Propozicija 4.5. *Neka je $f \in \mathcal{M}_k(\Gamma_1(N))$. Tada je*

$$\begin{aligned}(T_p f)(\tau) &= \sum_{n=0}^{\infty} a_{np}(f) q^n + \mathbb{1}_N(p) p^{k-1} \sum_{n=0}^{\infty} a_n(\langle p \rangle f) q^{np} \\ &= \left(a_{np}(f) + \mathbb{1}_N(p) p^{k-1} a_{n/p}(\langle p \rangle f)\right) q^n.\end{aligned}$$

Dokaz. Za prvi dio sume, izračunajmo za $j \in \{0, 1, \ldots, p-1\}$ kako matrica $\alpha_j = \left[\begin{smallmatrix} 1 & j \\ 0 & 1 \end{smallmatrix}\right]$ djeluje na f. Vrijedi:

$$\begin{aligned}(f[\alpha_j]_k)(\tau) &= p^{k-1}(0\tau + p)^{-k} f\left(\frac{\tau + j}{p}\right) \\ &= \frac{1}{p} \sum_{n=0}^{\infty} a_n e^{2\pi i \tau/p} e^{2\pi i j n/p}.\end{aligned}$$

Sumiranjem $e^{2\pi i j n/p}$ po $j \in \{0, 1, \ldots, p-1\}$ dobivamo 0 ako su n i p relativno prosti i p inače, pa iz toga dobivamo prvi član u formuli za $a_n(T_p f)$.

Za drugi dio, potrebno je izračunati kako matrica $\alpha = \left[\begin{smallmatrix} m & n \\ N & p \end{smallmatrix}\right]\left[\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right]$ djeluje na f.

Matrica $\left[\begin{smallmatrix} m & n \\ N & p \end{smallmatrix}\right]$ djeluje kao dijamantni operator $\langle p \rangle$ jer joj je p donji desni element, pa je

$$f[\alpha]_k = \langle p \rangle f[\left[\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right]]_k.$$

Direktno po definiciji, to je jednako

$$p^{k-1}(0\tau + 1)^{-k}(\langle p \rangle f)(p\tau) = p^{k-1} \sum_{n=0}^{\infty} a_n(\langle p \rangle f) q^{np},$$

iz čega slijedi tvrdnja koju smo trebali dokazati. □

Heckeovi operatori međusobno komutiraju.

Propozicija 4.6. *Neka su $d, e \in (\mathbb{Z}/N\mathbb{Z})^\times$ i neka su p, q prosti. Tada vrijedi*

(a) $\langle d\rangle T_p = T_p\langle d\rangle$,

(b) $\langle d\rangle\langle e\rangle = \langle e\rangle\langle d\rangle = \langle de\rangle$,

(c) $T_pT_q = T_qT_p$.

Dokaz. [1, 5.2.4]. □

Do sada smo definirali operatore $\langle d\rangle$ za d relativno prost sa N. Za d koji nije relativno prost sa N definiramo $\langle d\rangle$ kao nul-operator.

Uz ovu definiciju naravno vrijedi $\langle d\rangle\langle e\rangle = \langle de\rangle$ za sve $d, e \in \mathbb{N}$.

Sada ćemo definirati operatore T_n za složene n.

Kao prvo, definiramo T_1 kao identitetu na $\mathcal{M}_k(\Gamma_1(N))$. Nadalje, za prost broj p i za $r \geq 2$, definiramo

$$T_{p^r} = T_pT_{p^{r-1}} - p^{k-1}\langle p\rangle T_{p^{r-2}}.$$

Konačno, za n čija faktorizacija na proste faktore je $p_1^{e_1}\cdot\ldots\cdot p_k^{e_k}$ definiramo

$$T_n = T_{p_1^{e_1}} \cdot \ldots \cdot T_{p_k^{e_k}}.$$

Uz ovakve definicije, iz propozicije 4.6 slijedi da svi Heckeovi operatori međusobno komutiraju.

Promotrimo (formalnu) funkciju izvodnicu za operatore T_n,

$$g(s) = \sum_{n=1}^{\infty} T_n n^{-s}.$$

Tada iz definicije za proste potencije slijedi

$$g(s) = \prod_{p \text{ prost}} (1 - T_p p^{-s} + \langle p\rangle p^{k-1-2s})^{-1}. \tag{7}$$

Sljedeća propozicija govori o Fourierovim koeficijentima od T_nf.

Propozicija 4.7. *Neka su n i N prirodni brojevi, te neka je $f \in \mathcal{M}_k(\Gamma_1(N))$ s Fourierovim razvojem*

$$f(\tau) = \sum_{m=0}^{\infty} a_m(f)q^m.$$

Tada T_nf ima Fourierov razvoj

$$(T_nf)(\tau) = \sum_{m=0}^{\infty} a_m(T_nf)q^m,$$

gdje je

$$a_m(T_n f) = \sum_{d|\gcd(m,n)} d^{k-1} a_{mn/d^2}(f).$$

Dokaz. [1, 5.3.1]. □

Kako su Heckeovi operatori komponirani od operatora dvostrukih koseta, oni šalju cusp forme u cusp forme.

Sada je cilj definirati skalarni produkt na prostoru cusp formi $\mathcal{S}_k(\Gamma_1(N))$, u odnosu na koji su Heckeovi operatori normalni.

Definiramo hiperboličnu mjeru na gornjoj poluravnini $\mathcal{H}$ sa

$$d\mu(\tau) = d\mu(x+iy) = \frac{dxdy}{y^2}.$$

Ta mjera je invarijantna pod djelovanjem grupe $\mathrm{GL}_2(\mathbb{R})^+$ realnih 2×2 matrica s pozitivnom determinantom, odnosno vrijedi $\mu(\alpha(S)) = \mu(S)$ za sve izmjerive skupove $S \subset \mathcal{H}$ i sve $\alpha \in \mathrm{GL}_2(\mathbb{R})^+$.

Mjeru možemo koristiti i za integriranje na proširenoj gornjoj poluravnini $\mathcal{H}^* = \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$, tako da stavimo $\mu(\mathbb{P}^1(\mathbb{Q})) = 0$.

Fundamentalna domena za djelovanje $\mathrm{SL}_2(\mathbb{Z})$ na $\mathcal{H}^*$ je skup

$$\mathcal{D}^* = \{\tau \in \mathcal{H} : \mathrm{Re}(\tau) \in [-1/2, 1/2], |\tau| \geq 1\} \cup \{\infty\}.$$

Modularnu krivulju $X(1)$ možemo identificirati s $\mathcal{D}^*$.

Primijetimo da je

$$\begin{aligned}\int_{\mathcal{D}^*} \frac{dxdy}{y^2} &= \int_{-1/2}^{1/2} \int_{\sqrt{1-x^2}} \frac{dy}{y^2} dx \\ &= \int_{-1/2}^{1/2} \frac{dx}{\sqrt{1-x^2}} \\ &= \frac{\pi}{3} < \infty,\end{aligned}$$

pa je integral svake ograničene neprekidne funkcije po $\mathcal{D}^*$ po mjeri μ konačan.

Neka je Γ kongruencijska podgrupa od $\mathrm{SL}_2(\mathbb{Z})$, te neka su $\{\alpha_j\}_j$ reprezentanti za desne klase $\{\pm I\}\Gamma\backslash \mathrm{SL}_2(\mathbb{Z})$, odnosno imamo disjunktnu uniju

$$\mathrm{SL}_2(\mathbb{Z}) = \bigcup_j \{\pm I\}\Gamma\alpha_j.$$

Tada za Γ-invarijantnu funkciju $\varphi : \mathcal{H} \to \mathbb{C}$ suma

$$\sum_j \int_{\mathcal{D}^*} \varphi(\alpha(\tau)) d\mu(\tau) = \int_{\cup \alpha_j(\mathcal{D}^*)} \varphi(\tau) d\mu(\tau)$$

ne ovisi o izboru reprezentanata $\{\alpha_j\}_j$, te ima smisla definirati

$$\int_{X(\Gamma)} \varphi(\tau) d\mu(\tau) := \sum_j \int_{\mathcal{D}^*} \varphi(\alpha(\tau)) d\mu(\tau).$$

Posebno, za $\varphi = 1$, definiramo volumen od Γ, u oznaci V_Γ, kao $\int_{X(\Gamma)} 1 d\mu(\tau)$. Po definiciji, imamo

$$V_\Gamma = [\mathrm{SL}_2(\mathbb{Z}) : \{\pm I\}\Gamma] \cdot V_{\mathrm{SL}_2(\mathbb{Z})} = [\mathrm{SL}_2(\mathbb{Z}) : \{\pm I\}\Gamma] \cdot \frac{\pi}{3}.$$

Neka su sada $f, g \in \mathcal{S}_k(\Gamma)$ cusp forme. Tada je funkcija $f(\tau)\overline{g(\tau)}(\mathrm{Im}\,\tau)^k$ neprekidna i Γ-invarijantna, te se može pokazati da je ograničena na $\mathcal{H}$ promatrajući njen Fourierov razvoj (ovdje se koristi činjenica da su f i g cusp forme). Dakle, definicija koja slijedi je dobra.

Definicija 4.8. Neka je Γ kongruencijska podgrupa od $\mathrm{SL}_2(\mathbb{Z})$. *Peterssonov skalarni produkt* $\langle , \rangle_\Gamma : \mathcal{S}_k(\Gamma)^2 \to \mathbb{C}$ na vektorskom prostoru $\mathcal{S}_k(\Gamma)$ definiran je s

$$\langle f, g \rangle_\Gamma := \frac{1}{V_\Gamma} \int_{X(\Gamma)} f(\tau)\overline{g(\tau)}\,\mathrm{Im}(\tau)^k d\mu(\tau).$$

Napomena 4.9. Normalizacijski faktor $\frac{1}{V_\Gamma}$ služi za to da ako je $\Gamma' \subset \Gamma$, onda se Peterssonov skalarni produkt u odnosu na Γ i Γ' poklapaju na $\mathcal{S}_k(\Gamma)$.

U odnosu na ovaj skalarni produkt na $\mathcal{S}_k(\Gamma_1(N))$, može se izračunati operatore adjungirane Heckeovim operatorima.

Teorem 4.10. *U unitarnom prostoru $\mathcal{S}_k(\Gamma_1(N))$ s Peterssonovim skalarnim produktom, adjungirani operatori Heckeovih operatora T_p i $\langle p \rangle$ za $p \nmid N$ su*

$$\langle p \rangle^* = \langle p \rangle^{-1}, \quad T_p^* = \langle p \rangle^{-1} T_p.$$

Dakle, Heckeovi operatori $\langle n \rangle$ i T_n za n relativno prost s N su normalni.

Dokaz. [1, 5.5.3]. □

Iz linearne algebre znamo da ako je $\{A_j\}_j$ familija međusobno komutirajućih normalnih linearnih operatora na konačnodimenzionalnom vektorskom prostoru V, onda postoji baza za V koja se sastoji od međusobno ortogonalnih vektora koji su svojstveni vektori za sve operatore A_j odjednom. U našoj posebnoj situaciji, imamo sljedeću tvrdnju.

Teorem 4.11. *Prostor $\mathcal{S}_k(\Gamma_1(N))$ ima ortogonalnu bazu sastavljenu od simultanih svojstvenih vektora za sve Heckeove operatore*

$$\{\langle n \rangle, T_n : \gcd(n, N) = 1\}.$$

Bilo koju cusp formu koja je svojstveni vektor za sve Heckeove operatore ćemo zvati *svojstvena forma*.

Primijetimo da ako $M \mid N$, onda je $\mathcal{S}_k(\Gamma_1(M)) \subset \mathcal{S}_k(\Gamma_1(N))$.

Postoji i drugo ulaganje od $\mathcal{S}_k(\Gamma_1(M))$ u $\mathcal{S}_k(\Gamma_1(N))$. Naime, neka je d bilo koji djelitelj od N/M, i neka je $\alpha_d = \left[\begin{smallmatrix} d & 0 \\ 0 & 1 \end{smallmatrix}\right]$. Tada za svaku $f \in \mathcal{S}_(\Gamma_1(M))$ vrijedi da je

$$(f[\alpha_d]_k)(\tau) = d^{k-1} f(d\tau) \in \mathcal{S}_k(\Gamma_1(N)).$$

Ima smisla odvojiti forme iz $\mathcal{S}_k(\Gamma_1(N))$ koje na neki od ova dva načina nastaju od formi s niže razine, odnosno iz formi iz $\mathcal{S}_k(\Gamma_1(M))$ za neki $M \mid N$, pa to motivira sljedeću definiciju.

Definicija 4.12. Za svaki djelitelj d od N, definiramo preslikavanje

$$i_d : \mathcal{S}_k(\Gamma_1(N/d))^2 \to \mathcal{S}_k(\Gamma_1(N)), \quad i_d(f,g) = f + g[\alpha_d]_k.$$

Potprostor *starih formi* na razini N definiramo kao

$$\mathcal{S}_k(\Gamma_1(N))^{\text{old}} = \sum_{\substack{p \mid N \\ p \text{ prost}}} i_p(S_k(\Gamma_1(N/p))^2).$$

Nadalje, definiramo prostor *novih formi* na razini N kao ortogonalni komplement (u odnosu na Peterssonov skalarni produkt)

$$\mathcal{S}_k(\Gamma_1(N))^{\text{new}} = \left(S_k(\Gamma_1(N))^{\text{old}}\right)^{\perp}$$

Napomena 4.13. U definiciji prostora starih formi uzima se suma slika i_p za proste djelitelje p od N, ali može se pokazati da se isti rezultat dobije ako se umjesto toga sumira po slikama i_d za sve djelitelje d od N.

Ovako definirani potprostori se lijepo ponašaju pod Heckeovim operatorima.

Propozicija 4.14. *Potprostori $S_k(\Gamma_1(N))^{old}$ i $S_k(\Gamma_1(N))^{new}$ su invarijantni za Heckeove operatore T_n i $\langle n \rangle$ za sve $n \in \mathbb{N}$.*

Dokaz. [1, 5.6.2] □

Posljedica propozicije je da i prostori $S_k(\Gamma_1(N))^{\text{old}}$ i $S_k(\Gamma_1(N))^{\text{new}}$ imaju ortogonalne baze sastavljene od simultanih svojstvenih formi za sve Heckeove operatore T_n za koje je $\gcd(n, N) = 1$.

Definicija 4.15. Za nenul modularnu formu $f \in \mathcal{M}_k(\Gamma_1(N))$ koja je svojstveni vektor za Heckeove operatore T_n i $\langle n \rangle$ za sve $n \in \mathbb{N}$ kažemo da je *Heckeova svojstvena forma* ili kraće *svojstvena forma*.

Za svojstvenu formu $f = \sum_{n=0}^{\infty} a_n(f)q^n$ kažemo da je *normalizirana* ako je $a_1(f) = 1$. *Nova forma* je normalizirana svojstvena forma iz prostora $S_k(\Gamma_1(N))^{\text{new}}$.

Dirichletov karakter modulo N je homomorfizam grupa $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^*$. Dirichletove karaktere možemo standardno proširiti do funkcija na cijelom $\mathbb{N}$ tako da definiramo $\chi(n) = 0$ ako je $\gcd(n, N) > 1$ te proširimo χ po N-periodičnosti.

Dirichletovi karakteri modulo N čine grupu s obzirom na množenje po točkama, te je ta grupa izomorfna s $(\mathbb{Z}/N\mathbb{Z})^\times$.

Za Dirichletov karakter χ, definiramo njegov svojstveni potprostor

$$\mathcal{M}_k(N, \chi) = \{f \in \mathcal{M}_k(\Gamma_1(N)) : f[\gamma]_k = d_\gamma f \text{ za sve } \gamma \in \Gamma_0(N)\}.$$

Analogno definiramo $\mathcal{S}_k(N, \chi)$.

Lema 4.16. *Vektorski prostor $\mathcal{M}_k(\Gamma_1(N))$ je direktna suma svojstvenih potprostora pridruženih Dirichletovim karakterima, odnosno*

$$\mathcal{M}_k(\Gamma_1(N)) = \bigoplus_{\chi} \mathcal{M}_k(N, \chi).$$

Analogna tvrdnja vrijedi i za prostor cusp formi $\mathcal{S}_k(\Gamma_1(N))$.

Dokaz. [1, 4.3, Exercise 1]. □

Teorem 4.17. *Skup novih formi iz prostora $\mathcal{S}_k(\Gamma_1(N))^{new}$ čini ortogonalnu bazu za taj prostor. Svaka od tih novih formi leži u nekom svojstvenom potprostoru $\mathcal{S}_k(N, \chi)$, te vrijedi $T_n f = a_n(f)f$. Drugim riječima, n-ti Fourierov koeficijent od f je svojstvena vrijednost za T_n za koju je f svojstveni vektor.*

Dokaz. [1, 5.8.2]. □

4.2 L-funkcije pridružene modularnim formama

Svakoj modularnoj formi $f \in \mathcal{M}_k(\Gamma_1(N))$ možemo pridružiti L-funkciju na sljedeći način.

Definicija 4.18. Neka je $f \in \mathcal{M}_k(\Gamma_1(N))$ modularna forma s Fourierovim razvojem $f(\tau) = \sum_{n=0}^{\infty} a_n(f)q^n$. Definiramo njenu L-funkciju

$$L(s, f) = \sum_{n=1}^{\infty} a_n(f)n^{-s}.$$

Sljedeća propozicija govori o konvergenciji L-funkcija modularnih formi.

Propozicija 4.19. *Ako je $f \in \mathcal{M}_k(\Gamma_1(N))$ cusp forma, onda $L(s,f)$ konvergira apsolutno za sve s sa $\mathrm{Re}(s) > k/2+1$. Ako f nije cusp forma, onda $L(s,f)$ konvergira apsolutno za sve s sa $\mathrm{Re}(s) > k$.*

Skica dokaza. Dokazat ćemo tvrdnju samo za cusp forme. Ideja je ograditi koeficijente a_n odozgo koristeći Cauchyjevu integralnu formulu.

Neka je $g(q) = \sum_{n=1}^{\infty} a_n q^n$. To je holomorfna funkcija na disku $\{|q| < 1\}$, pa po Cauchyjevoj integralnoj formuli za svaki $r \in (0,1)$ vrijedi

$$a_n = \int_{|q|=r} g(q) q^{-(n+1)} dq.$$

Zamjenom varijabli $q = e^{2\pi i(x+iy)}$ za svaki $y > 0$ dobivamo

$$a_n = \int_0^1 f(x+iy) e^{-2\pi i n(x+iy)} dx.$$

Posebno, za $y = n$ dobivamo

$$a_n = e^{2\pi} \int_0^1 f(x+i/n) e^{-2\pi i n x} dx.$$

Sada koristimo činjenicu da za cusp forme vrijedi da je $|f(\tau)\,\mathrm{Im}(\tau)^{k/2}|$ ograničeno na $\mathcal{H}$, i dobivamo $|f(x+i/n)| \leq C n^{k/2}$ za neku konstantu C, iz čega slijedi $|a_n| \leq e^{2\pi} C n^{k/2} = \mathcal{O}(n^{k/2})$ (ovdje je bitno naglasiti da konstanta C ne ovisi o n).

Tvrdnja sada lagano slijedi jer je onda $|a_n n^{-s}| = \mathcal{O}(n^{k/2-\mathrm{Re}(s)})$, pa za $k/2 - \mathrm{Re}(s) < -1$ dobivamo traženu apsolutnu konvergenciju.

Argument za forme koje nisu cusp forme se nalazi u [1, 5.9.1]. □

L-funkcije normaliziranih svojstvenih formi su posebno lijepe. Moguće ih je zapisati kao Eulerov produkt. Preciznije, vrijedi sljedeća tvrdnja.

Teorem 4.20. *Neka je χ Dirichletov karakter modulo N i neka je $f \in \mathcal{M}_k(N,\chi)$, $f(\tau) = \sum_{n=0}^{\infty} a_n q^n$. Tada je f normalizirana svojstvena forma ako i samo ako vrijedi*

$$L(s,f) = \prod_{p \text{ prost}} (1 - a_p p^{-s} + \chi(p) p^{k-1-2s})^{-1}.$$

Dokaz. [1, 5.9.2]. □

Korolar 4.21. *Neka je $f \in \mathcal{S}_2(\Gamma_0(N))$ nova forma. Tada je*

$$L(s,f) = \prod_{p\nmid N}(1 - a_p(f)p^{-s} + p^{1-2s})^{-1} \prod_{p|N}(1 - a_p(f)p^{-s})^{-1}.$$

Korolar slijedi direktno iz teorema i činjenice da je $\mathcal{S}_k(\Gamma_0(N))$ zapravo jednak $\mathcal{S}_k(N, \mathbb{1}_N)$, gdje je $\mathbb{1}_N$ trivijalni karakter modulo N.

Još jedna bitna činjenica o L-funkcijama cusp formi $f \in \mathcal{S}_k(\Gamma_1(N))$ je da imaju analitičko proširenje na cijeli $\mathbb{C}$.

4.3 L-funkcije pridružene eliptičkim krivuljama

Eliptička krivulja nad poljem k je glatka projektivna ravninska krivulja genusa 1 definirana nad k, zajedno s istaknutom k-racionalnom točkom.

Svaka eliptička krivulja nad poljem $\mathbb{Q}$ je izomorfna krivulji u projektivnom prostoru $\mathbb{P}^2$ zadanoj jednadžbom

$$y^2z = x^3 + axz^2 + bz^3,$$

gdje su a i b racionalni brojevi takvi da polinom $x^3 + ax + b$ nema dvostrukih nultočaka, te je istaknuta točka $\mathcal{O} = (0 : 1 : 0)$.

Jednadžbu $y^2 = x^3 + ax + b$ zovemo Weierstrassov model za eliptičku krivulju.

Sada definiramo zeta funkcije eliptičkih krivulja.

Neka je V (afina ili projektivna) mnogostrukost definirana nad poljem $\mathbb{F}_q$, gdje je $q = p^r$ potencija prostog broja p. Sa $\#\mathbb{F}_q(V)$ označimo broj točaka na V iz $\mathbb{F}_q$. Definiramo kongruencijsku zeta funkciju od V u odnosu na $\mathbb{F}_q$ kao formalni red potencija

$$Z(V/\mathbb{F}_q; T) := \exp\left(\sum_{n=1}^{\infty} \#\mathbb{F}_{q^n}(V)\frac{T^n}{n}\right),$$

gdje je $\exp(X) := \sum_{n=0}^{\infty} \frac{X^n}{n!}$.

Dwork je dokazao da je zeta funkcija mnogostrukosti racionalna funkcija, odnosno element skupa $\mathbb{Q}(T)$.

Posebno, za zeta funkciju eliptičke krivulje, situacija je sljedeća.

Za prost broj p i eliptičku krivulju E definiranu nad $\mathbb{F}_p$, vrijedi

$$Z(E/\mathbb{F}_p; T) = \frac{1 - a_pT + pT^2}{(1 - T)(1 - pT)},$$

gdje je a_p cijeli broj takav definiran s $a_p = p+1-\#E(\mathbb{F}_p)$. Prema Hasseovom teoremu, vrijedi $|a_p| \leq 2\sqrt{p}$.

Koristeći ove rezultate, možemo jednostavnim uspoređivanjem koeficijenata preko broja točaka nad $\mathbb{F}_p$ odrediti broj točaka nad $\mathbb{F}_{p^r}$ za svaki r.

Naime, označimo sa α i $\overline{\alpha}$ recipročne nultočke brojnika, tako da je

$$Z(E/\mathbb{F}_p;T) = \frac{(1-\alpha T)(1-\overline{\alpha}T)}{(1-T)(1-pT)}.$$

Tada je $\#E(\mathbb{F}_{p^r}) = p^r + 1 - \alpha^r - \overline{\alpha}^r$, te vrijedi $\alpha\overline{\alpha} = p$ i $\alpha + \overline{\alpha} = a_p$.

Neka je E eliptička krivulja definirana nad $\mathbb{Q}$. Tada redukcija od E modulo p definira eliptičku krivulju nad $\mathbb{F}_p$ ako i samo ako p ne dijeli diskriminantu minimalnog modela od E. Inače kažemo da je redukcija loša.

Zbog jednostavnosti pretpostavimo da je $p \neq 2, 3$, tako da možemo pretpostaviti da je E definirana jednadžbom oblika

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

te da je to njen minimalni model.

Tada je redukcija loša ako i samo ako $x^3 + ax + b$ ima dvostruku ili trostruku nultočku modulo p, odnosno ako je redukcija modulo p oblika

$$y^2 = (x-u)^2(x-v).$$

Ako je $u = v$, kažemo da je redukcija aditivna, a ako je $u \neq v$ kažemo da je multiplikativna. Za multiplikativnu redukciju kažemo da je rascjepiva ako je $u - v$ kvadrat u $\mathbb{F}_p$, a inače kažemo da je nerascjepiva.

Ovisno o tipu redukcije modulo p, definiramo L-faktor $L_p(T)$ na sljedeći način:

$$L_p(T) = \begin{cases} 1 - a_pT + pT^2, & \text{ako E ima dobru redukciju mod p} \\ 1 - T, & \text{ako E ima rascjepivu mult. redukciju mod p} \\ 1 + T, & \text{ako E ima nerascjepivu mult. redukciju mod p} \\ 1, & \text{ako E ima aditivnu redukciju mod p.} \end{cases}$$

Za kompleksan broj s i eliptičku krivulju E, definiramo L-funkciju od E sa

$$L(E,s) := \prod_{p \text{ prost}} L_p(p^{-s})^{-1},$$

Ako za p dobre redukcije zapišemo

$$1 - a_pp^{-s} + p^{1-2s} = (1 - \alpha_pp^{-s})(1 - \overline{\alpha_p}p^{-s}),$$

onda za $\operatorname{Re} s > \frac{3}{2}$ (da bismo imali apsolutnu konvergenciju) vrijedi

$$\frac{1}{(1-\alpha_pp^{-s})(1-\overline{\alpha_p}p^{-s})} = \left(\sum_{k\geq 0} \alpha_p^k p^{-ks}\right)\left(\sum_{k\geq 0} \overline{\alpha_p}^k p^{-ks}\right).$$

Uzimanjem produkta po svim prostim brojevima i promatranjem koeficijenata uz n^{-s}, možemo zapisati L-funkciju kao Dirichletov red:

$$L(E,s) = \sum_{n=1}^{\infty} a_n n^{-s}.$$

Oznaka je u skladu s prethodnim oznakama jer se značenje koeficijenata a_{p^r} za proste brojeve s dobrom redukcijom poklapa s prijašnjom oznakom. Nadalje, vrijedi $a_{mn} = a_m a_n$ za relativno proste m, n.

Neka je E eliptička krivulja nad $\mathbb{Q}$. Za prost broj p, definiramo broj f_p sa

$$f_p = \begin{cases} 0, & \text{ako } E \text{ ima dobru redukciju mod } p, \\ 1, & \text{ako } E \text{ ima multiplikativnu redukciju mod } p, \\ 2, & \text{ako } E \text{ ima aditivnu redukciju mod } p \text{ i } p \neq 2,3, \\ 2+\delta_p, & \text{ako } E \text{ ima aditivnu redukciju mod } p \text{ i } p \in \{2,3\}, \end{cases}$$

gdje su $0 \leq \delta_2 \leq 6$ i $0 \leq \delta_3 \leq 3$ tehničke invarijante koje je teže definirati. Egzaktna definicija može se naći u [8, 4.10].

Pomoću brojeva f_p definiramo *konduktor* eliptičke krivulje E kao prirodan broj N definiran s

$$N_E := \prod_p p^{f_p},$$

gdje je umnožak po svim prostim brojevima (primijetimo da je umnožak konačan jer samo za konačno mnogo prostih brojeva imamo lošu redukciju).

Važnost konduktora je sljedeća.

Teorem 4.22. *Neka je E eliptička krivulja nad $\mathbb{Q}$. Tada je N_E najmanji prirodan broj za koji postoji modularna parametrizacija $X_0(N_E) \to E$ u smislu teorema 2.19.*

Sada smo spremni izreći još dvije verzije teorema o modularnosti.

Teorem 4.23 (Teorem o modularnosti, verzija s koeficijentima a_p)**.** *Neka je E eliptička krivulja definirana nad $\mathbb{Q}$ čiji konduktor je N_E. Tada postoji nova forma $f \in \mathcal{S}_2(\Gamma_0(N_E))$ takva da za svaki prost broj p vrijedi*

$$a_p(E) = a_p(f).$$

Ove jednakosti možemo izreći i preko L-funkcija.

Teorem 4.24 (Teorem o modularnosti, verzija s L-funkcijama)**.** *Neka je E eliptička krivulja definirana nad $\mathbb{Q}$ čiji konduktor je N_E. Tada postoji nova forma $f \in \mathcal{S}_2(\Gamma_0(N_E))$ takva da vrijedi*

$$L(s,E) = L(s,f).$$

Jedna od posljedica ove verzije teorema o modularnosti je činjenica da L-funkcije eliptičkih krivulja imaju analitičko proširenje na cijeli $\mathbb{C}$, jer to vrijedi za L-funkcije novih formi iz $\mathcal{S}_2(\Gamma_0(N_E))$.

Ispada da postoji duboka veza između L-funkcija eliptičkih krivulja i nekih aritmetičkih svojstava eliptičkih krivulja. Najpoznatija slutnja vezana za to je slutnja Bircha i Swinnerton-Dyera, koja povezuje rang eliptičke krivulje (odnosno rang grupe racionalnih točaka) s redom poništavanja L-funkcije u točki 1.

Slutnja 4.25 (Slutnja Bircha i Swinnerton-Dyera)**.** *Neka je E eliptička krivulja nad $\mathbb{Q}$. Tada je red poništavanja od $L(s, E)$ u točki 1 jednak rangu grupe racionalnih točaka $E(\mathbb{Q})$. Drugim riječima, ako je $E(\mathbb{Q})$ ranga r, onda je*

$$L(s, E) = (s-1)^r g(s)$$

za neku meromorfnu funkciju g koja nema ni nultočku ni pol u točki 1.

5 Modularni pristup diofantskim jednadžbama

U ovom poglavlju ćemo pokazati primjenu teorema o modularnosti na diofantske jednadžbe na primjeru velikog Fermatovog teorema. Ovo poglavlje bazira se na bilješkama [7].

Teorem 5.1 (veliki Fermatov teorem)**.** *Neka je $n \geq 3$ prirodan broj. Ne postoje prirodni brojevi a, b, c takvi da je*

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

Teorem je dokazao Andrew Wiles 1995. godine [11]. Wiles je zapravo dokazao teorem o modularnosti za semistabilne eliptičke krivulje.

Teorem o modularnosti za sve eliptičke krivulje su 2001. dokazali Breuil, Conrad, Diamond i Taylor.

U ovom poglavlju ćemo pretpostavljati da je svaka nova forma težine 2.

Trebat će nam nekoliko pomoćnih rezultata. Iskažimo prvo ponovno verziju teorema o modularnosti koju ćemo koristiti.

Teorem 5.2. *Za svaku novu formu $f = \sum_{n\in\mathbb{N}} a_n(f)q^n \in \mathcal{S}_2(\Gamma_0(N))$ s racionalnim Fourierovim koeficijentima postoji (do na izogeniju) jedinstvena eliptička krivulja E_f konduktora N takva da vrijedi*

$$a_p(f) = a_p(E_f)$$

za sve proste brojeve p koji ne dijele N.

Jedan smjer ovog teorema (surjektivnost preslikavanja $f \mapsto E_f$) je zapravo isti kao teorem 4.23. Drugi smjer je poznat još od 1959. pod nazivom Eichler-Shimura relacija.

Primijetimo da ovo ne govori da sve nove forme iz $\mathcal{S}_2(\Gamma_0(N))$ imaju racionalne Fourierove koeficijente. Ta tvrdnja niti ne vrijedi. Sljedeća propozicija govori o svojstvima koeficijenata novih formi.

Propozicija 5.3. *Neka je $f = q + \sum_{n\geq 2} a_n q^n$ nova forma iz $\mathcal{S}_2(\Gamma_0(N))$. Tada je $K = \mathbb{Q}(a_2, a_3, \ldots)$ totalno realno konačno proširenje od $\mathbb{Q}$, te su koeficijenti a_i algebarski cijeli brojevi. Nadalje, za svaki prost broj p i svako ulaganje $\sigma : K \to \mathbb{C}$ vrijedi*

$$|\sigma(a_p)| \leq 2\sqrt{p}.$$

Vratimo se velikom Fermatovom teoremu. Primijetimo da je dovoljno riješiti slučaj kad je n prost. Nadalje, slučajevi za $n = 3$ i $n = 4$ su klasični i poznati rezultati.

Pretpostavimo onda da je $p > 3$ prost broj te da su a, b, c cijeli brojevi različiti od 0 takvi da je

$$a^p + b^p + c^p = 0.$$

Bez smanjenja općenitosti možemo pretpostaviti da je $a \equiv -1 \pmod 4$ i da je b paran, te da su a, b, c u parovima relativno prosti.

Sad je ideja ovom hipotetskom rješenju (a, b, c) pridružiti eliptičku krivulju. Neka je E zadana jednadžbom

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

Diskriminanta minimalnog modela od E je jednaka

$$\Delta_{\min} = \frac{(abc)^{2p}}{2^8},$$

a konduktor je jednak

$$N = \mathrm{rad}(abc).$$

Krivulju E zovemo Freyova krivulja.

Ideja je sada Freyovoj krivulji pridružiti novu formu iz određenog prostora. Ali taj prostor će prema formulama za dimenzije biti trivijalan, i dobit ćemo kontradikciju.

Međutim, ako direktno pokušamo primijeniti teorem o modularnosti na E, nećemo dobiti ništa pametno jer konduktor N ovisi o rješenju. Zato trebamo teorem kojim ćemo spustiti N, odnosno spustiti razinu modularne forme pridružene našoj eliptičkoj krivulji. Prvo trebamo neke definicije.

Definicija 5.4. Neka je E eliptička krivulja nad $\mathbb{Q}$ konduktora N, i neka je f nova forma iz $\mathcal{S}_k(\Gamma_0(N'))$, te neka je K polje generirano njenim Fourierovim koeficijentima. Neka je p prost broj. Kažemo da E dolazi od f modulo p i pišemo $E \sim_p f$ ako postoji prost ideal $\mathfrak{p}$ od $\mathcal{O}_K$ iznad p takav da za sve osim konačno mnogo prostih brojeva ℓ vrijedi $a_\ell(f) \equiv a_\ell(E) \pmod{\mathfrak{p}}$.

Neka je E eliptička krivulja nad $\mathbb{Q}$ te neka su N i $\Delta_{\min}$ njeni konduktor i minimalna diskriminanta. Za prost broj p, definiramo broj N_p kao

$$N_p = N \Big/ \prod_{\substack{q \text{ prost} \\ \nu_q(N)=1 \\ p \mid \nu_q(\Delta_{\min})}} q.$$

Teorem 5.5 (Ribetov teorem o spuštanju razine)**.** *Neka je E eliptička krivulja nad $\mathbb{Q}$ i $p \geq 5$ prost broj. Pretpostavimo da E nema p-izogenija. Neka je N_p definiran kao gore. Tada postoji nova forma $f \in \mathcal{S}_2(\Gamma_0(N_p))$ takva da*

$$E \sim_p f.$$

Napomena 5.6. Ovo je zapravo pojednostavljena verzija Ribetovog teorema o spuštanju razine. Teorem po iskazu izgleda neovisno o teoremu o modularnosti, ali u dokazu se koristi teorem o modularnosti, odnosno činjenica da je E modularna.

Još smo dužni definirati što je p-izogenija. U drugom poglavlju smo definirali izogenije među kompleksnim torusima (odnosno eliptičkim krivuljama nad $\mathbb{C}$) kao nenul holomorfne homomorfizme između njih koji fiksiraju 0.

Možemo ih definirati i algebarski, kao nekonstantne morfizme između krivulja $\varphi : E_1 \to E_2$ definiranih nad poljem k takve da je $\varphi(\mathcal{O}_1) = \mathcal{O}_2$, gdje su $\mathcal{O}_1$ i $\mathcal{O}_2$ neutralni elementi za zbrajanje na E_1 i E_2.

Svaki morfizam φ inducira ulaganje funkcijskih polja $\varphi^* : \overline{k}(E_2) \hookrightarrow \overline{k}(E_1)$, gdje je $\overline{k}$ algebarsko zatvorenje od k. Stupanj izogenije φ je onda stupanj proširenja

$$[\overline{k}(E_1) : \varphi^*(\overline{k}(E_2))],$$

a za izogeniju stupnja N kraće kažemo da je N-izogenija. Više o izogenijama se može pronaći u [9, Chapter 4].

Sljedeći rezultat daje neke dovoljne uvjete da eliptička krivulja nema p-izogenija.

Za eliptičku krivulju E nad $\mathbb{Q}$ kažemo da je *semistabilna* ako ne postoji prost broj p takav da je redukcija od E modulo p aditivna.

Teorem 5.7 (Mazur)**.** *Neka je E eliptička krivulja nad $\mathbb{Q}$ i p prost broj, te pretpostavimo da vrijedi barem jedan od sljedećih uvjeta:*

- *$p \geq 17$ i $j(E) \notin \mathbb{Z}[1/2]$,*
- *$p \geq 11$ i E je semistabilna,*
- *$p \geq 5$ i $\#E(\mathbb{Q})[2] = 4$, odnosno E ima četiri racionalne točke P takve da je $P + P = \mathcal{O}$, te je E semistabilna.*

Tada E nema p-izogenija.

Ove tvrdnje su dovoljne za dokaz Velikog Fermatovog teorema. Vratimo se na Freyovu krivulju

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

Za nju je N_p jednak 2. Naime, za svaki prost broj q osim 2 koji dijeli $N = \mathrm{rad}(abc)$ vrijedi da $p \mid \nu_q(\Delta_{\min})$.

Nadalje, E je semistabilna jer ako bi redukcija modulo neki prost broj q bila aditivna, imali bismo da $x(x - a^p)(x + b^p)$ ima trostruku nultočku

modulo q, ali onda $q \mid a^p$ i $q \mid b^p$, kontradikcija s relativnom prostošću. Konačno, $\#E(\mathbb{Q})[2]$ je očito jednak 4, to su točke $\mathcal{O}, (0,0), (a^p, 0), (-b^p, 0)$. Zaključujemo da je treći uvjet Mazurovog teorema zadovoljen pa E nema p-izogenija.

Sada možemo primijeniti Ribetov teorem o spuštanju razine. Dakle, postoji nova forma $f \in \mathcal{S}_2(\Gamma_0(2))$ takva da je $E \sim_p f$. Međutim, $\mathcal{S}_2(\Gamma_0(2))$ je trivijalan prema primjeru 3.5, pa nema novih formi na razini 2, i dobili smo kontradikciju.

Ugrubo je recept za primjenu modularnosti u diofantskim jednadžbama sljedeći:

- Pridruži eliptičku krivulju E (Freyovu krivulju) hipotetskom rješenju. Krivulja treba biti takva da N_p ne ovisi o rješenju, odnosno da je diskriminanta od E oblika $C \cdot D^p$, gdje je C konstanta koja ne ovisi o rješenju, a D izraz koji ovisi o rješenju. Također, iz Ribetovog teorema želimo da E ima multiplikativnu redukciju u prostim brojevima koji dijele D.

- Dokaži da krivulja nema p-izogenija, te primijeni Ribetov teorem.

- Dokaži da među novim formama na razini N_p nijedna od njih ne dolazi modulo p od E.

Literatura

[1] F. Diamond and J. Shurman. *A first course in modular forms*, volume 228 of *Grad. Texts Math.* Berlin: Springer, 2005.

[2] A. Dujella. Eliptičke krivulje u kriptografiji, bilješke s predavanja, 2013. Dostupno na `https://web.math.pmf.unizg.hr/~duje/elkript/elkripto2.pdf`.

[3] N. Koblitz. *Introduction to elliptic curves and modular forms.*, volume 97 of *Grad. Texts Math.* New York: Springer-Verlag, 2. ed. edition, 1993.

[4] D. Loeffler. Modular curves, 2014. Dostupno na `https://warwick.ac.uk/fac/sci/maths/people/staff/fbouyer/modular_curves.pdf`.

[5] R. Miranda. *Algebraic curves and Riemann surfaces*, volume 5 of *Grad. Stud. Math.* Providence, RI: AMS, American Mathematical Society, 1995.

[6] J.-P. Serre. *A course in arithmetic. Translation of "Cours d'arithmetique". 2nd corr. print*, volume 7 of *Grad. Texts Math.* Springer, Cham, 1978.

[7] S. Siksek. The modular approach to diophantine equations, 2007. Dostupno na `https://homepages.warwick.ac.uk/staff/S.Siksek/papers/ihpnotes6.pdf`.

[8] J. H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Grad. Texts Math.* New York, NY: Springer-Verlag, 1994.

[9] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Grad. Texts Math.* New York, NY: Springer, 2nd ed. edition, 2009.

[10] T. Weston. The modular curves $X_0(N)$ and $X_1(N)$. Dostupno na `https://swc-math.github.io/notes/files/01Weston1.pdf`.

[11] A. Wiles. Modular elliptic curves and Fermat's Last Theorem. *Ann. Math. (2)*, 141(3):443–551, 1995.

Sažetak

U ovom radu bavili smo se teoremom o modularnosti i objektima vezanim za njega; eliptičkim krivuljama, modularnim formama i modularnim krivuljama.

Definirali smo modularne forme i odredili neka njihova osnovna svojstva. Nakon toga smo definirali eliptičke krivulje nad poljem kompleksnih brojeva kao kompleksne toruse, te odredili kako izgledaju holomorfne funkcije na njima. Također smo definirali modularne krivulje kao Riemannove plohe i dokazali da one parametriziraju klase eliptičkih krivulja zajedno s nekom informacijom o torziji. Iskazali smo teorem o modularnosti preko uvedenih kompleksno-analitičkih objekata.

Pomoću rezultata iz kompleksne analize o kompaktnim Riemannovim plohama smo vidjeli da su prostori modularnih formi za kongruencijske podgrupe konačnodimenzionalni, te iskazali formule za dimenzije.

Nakon toga smo definirali Heckeove operatore, normalne operatore na prostorima $\Gamma_1(N)$ koji međusobno komutiraju, uveli pojam svojstvenih formi te novih i starih formi. Definirali smo i L-funkcije modularnih formi te eliptičkih krivulja, te iskazali teorem o modularnosti preko Fourierovih koeficijenata odnosno L-funkcija.

Na kraju smo, uz pomoć niza ranije poznatih rezultata o eliptičkim krivuljama, skicirali dokaz Velikog Fermatovog teorema te time ustanovili važnost teorema o modularnosti kao povijesno najtežeg i posljednjeg koraka u dokazu.

Summary

In this paper, we explored the modularity theorem and the mathematical objects related to it: elliptic curves, modular forms, and modular curves.

We defined modular forms and discussed some of their basic properties. Afterwards, we defined elliptic curves over the field of complex numbers as complex tori and determined their function fields. We defined modular curves as Riemann surfaces and proved that they parameterize isomorphism classes of elliptic curves together with some information about their torsion. We stated the modularity theorem in terms of those complex-analytic objects.

Using results from complex analysis about compact Riemann surfaces, it follows that the spaces of modular forms for congruence subgroups are finite-dimensional and we provided the dimension formulas for those spaces.

Next, we defined Hecke operators, which are a family of commuting normal operators on the spaces $\Gamma_1(N)$. We introduced eigenforms as common eigenvectors for all Hecke operators and we explained the concept of newforms. We defined L-functions for modular forms and elliptic curves and stated the modularity theorem in terms of equality of their Fourier coefficients and, equivalently, their L-functions.

Finally, with the help of a series of previously known results about elliptic curves, we gave an outline of a proof of Fermat's last Theorem, thereby establishing the significance of the modularity theorem as the historically most difficult and final step in the proof.

Životopis

Ivan Novak rođen je 17.1.2000. u Zagrebu. Pohađao je II. Osnovnu školu Vrbovec i Srednju školu Vrbovec, smjer opća gimnazija. Tijekom svog školskog obrazovanja se natjecao na matematičkim natjecanjima, te je 2018. na 59. Međunarodnoj matematičkoj olimpijadi održanoj u Rumunjskoj osvojio srebrnu medalju.

Na Prirodoslovno-matematičkom fakultetu u Zagrebu je 2018. upisao preddiplomski studij matematike, te je 2021. upisao diplomski studij teorijske matematike.

Tijekom studiranja se nastavio baviti srednjoškolskim natjecanjima, ali u drugačijoj ulozi. Kao član volonterske udruge Mladi nadareni matematičari "Marin Getaldić" je mentorirao darovite učenike i sudjelovao u njihovoj pripremi za natjecanja, te je također bio voditelj hrvatske ekipe na nekoliko međunarodnih natjecanja.

Natjecao se i na nekim studentskim matematičkim natjecanjima, te je na natjecanju IMC 2019. i 2020. osvojio prvu nagradu, dok je 2022. na natjecanju Vojtech Jarnik IMC osvojio treće mjesto.

Godine 2021. osvojio je rektorovu nagradu za rad "Računanje drugog momenta familija eliptičkih krivulja" pod mentorstvom prof. dr. sc. Matije Kazalickog.