Modularne forme

Matija Kazalicki

Sadržaj

1 Uvod **2**
1.1 Funkcije izvodnica . . . 3
1.2 Problem sume četiri kvadrata . . . 3

2 Poincareova gornja poluravnina **6**
2.1 Modeli hiperbolne geometrije . . . 6
2.2 Möbiusove transformacije . . . 8
2.3 Fundamentalna domena . . . 8
2.4 Kongruencijske podgrupe . . . 10
2.5 Modularna krivulja i kaspovi . . . 11
2.6 Eliptičke točke . . . 12

3 Modularne forme **12**
3.1 Definicija . . . 12
3.2 Primjer: Eisensteinovi redovi za $\mathrm{SL}_2(\mathbb{Z})$ . . . 15

4 Lagrangeov teorem o sumi četiri kvadrata **22**
4.1 Fourierova transformacija i theta funkcije . . . 22
4.2 Eisensteinovi redovi za $M_2(\Gamma_0(4))$ . . . 25
4.3 Dimenzije prostora modularnih formi . . . 25
4.4 Problem sume četiri kvadrata i generalizacije . . . 29

5 Problem klasifikacije kongruentnih brojeva **30**
5.1 Od kongruentnih brojeva do eliptičkih krivulja . . . 32
5.2 Eliptičke krivulje . . . 33
5.3 Grupovna operacija na eliptičkoj krivulji . . . 34
5.4 Mordellov teorem i točke konačnog reda . . . 36

6 Hasse-Weilova L-funkcija eliptičkih krivulja **39**
6.1 Zeta funkcija . . . 39
6.2 Gaussove i Jacobijeve sume . . . 40
6.3 Zeta funkcija eliptičke krivulje E_n . . . 44
6.4 Dirichletove L-funkcije . . . 49
6.5 Hasse-Weilova L-funkcija $L(E_n, s)$ . . . 57

7 Analitičko proširenje i funkcijska jednadžba funkcije $L(E_n, s)$ 60

8 Heckeovi operatori 61
8.1 Dvostruki slash operatori 62
8.2 Hecke operatori na $\Gamma_1(N)$ 63
8.3 Glavna lema i newforme 65

9 Dodatak: Reprezentacije konačnih grupa 68

1 Uvod

Modularna forma težine $k \in \mathbb{Z}$ je funkcija gornje poluravnine $\mathbb{H} = \{z \in \mathbb{C} : \Im(z) > 0\}$, koja je holomorfna na proširenoj gornjoj poluravnini $\mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$ i koja se u odnosu na neku podgrupu (konačnog indeksa) $\Gamma < \mathrm{SL}_2(\mathbb{Z})$ transformira prema formuli

$$f\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^k f(\tau), \text{ za svaki } \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma.$$

Modularne forme imaju važnu ulogu u raznim granama matematike. U teoriji brojeva se pojavljuju u dokazu posljednjeg Fermatovom teorema kao i u Langlandsovom programu; povezane su sa L-funkcijama, eliptičkim krivuljama i sa Birch i Swinnerton-Dyerovom slutnjom. Primjenjuju se još u teoriji struna, kombinatorici, kriptografiji i matematičkoj fizici.

Ovaj kolegij je zamišljen kao uvod u teoriju modularnih formi sa naglaskom na primjenama u teoriji brojeva.

Definicija modularnih formi je komplicirana i možda malo neprirodna, a priori nije jasno zašto bi takve funkcije uopće postojale niti zašto bi bile zanimljive. U ovom uvodu ćemo motivirati definiciju i osnovnu teoriju na primjeru modularne forme koja je funkcija izvodnica brojeva prikaza prirodnog broja n kao sume četiri kvadrata. Klasičan Lagrangeov teorem tvrdi da se svaki prirodan broj može prikazati kao suma četiri kvadrata. Koristeći teoriju koju ćemo razviti u prvim poglavljima ove skripte pokazat ćemo da je broj različitih načina $r(n,4) = \#\{v \in \mathbb{Z}^4 : n = v_1^2 + v_2^2 + v_3^2 + v_4^2\}$ na koji se n može prikazati kao suma četiri kvadrata jednak

$$r(n,4) = 8 \sum_{d|n, 4\nmid d} d.$$

Ovaj odjeljak je preglednog (motivacijskog) karaktera, tvrdnje nećemo dokazivati (niti ćemo sve pojmove precizno definirati). To će biti napravljeno u idućim poglavljima.

Za početak ćemo objasniti ideju funkcije izvodnice na primjeru Fibonaccijevih brojeva.

1.1 Funkcije izvodnica

Obična funkcija izvodnica niza $(a_n)_n \in \mathbb{N}_0$ je red potencija

$$\sum_{n=0}^{\infty} a_n x^n.$$

Ponekad tako definirani red potencija definira funkciju na nekoj okolini točke $x = 0$, pa proučavajući svojstva te funkcije možemo saznati nešto o polaznom nizu. Klasičan primjer je funkcija izvodnica Fibonaccijevih brojeva pomoću koje možemo izvesti Binetovu formulu za opći član.

Fibonačijevi brojevi F_k, $k \in \mathbb{N}_0$, su definirani rekurzivnom relacijom

$$F_{k+2} = F_{k+1} + F_k, \tag{1}$$

gdje je $F_0 = 0$ i $F_1 = 1$. Njihova funkcija izvodnica je red potencija

$$f(x) = \sum_{k=0}^{\infty} F_k x^k. \tag{2}$$

Rekurzivna formula (1) je ekvivalentna funkcionalnoj jednadžbu

$$f(x) = x + xf(x) + x^2 f(x),$$

odakle slijedi da (2) definira funkciju $f(x) = \frac{x}{1-x-x^2}$ u nekoj okolini točke $x = 0$. Razvojem na parcijalne razlomke

$$\frac{x}{1-x-x^2} = \frac{1}{\sqrt{5}} \left(\frac{1}{1 - \frac{1+\sqrt{5}}{2} x} - \frac{1}{1 - \frac{1-\sqrt{5}}{2} x} \right),$$

i koristeći formule za geometrijski red dobivamo Binetovu formulu

$$F_k = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^k + \left(\frac{1-\sqrt{5}}{2} \right)^k \right).$$

U ovom primjeru funkcija izvodnica Fibonačijevih brojeva je Taylorov red funkcije $f(x)$, dok će u sljedećem primjeru funkcija izvodnica brojeva prikaza prirodnog broja n kao sume četiri kvadrata biti Fourierov red modularne forme.

1.2 Problem sume četiri kvadrata

U teoriji brojeva, u problemu sume četiri kvadrata (four squares problem) treba odrediti na koliko se načina prirodan broj može prikazati kao suma četiri kvadrata. Definirajmo općenito, za nenegativne cijele brojeve n i k, broj prikaza broja n kao sume k kvadrata

$$r(n,k) = \#\{v \in \mathbb{Z}^k : n = v_1^2 + \ldots + v_k^2\}.$$

Ako je $i+j=k$, tada elementarnim prebrojavanjem dobivamo $r(n,k)=\sum_{l+m=n} r(l,i)r(m,j)$ pa funkcija izvodnica za brojeve prikaza

$$\theta(\tau,k)=\sum_{n=0}^{\infty} r(n,k)q^n, \quad q=e^{2\pi i\tau},$$

zadovoljava relaciju ($\theta(\tau,k)$ konvergira apsolutno za $\tau\in\mathbb{H}$)

$$\theta(\tau,k_1)\theta(\tau,k_2)=\theta(\tau,k_1+k_2).$$

Označimo sa $\theta(\tau)=\theta(\tau,1)=\sum_{d\in\mathbb{Z}} q^{d^2}$.

Pitanje. Što možemo reći o funkciji $\theta(\tau,4)=\theta(\tau)^4$?

Iz definicije očito vrijedi

$$\theta(\tau+1)=\theta(\tau). \tag{3}$$

Nadalje, primjenom Poissonove sumacijske formule (ovo će biti detaljno objašnjeno u odjeljku §4.1)

$$\sum_{d\in\mathbb{Z}} h(x+d)=\sum_{m\in\mathbb{Z}} \hat{h}(m)e^{2\pi imx},$$

gdje je $\hat{h}$ Fourierova transformacija od h

$$\hat{h}(x)=\int_{-\infty}^{+\infty} h(t)e^{-2\pi ixt}dt,$$

sa $x=0$ i $h(d)=e^{2\pi id^2\tau}$ dobivamo

$$\theta(-1/(4\tau))=\sqrt{-2i\tau}\,\theta(\tau).$$

Odavde lako slijedi

$$\theta\left(\frac{\tau}{4\tau+1}\right)=\sqrt{4\tau+1}\,\theta(\tau),$$

odnosno

$$\theta\left(\frac{\tau}{4\tau+1},4\right)=(4\tau+1)^2\theta(\tau,4). \tag{4}$$

Neka je Γ_θ podgrupa od $\mathrm{SL}_2(\mathbb{Z})$ generirana matricama $\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$ i $\left(\begin{smallmatrix}1&0\\4&1\end{smallmatrix}\right)$. Iz formula (3) i (4) slijedi

$$\theta\left(\frac{a\tau+b}{c\tau+d},4\right)=(c\tau+d)^2\theta(\tau,4) \tag{5}$$

za svaku matricu $\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)\in\Gamma_\theta$.

Dakle, $\theta(\tau,4)$ je holomorfna funkcija gornje poluravnine koja se u odnosu na grupu Γ_θ prema formuli (5). Promotrimo sada skup svih takvih funkcija

(često možemo nešto saznati o danom objektu tako da proucavamo sve objekte sa sličnim svojstvima). Taj skup je vektorski prostor nad $\mathbb{C}$. Nažalost takvih funkcija ima previše - taj prostor nije konačno dimenzionalan, pa je potrebno uočiti još neka dodatna svojstva funkcije $\theta(\tau, 4)$.

Istražimo asimptotsko ponašanje funkcije $\theta(\tau, 4)$. Za početak, limes u beskonačnosti $i\infty$ je konačan

$$\lim_{\tau \to i\infty} \theta(\tau, 4) = 1.$$

Isto tako ima smisla promotriti ponašanje funkcije oko $\frac{a}{c} \in \mathbb{Q}$. Može se pokazati da funkcija "raste" na predvidljiv način, preciznije limes

$$\lim_{\tau \to i\infty} (c\tau + d)^{-2} \theta\left(\frac{a\tau + b}{c\tau + d}, 4\right)$$

je konačan, gdje je $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ neka matrica sa cjelobrojnim elementima determinante jedan (takva matrica postoji jer su a i c relativno prosti).

Može se pokazati (vidi §4.3) da je vektorski prostor holomorfnih funkcija gornje poluravnine koje zadovoljavaju (5) i koje imaju konačne limese u racionalnim brojevima (kao što je malo prije objašnjeno; to svojstvo se naziva holomorfnost u kaspovima) konačno dimenzionalan (dimenzije je dva).

Upravo smo definirali modularnu formu težine $k = 2$ za Γ_θ. Općenito vrijedi da su prostori modularnih formi konačno dimenzionalni.

Sada ćemo konstruirati bazu za vektorski prostor modularnih formi za Γ_θ težine 2 koristeći ("lažan") Eisensteinov red težine dva

$$G_2(\tau) = \sum_{c \in \mathbb{Z}} \sum_{d \in \mathbb{Z}, (c,d) \neq (0,0)} \frac{1}{(c\tau + d)^2}.$$

U §3.2 ćemo pokazati da ovaj red uvjetno konvergira te da ima sljedeći Fourierov razvoj

$$G_2(\tau) = 2\zeta(2) - 8\pi^2 \sum_{n=1}^{\infty} \sigma(n) q^m,$$

gdje je $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ Riemannova zeta funkcija, $q = e^{2\pi i \tau}$ i $\sigma(n) = \sum_{d|n} d$. Modularne forme $G_{2,2}(\tau) = G_2(\tau) - 2G_2(2\tau)$ i $G_{2,4}(\tau) = G_2(\tau) - 4G_2(4\tau)$ su baza traženog vektorskog prostora pa je $\theta(\tau, 4)$ njihova linearna kombinacija. Iz q-razvoja

$$\begin{aligned} \theta(\tau, 4) &= 1 + 8q + \cdots, \\ -\frac{3}{\pi^2} G_{2,2}(\tau) &= 1 + 24q + \cdots, \\ -\frac{1}{\pi^2} G_{2,4}(\tau) &= 1 + 8q + \cdots, \end{aligned}$$

se vidi da je $\theta(\tau, 4) = -\frac{1}{\pi^2} G_{2,4}(\tau)$. Izjednačavanjem odgovarajućih Fourierovih koeficijenata dobivamo

$$r(n, 4) = 8 \sum_{d|n, 4 \nmid d} d.$$

2 Poincareova gornja poluravnina

2.1 Modeli hiperbolne geometrije

U Euklidskoj geometriji, Euklidov postulat o paralelama je ekvivalentan tvrdnji da za zadani pravac (u ravnini) i točku izvan njega postoji jedinstveni pravac paralelan s njime koji prolazi kroz zadanu točku.

U hiperboličkoj geometriji Euklidov postulat ne vrijedi (ostali aksiomi geometrije su zadovoljeni), postoje barem dva pravca paralelna zadanom pravcu kroz proizvoljnu točku. Dva najpoznatija modela hiperboličke geometrije (koji su realizirani u Euklidskom prostoru uz odgovarajuću metriku) su Poincareov krug i Poincareova gornja poluravnina. Mi ćemo se dataljnije baviti Poincareovom gornjom poluravninom.

Definicija 2.1. Poincareova gornja poluravnina je skup

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

sa metrikom

$$ds = \frac{\sqrt{(dx)^2 + (dy)^2}}{y},$$

gdje $\Im(z) = y$ označava imaginarni dio od $z = x + iy \in \mathbb{C}$.

U geometriji prvo želimo razumijeti geodetske krivulje, "pravce" u zakrivljenom prostoru.

Propozicija 2.2. *Geodetske krivulje na* $\mathbb{H}$ *su vertikalni pravci* $\{z \in \mathbb{H} : \Re(z) = x_0\}$ *i polukružnice* $\{z \in \mathbb{H} : |z - z_0| = r_0\}$ *koje sijeku* $\mathbb{R}$ *pod pravim kutom.*

Napomena. Sad se može lako provjeriti da je (infinitezimalna) metrika iz definicije ekvivalentna metrici

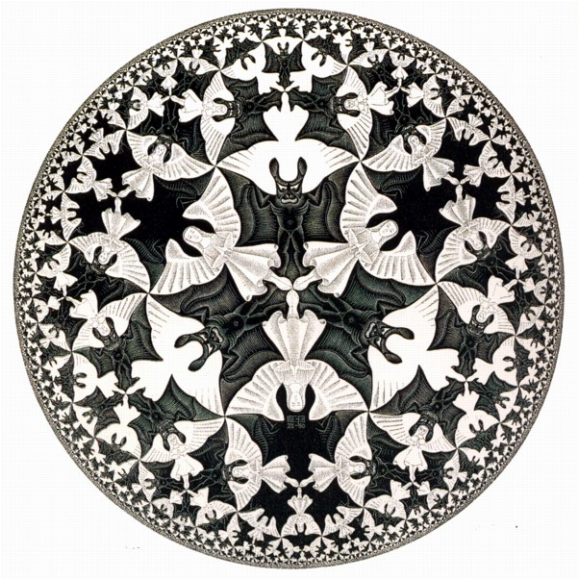
$$d(z, w) = \cosh^{-1}\left(1 + \frac{|z - w|^2}{2\Im(z)\Im(w)}\right).$$

Primjer 1. Imajmo na umu da je metrika na $\mathbb{H}$ različita od standardne Euklidske metrike. Npr. udaljenost između točaka $z = i$ i $z = iy$ je jednaka

$$\int_1 y\frac{\sqrt{1'^2 + t'^2}}{t}dt = |\ln(y)|,$$

dok je udaljenost između točaka $z = i$ i $z = e^{i\theta} \in \mathbb{H}$ jednaka

$$\int_{\pi/2}^{\theta} \frac{\sqrt{(\cos\theta')^2 + (\sin\theta')^2}}{\sin\theta} = \int_{\pi/2}^{\theta} \frac{1}{\sin\theta} = \log\tan\theta/2.$$



Slika 1: M. C. Escher, Circle limit IV: Heaven and Hell

2.2 Möbiusove transformacije

U ovom odjeljku proučavama grupu izometrija od $\mathbb{H}$. Prisjetimo se, izometrija je preslikavanje između metričkih prostora koje čuva metrika, tj. $f : \mathbb{H} \to \mathbb{H}$ za koja vrijedi $d(f(z), f(w)) = d(z, w)$, za svaki $z, w \in \mathbb{H}$.

Uvedimo prvo neke standardne oznake. Za proizvoljan komutativan prsten s jedinicom R, neka je

$$\mathrm{SL}_2(R) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) : a, b, c, d \in R, ad - bc = 1 \right\} \text{ i } \mathrm{PSL}_2(R) = \mathrm{SL}_2(R) / \left\{ \left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right) : a \in R^\times \right\}.$$

Definicija 2.3. Möbiusova transformacije je preslikavanje $\mathbb{H} \to \mathbb{C}$ dano formulom

$$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) z = \frac{az + b}{cz + d}, z \in \mathbb{H},$$

gdje je $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{R})$.

Propozicija 2.4. *Möbiusove transformacije su analitičke (i bijektivne) izometrije od* $\mathbb{H}$. *Definiraju djelvanje grupe* $\mathrm{PSL}_2(\mathbb{R})$ *na* $\mathbb{H}$.

Dokaz. Dokažimo prvo da Möbiusove transformacije čuvaju $\mathbb{H}$. Neka je $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{R})$. Vrijedi $\Im(\frac{az+b}{cz+d}) = \Im(\frac{(az+b)(c\bar{z}+d)}{|cz+d|^2}) = \frac{ad-bc}{|cz+d|^2}\Im(z)$. Dakle, $ad - bc = 1$ i $\Im(z) > 0$ povlači $\Im(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) z) > 0$.

Primjetimo da za $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{R})$ i $r \in \mathbb{R}^\times$ vrijedi $\left(\begin{smallmatrix} ra & rb \\ rc & rd \end{smallmatrix}\right) z = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) z$. Neka su $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right), \left(\begin{smallmatrix} e & f \\ g & h \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{R})$. Direktno se provjeri

$$\left(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\left(\begin{smallmatrix} e & f \\ g & h \end{smallmatrix}\right)\right) z = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \left(\left(\begin{smallmatrix} e & f \\ g & h \end{smallmatrix}\right) z\right),$$

dakle grupa $\mathrm{PSL}_2(\mathbb{R})$ djeluje na $\mathbb{H}$ Möbiusovim transformacijama. Specijalno, inverz Möbiusove transformacije je Möbiusova transformacija.

Preostaje još dokazati da je $z \mapsto \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) z$ izometrija. Dovoljno je dokazati da je $dz = dw$, gdje je $w = \frac{az+b}{cz+d}$ i $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{R})$. Neka je $z = x + iy$. Od prije imamo $\Im(w) = \frac{y}{|cz+d|^2}$ pa tvrdnja slijedi iz kratkog računa.

□

2.3 Fundamentalna domena

Primjetimo da su svake dvije točke $z_1, z_2 \in \mathbb{H}$, $\mathrm{SL}_2(\mathbb{R})$-ekvivalentne, tj. $z_2 = \frac{az_1+b}{cz_1+d}$, za neku matricu $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{R})$. Dovoljno je pokazati da je svaka točka $z \in \mathbb{H}$ ekvivalentna s i. Neka je $z = u + vi, u, v \in \mathbb{R}, v > 0$. Tada je $\left(\begin{smallmatrix} \sqrt{v} & 0 \\ 0 & \sqrt{v^{-1}} \end{smallmatrix}\right) i = vi$ i $\left(\begin{smallmatrix} 1 & u \\ 0 & 1 \end{smallmatrix}\right) iv = u + iv = z$, odnosno $\left(\begin{smallmatrix} 1 & u \\ 0 & 1 \end{smallmatrix}\right) \left(\begin{smallmatrix} \sqrt{v} & 0 \\ 0 & \sqrt{v^{-1}} \end{smallmatrix}\right) i = z$.

Neka je Γ podgrupa od $\mathrm{SL}_2(\mathbb{Z})$. Zanimat će nas klase ekvivalencija djelovanja grupe Γ (kao podgrupe od $\mathrm{SL}_2(\mathbb{R})$) na $\mathbb{H}$.

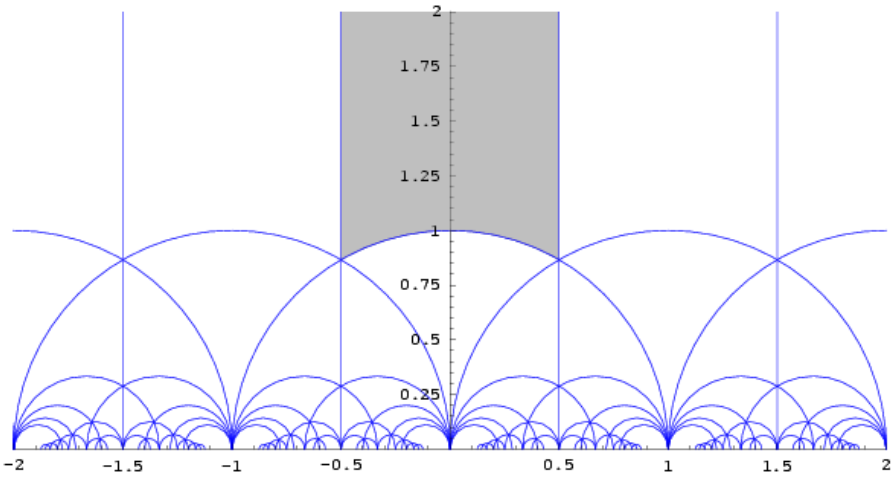
Definicija 2.5. Za zatvoren i povezan podskup F od $\mathbb{H}$ kažemo da je fundamentalna domena za podgrupu Γ ako je svaki $z \in \mathbb{H}$ Γ-ekvivalentan nekoj točki iz F, s time da nikoje dvije točke iz unutrašnjosti od F nisu Γ ekvivalentne.

Napomena. Uočimo da je fundamentalna domena F ima sljedeća dva svojstva

1) $\mathbb{H} = \cup_{\gamma\in\Gamma}(\gamma F)$

2) Unutrašnjost od $\gamma_1 F \cap \gamma_2 F$ je prazan skup za $\gamma_1 \neq \gamma_2, \gamma_1, \gamma_2 \in \Gamma$.

Vrijedi i obrat, zatvoren i povezan skup F koji zadovoljava 1) i 2) je fundamentalna domena za Γ.



Slika 2: Fundamentalna domena za $\mathrm{SL}_2(\mathbb{Z})$

Propozicija 2.6. *Skup*

$$F := \{z \in \mathbb{H} : -\frac{1}{2} \leq \Re(z) \leq \frac{1}{2}, |z| \geq 1\}$$

je fundamentalna domena za $\mathrm{SL}_2(\mathbb{Z})$.

Definirajmo prvo dvije matrice $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right), S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ za koje ćemo kasnije pokazati da su generatori grupe $\mathrm{SL}_2(\mathbb{Z})$. Primjetimo $Tz = z + 1$ i $Sz = -1/z$.

Dokaz. Prvo ćemo pokazati da je svaki $z \in \mathbb{H}$ $\mathrm{SL}_2(\mathbb{Z})$-invarijantan nekoj točki iz F. Ideja je koristeći translacije T^j točku z preslikati u traku $-\frac{1}{2} \leq \Re z \leq \frac{1}{2}$. Ako se tako dobivena točka ne nalazi u F, primjenimo preslikavanje S i ponovimo cijeli postupak.

Promotrimo što se dešava sa $\Im(z)$ tijekom ovog postupka. Označimo s Γ podgrupu od $\mathrm{SL}_2(\mathbb{Z})$ generiranu s S i T (kasnije ćemo pokazati da je $\Gamma = \mathrm{SL}_2(\mathbb{Z})$). Od prije znamo da vrijedi $\Im(\gamma z) = \frac{\Im z}{|cz+d|^2}$, za $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$. Kako su

brojevi c i d cijeli, postoji $\gamma_m \in \Gamma$ za koji funkcija $\gamma \mapsto \frac{\Im z}{|cz+d|^2}$, za $\gamma \in \Gamma$ postiže maksimum. Odaberimo sad $j \in \mathbb{Z}$ za koji se $T^j(\gamma_m z)$ nalazi u traci $|\Re(z) \leq \frac{1}{2}|$. Ako je $|T^j(\gamma_m z)| \geq 1$, onda smo gotovi jer se tocka $T^j(\gamma_m z)$ nalazi u F. Inače primjenimo S. Kako vrijedi $\Im(ST^j(\gamma_m z)) = \frac{\Im(T^j(\gamma_m z))}{|T^j(\gamma_m z)|^2} > \Im(T^j(\gamma_m z))$ dobili smo kontradikciju s maksimalnošću od γ_m.

Pokažimo još da nikoje dvije točke iz unutrašnjosti od F nisu $\mathrm{SL}_2(\mathbb{Z})$ ekvivalentne. Pretpostavimo suprotno. Neka su z_1 i z_2 iz F takve da je $z_1 = \gamma z_2$ za neki $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. Možemo još pretpostaviti da je $\Im(z_1) \geq \Im(z_2)$ (u protivnom zamjenimo z_1 s z_2 te γ s γ^{-1}). Iz formule za imaginarni dio od γz_2 slijedi da je $|cz_2 + d| \leq 1$. Budući da je $|z_2| \geq 1$ i $|\Re(z_2)| < \frac{1}{2}$, slijedi da je $\Im(z_2) \geq \frac{\sqrt{3}}{2}$ pa se lako vidi da je $|c| \leq 1$. Potrebno je promotriti sljedeća četiri slučaja: (i) $c = 0, d = \pm 1$, (ii) $c = \pm 1, d = 0$, (iii) $c = d = \pm 1$ i $z_2 = -\frac{1}{2} + \frac{\sqrt{-3}}{2}$, (iv) $c = -d = \pm 1$ i $z_2 = \frac{1}{2} + \frac{\sqrt{-3}}{2}$. Npr. ako je $c = 0$, tade je $\gamma = \pm \left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right)$ i $\Re(z_2) = \Re(z_1) \pm b$, odnosno $|b| = 1$ pa z_1 i z_2 ne mogu biti u unutrašnjosti od F. Ako je $|c| = 1$, tada $|cz_2 + d| \leq 1$ implicira $(\Re(z_2) + d)^2 + \Im(z_2)^2 \leq 1$ i $(\Re(z_2) + d)^2 \leq 1 - \Im(z_2)^2 \leq 1 - 3/4 = 1/4$, odnosno $|\Re(z_2) + d| \leq 1/2$ iz čega slijedi $|d| \leq 1$. Ostatak dokaza propozicije ostavljamo čitatelju.

□

Napomena. Iz dokaza prethodne propozicije slijedi da je grupa $\mathrm{SL}_2(\mathbb{Z})$ (odnosno $\mathrm{PSL}_2(\mathbb{Z}) := \mathrm{SL}_2(\mathbb{Z})/\{\pm I\}$) generirana matricama S i T (zanimljivo je da smo dokazali tvrdnju iz teorije grupa koristeći geometrijske metode). Lako se vidi da su jedine relacije između S i T (u $\mathrm{PSL}_2(\mathbb{Z})$) $S^2 = (ST)^3 = I$.

Metrika na $\mathbb{H}$, $ds = \frac{\sqrt{(dx)^2+(dy)^2}}{y}$, inducira volumnu formu $\frac{dxdy}{y^2}$ koja je invarijantna na djelovanje $\mathrm{SL}_2(\mathbb{Z})$, npr. $\int_A \frac{dxdy}{y^2} = \int_{\gamma A} \frac{dxdy}{y^2}$ za svaki izmjerljiv skup A i $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.

Propozicija 2.7. *Površina fundamentalne domene F je jednaka $\pi/3$.*

Dokaz. Površina je jednaka

$$\int_F \frac{dxdy}{y^2} = \int_{-\frac{1}{2}}^{\frac{1}{2}} dx \int_{(1-x^2)^{1/2}}^{\infty} dy/y^2 = \int_{-\frac{1}{2}}^{\frac{1}{2}} (1-x^2)^{-1/2} dx = \arcsin x|_{-\frac{1}{2}}^{\frac{1}{2}} = \pi/3.$$

□

2.4 Kongruencijske podgrupe

Osim grupe $\mathrm{SL}_2(\mathbb{Z})$ nas će zanimati i njene kongruencijske podgrupe.

Definicija 2.8. Neke je N prirodan broj. Glavna kongruencijska podgrupa nivoa N je grupa

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

Kongruencijska podgrupa je podgrupa od $\mathrm{PSL}_2(\mathbb{Z})$ koja sadrži neku glavnu kongruencijsku podgrupu nivoa N i najmanji takav N se naziva nivo kongurencijske podgrupe.

Primjer 2. Dvije kongruencijske podgrupe koje ćemo načešće susretati su $\Gamma_1(N)$ i $\Gamma_0(N)$:

$$\Gamma_1(N) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{PSL}_2(\mathbb{Z}) : a \equiv d \equiv 1 \bmod N \text{ i } c \equiv 0 \pmod N\},$$

$$\Gamma_0(N) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{PSL}_2(\mathbb{Z}) : c \equiv 0 \pmod N\}.$$

Napomena. Grupa $\mathrm{PSL}_2(\mathbb{Z})$ se još zove i modularna grupa i često se označava sa Γ. Njene kongruencijske podgrupe $\Gamma(N)$, $\Gamma_1(N)$ i $\Gamma_0(N)$ obično se nazivaju modularne podgrupe.

Navedimo nekoliko svojstava gore definiranih kongruencijskih grupa. Grupa $\Gamma(N)$ je po definiciji jezgra redukcije mod N, $\mathrm{PSL}_2(\mathbb{Z}) \to \mathrm{PSL}_2(\mathbb{Z}/N\mathbb{Z})$, pa je onda i normalna podgrupa grupe $\mathrm{PSL}_2(\mathbb{Z})$.

Zadatak 1. a) Pokažite da je indeks $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N)]$ jednak $\#\,\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) = N^3 \prod_{p|N}(1 - 1/p^2)$.

b) Pokažite da je preslikavanje $\Gamma_1(N) \to \mathbb{Z}/N\mathbb{Z}$ dano sa $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto b \pmod N$ surjekcija s jezgrom $\Gamma(N)$. Koliki je indeks od $\Gamma_1(N)$ u $\mathrm{SL}_2(\mathbb{Z})$?

c) Pokažite da je preslikavanje $\Gamma_0(N) \to (\mathbb{Z}/N\mathbb{Z})^\times$ dano sa $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto d \pmod N$ surjekcija sa jezgrom $\Gamma_1(N)$. Koliki je indeks od $\Gamma_0(N)$ u $\mathrm{SL}_2(\mathbb{Z})$?

Pitanje. Što možemo reći o fundamentalnoj domeni kongruencijske podgrupe Γ?

Neka su $x_1, x_2, \ldots, x_r$ predstavnici klasa od $\Gamma\backslash \mathrm{SL}_2(\mathbb{Z})$, tj. $\mathrm{SL}_2(\mathbb{Z}) = \cup_i \Gamma x_i$. Tada skup $\tilde{F} = \cup_i x_i F$ zadovoljava sve uvjete iz definicije fundamentalne domene za Γ osim što ne mora biti povezan. Može se pokazati da će uz odgovarajučci odabir predstavnika klasa x_i skup $\tilde{F}$ biti i povezan. Kako skupovi $x_i F$ svi imaju jednaku površinu $\pi/3$, površina fundamentalne domene za Γ je jednaka $\frac{\pi}{3}[\mathrm{SL}_2(\mathbb{Z}) : \Gamma]$.

2.5 Modularna krivulja i kaspovi

Definicija 2.9. Za kongruencijsku podgrupu $\Gamma < \mathrm{PSL}_2(\mathbb{Z})$ (koja djeluje na $\mathbb{H}$), modularna krivulja $Y(\Gamma)$ se definira kao kvocijentni prostor orbita tog djelovanja,

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

Modularne krivulje možemo identificirati s njihovim fundamentalnih domena i na taj način ih realizirati kao povezane podskupove od $\mathbb{H}$. Pomoću te identifikacije na prirodan način možemo na njima definirati strukturu Riemannove plohe (jedino treba pažljivo definirati karte oko eliptičkih točaka). Na taj način dobivena Riemanova ploha nije kompaktna (što je vidljivo sa Slike 2.3). Kako su kompaktne Riemannove plohe zapravo algebarski objekti (može se pokazati da je teorija kompaktnih Riemannovih ploha ekvivalentna teoriji projektivnih algebarskih krivulja), modularne krivulje ćemo kompaktificirati (dodavanjem konačnog broja točaka). Te točke nazivamo kaspovima (engleski cusp).

Definirajmo djelovanje kongruencijske podgrupe Γ na skup $\mathbb{Q}\cup\{\infty\}$ na sljedeći način:

$$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)s = \frac{as+b}{cs+d}, \text{ i } \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\infty = \frac{a}{c},$$

gdje je $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$ i $s \in \mathbb{Q}$.

Zadatak 2. Provjerite da je gore definirana operacija djelovanje grupe.

Definicija 2.10. Klase ekvivalencija djelovanja podgrupe Γ na $\mathbb{Q}\cup\{\infty\}$ se nazivaju kaspovi (od podgrupe Γ ili od modularne krivulje $Y(\Gamma)$).

Zadatak 3. Dokažite da $Y(1) := Y(\Gamma(1))$ ima samo jedan kasp i da općenito $\mathrm{Y}(\Gamma)$ ima konačno mnogo kaspova.

Definicija 2.11. Kompaktificirana modularna krivulja $X(\Gamma)$ je kvocijentni prostor

$$X(\Gamma) = \Gamma\backslash(\mathbb{H}\cup\mathbb{Q}\cup\{\infty\}).$$

2.6 Eliptičke točke

Definicija 2.12. Neka je Γ kongruencijska podgrupa od $\mathrm{SL}_2(\mathbb{Z})$. Za svaki $\tau \in \mathbb{H}$ neka je Γ_τ izotropna podgrupa od τ,

$$\Gamma_\tau = \{\gamma \in \Gamma : \gamma\tau = \tau\}.$$

Točka $\tau \in \mathbb{H}$ je eliptička točka od Γ ako je Γ_τ netrivijalna (nije sadržana u $\{\pm I\}$).

3 Modularne forme

3.1 Definicija

Modularnu formu ćemo definirati kao holomorfnu funkciju gornje poluravnine $\mathbb{H}$ koja je slabo modularna (u odnosu na neku podgrupu $\Gamma < \mathrm{SL}_2(\mathbb{Z})$) i koja je holomorfna u kaspovima. Definirajmo sada ove pojmove.

Definicija 3.1. Neka je k cijeli broj i neka je $f : \mathbb{H} \to \mathbb{C}$ funkcija. Za $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ definirajmo (slash) operator $[\gamma]_k$

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

gdje je $j(\gamma,\tau) := (c\tau+d)$. Kažemo da je funkcija $f : \mathbb{H} \to \mathbb{C}$ slabo modularna u odnosu na $\Gamma < \mathrm{PSL}_2(\mathbb{Z})$ ako za svaki $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$ vrijedi $f[\gamma]_k = f$. Odnosno

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

za svaki $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$.

Napomena. Uočimo, ako je f slabo modularna u odnosu na Γ, tada je $f[\gamma]_k$ slabo modularna u odnosu na $\gamma^{-1}\Gamma\gamma$.

Osnovna svojstva slash operatora su dana sljedećom lemom.

Lema 3.2. *Za sve* $\gamma, \gamma' \in \mathrm{SL}_2(\mathbb{Z})$ *i* $\tau \in \mathbb{H}$ *vrijedi*

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

b) $[\gamma\gamma']_k = [\gamma]_k[\gamma']_k$.

Dokaz. Neka je $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ i $\gamma' = \left(\begin{smallmatrix} e & f \\ g & h \end{smallmatrix}\right)$. Tada je $\gamma\gamma' = \left(\begin{smallmatrix} * & * \\ ec+dg & cf+dh \end{smallmatrix}\right)$ pa je $j(\gamma\gamma', \tau) = (ec + dg)\tau + cf + dh$. S druge strane, $j(\gamma, \gamma'\tau) = c\frac{ez+f}{gz+h} + d$ i $j(\gamma', \tau) = (gz + h)$ pa tvrdnja iz a) slijedi.

Po definiciji, $f[\gamma\gamma']_k = j(\gamma\gamma', \tau)^{-k} f(\gamma\gamma'\tau)$ i

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

Tvrdnja slijedi iz a) dijela leme. □

Napomena. Primjetimo da iz prethodne leme proizlazi da ako je f slabo modularna u odnosu na $\Gamma < \mathrm{SL}_2(\mathbb{Z})$, da je tada $f[\alpha]_k$ slabo modularna u odnosu na $\alpha^{-1}\Gamma\alpha$, gdje je $\alpha \in \mathrm{SL}_2(\mathbb{Z})$.

Za holomorfnu i slabo modularnu funkciju $f(\tau)$ kažemo da je meromorfna u kaspu ∞, ako za neki $N \in \mathbb{N}$ funkcija $f(\tau)$ ima Laurentov razvoj u $q_N = e^{2\pi i\tau/N}$

$$f(\tau) = \sum_{n=l}^{\infty} a_n q_N^n,$$

za neki $l \in \mathbb{Z}$ takav da je $a_l \neq 0$. Broj l zovemo red (poništavanja) funkcije $f(\tau)$ u kaspu ∞ i označavamo sa $v_\infty(f)$. Funkcija je holomorfna ako je $l \geq 0$.

Općenitije, neka je c bilo koji kasp od Γ i neka je $\gamma \in \Gamma$ takva da je $\gamma\infty = c$ (vidi 2.5). Kažemo da je funkcija $f(\tau)$ meromorfna (holomorfna) u c ako je funkcija $f[\gamma]_k$ meromorfna (holomorfna) u kaspu ∞. Laurentov razvoj funkcije $f[\gamma]_k$ zovemo Laurentov (ili $q-$) razvoj od $f(\tau)$ u kaspu c. Taj razvoj nije jedinstven i ovisi o odabiru matrice γ, ali se može pokazati da je red poništavanja od $f(\tau)$ u kaspu c, $v_c(f) := v_\infty(f[\gamma]_k)$ dobro definiran i ne ovisi o odabiru matrice γ.

Definicija 3.3. Neka je Γ podgrupa od $\mathrm{SL}_2(\mathbb{Z})$ konačnog indeksa i neka je k cijeli broj. Funkcija $f : \mathbb{H} \to \mathbb{C}$ je modularna forma težine k za Γ ako

(1) f je holomorfna,

(2) f je slabo modularna težine k u odnosu na Γ,

(3) f je holomorfna u svakom kaspu od Γ.

Ako uz to f poništava svaki kasp, kažemo da je f kasp forma (težine k za Γ). Oznaka za skup modularnih (odnosno kasp) formi težine k za Γ je $\mathcal{M}_k(\Gamma)$ (odnosno $\mathcal{S}_k(\Gamma)$).

Pretpostavimo da je Γ kongruencijska podgrupa od $\mathrm{SL}_2(\mathbb{Z})$ nivoa N, tj. $\Gamma(N) < \Gamma$. Tada Γ sadrži matricu

$$\left(\begin{smallmatrix} 1 & N \\ 0 & 1 \end{smallmatrix}\right) : \tau \mapsto \tau + N.$$

Ako je funkcija $f : \mathbb{H} \to \mathbb{C}$ slabo modularna u odnosu na Γ, tada je $f(\tau)$ specijalno i N-periodička, tj. vrijedi $f(\tau + N) = f(\tau)$. Označimo sa $D = \{q_N \in \mathbb{C} : |q_N| < 1\}$ otvoreni jedinični disk i neka je $D' = D - \{0\}$. Tada N-periodičko holomorfno preslikavanje $\tau \mapsto e^{2\pi/N}$ preslikava $\mathbb{H}$ u D'. Funkcija $g : D' \mapsto \mathbb{C}$, $g(q_N) = f(\log(q_N)/(2\pi i/N))$ je zbog prediodičnosti od $f(\tau)$ dobro definirana iako je vrijednost logaritma određena samo do na $2\pi i\mathbb{Z}$. Vrijedi

$$f(\tau) = g(e^{2\pi i/N}).$$

Ako je f holomorfna na $\mathbb{H}$, onda je i g holomorfna na probušenom disku D' budući da je logaritamska funkcija dobro definirana holomorfna funkcija oko svake točke u $\mathbb{H}$ (iako, kao što smo rekli, se ne može definirati na cijelom $\mathbb{H}$). Tada g ima Laurentov razvoj $g(q_N) = \sum_{n\in\mathbb{Z}} a_n q_N^n$ za $q_N \in D'$. Lako se vidi da $q_N \to 0$ kad $\tau \to \infty$ ($\Im(\tau) \to +\infty$) pa vidimo da je po definiciji f holomorfna u kaspu ∞, ako i samo ako se g može holomorfno proširiti do cijelog diska D. Tada f ima Fourierov razvoj

$$f(\tau) = \sum_{n=0}^{\infty} a_n q_N^n.$$

Neka je c neki kasp od Γ i neka za $\alpha \in \mathrm{SL}_2(\mathbb{Z})$ vrijedi $\alpha\infty = c$. Kako je $\Gamma(N)$ normalna podgrupa od $\mathrm{SL}_2(\mathbb{Z})$ (jer je jezgra redukcije mod N), tada je $\tilde{\Gamma} = \alpha^{-1}\Gamma\alpha$ također kongruencijska podgrupa nivoa N, pa prema prethodnom odjeljku funkcija $f[\alpha]_k$ ima Fourierov razvoj

$$(f[\alpha]_k)(\tau) = \sum_{n=-l}^{\infty} a_n q_h^n, \quad q_h = e^{2\pi i\tau/h},$$

gdje je $h \in \mathbb{N}$ najmanji broj za koji $\left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right) \in \tilde{\Gamma}$ (dakle $h|N$). Funkcija f je holomorfna u kaspu c ako je $l \geq 0$.

Neka je $j \in \mathbb{Z}$ i $\beta = \left(\begin{smallmatrix} 1 & j \\ 0 & 1 \end{smallmatrix}\right)$. Tada matrica $\pm\alpha\beta$ također preslikava kasp ∞ u c. Izračunajmo Fourierov razvoj funkcije $f[\pm\alpha\beta]_k$ u caspu ∞. Lako se vidi da je $f[\pm\alpha\beta]_k(\tau) = (\pm 1)^k f[\alpha]_k(\tau + j)$. Budući da je $e^{2\pi i(\tau+j)/h} = \mu_h^j q_h$, gdje je $\mu_h = e^{2\pi i/h}$ kompleksni h-ti korijen iz jedinice, pa imamo

$$(f[\pm\alpha\beta]_k)(\tau) = (\pm 1)^k \sum_{n=0}^{\infty} a_n \mu_h^{nj} q_h^n.$$

Često nije praktično određivati holomorfnost funkcije u kaspovima koristeći samo definiciju. Srećom, sljedeća propozicija nas spašava.

Propozicija 3.4. *Neka je Γ kongruencijska podgrupa od $\mathrm{SL}_2(\mathbb{Z})$ nivoa N. Pretpostavimo da funkcija $f : \mathbb{H} \to \mathbb{C}$ zadovoljava uvjete (1) i (2) iz Definicije 3.3 i zadovoljava*

(3') *f je holomorfna u kaspu ∞ i koeficijenti Fourierovog razvoj $f(\tau) = \sum_{n=0}^{\infty} a_n q_N^n$ zadovoljavaju $|a_n| \leq Cn^r$ za neke pozitivne konstante C i r.*

Tada je f holomorfna u svakom kaspu od Γ, odnosno $f \in M_k(\Gamma)$.

3.2 Primjer: Eisensteinovi redovi za $\mathrm{SL}_2(\mathbb{Z})$

U ovom odjeljku ćemo dati primjer najjednostavnijih modularnih formi: Eisensteinovih redove za $\mathrm{SL}_2(\mathbb{Z})$. Izračunat ćemo njihove Fourierove razvoje.

Pitanje. Kako konstruirati funkciju $f : \mathbb{H} \to \mathbb{C}$ koja zadovoljava $f[\gamma]_k = f$ za svaki $\gamma \in \mathrm{SL}_2(\mathbb{Z})$?

Možemo pokušati sljedeće. Neka je $g : \mathbb{H} \to \mathbb{C}$ bilo koja funkcija. Definirajmo (formalno)

$$f = \sum_{\gamma \in \Gamma(1)} g[\gamma]_k. \tag{6}$$

Formalno, za $\alpha \in \mathrm{SL}_2(\mathbb{Z})$ vrijedi

$$f[\alpha]_k = \sum_{\gamma \in \Gamma(1)} g[\gamma]_k[\alpha]_k = \sum_{\gamma \in \Gamma(1)} g[\gamma\alpha]_k = [\gamma' := \gamma\alpha] = \sum_{\gamma' \in \Gamma(1)} g[\gamma']_k = f.$$

Dakle ako (6) apsolutno konvergira, onda će f biti invarijantna na djelovanje od $[\alpha]_k$ za svaki $\alpha \in \mathrm{SL}_2(\mathbb{Z})$.

Ovu ideju možemo poopćiti na sljedeći način. Neka je Γ neka podgrupa od $\Gamma(1)$ i g funkcija takva da vrijedi $g[\gamma]_k = g$ za svaki $\gamma \in \Gamma$. Tada je funkcija

$$f = \sum_{\gamma \in \Gamma \backslash \Gamma(1)} g[\gamma]_k$$

(formalno) dobro definirana. (Sumira se po predstavnicima desnih susjednih klasa (right coset representatives) podgrupe Γ).

Kao i ranije, za $\alpha \in \mathrm{SL}_2(\mathbb{Z})$ vrijedi

$$f[\alpha]_k = \sum_{\gamma \in \Gamma \backslash \Gamma(1)} g[\gamma]_k[\alpha]_k = \sum_{\gamma \in \Gamma \backslash \Gamma(1)} g[\gamma\alpha]_k = [\gamma' := \Gamma\gamma\alpha] = \sum_{\gamma' \in \Gamma \backslash \Gamma(1)} g[\gamma']_k = f,$$

budući da množenje s desna s α permutira desne susjedne klase podgrupe Γ.

U suštini, za definiciju Eisensteinovih redova odabrat ćemo paran broj $k > 2$, $g = 1$ i $\Gamma = \{\left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right) : n \in \mathbb{Z}\}$. Primjetimo da je za $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ vrijedi

$$1[\gamma]_k = (c\tau + d)^{-k} = j(\gamma, \tau),$$

specijalno $1[\gamma]_k = 1$ za $\gamma \in \Gamma$.

Definicija 3.5. Za prirodan broj $k > 1$, Eisensteinov red težine $2k$ definiramo formulom

$$G_{2k}(\tau) = \sum_{\substack{m,n \in \mathbb{Z} \\ (m,n) \neq (0,0)}} \frac{1}{(m\tau + n)^{2k}} \tag{7}$$

Propozicija 3.6. *Red* (7) *(za* $G_{2k}(\tau)$*) je apsolutno konvergentan i definira holomorfnu funkciju na* $\mathbb{H}$*.*

Dokaz. Uočimo da brojevi $m\tau + n : m, n \in \mathbb{Z}$ čine rešetku $\Lambda = \mathbb{Z} + \tau\mathbb{Z}$, pa tvrdnja o apsolutnoj konvergenciji slijedi iz sljedeće leme.

Lema 3.7. *Neka je* Λ *rešetka u* $\mathbb{C}$ *i* $s > 2$*. Tada red*

$$\sum_{l \in \Lambda} \frac{1}{|l|^s}$$

konvergira.

Dokaz. Elemente rešetke Λ ćemo particionirati u skupove

$$S_n := \{l \in \Lambda : n - 1 < |l| \leq n\},$$

za $n = 1, 2, \ldots$. Uočimo da je broj elemenata u S_n ugrubo jednak površini kružnog vijenca radiusa $n-1$ i n podijeljenog sa $P(\Lambda)$ -površinom fundamentalne domene od Λ. Točnije $\#S_n \leq 8\pi(n-1)/P(\Lambda)$, tj. $\#S_n < Cn$ za neku apsolutnu konstantu C. Računamo

$$\sum_{l \in \Lambda} \frac{1}{|l|^s} = \sum_{n=1}^{\infty} \sum_{l \in S_n} \frac{1}{|l|^s} < D + \sum_{n=2}^{\infty} Cn(n-1)^{-s} < E \sum_{n} \frac{1}{n^{s-1}} < \infty,$$

za neke konstante D i E. □

Prvo ćemo dokazati da (7) konvergira apsolutno na fundamentalnoj domeni F (vidi Propoziciju 2.6). Neka je $\tau \in F$ (tj. $|\tau| \geq 1$ i $|\Re(\tau)| \leq 1/2$). Vrijedi

$$|m\tau + n|^2 = m^2\tau\bar{\tau} + 2mn\Re(\tau) + n^2 \geq m^2 - mn + n^2 = |m\omega - n|^2,$$

gdje je $\omega = e^{2\pi i/3}$. Kako prema prethodnoj lemi $\sum \frac{1}{|m\omega - n|^{2k}}$ konvergira, slijedi da (6) konvergira uniformno na F, odnosno definira holomorfnu funkciju na F. Iz modularnosti od $G_{2k}(\tau)$ (vidi Korolar 3.12) slijedi da je $G_{2k}(\tau)$ holomorfna na γF za svaki $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. Budući da je $\cup_{\gamma \in \mathrm{SL}_2(\mathbb{Z})} \gamma F = \mathbb{H}$, tvrdnja slijedi.

□

U Fourierovom razvoju Eisensteinovih redova javlja se Riemannova zeta funkcija.

Definicija 3.8. Neka je $\Re(s) > 1$. Riemannova zeta funkcija $\zeta(s)$ je definirana sljedećim redom

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

Propozicija 3.9. *Vrijedi*

$$G_{2k}(\tau) = 2\zeta(2k) \sum_{\gamma \in \Gamma \backslash \Gamma(1)} 1[\gamma]_{2k},$$

gdje je $\Gamma = \{\left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right) : n \in \mathbb{Z}\}$.

Dokaz. Odredimo za početak predstavnike susjednih klasa od $\Gamma\backslash\Gamma(1)$.

Lema 3.10. *Neka su* $\gamma_1 = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ *i* $\gamma_2 = \left(\begin{smallmatrix} e & f \\ c & d \end{smallmatrix}\right)$ *matrice iz* $\mathrm{SL}_2(\mathbb{Z})$. *Tada vrijedi* $\Gamma\gamma_1 = \Gamma\gamma_2$. *Vrijedi i obrat, ako je* $\gamma \in \Gamma\gamma_1$, *tada je* $\gamma = \left(\begin{smallmatrix} g & h \\ c & d \end{smallmatrix}\right)$, *za neke* $g, h \in \mathbb{Z}$.

Dokaz. Računamo

$$\left(\begin{smallmatrix} e & f \\ c & d \end{smallmatrix}\right)\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)^{-1} = \left(\begin{smallmatrix} e & f \\ c & d \end{smallmatrix}\right)\left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & -eb+fa \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma.$$

Obrat slijedi iz

$$\left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \left(\begin{smallmatrix} a+nc & b+nd \\ c & d \end{smallmatrix}\right).$$

□

Neka su c i d relativno prosti cijeli brojevi različiti od nule. Tada postoje (Euklidov algoritam) cijeli brojevi a i b takvi da je $ad-bc=1$, odnosno $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. Iz prethodne leme slijedi da svakom takvom paru (c,d) odgovara jedna klasa iz $\Gamma\backslash\Gamma(1)$ (klase koje odgovaraju parovima (c,d) i $(-c,-d)$ su jednake jer je riječ o klasama u grupi $\mathrm{PSL}_2(\mathbb{Z})$).

Još preostaje odrediti predstavnike $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ za koje je $c=0$ ili $d=0$. Ako je $c=0$ tada je $a=d=\pm 1$ pa za predstavnika možemo odabrati matricu $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Ako je $d=0$, tada je $c=\pm 1$ pa za predstavnika možemo odabrati matricu $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. Dakle, dokazali smo sljedeću lemu.

Lema 3.11. *Skup*

$$S = \left\{\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)\right\} \cup \left\{\left(\begin{smallmatrix} * & * \\ c & d \end{smallmatrix}\right) : (c,d) \in \mathbb{Z}^2, c > 0, d \neq 0 \text{ i } NZM(c,d) = 1\right\},$$

je skup predstavnika susjednih desnih klasa od $\Gamma\backslash\Gamma(1)$.

Računamo

$$\begin{aligned} G_{2k}(\tau) &= \sum_{\substack{m,n\in\mathbb{Z} \\ (m,n)\neq(0,0)}} \frac{1}{(m\tau+n)^{2k}} \\ &= \sum_{\substack{m,n\in\mathbb{Z} \\ m\neq 0, n\neq 0}} \frac{1}{(m\tau+n)^{2k}} + \sum_{0\neq m\in\mathbb{Z}} \frac{1}{(m\tau)^{2k}} + \sum_{0\neq n\in\mathbb{Z}} \frac{1}{n^{2k}} \\ &= \zeta(2k)\left(\sum_{\substack{m,n\in\mathbb{Z} \\ m\neq 0, n\neq 0 \\ GCD(m,n)=1}} \frac{1}{(m\tau+n)^{2k}} + \frac{2}{\tau^{2k}} + 2\right) \\ &= 2\zeta(2k)\left(\sum_{\gamma\in S} 1[\gamma]_{2k}\right). \end{aligned}$$

□

Korolar 3.12. *Za $k > 1$, $G_{2k}(\tau)$ je modularna forma težine $2k$.*

Dokaz. Iz Propozicije 3.6 slijedi da je $G_{2k}(\tau)$ holomorfna na $\mathbb{H}$ i apsolutno konvergentna. Apsolutna konvergencija zajedno sa Propozicijom 3.9 implicira modularnost (što je objašnjeno na početku odjeljka). Još treba provjeriti holomorfnost u beskonačnosti. Vrijedi

$$\begin{aligned}\lim_{\tau\to i\infty} G_{2k}(\tau) &= \lim_{\tau\to i\infty} \sum_{\substack{m,n\in\mathbb{Z}\\(m,n)\neq(0,0)}} \frac{1}{(m\tau+n)^{2k}} \\ &= \sum_{\substack{m,n\in\mathbb{Z}\\(m,n)\neq(0,0)}} \lim_{\tau\to i\infty} \frac{1}{(m\tau+n)^{2k}} = 2\zeta(2k),\end{aligned}$$

gdje druga jednakost slijedi iz apsolutne konvergencije (6). □

Lema 3.13. *Neka je $k \geq 1$ prirodan broj. Tada za svaki $\tau \in \mathbb{H}$ vrijedi*

$$\sum_{n\in\mathbb{Z}} \frac{1}{(\tau+n)^{2k}} = (2\pi i)^{2k} \sum_{r=1}^{\infty} r^{2k-1} e^{2\pi i r\tau}.$$

Dokaz. Koristit ćemo produktni razvoj funkcije sinus

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

Računamo

$$\begin{aligned}\frac{d}{d\tau}\log(\sin(\pi\tau)) &= \frac{1}{\tau} + \sum_{0\neq n\in\mathbb{Z}} \frac{-2\tau}{n^2-\tau^2} \\ &= \frac{1}{\tau} + \sum_{0\neq n\in\mathbb{Z}} \left(\frac{-1}{n+\tau} + \frac{1}{n-\tau}\right).\end{aligned}$$

Sad derivirajući još $(2k-1)$ puta dobivamo

$$\begin{aligned}\frac{d^{2k}}{d\tau^{2k}}\log(\sin(\pi\tau)) &= (2k-1)!\left\{\frac{1}{\tau^{2k}} + \sum_{n=1}^{\infty}\left(\frac{1}{(n+\tau)^{2k}} + \frac{1}{(n-\tau)^{2k}}\right)\right\} \\ &= (2k-1)!\sum_{n\in\mathbb{Z}} \frac{1}{(n+\tau)^{2k}}.\end{aligned}$$

Izračunajmo sad Fourierov red od $\log(\sin(\pi\tau))$. Vrijedi

$$\sin(\pi\tau) = \frac{1}{2\pi}(e^{\pi i\tau} - e^{-\pi i\tau}) = -\frac{1}{2i}e^{-\pi i\tau}(1 - e^{2\pi i\tau}),$$

pa za $\tau \in \mathbb{H}$ imamo

$$\begin{aligned}\log(\sin(\pi\tau)) &= -\log(-2i) - \pi i\tau + \log(1 - e^{2\pi i\tau}) \\ &= -log(-2i) - \pi i\tau + \sum_{r=1}^{\infty} \frac{1}{r} e^{2\pi i r\tau}.\end{aligned}$$

Deriviranjem $2k$ puta dobivamo

$$\frac{d^{2k}}{d\tau^{2k}} \log(\sin(\pi\tau)) = \sum_{r=1}^{\infty} (2\pi i)^{2k} r^{2k-1} e^{2\pi i r\tau}.$$

Tvrdnja slijedi. □

Napomena. Primjetimo da funkcija $\log(\sin(\pi\tau))$ nije dobro definirana na cijelom $\mathbb{H}$, ali njena derivacija je.

Propozicija 3.14. *Neka je $k \geq 2$. Tada je*

$$G_{2k}(\tau) = 2\zeta(2k) + 2\frac{(2\pi i)^{2k}}{(2k-1)!} \sum_{n \geq 1} \sigma_{2k-1}(n) q^n.$$

Dokaz. Vrijedi

$$G_{2k}(\tau) = \sum_{\substack{m,n \in \mathbb{Z} \\ (m,n) \neq (0,0)}} \frac{1}{(m\tau + n)^{2k}} = \sum_{\substack{n \in \mathbb{Z} \\ n \neq 0}} \frac{1}{n^{2k}} + 2 \sum_{m=1}^{\infty} \sum_{n \in \mathbb{Z}} \frac{1}{(m\tau + n)^2}.$$

Prva suma je jednaka $2\zeta(2k)$, dok za drugu sumu koristimo Lemu 3.13 pa dobivamo

$$\begin{aligned}G_{2k}(\tau) &= 2\zeta(2k) + 2\frac{(2\pi i)^{2k}}{(2k-1)!} \sum_{m=1}^{\infty} \sum_{r=1}^{\infty} r^{2k-1} e^{2\pi i r m \tau} \\ &= 2\zeta(2k) + 2\frac{(2\pi i)^{2k}}{(2k-1)!} \sum_{n=1}^{\infty} \sum_{r|n} r^{2k-1} e^{2\pi i n \tau} \\ &= 2\zeta(2k) + 2\frac{(2\pi i)^{2k}}{(2k-1)!} \sum_{n=1}^{\infty} \sigma_{2k-1}(n) q^n.\end{aligned}$$

□

Definicija 3.15. Bernoullievi brojevi B_k su definirani kao koeficijenti sljedećeg reda

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

Npr. $B_1 = -\frac{1}{2}, B_4 = -\frac{1}{30}$ i $B_6 = \frac{1}{42}$.

Zadatak 4. Dokažite da je $B_{2k+1} = 0$ za $k \in \mathbb{N}$.

Zadatak 5. Neka je $k \in \mathbb{N}$. Tada je

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

(Uputa: Izrazite Taylorov red od $\pi\tau \cot(\pi\tau)$ na dva načina: direktno iz definicije i koristeći formulu $\frac{d}{d\tau} \log(\sin(\pi\tau)) = \pi \cot(\pi\tau)$.)

Definicija 3.16. Normalizirani Eisensteinov red $E_{2k}(\tau)$ je red

$$E_{2k}(\tau) := \frac{G_{2k}(\tau)}{2\zeta(2k)}.$$

Iz Zadatka 5. slijedi

$$E_{2k}(\tau) = 1 - \frac{4k}{B_{2k}} \sum_{n \geq 1} \sigma_{2k-1}(n) q^n.$$

Kao što smo spomenuli u Uvodu, Eisensteinov red se može definirati i za $k = 1$

$$G_2(\tau) = \sum_{c \in \mathbb{Z}} {\sum_{d \in \mathbb{Z}}}' \frac{1}{(c\tau + d)^2}.$$

Nije teško vidjeti da red ne konvergira apsolutno (konvergira uvjetno), pa više ne možemo zaključiti kao ranije da je $G_2(\tau)[\alpha]_2 = G_2(\tau)$ za svaki $\alpha \in \mathrm{SL}_2(\mathbb{Z})$ (gdje smo točno koristili apsolutnu konvergenciju?). Zanimljivo je da $G_2(\tau)$ ipak ima neka modularna svojstva.

Propozicija 3.17. *Za $\tau \in \mathbb{H}$ i $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ vrijedi*

$$G_2\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^2 G_2(\tau) - 2\pi i c(c\tau + d).$$

Dokaz. Ideja dokaza (Hecke) je vrlo zanimljiva. Primjetimo da red (6) za $k = 1$ prema Lemi 3.7 "skoro" apsolutno konvergira, tj. ako malo modificiramo sumu dobit ćemo apsolutno konvergenti red

$$G_{2,\varepsilon}(\tau) = {\sum_{m,n}}' \frac{1}{(m\tau + n)^2 |m\tau + n|^{2\varepsilon}} \qquad \text{za } \tau \in \mathbb{H}, \varepsilon > 0,$$

gdje sumiramo po parovima cijelih broja takvih da je $(m, n) \neq (0, 0)$. Slično kao i $G_{2k}(\tau)$, zbog apsolutne konvergencije $G_{2,\varepsilon}(\tau)$ se transformira prema formuli

$$G_{2,\varepsilon}\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^2 |c\tau + d|^{2\varepsilon} G_{2,\varepsilon}(\tau)$$

(umjesto slash operatora $[\alpha]_2$ za "usrednjavanje" koristimo operator $f(\tau) \mapsto f(\frac{a\tau+b}{c\tau+d})(c\tau + d)^{-2} |c\tau + d|^{-2\varepsilon}$). Pokazat ćemo da je

$$\lim_{\varepsilon \to 0} G_{2,\varepsilon}(\tau) = G_2(\tau) - \frac{\pi}{y},$$

gdje je $\tau = x + iy$. Iz toga slijedi da se (ne-holomorfna) funkcija $G_2(\tau) - \frac{\pi}{y}$ transformira kao modularna forma težine 2, pa tvrdnja propozicije slijedi iz sljedećeg računa (prisjetimo se $\Im(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\tau) = \frac{\Im\tau}{|c\tau+d|^2}$)

$$\begin{aligned} G_2\left(\frac{a\tau+b}{c\tau+d}\right) &= (c\tau+d)^2(G_2(\tau) - \frac{\pi}{y}) + \frac{\pi}{y/|c\tau+d|^2} \\ &= (c\tau+d)^2 G_2(\tau) + \frac{\pi}{y}\left(|c\tau+d|^2 - (c\tau+d)^2\right) \\ &= (c\tau+d)^2 G_2(\tau) + \frac{\pi}{y}\left(c^2(|\tau|^2 - \tau^2) + 2cd(x-\tau)\right) \\ &= (c\tau+d)^2 G_2(\tau) + \frac{\pi}{y}\left(c^2(2y^2 - 2ixy) - 2cdyi\right) \\ &= (c\tau+d)^2 G_2(\tau) - 2i\pi c(c\tau+d). \end{aligned}$$

Da bi izračunali limes, definirajmo funkciju I_ε formulom

$$I_\varepsilon(\tau) = 2\int_{-\infty}^{\infty} \frac{dt}{(\tau+t)^2|\tau+t|^{2\varepsilon}} \quad \text{za } \tau \in \mathbb{H}, \varepsilon > -\frac{1}{2}.$$

Tada za $\varepsilon > 0$ imamo

$$G_{2,\varepsilon}(\tau) - \sum_{m=1}^{\infty} I_\varepsilon(m\tau) = 2\sum_{n=1}^{\infty} \frac{1}{n^{2+2\varepsilon}} \tag{8}$$

$$+ 2\sum_{m=1}^{\infty}\sum_{n=-\infty}^{\infty}\left[\frac{1}{(m\tau+n)^2|m\tau+n|^{2\varepsilon}} - \int_n^{n+1} \frac{dt}{(m\tau+t)^2|m\tau+t|^{2\varepsilon}}\right]. \tag{9}$$

Ovim trikom smo postigli to da obje sume u prethodnoj formuli konvergiraju apsolutno i lokalno uniformno za $\varepsilon > -\frac{1}{2}$ pa limes postoji kad $\varepsilon \to 0$ i možemo ga izračunati tako da u formulu uvrstimo $\varepsilon = 0$. Da bi vidjeli zašto je to tako, primjetimo da je izraz u uglatoj zagradi jednak

$$\int_n^{n+1}\left[\frac{1}{(m\tau+n)^2|m\tau+n|^{2\varepsilon}} - \frac{1}{(m\tau+t)^2|m\tau+t|^{2\varepsilon}}\right] dt.$$

Prema teoremu o srednjoj vrijednosti

$$\begin{aligned} \left|\frac{1}{(m\tau+n)^2|m\tau+n|^{2\varepsilon}} - \frac{1}{(m\tau+t)^2|m\tau+t|^{2\varepsilon}}\right| &\leq \max_{t\in[n,n+1]}\left|\frac{d}{dt}\frac{1}{(m\tau+t)^2|m\tau+t|^{2\varepsilon}}\right| \\ &<< |m\tau+n|^{-3-2\varepsilon}, \end{aligned}$$

pa prema Lemi 3.7 druga suma konvergira apsolutno (i lokalno uniformno) za $3 + 2\varepsilon > 2$.

Budući da je $\int_{-\infty}^{\infty} \frac{1}{(m\tau+t)^2} dt = 0$, ako uvrstimo $\varepsilon = 0$ u desnu stranu jednakosti (8) dobit ćemo $G_2(\tau)$.

Preostaje nam još izračunati $\sum_{m=1}^{\infty} I_\varepsilon(m\tau)$.

Za $\varepsilon > -\frac{1}{2}$ imamo

$$\begin{aligned} I_\varepsilon(x+iy) &= 2\int_{-\infty}^{\infty} \frac{dt}{(x+t+iy)^2((x+t)^2+y^2)^\varepsilon} \\ &= 2\int_{-\infty}^{\infty} \frac{dt}{(t+iy)^2(t^2+y^2)^\varepsilon} = \frac{I(\varepsilon)}{y^{1+2\varepsilon}}, \end{aligned}$$

gdje je $I(\varepsilon) = 2\int_{-\infty}^{\infty}(t+i)^{-2}(t^2+1)^{-\varepsilon}dt$, pa je $\sum_{m=1}^{\infty} I_\varepsilon(m\tau) = I(\varepsilon)\zeta(1+2\varepsilon)/y^{1+2\varepsilon}$ za $\varepsilon > 0$. Kako je $I(0) = 0$,

$$I'(0) = -2\int_{-\infty}^{\infty} \frac{\log(t^2+1)}{(t+i)^2}dt = 2\left(\frac{1+\log(t^2+1)}{t+i} - \tan^{-1}t\right)\Bigg|_{-\infty}^{\infty} = -2\pi,$$

i $\zeta(1+2\varepsilon) = \frac{1}{2\varepsilon} + O(1)$ kad $\varepsilon \to 0$ (vidi Zadatak 6), umnožak $I(\varepsilon)\zeta(1+2\varepsilon)/y^{1+2\varepsilon}$ teži u $-2\pi/y$ kad $\varepsilon \to 0$. Tvrdnja slijedi.

□

Napomena. Funkcija $G_2(\tau)$ je primjer kvazi-modularne forme.

Zadatak 6. Dokažite da vrijedi

$$\zeta(1+s) = \frac{1}{s} + O(1), \text{ kad } s \to 0.$$

Primjetimo da Fourierov razvoj funkcije $G_2(\tau)$ možemo izračunati kao i u Propoziciji 3.14 pa vrijedi

$$G_2(\tau) = \frac{\pi^2}{3} - 8\pi^2 \sum_{n\geq 1} \sigma(n)q^n. \tag{10}$$

4 Lagrangeov teorem o sumi četiri kvadrata

4.1 Fourierova transformacija i theta funkcije

Referenca za ovaj odjeljak je §4.9 iz [1].

Za prirodan broj l, prostor izmjerljivih i apsolutno integrabilnih funkcija na $\mathbb{R}^l$ označavamo sa

$$\mathcal{L}^1(\mathbb{R}^l) = \{f : \mathbb{R}^l \to \mathbb{C} : f \text{ izmjerljiva}, \int_{x\in\mathbb{R}^l} |f(x)|dx < \infty\}.$$

Za $f \in \mathcal{L}^1(\mathbb{R}^l)$ definiramo Fourierovu transformaciju $\hat{f} : \mathbb{R}^l \to \mathbb{C}$ formulom

$$\hat{f}(x) = \int_{y\in\mathbb{R}^l} f(y)e^{-2\pi i\langle y,x\rangle}dy,$$

gdje je $\langle\ ,\ \rangle$ standardni skalarni produkt.

Fourierova transformacija $\mathcal{L}^1$ funkcije ne mora biti u $\mathcal{L}^1$, ali ako još vrijedi $\int |f(x)|^2 dx < \infty$, tada vrijedi $\int |\hat{f}(x)|^2 dx < \infty$ (vidi **??**).

Višedimenzionalna generalizacija theta funkcije $\theta(\tau)$ je funkcija $\vartheta(,l) : \mathbb{H} \to \mathbb{C}$ dana formulom

$$\vartheta(\tau, l) = \sum_{n \in \mathbb{Z}^l} e^{\pi i |n|^2 \tau}, \quad \tau \in \mathbb{H},$$

gdje je $|\ |$ standardna apsolutna vrijednost. Red konvergira apsolutno i lokalno uniformno pa definira holomorfnu funkciju. Za $\tau = it$, $t > 0$ i Gaussian $f(x) = e^{-\pi |x|^2}$ imamo

$$\vartheta(it, l) = \sum_{n \in \mathbb{Z}^l} f(nt^{1/2}).$$

Izračunajmo Fourierovu transformaciju Gaussiana $f(x)$ za $l = 1$

$$\hat{f}(x) = \int_{-\infty}^{\infty} e^{-\pi y^2 - 2\pi i x y} dy = e^{-\pi x^2} \int_{-\infty}^{\infty} e^{-\pi (y+ix)^2} dy.$$

Neka je $M > 0$ i C_M pravokutnik $ABCD$ gdje je $A = M$, $B = M + ix$, $C = -M + ix$ i $D = -M$. Kako funkcija $f(z) = e^{-\pi z^2}, z \in \mathbb{C}$ nema polova unutar C_M, Cauchyev integralni teorem povlači $\int_{C_M} f(z) dz = 0$. Kad $M \to \infty$, integrali $\int_{AB} f(z) dz$ i $\int_{CD} f(z) dz$ teže u 0 (jer $f(z)$ na dužinama AB i CD teži u 0) pa imamo da $\int_{-\infty}^{\infty} e^{-\pi (y+ix)^2} dy = \int_{-\infty}^{\infty} e^{-\pi y^2} dy$. Znamo da je $\int_{-\infty}^{\infty} e^{-\pi y^2} dy = 1$ (vidi Zadatak 7), pa smo dokazali da je $\hat{f}(x) = f(x)$ za $l = 1$.

Zadatak 7. Dokažite

$$\int_{-\infty}^{\infty} e^{-\pi x^2} dx = 1.$$

Zadatak 8. Dokažite da je $\hat{f}(x) = f(x)$ za proizvoljan $l \in \mathbb{N}$.

Zadatak 9. Za $l \in \mathbb{N}$ i neka je $h \in \mathcal{L}^1(\mathbb{R}^l)$. Dokažite da je za $r \in \mathbb{R}$ Fourierova transformacija funkcije $h(rx)$ jednaka $r^{-l} \hat{h}(x/r)$.

Za utvrđivanje modularnost theta funkcije trebat će nam formula Poissonove sumacije.

Neka je $h \in \mathcal{L}^1(\mathbb{R}^l)$ takva da suma $\sum_{d \in \mathbb{Z}^l} h(x + d)$ konvergira apsolutno i lokalno uniformno te je još uz to beskonačno diferencijabilna (po x). Formula Poissonove sumacije je nam daje Fourierov razvoj funkcije $\sum_{d \in \mathbb{Z}^l} h(x+d)$ (koja je periodička u odnosu na $\mathbb{Z}^l$)

$$\sum_{d \in \mathbb{Z}^l} h(x + d) = \sum_{m \in \mathbb{Z}^l} \hat{h}(m) e^{2\pi i \langle m, x \rangle}. \tag{11}$$

Prema Zadatku 9, za $t > 0$, Foureirova transformacija funkcije $f(xt^{1/2})$ je jednaka $t^{-l/2} f(xt^{-1/2})$. Ako u formulu (11) uvrstimo $h(x) = f(xt^{-1/2})$ i $x = 0$ (lako se vidi da su pretpostavke zadovoljene), dobit ćemo $\sum f(nt^{1/2}) = t^{l/2} \sum f(nt^{-1/2})$ odnosno

$$\vartheta(i/t, l) = t^{l/2} \vartheta(it, l), \quad t > 0.$$

Kako je holomorfna funkcija $\vartheta(-1/\tau, l) - (-i\tau)^{l/2}\vartheta(\tau, l), \tau \in \mathbb{H}$ jednaka nuli za $\tau \in i\mathbb{R}$, iz teoremu o jedinstvenosti analitičke funkcije (vidi Zadatak 10) jednaka je nuli za svaki $\tau \in \mathbb{H}$, odnosno

$$\vartheta(-1/\tau, l) = (-i\tau)^{l/2}\vartheta(\tau, l), \quad \tau \in \mathbb{H}.$$

Dokažimo sad slabu modularnost funkcije $\theta(\tau) = \vartheta(\tau, 1)$ u odnosu na $\Gamma_0(4)$. Imamo

$$\begin{aligned}\theta\left(\frac{\tau}{4\tau+1}\right) &= \theta\left(-\frac{1}{4(-1/(4\tau)-1)}\right) = \sqrt{2i(\frac{1}{4\tau}+1)}\theta\left(-\frac{1}{4\tau}-1\right)\\ &= \sqrt{2i(\frac{1}{4\tau}+1)}\theta\left(-\frac{1}{4\tau}\right) = \sqrt{2i(\frac{1}{4\tau}+1)(-2i\tau)}\theta(\tau)\\ &= \sqrt{4\tau+1}\theta(\tau).\end{aligned}$$

Formula $\theta(\tau, 4) = \theta(\tau)^4$ daje

$$\theta\left(\frac{\tau}{4\tau+1}, 4\right) = (4\tau+1)^2\theta(\tau, 4).$$

Dakle,

$$\theta(\gamma\tau, 4) = (c\tau+d)^2\theta(\tau, 4), \text{ za } \gamma = \pm\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right) \text{ i } \gamma = \pm\left(\begin{smallmatrix}1 & 0\\ 4 & 1\end{smallmatrix}\right),$$

odnosno

$$\theta(\gamma\tau, 4) = (c\tau+d)^2\theta(\tau, 4), \text{ za } \gamma \in \Gamma_\theta,$$

gdje je $\Gamma_\theta < \mathrm{SL}_2(\mathbb{Z})$ grupa generirana matricama $\pm\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$ i $\pm\left(\begin{smallmatrix}1 & 0\\ 4 & 1\end{smallmatrix}\right)$.

Zadatak 10. Neka je $h(z)$ holomorfna funkcija na otvorenom skupu $\Omega \subset \mathbb{C}$ i $a \in \Omega$. Ako postoji gomilište skupa $\{z \in \Omega : f(z) = 0\}$, dokažite da je onda h jednaka nuli na Ω.

Zadatak 11. Dokažite da je $\Gamma_\theta = \Gamma_0(4)$.

Podsjetimo se, dokazali smo da je $\theta(\tau, 4)$ holomorfna funkcija gornje poluravnine koja je slabo modularna težine 2 u odnosu na grupu $\Gamma_0(4)$ (vidi prethodni zadatak) i koja je holomorfna u kaspu ∞. Prema Propoziciji 3.4, za holomorfnost u ostalim kaspovima dovoljno je pokazati da Fourierovi koeficijenti od $\theta(\tau, 4)$ u kaspu ∞ imaju najviše "polinomijalni rast". To slijedi iz trivijalne ocjene

$$r(n, 4) \leq 16(n+1)^2, \text{ za svaki } n \in \mathbb{N}.$$

Dokazali smo sljedeći teorem

Teorem 4.1.

$$\theta(\tau, 4) \in M_2(\Gamma_0(4))$$

4.2 Eisensteinovi redovi za $M_2(\Gamma_0(4))$

U ovom odjeljku ćemo konstruirati bazu za $M_2(\Gamma_0(4))$. Općenito, za prirodan broj $N > 1$, definirajmo

$$G_{2,N}(\tau) = G_2(\tau) - NG_2(N\tau).$$

Propozicija 4.2. *Neka je $N > 1$ prirodan broj. Vrijedi*

$$G_{2,N}(\tau) \in M_2(\Gamma_0(N)).$$

Dokaz. Neka je $\gamma = \left(\begin{smallmatrix} a & b \\ Nc & d \end{smallmatrix}\right) \in \Gamma_0(N)$. Prema Propoziciji 3.17 vrijedi

$$G_2(\gamma\tau) = (Nc\tau + d)^2 G_2(\tau) - 2\pi i Nc(Nc\tau + d)$$

i

$$G_2(N\gamma\tau) = G_2\left(\frac{a(N\tau) + Nb}{c(N\tau) + d}\right) = (cN\tau + d)^2 G_2(N\tau) - 2\pi i c(cN\tau + d).$$

Dakle, $G_{2,N}(\tau)$ je slabo modularna u odnosu na $\Gamma_0(N)$. Budući da je $G_2(\tau)$ holomorfna na $\mathbb{H}$ i u kaspu ∞, tvrdnja propozicije slijedi iz polinomijalnog rasta Fourierovih koeficijenata od $G_{2,N}(\tau)$ (u suštini koristimo $\sigma(n) = \sum_{d|n} d < 2n$, vidi (10)) i Propozicije 3.4. □

Budući da je $\Gamma_0(2) < \Gamma_0(4)$, vrijedi $M_2(\Gamma_0(2)) \subset M_2(\Gamma_0(4)$. Specijalno $G_{2,2}(\tau), G_{2,4}(\tau) \in M_2(\Gamma_0(4)$.

Prema (10) modularne forme $G_{2,2}(\tau), G_{2,4}(\tau) \in M_2(\Gamma_0(4))$ imaju sljedeći Fourierov razvoj

$$G_{2,2}(\tau) = -\frac{\pi^3}{3}\left(1 + 24\sum_{n=1}^{\infty}\left(\sum_{d|n, 2\nmid d} d\right) q^n\right), \tag{12}$$

$$G_{2,4}(\tau) = -\pi^2\left(1 + 8\sum_{n=1}^{\infty}\left(\sum_{d|n, 4\nmid d} d\right) q^n\right). \tag{13}$$

Specijalno, $G_{2,2}(\tau)$ i $G_{2,4}(\tau)$ su linearno nezavisni. U sljedećem odjeljku ćemo pokazati da razapinju prostor $M_2(\Gamma_0(4))$.

4.3 Dimenzije prostora modularnih formi

U ovom odjeljku ćemo dokazati konačnodimenzionalnost vektorskih prostora modularnih formi i pritom ćemo odrediti $\dim \mathcal{M}_2(\Gamma_0(4))$.

Najelegantniji dokaz koristi Riemann-Rochov teorem (modularne forme interpretiramo kao diferencijale na modularnoj krivulji - Riemannovoj plohi) koji

daje formulu za dimenzije prostora. Samo konačnodimenzionalnost (bez formule) se može dokazati i na elementaran način, koristeći formulu valencije. Pomoću formule valencije, ponekad se može za podgrupe malog indeksa odrediti i dimenzija (što će biti slučaj sa $\Gamma_0(4)$).

Prvo ćemo dokazati formulu valencije (formulu za stupanj divizora diferencijalne forme pridružene modularnoj formi) za $\Gamma(1)$.

Teorem 4.3. *[3, §3.2] Neka je $f(z)$ ne-nul meromorfna modularna forma težine k za $\Gamma(1)$. Za $P \in \mathbb{H}$, neka $v_P(f)$ označava red nultočke od $f(z)$ u točki P (ili minus red pola). Neka je $v_\infty(f)$ red od $f(z)$ u kaspu ∞. Tada vrijedi*

$$v_\infty(f) + \frac{1}{2}v_i(f) + \frac{1}{3}v_\omega(f) + \sum_{P \in \Gamma\backslash\mathbb{H}, P \neq i,\omega} v_P(f) = \frac{k}{12}.$$

Dokaz. Ideja je prebrojiti nultočke i polove u $\Gamma\backslash\mathbb{H}$ integrirajući logaritamsku derivaciju od $f(z)$ oko ruba fundamentalne domene F.

Preciznije, neka je C kontura iz slike ?. Kontura je izabrana tako da sadrži sve nultočke i polove od $f(z)$ u F točno jednom (osim možda i i ω) - točke A i H imaju imaginaran dio jednak M, gdje je M veći od imaginarnog dijela svake nultočke i pola od $f(z)$. To je moguće jer je $f(z)$ meromorfna i u ∞, što znači da točka ∞ nije gomilište nultočaka i polova od ∞ (kod zamjene varijabli $z \mapsto e^{2\pi i z}$ točka ∞ se preslika u 0, dok se niz točaka koji konvergira u ∞ preslika u niz koji konvergira u 0...). Ako se neka nultočka ili pol nalazi na rubu od F, onda konturu deformiramo (vidi sliku, točke P i Q) tako da se unutar konture nalazi točno jedna točka ekvivalentna toj nultočki ili polu.

Prema Cauchyevom teoremu vrijedi

$$\frac{1}{2\pi i}\int_C \frac{f'(z)}{f(z)}dz = \sum_{P \in \Gamma\backslash\mathbb{H}, P \neq i,\omega} v_P(f).$$

Sada ćemo integral izračunati dio po dio. Prvo, integral od A do B (slika ?) se poništava sa integralom od G do H jer je $f(z+1) = f(z)$. Nadalje, integral od H do A ćemo izračunati pomoću zamjene varijabli $q = e^{2\pi i z}$. Neka je $\tilde{f}(q) = f(z) = \sum a_n q^n$ q-razvoj od $f(z)$. Kako je $f'(z) = \frac{d}{dq}\tilde{f}(q)\frac{dq}{dz}$ vidimo da je integral jednak

$$\frac{1}{2\pi i}\int \frac{d\tilde{f}dq}{\tilde{f}q}dq,$$

gdje integriramo po kružnici radijusa $e^{-2\pi M}$ sa središtem u 0. Prema Cauchyevom teoremu taj integral je jednak $-v_\infty(f)$ (minus zbog negativne orijentacije).

Sljedeće računamo integral nad lukovima BC, DE i FG. Prisjetimo se, ako $f(z)$ ima Laurentov razvoj $f(z) = \sum c_m(z-a)^m$, tada je $f'(z)/f(z) = \frac{m}{z-a} + g(z)$, gdje je $g(z)$ holomorfna funkcija u a. Zato će integral od $f'(z)/f(z)$ oko kružnog luka kuta θ (pozitivno orijentiranog), radiusa ε oko a, težiti u $mi\theta$ kad ε teži u θ (integral od $g(z)$ će težiti u nulu). U našem slučaju kutevi koji odgovaraju lukovima BC, DE i FG su $\pi/3$, π i $\pi/3$, pa integrali (kad radius lukova teži u nulu) teže u redom $-v_\omega(f)/6$, $-v_i(f)/2$ i $-v_{-\bar{\omega}}(f)/6 = -v_\omega(f)/6$.

Za kraj, potrebno je još pokazati

$$\frac{1}{2\pi}\int_{CD}\frac{f'(z)}{f(z)}dz+\frac{1}{2\pi}\int_{EF}\frac{f'(z)}{f(z)}dz\to\frac{k}{12}. \tag{14}$$

Primjetimo da transformacija $S:z\mapsto -1/z$ preslikava CD na EF (i pritom mijenja orijentaciju) pa će tvrdnja slijediti iz sljedeće leme.

Lema 4.4. *Neka je* $\gamma=\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right)\in \mathrm{PSL}_2(\mathbb{Z})$, $c\neq 0$ *i neka je* $f(z)$ *meromorfna funkcija na* $\mathbb{H}$ *bez polova i nultočaka na konturi* $C\subset\mathbb{H}$. *Pretpostavimo da vrijedi* $f(\gamma z)=(cz+d)^k f(z)$. *Tada*

$$\int_C\frac{f'(z)}{f(z)}dz-\int_C\frac{f'(z)}{f(z)}dz=-k\int_C\frac{dz}{z+d/c}. \tag{15}$$

Dokaz. Deririvarnjem $f(\gamma z)=(cz+d)^k f(z)$ dobivamo

$$f'(\gamma z)\frac{d\gamma z}{dz}=(cz+d)^k f'(z)+kc(cz+d)^{k-1}f(z).$$

Dijeljenjem dobivamo

$$\frac{f'(\gamma z}{f(\gamma z)}d\gamma z=\frac{f'(z)}{f(z)}dz+k\frac{cdz}{cz+d}.$$

Lijepa strana of (15) je jednaka (nakon supstitucije)

$$\int_C\left(\frac{f'(z)}{f(z)}dz-\frac{f'(\gamma z)}{f'(\gamma z)}d\gamma z\right)=-k\int_C\frac{cdz}{cz+d},$$

pa tvrdnja slijedi. □

Tvrdnja (14) slijedi iz prethodne leme, ako odaberemo $\gamma=\left(\begin{smallmatrix}0 & -1\\ 1 & 0\end{smallmatrix}\right)$. Primjetimo $S(CD)=FE$ pa kad $\varepsilon\to 0$ imamo

$$\frac{1}{2\pi}\int_{CD}\frac{dz}{z}\to\int_{1/3}^{1/4}d\theta=-\frac{1}{12}\quad(\text{gdje je } z=e^{2\pi i\theta}).$$

□

Neka je sada Γ podgrupa od $\Gamma(1)$ konačnog indeksa $[\Gamma(1):\Gamma]$. Za $z\in\mathbb{H}$, označimo sa $n_\Gamma(z):=\#\Gamma_z$, gdje je $\Gamma_z=\{\gamma\in\Gamma:\gamma z=z\}$ stabilizator od z u Γ. Točke za koje je $n_\Gamma(z)>1$ se nazivaju eliptičke točke. Modularna grupa $\Gamma(1)$ ima dvije eliptičke tocke, i i ω.

Zadatak 12. Dokažite da su i i ω jedine eliptičke točke od $\Gamma(1)$, te pokažite da je $n_{\Gamma(1)}(i)=2$ i $n_{\Gamma(1)}(\omega)=3$.

Sljedeći rezultat generalizira prethodni teorem.

Korolar 4.5. *Neka je $f(z)$ ne-nul meromorfna modularna forma težine k za Γ. Tada vrijedi*

$$\sum_{c\in C(\Gamma)} v_c(f) + \sum_{P\in\Gamma\backslash\mathbb{H}} \frac{v_P(f)}{n_\Gamma(P)} = \frac{k[\Gamma(1):\Gamma]}{12}, \tag{16}$$

gdje je $C(\Gamma)$ skup (neekvivalentnih) kaspova od Γ.

Dokaz. Neka je $g(z) = \prod_{\gamma\in\Gamma(1)/\Gamma} f[\gamma]_k$. Uočimo da je $g(z)$ modularna forma težine $k[\Gamma(1):\Gamma]$ za $\Gamma(1)$. Naime za $\alpha\in\Gamma(1)$ imamo

$$g[\alpha] = \prod_{\gamma\in\Gamma\backslash\Gamma(1)} f[\gamma]_k[\alpha]_k = \prod_{\gamma\in\Gamma\backslash\Gamma(1)} f[\gamma\alpha]_k = \prod_{\gamma'\in\Gamma\backslash\Gamma(1)} f[\gamma']_k = g,$$

jer množenje s α s desna permutira elemente skupa $\Gamma\backslash\Gamma(1)$. Prema formuli valencije za $\Gamma(1)$ vrijedi

$$\sum_{c\in C(\Gamma(1))} v_c(g) + \sum_{P\in\Gamma(1)\backslash\mathbb{H}} \frac{v_P(g)}{n_\Gamma(P)} = \frac{k[\Gamma(1):\Gamma]}{12}.$$

S druge strane, za $z\in\tilde{\mathbb{H}}$ i valuaciju v_z vrijedi

$$v_z(g) = v_z\left(\prod_{\gamma\in\Gamma\backslash\Gamma(1)} f[\gamma]_k\right) = \sum_{\gamma\in\Gamma\backslash\Gamma(1)} v_z(f[\gamma]_k) = \sum_{\gamma\in\Gamma\backslash\Gamma(1)} v_{\gamma z}(f),$$

pa tvrdnja slijedi. □

Korolar 4.6. *Prostor $M_k(\Gamma)$ je konačno dimenzionalan. Vrijedi*

$$\dim M_k(\Gamma) \le \frac{k[\Gamma(1):\Gamma]}{12} + 1.$$

Dokaz. Prema (16), modularna forma iz $M_k(\Gamma)$ imau u kaspu ∞ nultočku reda najviše $\frac{k[\Gamma(1):\Gamma]}{12}$. Pretpostavimo da postoji više od $\frac{k[\Gamma(1):\Gamma]}{12}+1$ linearno nezavisnih modularnih formu. Onda možemo konstruirati (npr. Gaussovom eliminacijom) njihovu linearnu kombinaciju čijih prvih $\frac{k[\Gamma(1):\Gamma]}{12}+1$ Fourierovih koeficijenata izčezava, što je kontradikcija sa pretpostavkom o redu nultočke u kaspu ∞. □

Korolar 4.7. *Vrijedi*

$$\dim M_2(\Gamma_0(4)) = 2.$$

Dokaz. Iz §4.2 slijedi da je $\dim M_2(\Gamma_0(4)) \ge 2$. Indeks od $\Gamma_0(4)$ u $\Gamma(1)$ je šest (vidi Zadatak 1), tako da tvrdnja slijedi iz prethodnog korolara. □

4.4 Problem sume četiri kvadrata i generalizacije

U prethodna dva odjeljka smo pokazali da su modularne forme $G_{2,2}(\tau) = G_2(\tau) - 2G_2(2\tau)$ i $G_{2,4}(\tau) = G_2(\tau) - 4G_2(4\tau)$ baza za $M_2(\Gamma_0(4))$, pa je $\theta(\tau, 4)$ njihova linearna kombinacija. Iz q-razvoja

$$\begin{aligned} \theta(\tau,4) &= 1 + 8q + \cdots, \\ -\frac{3}{\pi^2} G_{2,2}(\tau) &= 1 + 24q + \cdots, \\ -\frac{1}{\pi^2} G_{2,4}(\tau) &= 1 + 8q + \cdots, \end{aligned}$$

se vidi da je $\theta(\tau, 4) = -\frac{1}{\pi^2} G_{2,4}(\tau)$. Izjednačavanjem odgovarajućih Fourierovih koeficijenata dobivamo

$$r(n,4) = 8 \sum_{d|n, 4\nmid d} d.$$

Postoji li za druge vrijednosti od k slična formula za $r(n, k)$?

Kad je $k > 1$ neparan, $\theta(\tau, k)$ je modularna forma polucijele težine $k/2$ (tu klasu modularnih formi ćemo definirat u jednom od narednih poglavlja) i u tom slučaju ne postoji jednostavna formula za Fourierov razvoj Eisensteinovih redova. Npr. za $k = 3$ i $n \equiv 3 \pmod 4$ kvadratno slobodan, može se pokazati da je $r(n, 3)$ u suštini jednak broja klasa $h(-n)$ kvadratno imaginarnog polja $\mathbb{Q}(\sqrt{-n})$.

Ako je k paran tada možemo primjeniti istu metodu kao za $k = 4$ (u slučaju kad je $k \equiv 2 \pmod 4$ vrijedi $\theta(\tau, k) \in M_{k/2}(\Gamma_1(4))$; primjetimo da je $\Gamma_1(4) = \{\pm I\}\Gamma_0(4))$. Jedino je upitno hoće li se $\theta(\tau, k)$ moći prikazati pomoću Eisensteinovih redova (za čije Fourierove koeficijente imamo jednostavne formule). Može se pokazati da se za $k \in \{2, 4, 6, 8\}$ prostor $M_2(\Gamma_1(4))$ sastoji samo od Eisensteinovih redova i pa onda za takve k postoji jednostavna formula za $r(n, k)$.

Zadatak 13. Nađite formulu za $r(n, 8)$.

Može se pokazati (Tasaka [4]) da je prostor $M_k(\Gamma_0(2))$, za $k \geq 4$ paran, razapet sa produktima Eisensteinovih redova manje težine, tj. skup

$$\{G_k^0(\tau), G_{2l}^0(\tau) G_{k-2l}^0(\tau) : (2 \leq l \leq [k/4])\}$$

je njegova baza. Ovdje je $G_k^0(\tau) = \frac{1}{2(2\pi i)^k} \sum_{m \in 2\mathbb{Z}, n \in 2\mathbb{Z}+1} \frac{1}{(m\tau + n)^k}$ Eisensteinov red iz $M_k(\Gamma_0(2))$ pridružen kaspu 0.

Odavde slijedi da se $r(n, k)$ uvijek može prikazati kao linearna kombinacija "konvolucija" $\rho_{r,s}^0(n) = \sum_{m=1}^{n-1} \sigma_r^0(m)\sigma_s^0(n-m)$ divizorskih funkcija $\sigma_k^0(n) = \sum_{d|n, n/d \equiv 1 \bmod 2} d^{k-1}$.

Osim točnih formula, može se proučavati i asimptotsko ponašanje brojeva $r(n,k)$, kad $n \to \infty$. Npr. za $k \geq 5$, Hardy i Littlewood su koristeći "circle method" dokazali

$$r(n,k) \sim A_k n^{\frac{k}{2}-1} \sum_{d|n} (-1)^{N+N/d} d^{1-k/2},$$

za neku (eksplicitnu) konstantu A_k.

Za kraj spomenimo još dva zanimljiva rezultata iz teorije kvadratnih formi. Za pozitivno definitnu kvadratnu formu kažemo da je univerzalna ako reprezentira sve prirodne brojeve (tj. ako se svi prirodni brojevi nalaze u njenoj slici). Npr. pokazali smo da je forma $Q(x,y,z,w) = x^2 + y^2 + z^2 + w^2$ univerzalna. Integralnost kvadratnih formi možemo definirati na dva načina. Kažemo da je kvadratna forma integralna ako su joj svi koeficijenti cjelobrojni, dok kažemo da ima integralnu matricu ako joj je pridružena matrica cjelobrojna (matrica A je pridružena kvadrtnoj formu $Q(x_1,\ldots,x_n)$ ako vrijedi $Q(x_1,\ldots x_n) = (x_1,\ldots,x_n)A(x_1,\ldots,x_n)^t$). Npr. forma $x^2 + xy + y^2$ je integralna ali nema integralnu matricu. Sljedeća dva teorema na vrlo elegantan način opisuju univerzalne (integralne) kvadratne forme.

Teorem 4.8 (Teorem 15; Conway, Schneeberger)**.** *Ako integralna pozitivno definitna kvadratna forma s integralnom matricom reprezentira sve brojeve od* 1 *do* 15*, onda je univerzalna.*

Tvrdnja je najbolja moguća jer npr. forma $x^2+2y^2+5z^2+5w^2$ reprezentira sve prirodne brojeve osim 15.

Teorem 4.9 (Teorem 290; Bhargava, Hanke)**.** *Ako integralna pozitivno definitna kvadratna forma reprezentira sve prirodne brojeve do* 290*, onda je univerzalna.*

5 Problem klasifikacije kongruentnih brojeva

Počnimo s definicijom.

Definicija 5.1. Kažemo da je pozitivan racionalan broj $r \in \mathbb{Q}$ kongruentan broj ako postoji pravokutan trokut s racionalnim stranicama čija je površina jednaka r.

Npr. 5 je kongruentan broj jer pravokutni trokut sa stranicama $(20/3, 3/2, 41/6)$ ima površinu 5.

Zadatak 14. Dokažite da 1 nije kongruentni broj.

Pretpostavimo da je $r \in \mathbb{Q}$ površina pravokutnog trokuta sa stranicama $X, Y, Z \in Q$. Tada je za svaki $s \in \mathbb{Q}$ i broj $s^2 r$ površina pravokutnom trokuta sa racionalnim stranicama (sX, sY, sZ) pa ćemo ubuduće pretpostaviti da je $r = n$ kvadratno slobodan prirodan broj.

Pitanje. Neka je n prirodan broj. Je li n kongruentan broj? Postoji li neki jednostavan kriterij ili postupak koji bi nam dao odgovor na to pitanje?

Iako su još i stari Grci proučavali pravokutne trokute s racinalnim stranicama, problem klasifikacije su prvi put ozbiljno počeli izučavati arapski matematičari u desetom stoljeću (vidi [2, Poglavlje 16]). Nakon toga je više slavnih matematičara puno truda uložilo u rješavanje nekih specijalnih slučajeva. Tako je Euler prvi pokazao da je 7 kongruentan broj dok je Fermat je pokazao da 1 nije (taj rezultat je ekvivalentan činjenici da jednadžba $X^4+Y^4 = Z^4$ nema cjelobrojnih rješenja).

Nije bilo značajnijeg napretka na rješavanju problema sve do druge polovice dvadesetog stoljeća kada je Tunnel dokazao ovaj fantastičan teorem.

Teorem 5.2 (Tunnell, 1983)**.** *Neka je n neperan kvadratno slobodan prirodan broj. Promotrimo sljedeće dvije tvrdnje:*

a) n je kongruentan

b) broj trojki cijelih brojeva (x, y, z) koje zadovoljavaju jednadžbu $2x^2 + y^2 + 8z^2 = n$ je dvostruko veći od broja trojki koji zadovoljavaju $2x^2 + y^2 + 32z^2 = n$.

Tada a) implicira b). Ako pretpostavimo da je slabi oblik Birch i Swinnerton-Dyerove slutnje točan, onda i b) implicira a).

U ovom poglavlju ćemo se upoznati s matematikom potrebnom za razumijevanje Tunnellovog rezultata. Ukratko, pokazat ćemo da je $n \in \mathbb{N}$ kongruentan broj ako i samo ako eliptička krivulja $E_n : y^2 = x^3 - n^2x$ ima beskonačno mnogo racionalnih točaka, odnosno ako ima pozitivan rang. Birch i Swinnerton-Dyerova (BSD) slutnja povezuje rang eliptičke krivulje sa kritičnom vrijednošću Hasse-Weil L-funkcije $L(E_n, s)$ u točki $s = 1$, preciznije $\text{rang}(E_n) > 0 \iff L(E_n, 1) = 0$. S druge strane, za svaku eliptičku krivulju E definiranu nad poljem racionalnih brojeva postoji modularna forma težine 3/2 (Shimurina korespodencija) čiji Fourierovi koeficijenti sadrže informaciju o kritičnim vrijednostima L-funkcija pridruženih kvadratnim zakreti krivulje E. Budući da su naše krivulje E_n kvadratni zakreti krivulje E_1, potrebno je istražiti koji su Fourierovi koeficijenti modularne forme $f(\tau)$ pridružene krivulji E_1 jednaki nuli. Pokaže se da je $f(\tau)$ linearna kombinacija theta funkcija pridruženih kvadratnim formama iz Teorema 5.2 pa će n-ti koeficient biti jednak nuli upravo onda kada je zadovoljen uvjet b) iz Teorema 5.2. Dakle, uz pretpostavku BSD slutnje, kvadratno slobodan neparan broj n je kongruentan broj ako i samo ako je odgovarajući koeficijent konkretne modularne forme jednak nuli (tj. ako je uvjet b) iz Teorema 5.2 zadovoljen). BSD slutnja nije dokazana, ali je npr. poznato da $L(E, 1) \neq 0$ implicira $\text{rang}(E) = 0$ (Kolyvagin), pa je onda implikacija $a) \Rightarrow b)$ iz Teorema 5.2 "bezuvjetno" točna.

Glavna referenca za ovo poglavlje je odlična knjiga: N. Koblitz, Introduction to Elliptic Curves and Modular Forms [3].

5.1 Od kongruentnih brojeva do eliptičkih krivulja

U ovom odjeljku ćemo na elementaran način objasniti vezu između kongruentnih brojeva i racionalnih rješenja kubične jednadžbe $y^2 = x^3 - n^2x$. Prvi korak u tom smjeru je sljedeća propozicija.

Propozicija 5.3. *Neka je n kvadratno slobodan prirodan broj. Neka su X, Y, Z pozitivni racionalni brojevi za koje vrijedi $X < Y < Z$. Postoji bijekcija između pravokutnih trokuta s katetama X i Y, hipotenuzom Z površine n i $x \in \mathbb{Q}$ za koje su brojevi $x, x+n$ i $x-n$ kvadrati racionalnih brojeva. Bijekcija je dana formulama:*

$$X, Y, Z \to x = (Z/2)^2$$

$$x \to X = \sqrt{x+n} - \sqrt{x-n}, \quad Y = \sqrt{x+n} + \sqrt{x-n}, \quad Z = 2\sqrt{x}.$$

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

Dokaz. Pretpostavimo prvo da su X, Y, Z stranice pravokutnog trokuta površine n, tj. $X^2 + Y^2 = Z^2$ i $\frac{1}{2}XY = n$. Ako dodamo ili oduzmemo četiri puta drugu jednadžbu od prve dobit ćemo $(X \pm Y)^2 = Z^2 \pm 4n$. Ako sad podijelimo izraz sa 4, vidimo za $x = (Z/2)^2$ vrijedi da su brojevi $x \pm n$ kvadrati brojeva $(X \pm Y)/2$. Obratno, za x sa traženim svojstvom, lako se vidi da X, Y i Z (dani formulama iz propozicije) zadovoljavaju $XY = 2n$, $X^2 + Y^2 = Z^2$ i $0 < X < Y < Z$. Bijektivnost slijedi iz činjenice da ne postoje dva racionalna trokuta iste površine s jednakom hipotenuzom. □

Pretpostavimo da je n kongruentan broj i x takav da su x, $x-n$ i $x+n$ kvadrati racionalnih brojeva. Posebno, $y = \sqrt{x(x-n)(x+n)}$ je racionalan broj pa par racionalnih brojeva (x, y) zadovoljava kubičnu jednadžbu

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

Nas zanima obrat ove tvrdnje, tj. zanima nas koja racionalna rješenja (x, y) gornje jednadžbe "dolaze" od pravokutnog trokuta (kao u prethodnoj propoziciji). Kako je $x = (Z/2)^2$ vidimo da je prvi nužan uvjet taj da x mora biti kvadrat racionalnog broja. Također, nazivnik od x mora biti paran. To je zato što postoji $s \in \mathbb{Z}$ takav da su sX, sY, sZ primitivna Pitagorina trojka (relativno prosti prirodni brojevi koji čine stranice pravokutnog trokuta). Lako se vidi da je sZ neparan broj (kvadrat prirodnog broja daje ostatak 0 ili 1 pri djeljenju sa 4 pa je za neparne a i b, $a^2 + b^2 \equiv 2 \not\equiv c^2 \pmod 4$) pa onda $Z/2 = sZ/(2s)$ ima paran nazivnik. Treći nužan uvjet je da brojnik od x mora biti relativno prost sa n, jer ako postoji prost broj $p > 2$ koji dijeli brojnik od x, tada p dijeli i brojnik od $x \pm n = ((X \pm Y)/2)^2$ pa onda dijeli i brojnik od $(X \pm Y)/2$, a onda i brojnik od $(X+Y)+(X-Y)$ i $(X+Y)-(X-Y)$. Dakle $p^2 | \frac{1}{2}XY = n$ što nije moguće jer je n po pretpostavci kvadratno slobodan. Pokazat ćemo da su ova tri nužna uvjeta ujedno i dovoljna.

Propozicija 5.4. *Neka je (x, y) točka s racionalnim koordinatama (kažemo racionalna točka) na krivulji $y^2 = x^3 - n^2x$. Pretpostavimo da x zadovoljava tri uvjeta:*

a) kvadrat je racionalnog broja

b) ima paran nazivnik

c) brojnik mu je relativno prost sa n.

Tada postoji pravokutni trokut sa racionalnim stranicama površine n (koji je u korespodenciji s brojem x po bijekciji iz Propozicije 5.3).

Dokaz. Neka je $u = \sqrt{x} \in \mathbb{Q}^+$ i neka je $v = y/u$, tj. $n^2 + v^2 = x^2$. Neka je t nazivnik od u. Po pretpostavci t je paran. Primjetimo da v^2 i x^2 imaju isti nazivnik (jer $x^2 - v^2 \in \mathbb{Z}$) koji je jedanak t^4 pa je t^2v, t^2n i t^2x primitivna Pitagorina trojka (to slijedi iz uvjeta c)). Iz klasifikacije primitivnih Pitagorinih trojki slijedi da postoje prirodni brojevi a i b takvi da je $t^2n = 2ab, t^2v = a^2 - b^2$ i $t^2x = a^2 + b^2$. Tada pravokutni trokut sa stranicama $2a/t, 2b/t, 2u$ ima površinu $2ab/t^2 = n$. Slika tog pravokutnika po bijekciji iz Propozicije 5.3 je $x = (Z/2)^2 = u^2$ što je trebalo i dokazati. □

U sljedećem odjeljku ćemo okarakterizirati točke na (eliptičkoj) krivulji $y^2 = x^3 - n^2x$ koje odgovaraju racionalnim pravokutnim trokutima pomoću grupovne operacije na eliptičkoj krivulji.

5.2 Eliptičke krivulje

Krivulja $y^2 = x^3 - n^2x$ koju smo susreli u prethodnom odjeljku je primjer eliptičke krivulje

Definicija 5.5. Neka je K polje karakteristike različite od 2 i neka je $f(x) \in K[x]$ kubični polinom bez višestrukih korijena. Neka je K' proširenje od K. Skup K'-racionalnih točaka na eliptičkoj krivulji

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

je skup svih točaka $(x, y) \in K' \times K'$ koje zadovoljavaju gornju jednadžbu zajedno s još jednom točkom koju označavamo s $\mathcal{O}$ i zovemo točka u beskonačnosti. Kažemo da je eliptička krivulja E definirana nad poljem K.

Općenito, za točku $(x_0, y_0) \in K' \times K'$ na krivulji C definiranoj jednadžbom $F(x, y) = 0$ (gdje je $F(x, y) \in K[x, y]$) kažemo da je nesingularna ako parcijalne derivacije $\partial F/\partial x$ i $\partial F/\partial y$ nisu oboje jednake nuli u točki (x_0, y_0). U našem slučaju $F(x, y) = y^2 - f(x)$ pa su parcijelne derivacije u točki (x_0, y_0) jednake $2y_0$ i $-f'(x_0)$. Budući da polje K nije karakteristike 2, parcijalne derivacije mogu oboje biti jednake nuli samo ako je $y_0 = 0$ i $f'(x_0) = 0$, odnosno ako je x_0 dvostruka nultočka polinoma $f(x)$. Dakle, eliptička krivulja je nesingularna u svakoj svojoj točki. Ta činjenica će nam biti važna kod definicije grupovne operacije jer nam osigurava postojanje tangente u svakoj točki eliptičke krivulje.

Za razumijevanje točke u beskonaćnosti, napišimo jednadžbu eliptičke krivulje u projektivnim koordinatama. Za polinom $F(x,y)$ stupnja n definiramo njemu pridruženi homogeni polinom $\tilde{F}(x,y,z)$ sljedećom formulom

$$\tilde{F}(x,y,z) = z^n F\left(\frac{x}{z}, \frac{y}{z}\right).$$

Npr. ako je $F(x,y) = y^2 - x^3 + n^2 x$, onda je $\tilde{F}(x,y,z) = zy^2 - x^3 + n^2 xz^2$. Primjetimo, $F(x,y) = \tilde{F}(x,y,1)$. Vrijedi

a) $\tilde{F}(\lambda x, \lambda y, \lambda z) = \lambda^n \tilde{F}(x,y,z)$

b) za $z \neq 0$, $\tilde{F}(x,y,z) = 0$ ako i samo ako $\mathbb{F}(x/z, y/z) = 0$.

Dakle, ako je (x,y,z) nultočka polinoma $\tilde{F}$ onda je i $(\lambda x, \lambda y, \lambda z)$ nultočka za svaki $\lambda \in K$. Ovo svojstvo homogenih polinoma motivira sljedeću definiciju.

Definicija 5.6. Projektivna ravnina $\mathbb{P}^2_K$ je skup klasa ekvivalencija trojki $(x,y,z) \in K^3, (x,y,z) \neq (0,0,0)$, gdje dvije trojke (x,y,z) i (x',y',z') identificiramo ako postoji $\lambda \in K$ takva da je $(x,y,z) = \lambda(x',y',z')$.

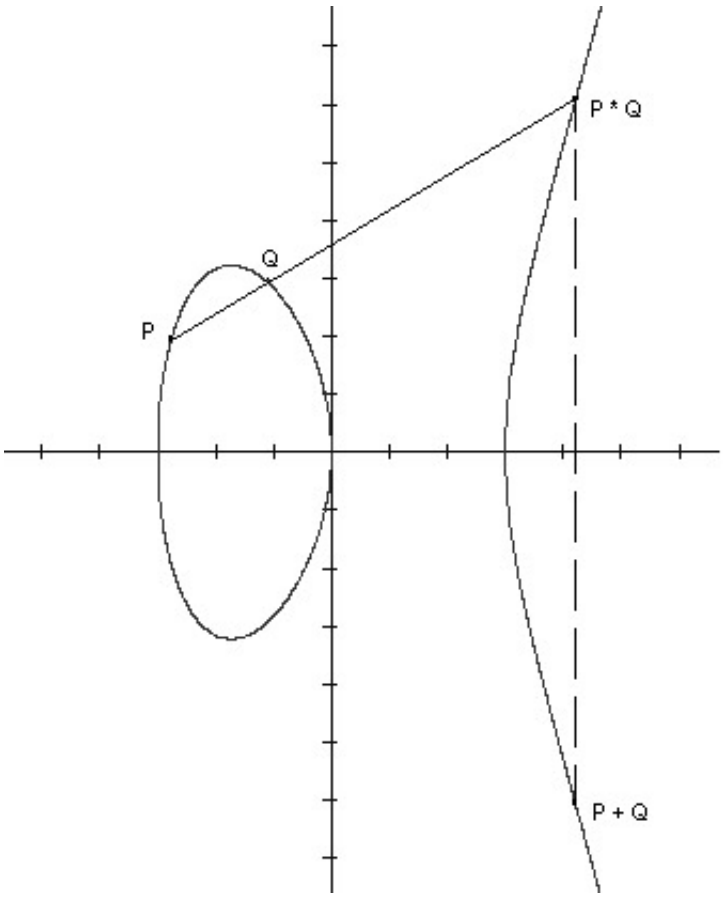
Promotrimo skup rješenja jednadžbe $\tilde{F}(x,y,z) = 0$ u $\mathbb{P}^2_K$. Rješenja za koje je $z \neq 0$ su u bijekciji s rješenjima $F(x,y) = 0$, pa krivulju $\tilde{F}(x,y,z) = 0$ zovemo projektivno proširenje krivulje $F(x,y) = 0$. Preostale točke leže na projektivnom pravcu $z = 0$ koji nazivamo pravac u beskonačnosti. U našem primjeru, $\tilde{F}(x,y,z) = y^2 z - x^3 + n^2 xz^2 = 0$, točke u beskonačnosti su rješenja $\tilde{F}(x,y,0) = -x^3 = 0$. U projektivnom prostoru postoji samo jedno rješenje ove jednadžbe i to je točka $(0,1,0)$. Ta točka odgovara točki $\mathcal{O}$ iz definicije eliptičke krivulje. Primjetimo da je $\mathcal{O}$ (K-)racionalna točka, tj. $\mathcal{O} \in E(K)$.

5.3 Grupovna operacija na eliptičkoj krivulji

U ovom odjeljku ćemo definirati operaciju zbrajanja na eliptičkoj krivulji E. Radi jednostavnosti pretpostavimo da je eliptička krivulja definirana nad polje realnih brojeva. Neka su $P, Q \in E(\mathbb{R})$ točke različite od $\mathcal{O}$. Pretpostavimo prvo $P \neq Q$. Pravac kroz P i Q siječe $E(\mathbb{R})$ u točki $P * Q$. Zbroj točaka P i Q definiramo kao točku osno simetričnu točki $P * Q$ u odnosu na x-os.

Ako je $P = Q$, tada je točka $P * Q$ presjek od $E(\mathbb{R})$ i tangente na krivulju kroz P. Po definiciji je $\mathcal{O} + P = P + \mathcal{O} = P$ i $\mathcal{O} + \mathcal{O} = \mathcal{O}$. Uz ovako definirano zbrajanje E je abelova grupa. Očito je da je $\mathcal{O}$ neutralni element i da je $-P$ točka osnosimetrična točki P i odnosu na x-os (primjetimo da pravac kroz P i $-P$ prolazi kroz točku u beskonačnosti $\mathcal{O}$). Asocijativnost je najteže provjeriti.

Operaciju zbrajanja možemo opisati i pomoću koordinata. Radi određenosti pretpostavimo da je $f(x) = x^3 + ax + b$. Ako je $P = (x_1, y_1)$ i $Q = (x_2, y_2)$ tada



Slika 3: Operacija zbrajanja na eliptičkoj krivulji $y^2 = x^3 - 9x$

vrijedi

$$\begin{aligned} x(P+Q) &= \left(\frac{y_2-y_1}{x_2-x_1}\right)^2 - x_1 - x_2, \\ y(P+Q) &= -y_1 + (x_1 - x(P+Q))\,\frac{y_2-y_1}{x_2-x_1}, \\ x(2P) &= \left(\frac{3x_1^2+a}{2y_1}\right)^2 - 2x_1, \\ y(2P) &= -y_1 + (x_1 - x(2P))\frac{3x_1^2+a}{2y_1}. \end{aligned} \tag{17}$$

Pomoću ovih formule možemo definirati zbrajanje na eliptičkim krivuljama koje su definirane nad poljima karakteristike različite od 2 i 3. Važno je primjetiti da ako su $P, Q \in E(K')$, da je onda i $P+Q \in E(K')$.

Iz formula za zbrajanje (17) lako se dokazuje sljedeća propozicija.

Propozicija 5.7. *Neka je P racionalna točka na eliptičkoj krivulji $E_n : y^2 = x^3 - n^2x$ (n je neparan i kvadratno slobodan). Ako P nije reda 2 (tj. $y(P) \neq 0$), tada je x-koordinata točke $2P$ kvadrat racionalnog broja sa parnim nazivnikom i brojnikom koji je relativno prost sa n.*

Dokaz. Neke je $P = (x_1, y_1) \in E_n(\mathbb{Q})$. Tada iz (17) slijedi

$$\begin{aligned} x(2P) &= \left(\frac{3x_1^2-n^2}{2y_1}\right)^2 - 2x_1 = \frac{(3x_1^2-n^2)^2 - 2x_1 4y_1^2}{(2y_1)^2} \\ &= \left(\frac{x_1^2+n^2}{2y_1}\right)^2. \end{aligned}$$

Neka je $x = \frac{p_1}{q_1}$ i $y = \frac{p_2}{q_2}$, gdje su $p_1, q_1, p_2, q_2 \in \mathbb{Z}$ i $NZM(p_1, q_1) = 1$ i $NZM(p_2, q_2) = 1$. Treba dokazati da je nazivnik razlomka $\frac{(p_1^2+n^2q_1^2)q_2}{2p_2q_1^2}$ paran. Ako $2^k | q_2$, onda iz $p_2^2q_1^3 = p_1^3q_2^2 - n^2p_1q_2^2q_1^2$ slijedi $2^k | q_1^2$ i $p_1^2 + q_1^2n^2$ je neparan. Ako $2 \nmid q_2$ i $2 | p_1^2 + q_1^2n^2$, onda imamo dva slučaja. Prvo, ako su p_1 i q_1 neparni, onda iz prethodnog identiteta slijedi $2 | p_2$, no $4 \nmid p_1^2 + n^2q_1^2$ (kvadrat daje ostatak 0 ili 1 modulo 4). Ako je p_1 ili q_1 paran onda $2 \nmid p_1^2 + n^2q_1^2$ pa je nazivnik paran.

Pretpostavimo da prost p dijeli n i brojnik od $x(2P) = \frac{r}{s}$. Budući da je n kvadratno slobodan $p || n$, a kako je $x(2P)$ kvadrat $p^2 | r$. Iz jednadžbe eliptičke krivulje E_n slijedi da p^3 točno dijeli brojnik od $y(2P)^2$ što nije moguće. □

5.4 Mordellov teorem i točke konačnog reda

U prethodnom odjeljku smo pokazali kako na skupu racionlnih točaka eliptičke krivulje $E(\mathbb{Q})$ možemo definirati strukturu abelove grupe. Vrijedi i puno više.

Teorem 5.8 (Mordell)**.** *Neka je E eliptička krivulja definirana nad $\mathbb{Q}$. Tada je grupa $E(\mathbb{Q})$ konačno generirana.*

Svaka konačno generirana abelova grupa G je izomorfna s $\mathbb{Z}^r \oplus G_{\text{tors}}$, gdje je r nenegativan cijeli broj, a G_{tors} konačna podgrupa elemenata konačnog reda. Dakle, $E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})_{\text{tors}}$. Broj r se naziva rang eliptičke krivulje, a $E(\mathbb{Q})_{\text{tors}}$ se zove torzija eliptičke krivulje. Primjetimo da eliptička krivulja ima beskonačno mnogo racionalnih točaka ako i samo ako joj je rang pozitivan.

Pitanje. Što možemo reći o torziji eliptičke krivulje?

Propozicija 5.9. *Neka je E eliptička krivulja definirana nad bilo kojim poljem algebarskih brojeva K. Tada postoji najviše N^2 točaka reda koji dijeli N nad nekim proširenjem K' od K. Jednakost se postiže ako je $K' = \overline{K}$ algebarski zatvarač od K.*

Ako nas zanima racionalna torzija eliptičke krivulje definirane nad $\mathbb{Q}$, možemo biti puno precizniji.

Teorem 5.10 (Mazur)**.** *Neka je E eliptička krivulja definirana nad poljem racionalnih brojeva. Tada je racionalna torzija $E(\mathbb{Q})_{\text{tors}}$ izomorfna jednoj od sljedećih petnaest grupa:*

- $\mathbb{Z}/n\mathbb{Z}$ *za* $1 \leq n \leq 10$ *ili* $n = 12$,
- $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ *za* $n \in \{2, 4, 6, 8\}$.

Vratimo se sad na našu eliptičku krivulju $E_n : y^2 = x^3 - n^2 x$. Vidimo da se na njoj nalaze tri točke reda 2: $(0,0), (n,0), (-n,0)$, kao i točka u beskonaćnosti $\mathcal{O}$. Pokazat ćemo da su to jedine racionalne točke konačnog reda na E_n.

Propozicija 5.11. $\#E_n(\mathbb{Q}) = 4$.

Dokaz propozicije se bazira na injektivnosti redukcije racionalne torzije eliptičke krivulje modulo prost broj p. Ideja je vrlo jednostavna. Neka je p prost broj. Postoji prirodno preslikavanje $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p$: $a \in \mathbb{Z} \mapsto \overline{a} = a \bmod p \in \mathbb{Z}/p\mathbb{Z}$. Primjetimo da se element iz $\mathbb{P}^2(\mathbb{Q})$ može zapisati kao (x, y, z) gdje su $x, y, z \in \mathbb{Z}$ takvi da je njihova zajednička mjera jednaka 1, tako da prethodno definirano preslikavanje proširujemo do preslikavanja $\mathbb{P}^2(\mathbb{Q}) \to \mathbb{P}^2(\mathbb{F}_p)$ koje trojci (x, y, z) pridružuje $(\overline{x}, \overline{y}, \overline{z})$.

Ako je $E : y^2 = ax^3 + bx^2 + cx + d$ eliptička krivulja definirana nad $\mathbb{Q}$, tada se broj $\Delta = b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd$ naziva diskriminanta eliptičke krivulje E. Vrijedi $\Delta = a^4 \prod_{i<j} (r_i - r_j)^2$, gdje su r_1, r_2 i r_3 nultočke polinoma $f(x) = ax^3 + bx^2 + cx + d$. Dakle, polinom $f(x)$ nema višestrukih nultočaka ako i samo ako je $\Delta \neq 0$.

Pretpostavimo sada da su a, b, c i d cijeli brojevi. Za prost broj p promotrimo krivulju $\overline{E} : y^2 = \overline{a}x^3 + \overline{b}x^2 + \overline{c}x + \overline{d}$ definiranu nad $\mathbb{F}_p$. Ako je $\overline{\Delta} \neq 0$ (tj. ako p ne dijeli diskriminantu Δ), onda je $\overline{E}$ eliptička krivulja. Kažemo da je $\overline{E}$ redukcija eliptičke krivulje E modulo p. Ponekad pišemo E umjesto $\overline{E}$ (npr. $E(\mathbb{F}_p) := \overline{E}(\mathbb{F}_p)$). Za takav p kažemo da je prost broj dobre redukcije za E.

Neka je sada $P \in E(\mathbb{Q})$. U homogenim koordinatama P možemo zapisati kao $P = (x, y, z) \in \mathbb{P}^2(\mathbb{Q})$, gdje su $x, y, z \in \mathbb{Z}$ takvi da je $NZM(x, y, z) = 1$.

Definiramo $\overline{P} = (\overline{x}, \overline{y}, \overline{z}) \in \mathbb{P}^2(\mathbb{F}_p)$. Lako se vidi da je $\overline{P} \in E(\mathbb{F}_p)$. Dakle, racionalna točka na $E/\mathbb{Q}$ daje točku na redukciji $\overline{E}$, tj. imamo preslikavanje $E(\mathbb{Q}) \to \overline{E}$ koje zovemo redukcija mod p. Lako se vidi da je to preslikavanje homomorfizam grupa.

Zadatak 15. Neka je $E/\mathbb{Q}$ i p prost broj dobre redukcije za E. Tada je preslikavanje redukcija modulo p, $E(\mathbb{Q}) \to \overline{E}$, homomorfizam grupa.

Dakle, redukcija torzije $E_n(\mathbb{Q})_{\text{tors}}$ mod p je podgrupa od $E_n(\mathbb{F}_p)$. Ako je p prost broj za koji se $E_n(\mathbb{Q})_{\text{tors}}$ ulaže u $E_n(\mathbb{F}_p)$, tada $\#E_n(\mathbb{Q})_{\text{tors}} | \#E_n(\mathbb{F}_p)$ što je vrlo korisno ako možemo izračunati $\#E_n(\mathbb{F}_p)$.

Propozicija 5.12. *Neka je $q = p^f$, gdje je $p \nmid 2n$ prost broj. Ako je $q \equiv 3 \pmod 4$, tada je $\#E_n(\mathbb{F}_q) = q + 1$.*

Dokaz. Prvo, postoje četiri točke reda koji dijeli 2: $\mathcal{O}$, $(0,0)$ i $(\pm n, 0)$. Neka je sad $x \neq 0, \pm n$. Kako je $f(x) = x^3 - n^2 x = -f(-x) \neq 0$ i -1 nije kvadrat u $\mathbb{F}_q$ (jer je $q \equiv 3 \pmod 4$), zaključujemo da je ili $f(x)$ ili $f(-x)$ kvadrat u $\mathbb{F}_q$ pa postoji točno jedna točka u $E(\mathbb{F}_q)$ s prvom koordinatom jednakoj x. Prema tome $\#E_n(\mathbb{F}_q) = 4 + (q-3) = q + 1$. □

Zanima nas injektivnost redukcije mod p na racionalnoj torziji $E(\mathbb{Q})_{\text{tors}}$. Trebat će na sljedeća tehnička lema.

Lema 5.13. *Neka su $P_1 = (x_1, y_1, z_1), P_2 = (x_2, y_2, z_2) \in \mathbb{P}^2(\mathbb{Q})$. Tada je $\overline{P_1} = \overline{P_2} \in \mathbb{P}^2(\mathbb{F}_p)$ ako i samo ako p dijeli koordinate njihovog vektorskog produkta, tj. p dijeli $y_1 z_2 - y_2 z_1$, $x_2 z_1 - x_1 z_2$ i $x_1 y_2 - x_2 y_1$.*

Dokaz. Pretpostavimo prvo da p dijeli vektorski produkt. Promatramo dva slučaja

a) p dijeli x_1: Tada p dijeli $x_2 y_1$ i $x_2 z_1$ pa mora dijeliti x_2 (jer inače mjera brojeva x_1, y_1 i z_1 nije 1). Pretpostavimo da p ne dijeli y_2. Tada $\overline{P_2} = (0, \overline{y_1 y_2}, \overline{y_1 z_2}) = (0, \overline{y_1 y_2}, \overline{y_2 z_1}) = \overline{P_2}$. Slučaj $p \nmid z_2$ (tada $p | y_1$) se na sličan način dokazuje.

b) p ne dijeli x_1: Tada $\overline{P_2} = (\overline{x_1 x_2}, \overline{x_1 y_2}, \overline{x_1 z_2}) = (\overline{x_1 x_2}, \overline{x_2 y_1}, \overline{x_2 z_1}) = \overline{P_1}$.

Pretpostavimo sada $\overline{P_1} = \overline{P_2}$. Bez smanjenja općenitosti možemo pretpostaviti da $p \nmid x_1$. Tada $p \nmid x_2$. Vrijedi

$$\overline{P_2} = (\overline{x_1 x_2}, \overline{x_1 y_2}, \overline{x_1 z_2}) = (\overline{x_2 x_1}, \overline{x_2 y_1}, \overline{x_2 z_1} = \overline{P_1}),$$

iz čega slijedi da $p | x_1 y_2 - x_2 y_1$ i $p | x_1 z_2 - x_2 z_1$. Treba još pokazati da $p | y_1 z_2 - y_2 z_1$. Ako $p | y_1, z_1$ tvrdnja je očita, inače ponovimo gornji argument sa y_1, y_2 ili z_1, z_2 umjesto x_1, x_2. □

Sad možemo dokazati Propoziciju 5.11.

Dokaz. Pretpostavimo suprotno, tj. da $E(\mathbb{Q})$ sadrži element reda većeg od dva. Tada $E(\mathbb{Q})$ ima podgrupu G neparnog reda ili reda 8 (ako $E(\mathbb{Q})$ sadrži element reda 4). Neka su $P_1, \ldots, P_m$ elementi te podgrupe, $P_i = (x_i, y_i, z_i) \in \mathbb{P}^2(\mathbb{Q})$ (prisjetimo se $x_i, y_i, z_i \in \mathbb{Z}$ i $NZM(x_i, y_i, z_i) = 1$) za $i = 1, \ldots, m$. Budući da P_i i P_j (za $i \neq j$) nisu kolinearni, njihov vektorski produkt nije nul vektor. Označimo se n_{ij} najveću zajedničku mjeru komponenti tog vektorskog produkta. Prema Lemi 5.13 P_i i P_j će imati istu redukciju modulo p ako i samo ako $p|n_{ij}$. To znači da ako je p prost broj dobre redukcije za E_n (tj. $p \nmid 2n$) koji je veći od svih prostih djeljitelja svih brojeva $n_{ij}, i \neq j$, onda je redukcija modulo p injekcija sa G u $E(\mathbb{F}_p)$. Za takave p vrijedi $m|\#E(\mathbb{F}_p)$. Posebno, za sve osim konačno mnogo prostih brojeva $p \equiv 3 \pmod 4$ vrijedi $m|p+1$, odnosno $p \equiv -1 \pmod m$.

Ako je $m = 8$ tada za sve osim konačno mnogo prostih brojeva $p \equiv 3 \pmod 4$ vrijedi $p \equiv 7 \pmod 8$, odnosno postoji konačno mnogo prostih brojeva $p \equiv 3 \pmod 8$ što je u kontradikciji sa Dirichletovim teorem o prostim brojevima u aritmetičkim nizovima. Slučaj kad je m neparan ostavljamo čitatelju. □

Teorem 5.14. *Broj n je kongruentan ako i samo ako $E_n(\mathbb{Q})$ ima pozitivan rang.*

Dokaz. Pretpostavimo da je n kongruentan. Tada iz diskusije nakon Propozicije 5.3 slijedi da postoji racionalna točka na E_n čija x koordinata je kvadrat racionalnog broja sa parnim nazivnikom. To očito nije jedna od četiri točke reda koji dijeli 2, što su prema prethodnoj propoziciji jedine točke konačnog reda na $E_n(\mathbb{Q})$ pa je riječ o točki beskonaćnog reda, dakle rang od E_n je pozitivan.

Neka sad $E_n(\mathbb{Q})$ ima pozitivan rang i neka je P jedna točka beskonaćnog reda. Prema Propoziciji 5.7, $x(2P)$ je kvadrat racionalnog broja s parnim nazivnikom i brojnikom koji je relativno prost sa n pa prema Propoziciji 5.4 postoji pravokutan trokut s racionalnim stranicama površine n. □

U ovom odjeljku smo pomoću grupovne operacije okarakterizirali točke $P = (x, y)$ na $E_n(\mathbb{Q})$ za koje su $x, x-n, x+n$ kvadrati racionalnog broja: to su točke $P \in 2E(\mathbb{Q})$. Ova tvrdnja se može generalizirati na sve eliptičke krivulje nad $\mathbb{Q}$ čije su sve točke reda 2 racionalne.

Zadatak 16. Neka je E eliptička krivulja $y^2 = (x - e_1)(x - e_2)(x - e_3)$ gdje su $e_1, e_2, e_3 \in \mathbb{Q}$. Tada je $P = (x_0, y_0) \in 2E(\mathbb{Q}) - \mathcal{O}$ ako i samo ako su $x_0 - e_1$, $x_0 - e_2$ i $x_0 - e_3$ kvadrati racionalnih brojeva.

6 Hasse-Weilova L-funkcija eliptičkih krivulja

6.1 Zeta funkcija

Neka je p prost broj i neka je $\mathbb{F}_q$ konačno polje sa $q = p^r$ elemenata. Ugrubo, nesingularna projektivna mnogostrukost V (podmnogostrukost od $\mathbb{P}^n$) nad poljem $\mathbb{F}_q$ je sustav homogenih polinomijalnih jednadžbi u $n+1$ varijabli oblika

$$f_j(x_0, x_1, \ldots, x_n) = 0, \text{ za } j \in I$$

gdje su koeficijenti polinoma $f_j(x_0, \ldots, x_n)$ iz konačnog polja $\mathbb{F}_q$. Mnogostrukost je nesingularna ako svaka $\overline{\mathbb{F}}_q$-racionalna točka (rješenje sustava) ima tangentu, tj. barem jedna njena parcijalna derivacija je različita od nule. Primjer nesingularna projektivne mnogostrukosti je eliptička krivulja E_n nad poljem $\mathbb{F}_p$ (gdje $p \nmid 2n$) koja je definirana jednom jednadžbom $y^2z - x^3 + n^2xz^2 = 0$. Sa $\#V(\mathbb{F}_q^r)$ ćemo označavati broj $\mathbb{F}_q$-točaka na V. Npr. u Propoziciji 5.12 smo pokazali da je $\#E_n(\mathbb{F}_q) = q + 1$ ako $q \equiv 3 \pmod 4$. Općenito, nizu brojeva $N_1, N_2, \ldots$ pridružujemo funkciju izvodnicu (zeta funkciju) definiranu sljedećim formalnim redom

$$Z(T) = \exp\left(\sum_{r=1}^{\infty} N_r \frac{T^r}{r}\right),$$

gdje je $\exp(x) = \sum_{k=0}^{\infty} \frac{x^k}{k!}$. Zeta funkciju pridruženu brojevima $N_r = \#V(\mathbb{F}_q^r)$ zovemo zeta funkcija od V nad $\mathbb{F}_q$ i označavamo sa $Z(V/\mathbb{F}_q; T)$. Na prvi pogled, ova definicija izgleda neprirodno, no ovako definirana funkcija zadovoljava ova dva važna svojstva.

Zadatak 17. Dokažite da ako je $N_r = N_r^* + N_r^{**}$ (za $r \geq 1$) i ako su $Z(T)$, $Z^*(T)$ i $Z^{**}(T)$ zeta funkcije odgovarajućih nizova, onda vrijedi $Z(T) = Z^*(T)Z^{**}(T)$.

Zadatak 18. Dokažite da ako postoje $\alpha_1, \ldots, \alpha_s$ i $\beta_1, \ldots, \beta_t$ takvi da za svaki r vrijedi $N_r = \beta_1^r + \ldots \beta_t^r - \alpha_1^r - \alpha_2^r \ldots - \alpha_s^r$, onda vrijedi

$$Z(T) = \frac{(1 - \alpha_1 T)(1 - \alpha_2 T) \cdots (1 - \alpha_s T)}{(1 - \beta_1 T)(1 - \beta_2 T) \cdots (1 - \beta_t T)}.$$

Može se pokazati da zeta funkcija eliptičke krivulje definirane nad $\mathbb{F}_q$ ima sljedeći oblik

$$Z(E/\mathbb{F}_q; T) = \frac{1 - 2a_E T + qT^2}{(1 - T)(1 - qT)},$$

gdje je $2a_E \in \mathbb{Z}$. Prema prethodnom zadatku ovaj identitet je ekvivalentan sljedećoj formuli za $N_r = \#E(\mathbb{F}_{q^r})$

$$N_r = q^r + 1 - \alpha^r - (q/\alpha)^r.$$

Posebno, ako je $r = 1$, onda $N_1 = q + 1 - \alpha - \frac{q}{\alpha} = q + 1 - 2a_E$ pa vidimo da je za određivanje zeta funkcije eliptičke krivulje dovoljno odrediti broj točaka krivulje nad $\mathbb{F}_q$.

Naš cilj će biti određivanje zeta funkcija $Z(E_n/\mathbb{F}_p; T)$ koje ćemo kasnije koristiti pri konstrukciji Hasse-Weil L-funkcije.

6.2 Gaussove i Jacobijeve sume

Karakteri, odnosno Gaussove i Jacobijeve sume su osnovni alat koji koristimo za prebrojavanju točaka na algebarskim mnogostrukostima definiranim nad konačnim poljima.

Neka je $q = p^f$. Tada je $\mathbb{F}_q$ proširenje stupnja f nad $\mathbb{F}_p$ s cikličkom Galoisovom grupom generiranom automorfizmom $x \mapsto x^p$. Trag proširenja

$Tr : \mathbb{F}_q \mapsto \mathbb{F}_p$ ($Tr(x)$ je po definiciji jednak sumi konjugata od x) je aditivno preslikavanje (tj. $Tr(x+y) = Tr(x) + Tr(y)$) dano formulom

$$Tr(x) = x + x^p + x^{p^2} + \cdots + x^{p^{f-1}} \text{ za } x \in \mathbb{F}_q.$$

Neka je $\zeta_p = e^{2\pi i/p}$ (primitivan) p-ti korijen iz jedinice.

Definicija 6.1. Homomorfizam grupa $\psi : \mathbb{F}_q \to \mathbb{C}^\times$ se naziva aditivni karakter (vrijedi $\psi(a+b) = \psi(a)\psi(b)$ za sve $a, b \in \mathbb{F}_q$), dok se homomorfizam $\chi : \mathbb{F}_q^\times \to \mathbb{C}^\times$ zove multiplicativni karakter (i vrijedi $\chi(ab) = \chi(a)\chi(b)$ za sve $a, b \in \mathbb{F}_q^\times$).

Lako se provjeri da je preslikavanje $\psi : \mathbb{F}_q \to \mathbb{C}^\times$ dano formulom $\psi(x) = \zeta_p^{Tr(x)}$ aditivan karakter. Od sada pa nadalje fiksirajmo taj ψ.

Primjer 3. Jedan primjer multiplicativnog karaktera je Legendrov simbol $\left(\frac{\cdot}{p}\right) : \mathbb{F}_p^\times \to \{-1, +1\}$.

Zadatak 19. Dokažite da je multiplikativna grupa konačnog polja ciklička.

Općenito ako je g generator cikličke grupe $\mathbb{F}_q^\times$, tada je proizvoljan karakter $\chi : \mathbb{F}_q^\times \to \mathbb{C}^\times$ određen s $\chi(g)$. Budući da je $g^{q-1} = 1$, slijedi $1 = \chi(g^{q-1}) = \chi(g)^{q-1}$ pa je $\chi(g) \in \mu_{q-1}$ neki $q-1$-i korijen iz jedinice. Pokazali smo da je grupa karaktera grupe $\mathbb{F}_q^\times$ (uz operaciju $(\chi_1\chi_2)(x) = \chi_1(x)\chi_2(x)$) izomorfna grupi $\mu_{q-1} \cong \mathbb{F}_q^\times$. Grupu karaktera konačne abelove grupe G označavamo sa $\widehat{G}$. Karakter koji G preslikava u jedinicu se zove trivijalan karakter i označava se s χ_0. Svaki (i trivijalan) multiplikativni karakter χ proširujemo do funkcije na $\mathbb{F}_q$ formulom $\chi(0) = 0$.

Zadatak 20. Neka je G konačna abelova grupa. Dokažite da je $\widehat{G} \cong G$.

Trebat će nam neka osnovna svojstva karaktera.

Lema 6.2. *Neka je G konačna abelova grupa i $\chi \in \widehat{G}$ njen netrivijalan karakter. Tada vrijedi*

$$\sum_{g \in G} \chi(g) = 0.$$

Dokaz. Označimo gornju suma sa S. Neka je $h \in G$. Vrijedi

$$\chi(h)S = \sum_{g \in G} \chi(hg) = [g' = hg] = \sum_{g' \in G} \chi(g') = S.$$

Odnosno, $S(1 - \chi(h)) = 0$ za svaki $h \in G$. Budući da je χ netrivijalan, slijedi da je $S = 0$. □

Ako identificiramo $\widehat{\widehat{G}}$ s G pomoću prirodnog izomorfizma $g \mapsto (\chi \mapsto \chi(g))$, gornja lema primjenjena na $G = \widehat{G}$ nam daje sljedeću tvrdnju.

Lema 6.3. *Neka je G konačna abelova grupa i $g \neq 1$ njen element. Tada je*

$$\sum_{\chi \in \widehat{G}} \chi(g) = 0.$$

Ove dvije leme su posljedica tzv. relacije ortogonalnosti.

Zadatak 21. Na prostoru kompleksnih funkcija definiranih na konačnoj abelovoj grupi G definiran je skalarni produkt

$$\langle \alpha, \beta \rangle = \frac{1}{\#G} \sum_{g \in G} \alpha(g)\overline{\beta(g)}.$$

Dokažite da karakteri od G čine ortonormiranu bazu u odnosu na ovaj skalarni produkt.

Sljedeća propozicija povezuje karaktere s određivanjem broja rješenja jednadžbi nad konač nim poljima.

Propozicija 6.4. *Neka $m|q-1$ i $a \in \mathbb{F}_q^\times$. Tada*

$$\#\{x \in \mathbb{F}_q | x^m = a\} = \sum_{\chi^m = \chi_0} \chi(a).$$

Lema 6.5. *Neka je $a \in F_q^\times$ i $m \in \mathbb{N}$.*

$$\#\{x \in F_q | x^m = a\} = \begin{cases} m, & \textit{ako je } a \textit{ } m\textit{-ta potencija} \\ 0, & \textit{inače.} \end{cases}$$

Dokaz. Neka je g generator od cikličke grupe $\mathbb{F}_q^\times$ i neka je $h = g^{\frac{q-1}{m}}$ reda element reda m. Tada su elementi oblika h^i, za $i = 1, \dots m$, različiti m-ti korijeni iz jedinice. Ako postoji x za koji je $x^m = a$, onda je $(xh^i)^m = a$ za $i = 1, \dots, m$, odnosno jednadžba ima m rješenja. Lako se vidi da nema drugih rješenja jer polinom m-tog stupnja nad bilo kojim poljem ima najviše m nultočaka. □

Dokaz. Ako je $a = h^m$ za neki $h \in \mathbb{F}_q^\times$, onda $\chi(a) = \chi(h^m) = \chi(h)^m = 1$ pa se prema prehodnoj lemi lijeva strana jednakosti podudara s desnom. Pretpostavimo da a nije m-ta potencija. Označimo s H podgrupu elemenata od $\mathbb{F}_q^\times$ reda koji dijeli m. Tada $\widehat{H}$ možemo identificirati s restrikcijama na H karaktera od $\mathbb{F}_q^\times$ reda koji dijeli m. Prema Lemi 6.3 primjenjenoj na $G = H$ dovoljno je dokazati da a kao karakter od $\widehat{H}$ (uz kanonsku identifikaciju $\mathbb{F}_q^\times \cong \widehat{\widehat{\mathbb{F}_q^\times}}$) nije trivijalan, tj. da postoji $\chi \in \widehat{H}$ takav da je $\chi(a) \neq 1$. Neka je χ primitivan karakter reda m (generator od $\widehat{H}$) i neka je $a = g^k$ gdje je g generator od $\mathbb{F}_q^\times$ i $m \nmid k$ prema pretpostavci. Tada $\chi(a) = \chi(g^k) = \chi(g)^k$ ne može biti jednak jedan jer je $\chi(g)$ primitivni m-ti korijen iz jedinice. □

Prilikom rada sa karakterima javljaju se Jacobijeve sume za čije razumijevanje je potrebno poznavati Gaussove sume.

Definicija 6.6. Neka su χ, χ_1 i χ_2 multiplikativni karakteri od $\mathbb{F}_q$ i neka je ψ aditivan karakter definiran na početku ovog odjeljka. Gaussova suma $g(\chi)$ karaktera χ se definira formulom

$$g(\chi) = \sum_{x \in \mathbb{F}_q} \chi(x)\psi(x),$$

dok je Jacobijeva suma po definiciji jednaka

$$J(\chi_1, \chi_2) = \sum_{x \in \mathbb{F}_q} \chi_1(x)\chi_2(1-x).$$

Propozicija 6.7. *Neka su χ, χ_1 i χ_2 netrivijalni karakteri od $\mathbb{F}_q^\times$ (χ_0 je trivijalan karakter). Vrijedi*

a)

$$g(\chi_0) = -1 \quad J(\chi_0, \chi) = -1$$
$$J(\chi_0, \chi_0) = q - 2 \quad J(\chi, \bar{\chi}) = -\chi(-1)$$
$$J(\chi_1, \chi_2) = J(\chi_2, \chi_1)$$

b)

$$g(\chi)g(\bar{\chi}) = \chi(-1)q$$
$$|g(\chi)| = \sqrt{q}$$

c)

$$J(\chi_1, \chi_2) = \frac{g(\chi_1)g(\chi_2)}{g(\chi_1\chi_2)} \text{ ako } \chi_2 \neq \bar{\chi_1}.$$

Dokaz. Dokazat ćemo c) dio, ostatak ostavljamo čitatelju za vježbu. Računamo

$$\begin{aligned}
g(\chi_1)g(\chi_2) &= \sum_x \chi_1(x)\psi(x)\sum_y \chi_2(y)\psi(y) = \sum_{x,y\in\mathbb{F}_q} \chi_1(x)\chi_2(y)\psi(x+y) \\
&= [s = x_1 + x_2] = \sum_{s\in\mathbb{F}_q}\left(\sum_{x\in\mathbb{F}_q}\chi_1(x)\chi_2(s-x)\right)\psi(s) \\
&= \sum_{s\in\mathbb{F}_q^\times}\left(\sum_{x\in\mathbb{F}_q}\chi_1(x)\chi_2(s-x)\right)\psi(s) + \sum_{x\in\mathbb{F}_q}\chi_1(x)\chi_2(-x) \\
&= [x = sx'] = \sum_{s\in\mathbb{F}_q}\left(\chi_1\chi_2(s)\sum_{x'\in\mathbb{F}_q}\chi_1(x')\chi_2(1-x')\right)\psi(s) + \chi_2(-1)\sum_{x\in\mathbb{F}_q}\chi_1\chi_2(x) \\
&= J(\chi_1,\chi_2)\sum_{s\in\mathbb{F}_q^\times}\chi_1\chi_2(s)\psi(s) = J(\chi_1,\chi_2)g(\chi_1\chi_2)
\end{aligned}$$

□

6.3 Zeta funkcija eliptičke krivulje E_n

U ovom odjeljku ćemo izračunati zeta funkciju eliptičke krivulje $E_n : y^2 = x^3 - n^2x$. Za $p \nmid 2n$ odredit ćemo $\alpha \in \mathbb{Q}(i)$ takav da $\#E_n(\mathbb{F}_{p^r}) = p^r + 1 - \alpha^r - p^r/\alpha^r$ za svaki $r \in \mathbb{N}$.

Prvo ćemo jednadžbu od E_n transformirat u (dijagonalni) oblik pogodniji za računanje. Zamjenom varijabli $(x, y) = (\frac{1}{2}(u + v^2), \frac{1}{2}v(u + v^2))$ E_n se transformira u krivulju $E_n' : u^2 = v^4 + 4n^2$. Obratno, točki (x, y) na E_n odgovara točka $(2x - y^2/x^2, y/x)$ na E_n'. Ova dva preslikavanja su inverz jedan drugome (kažemo da su krivulje E_n i E_n' biracionalno ekvivalentne) i definiraju bijekciju između točaka na E_n' i $E_n - \{(0, 0)\}$. Neka je $q = p^f$ i $q \equiv 1 \pmod 4$ (znamo iz Propozicije 5.12 da je $\#E_n(\mathbb{F}_q) = q+1$ za $q \equiv 3 \pmod 4$). Označimo sa χ_4 neki

multiplikativni karakter reda 4 i neka je $\chi_2 = \chi_4^2$ karakter reda 2. Računamo

$$\begin{aligned}
\#E'_N(\mathbb{F}_q) &= \#\{\text{točka u beskonaćnosti}\} + \#\{u \in \mathbb{F}_q | u^2 = 4n^2\} + \#\{v \in \mathbb{F}_q | 0 = v^4 + 4n^2\} \\
&\quad + \#\{u, v \in \mathbb{F}_q^\times | u^2 = v^4 + 4n^2\} \\
&= 3 + \sum_{j=1}^{4} \chi_4^j(-4n^2) + \sum_{\substack{a,b \in \mathbb{F}_q \\ a = b + 4n^2}} \#\{u^2 = a\} \#\{v^4 = b\} \\
&= 5 + 2\chi_4(-4n^2) + \sum_{\substack{a \in \mathbb{F}_q^\times \\ a - 4n^2 \in \mathbb{F}_q^\times}} \sum_{\substack{k=1,2 \\ j=1,2,3,4}} \chi_2^k(a)\chi_4^j(a - 4n^2) \\
&= [x := \frac{a}{4n^2}] \\
&= 5 + 2\chi_4(-4n^2) + \sum_{k,j} \chi_4(-4n^2)^j \sum_{x \in \mathbb{F}_q^\times} \chi_2(x)^k \chi_4(1-x)^j \\
&= 5 + 2\chi_4(-4n^2) + \sum_{k,j} \chi_4(-4n^2)^j J(\chi_2^k, \chi_4^j) \\
&= q + \chi_4(-4n^2)\left(J(\chi_2, \chi_4) + J(\chi_2, \bar{\chi_4})\right).
\end{aligned}$$

Kod zadnje jednakosti smo koristili Propoziciju 6.7 a). Dakle,

$$\#E_n(\mathbb{F}_q) = q + 1 - \alpha - \bar{\alpha},$$

gdje je $\alpha = \alpha_{n,q} = -\chi_4(-4n^2)J(\chi_2, \chi_4) = -\chi_2(n)J(\chi_2, \chi_4)$ (budući da je $\chi_4(-4) = 1$).

Zadatak 22. Neka je $q \equiv 1 \pmod 4$. Dokažite da je $\chi_4(-4) = 1$ i $\chi_4(-1) = -1$ ili 1.

Želimo točno odrediti α za $q = p$ i $p \equiv 3 \pmod 4$ odnosno za $q = p^2$ i $p \equiv 3 \pmod 4$. Primjetimo da je $J(\chi_2, \chi_4)$ element prstena Gaussovih brojeva $\mathbb{Z}[i]$. Uz to prema Propoziciji 6.7 b) i c) $J(\chi_2, \chi_4)$ je element norme q, tj. vrijedi $a^2 + b^2 = q$, gdje je $J(\chi_2, \chi_4) = a + bi$. Iz teorije kvadratnih polja znamo da se ideal $p\mathbb{Z} \subset \mathbb{Z}$ cijepa na dva ideala $\mathfrak{P}_1$ i $\mathfrak{P}_2$, tj. $p\mathbb{Z}[i] = \mathfrak{P}_1\mathfrak{P}_2$, ako je $p \equiv 1 \pmod 4$. Kako je norma ideala $\mathfrak{P}_1$ i $\mathfrak{P}_2$ jednaka p, slijedi da generatori tih ideala (u prstenu Gaussovih brojeva svi ideali su glavni) $a \pm bi$ zadovoljavaju $a^2 + b^2 = p$. Budući da je generator ideala jednoznačno određen do na množenje s invertibilnim elementom ($\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$) zaključujemo da je u ovom slučaju α jednak $\pm a \pm bi$ ili $\pm b + \pm ai$.

U slučaju $p \equiv 3 \pmod 4$, p je inertan (tj. $p\mathbb{Z}[i]$ je prost ideal) pa je jedino rješenje jednadžbe $a^2 + b^2 = q = p^2$ dano s $a = \pm p$, $b = 0$ odnosno $a = 0$, $b = \pm p$. Prema tome α je jednak $\pm p$ ili $\pm pi$.

Sljedeća lema će nam pomoći da točno odredimo α.

Lema 6.8. *Neka je* $q \equiv 1 \pmod 4$. *Tada*

$$2 + 2i \mid 1 + J(\chi_2, \chi_4).$$

Dokaz. Prema Propoziciji 6.7 imamo

$$J(\chi_2,\chi_4) = J(\chi_4,\chi_4)\frac{g(\chi_2)^2}{g(\chi_4)g(\bar{\chi_4})} = \chi_4(-1)J(\chi_4,\chi_4).$$

Nadalje,

$$J(\chi_4,\chi_4) = \sum_{x\in\mathbb{F}_q}\chi_4(x)\chi_4(1-x) = \chi(\frac{q+1}{2})^2 + 2\sum\chi_4(x)\chi_4(1-x),$$

gdje sumiramo po $\frac{q-1}{2}$ elemenata, po jedan iz svakog para $(x,1-x)$ $(x\neq\frac{q+1}{2})$. Budući da je za $x\neq 0$ $\chi_4(x)$ potencija od i, vrijedi $\chi_4(x)\equiv 1 \pmod{1+i}$ pa je $J(\chi_4,\chi_4)\equiv\chi_4(\frac{q+1}{2})^2+(\frac{q-1}{2}-1)+0 \pmod{2+2i}$. Kako je $\chi_4(\frac{q+1}{2})^2=\chi_4(\frac{1}{4}) = \chi_4(4)^{-1}$ (jer $\frac{q+1}{2}=\frac{1}{2}$ u $\mathbb{F}_q$), dobivamo $J(\chi_4,\chi_4)\equiv\chi_4(4)^{-1}+2 \pmod{2+2i}$ (jer je $q\equiv 1 \pmod 4$).

Konačno,

$$1+J(\chi_2,\chi_4)\equiv 1+\chi_4(-1)\chi_4(4)^{-1}+2\chi_4(-1)\equiv 2(1+\chi_4(-1))\equiv 0 \pmod{2+2i}.$$

Ovdje smo koristili da je $\chi_4(-1)=\pm 1$. □

Sada ćemo dokazati glavni rezultat ovog odjeljka.

Teorem 6.9. *Neka je E_n eliptička krivulja $y^2=x^3-n^2x$ definirana nad $\mathbb{F}_p$, gdje $p\nmid 2n$. Tada je*

$$Z(E_n/F_p;T) = \frac{1-2aT+pT^2}{(1-T)(1-pt)} = \frac{(1-\alpha T)(1-\bar{\alpha}T)}{(1-T)(1-pT)}$$

gdje je $a=\Re(\alpha)$; $\alpha = i\sqrt{p}$ za $p\equiv 3 \pmod 4$, odnosno za $p\equiv 1 \pmod 4$ α je element od $\mathbb{Z}[i]$ norme p koji je kongruentan $\left(\frac{n}{p}\right)$ modulo $2+2i$.

Dokaz. Trebamo izračunati $N_r = \#E_n(\mathbb{F}_{p^r})$ za $p\equiv 1 \pmod 4$ i $N_{2r}=\#E_n(\mathbb{F}_{q^r})$ za $p\equiv 3 \pmod 4$ i $q=p^2$. Fiksirajmo $q=p$ u prvom slučaju i $q=p^2$ u drugom. Također za svaki r fiksirat ćemo po jedan karakter reda 4 i red 2 na $\mathbb{F}_q^\times$ (zapravo karakter reda 2 je jedinstven) formuloma $\chi_{4,r}=\chi_4\circ\mathbb{N}_r$ i $\chi_{2,r}=\chi_2\circ\mathbb{N}_r$ gdje je N_r norma sa $\mathbb{F}_{q^r}$ u $\mathbb{F}_q$ (po definiciji $\mathbb{N}_r(x)=x^{1+q+q^2+\cdots+q^{r-1}}$). Vrijedi $\mathbb{N}_r(xy)=\mathbb{N}_r(x)\mathbb{N}_r(y)$ za svaki $x,y\in\mathbb{F}_q^r$ pa iz toga slijedi da su $\chi_{4,r}$ i $\chi_{2,r}$ multiplikativni karakteri od $\mathbb{F}_{q^r}$. Pokazali smo

$$\#E_n(\mathbb{F}_q^r) = q^r+1-\alpha_{n,q^r}-\overline{\alpha_{n,q^r}},$$

gdje je

$$\alpha_{n,q^r} = -\chi_{2,r}(n)\frac{g(\chi_{2,r})g(\chi_{4,r})}{g(\chi_{2,r}\chi_{4,r})} = -\chi_{2,r}(n)\frac{g(\chi_{2,r})g(\chi_{4,r})}{g(\overline{\chi_{4,r}})}.$$

Treba još dokazati $\alpha_{n,q^r} = \alpha_{n,q}^r$ (vidi diskusiju nakon Zadatka 18).

Tvrdnja slijedi direktno iz Hasse-Davenportove formule za multiplikativni karakter χ (vidi Propoziciju 6.10)

$$-g(\chi \circ \mathbb{N}_r) = (-g(\chi))^r.$$

□

Propozicija 6.10. *Neka je χ multiplikativni karakter polja $\mathbb{F}_q$ i $\mathbb{N}_r$ norma sa $\mathbb{F}_{q^r}$ u $\mathbb{F}_q$. Tada vrijedi*

$$-g(\chi \circ \mathbb{N}_r) = (-g(\chi))^r.$$

Dokaz. Dokazat ćemo niz lema koje će implicirati propoziciju.

Lema 6.11. *Neka je S skup svih normiranih polinoma u $\mathbb{F}_q[x]$ i neka je S' podskup svih ireducibilnih normiranih polinoma. Indeks će označavati stupanj. Vrijedi*

$$x^{q^r} - x = \prod f,$$

gdje se množi po svim $f \in S'_d$ za sve $d|r$.

Dokaz. Znamo $x^{q^r} - x = \prod_{\alpha \in \mathbb{F}_q}(x - \alpha)$. Budući da je svaki $\alpha \in \mathbb{F}_q$ nultočka svog ireducibilnog polinoma (koji je normiran i ireducibilan polinom stupnja $d|n$), slijedi da $x^{q^r} - x | \prod f$. Budući da dva različita ireducibilna polinoma ne mogu imati zajednički korijen, jednakost slijedi. □

Lema 6.12. *Neka je $f \in S$, $f(x) = x^d - c_1 x^{d-1} + \cdots + (-1)^d c_d$ i neka su χ i ψ netrivijalni multiplikativni i aditivni karakteri od F_q. Definirajmo preslikavanje $\lambda : S \to \mathbb{C}$ formulom $\lambda(f) = \chi(c_d)\psi(c_1)$ ($\lambda(1) = 1$). Vrijedi $\lambda(f_1 f_2) = \lambda(f_1)\lambda(f_2)$ i $g(\chi) = \sum_{f \in S_1} \lambda(f)$.*

Dokaz. Tvrdnja slijedi direktno iz definicije. □

Lema 6.13. *Pretpostavimo da je $\alpha \in \mathbb{F}_{q^r}$ nultočka normiranog, ireducibilnog polinoma $f \in S'_d$, gdje $d \mid n$. Tada je $\lambda(f)^{r/d} = \chi_r(\alpha)\psi_r(\alpha)$, gdje je $\chi_r = \chi \circ \mathbb{N}_r$ i $\psi_r = \psi \circ T_r$ (T_r je trag sa $\mathbb{F}_{q^r}$ u $\mathbb{F}_q$).*

Dokaz. Neka je $f(x) = x^d - c_1 x^{d-1} + \cdots + (-1)^d c_d$. Tada su c_d i c_1 norma odnosno trag od α sa $\mathbb{F}_{q^d}$ u $\mathbb{F}_q$. Kako su norma odnosno trag od α sa $\mathbb{F}_{q^r}$ u $\mathbb{F}_{q^d}$ jednaki $\alpha^{r/d}$ i $r/d\alpha$ tvrdnja slijedi iz definicije preslikavanja λ. □

Lema 6.14. *Vrijedi*

$$g(\chi_r) = \sum_{d|r} \sum_{f \in S'_d} d\lambda(f)^{r/d}.$$

Dokaz. Iz prethodne leme slijedi

$$g(\chi_r) = \sum_{\alpha \in \mathbb{F}_{q^r}} \lambda(f_\alpha)^{r/d},$$

gdje je f_α minimalan polinom od α. Kako svaki normiran, ireducibilan polinom stupnja $d|r$ ima d nultočaka, iz Leme 6.11 slijedi tvrdnja. □

Lema 6.15. *Vrijedi sljedeći identitet*

$$\sum_{f\in S}\lambda(f)T^{\deg f}=\prod_{f\in S'}(1-\lambda(f)T^{\deg f})^{-1}.$$

Dokaz. Vrijedi $\frac{1}{1-\lambda(f)T^{\deg f}}=\sum_{i=0}^{\infty}\lambda(f^i)T^{\deg f^i}$. Tvrdnja slijedi iz jedinstvenosti faktorizacije polinoma iz S i multiplikativnosti funkcije λ. □

Lema 6.16. *Za $d>1$ vrijedi*

$$\sum_{f\in S_d}\lambda(f)=0.$$

Dokaz. □

Uzimajući u obzir prethodnu lemu, računamo logaritamsku derivaciju izraza iz 6.15

$$\begin{aligned}\log(1+g(\chi)T)'=g(\chi)\,(1-g(\chi)T+\cdots)&=\sum_{f\in S'}\frac{\lambda(f)\deg f\,T^{\deg f-1}}{1-\lambda(f)T^{\deg f}}\\&=\sum_{f\in S'}\sum_{i=0}^{\infty}\lambda(f)\deg f\,T^{\deg f-1}\lambda(f)^iT^{i\deg f}\\&=\sum_{f\in S'}\sum_{j=1}^{\infty}\deg f\lambda(f)^jT^{j\deg f-1}.\end{aligned}$$

Uspoređujući koeficijent uz T^{r-1} na obje strane dobivamo

$$(-1)^{r-1}g(\chi)^r=\sum_{d|r}\sum_{f\in S'_d}d\lambda(f)^{r/d}.$$

Tvrdnja slijedi iz Leme 6.14. □

Sada ćemo definirati Hasse-Weil L-funkciju.

Definicija 6.17. Neka je E eliptička krivulja. Hasse-Weil L-funkcija $L(E,s)$ se definira formulom

$$L(E,s)=\frac{\zeta(s)\zeta(s-1)}{\prod_p Z(E/\mathbb{F}_p;p^{-s})},\ \text{za } s\in\mathbb{C}.$$

Ovdje $\zeta(s)$ označava Riemannovu zeta funkciju. Npr. lako se vidi da je

$$L(E_n,s)=\prod_{p\nmid 2n}\frac{1}{1-2a_{E_n,p}p^{-s}+p^{1-2s}}.$$

Pokazat ćemo da produkt konvergira za $\Re(s) > \frac{3}{2}$ i da se može analitički proširiti na cijeli $\mathbb{C}$. To neće biti osobito teško, analitičko proširenje eliptičkih krivulja sa kompleksnim množenjem (E_n pripada toj klasi) je već duže vrijeme poznato. Za eliptike krivulje koje nemaju kompleksno množenje analitičko proširenje je puno teže dobiti - to je jedna od formulacija Wilesovog teorema o modularnosti (koji implicira Veliki Fermatov teorem). Vrijednost $L(E,1)$ tako analitički proširene funkcije se zove "kritična vrijednost". Važnost kritičnih vrijednosti dolazi od sljedeće slavne slutnje.

Slutnja 6.18 (B.J. Birch i H.H.F. Swinnerton-Dyer, 1965.)**.** *Neka je E eliptička krivulja definirana nad $\mathbb{Q}$. Vrijedi*

$$L(E,1) = 0 \iff E(\mathbb{Q}) \text{ je konačan.}$$

Napomena. Ovo je "slabi" oblik slutnje. U najopćenitijoj formi se tvrdi da je rang eliptičke krivulje jednak redu poništavanja $L(E,s)$ u točki $s=1$. Uz to se predlaže eksplicitna formula za vodeći Taylorovom koeficijent (u točki $s=1$).

Postoji jednostavna (ali potpuno pogrešna) heuristika koja "objašnjava" gornju hipotezu. Ako u formulu za $L(E,s)$ uvrstimo (posve neopravdano) $s=1$ dobit ćemo

$$L(E,1) = \prod_p \frac{p}{p+1-2a_{E,p}} = \prod_p \frac{p}{N_p},$$

gdje je $N_p = \#E(\mathbb{F}_p)$. Poznato je da se N_p nalazi u intervalu $[p-\sqrt{p}, p+\sqrt{p}]$, ugrubo $N_p \approx p \pm \sqrt{p}$. Ako E ima beskonačno mnogo racionalnih točaka onda je razumno očekivati da će njihove redukcije mod p "gurati" N_p-ove prema desnom rubu intervala, tj. $N_p \approx p + \sqrt{p}$, što bi onda impliciralo da produkt $\prod_p p/N_p$ konvergira u nulu. Zapravo je BSD slutnja prvotno i bila iskazana na sličan način:

$$\prod_{p \le x} \frac{N_p}{p} \approx C \log(x)^r \text{ kad } x \to \infty,$$

gdje je r rang eliptičke krivulje i C neka konstanta.

6.4 Dirichletove L-funkcije

Hasse-Weilove L-funkcije pridruženu eliptičkim krivuljama $E_n : y^2 = x^3 - n^2 x$ su generalizacija "jednostavnijih" Dirichletovih L-funkcija. U ovom odjeljku ćemo proučiti analitičko proširenje najjednostavnije Dirichletove L-funkcije - Riemannove zeta funkcije. Argument koji ćemo pri tome koristiti se generalizira i na analitičko proširenje od $L(E_n,s)$. No prije toga, kao motivaciju, pokazat ćemo kako se Dirichletove L-funkcije koriste u dokazu Dirichletovog teorema o prostim brojevima u aritmetičkim nizovima.

Teorem 6.19 (Dirichlet)**.** *Neka su a i N relativno prosti prirodni brojevi. Tada postoji beskonaćno mnogo prostih brojeva p takvih da je $p \equiv a \pmod N$.*

Označimo sa $\mathcal{P}_a$ skup prostih brojava $p \equiv a \pmod N$. Definirajmo funkciju $P_a(s) = \sum_{p\in\mathcal{P}_a} \frac{1}{p^s}$, za $\Re(s) > 1$. Pokazat ćemo da je $\lim_{s\to 1^+} P_a(s) = \infty$, što onda naravno implicira da je skup $\mathcal{P}_a$ beskonačan.

Definirajmo prvo odgovarajuće L-funkcije.

Definicija 6.20. Neka je $N \in \mathbb{N}$ i $\chi \in \widehat{(\mathbb{Z}/N\mathbb{Z})^\times}$ multiplikativan karakter $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$. Takav karakter se zove Dirichletov karakter modulo N. Proširujemo ga do funkcije na $\mathbb{N}$ formulom $\chi(n) = \chi(n \bmod N)$, gdje je $\chi(n) = 0$ za $GCD(n, N) \neq 1$. Dirichletovu L-funkciju definiramo konvergentnim redom

$$L(\chi, s) = \sum_{n\in\mathbb{N}} \frac{\chi(n)}{n^s}, \quad \Re(s) > 1.$$

Ako je $N = 1$ onda se pripadna L- funkcija (karakter je trivijalan) zove Riemannova zeta funkcija i označava se $\zeta(s)$.

Lako se vidi da Dirichletova L-funkcija konvergira apsolutno za $\Re(s) > 1$. Ako je karakter ne-trivijalan tada red konvergira za $\Re(s) > 0$.

Lema 6.21. *Neka je $N \in \mathbb{N}$ i χ netrivijalan karakter modulo N. Tada red od $L(\chi, s)$ konvergira i za $\Re(s) > 0$ (i definira holomorfnu funkciju).*

Dokaz. Vrijedi

$$L(\chi, s) = \sum_{n=1}^{\infty} \left(\chi(1) + \chi(2) + \ldots + \chi(n)\right) \left(n^{-s} - (n+1)^{-s}\right).$$

Primjetimo dvije stvari. Prvo suma $\chi(1)+\ldots+\chi(n)$ je ograničena jer je karakter χ netrivijalan pa vrijedi $\sum_{n\in\mathbb{Z}/N\mathbb{Z}} \chi(n) = 0$. Drugo, prema teoremu o srednjoj vrijednosti $|n^{-s} - (n+1)^{-s}| \leq \frac{|s|}{|n^{s+1}|}$. Dakle, gornji red konvergira apsolutno za $\Re(s) > 0$. □

Ako je karakter trivijalan, tada $L(\chi, s)$ ima analitičko proširenje na $\Re(s) > 0$ s jednostavnim polom u točki $s = 1$. Ova tvrdnja je posljedica sljedeće leme.

Lema 6.22. *$\zeta(s) - \frac{1}{s-1}$ ima analitičko proširenje na $\Re(s) > 0$.*

Dokaz. Vrijedi

$$\zeta(s) - \frac{1}{s-1} = \sum_{n=1}^{\infty} \frac{1}{n^s} - \int_1^{\infty} \frac{1}{x^s} dx = \sum_{n=1}^{\infty} \left(\frac{1}{n^s} - \frac{1}{x^s}\right) dx.$$

Desna strana konvergira apsolutno za $\Re(s) > 0$ jer po teoremu o srednjoj vrijednosti $|n^{-s} - (n+1)^{-s}| \leq \frac{|s|}{|n^{s+1}|}$. □

Dirichletove L-funkcije su povezane s prostim brojevima preko Eulerove produktne formule.

Lema 6.23. *Za $\Re(s) > 1$ vrijedi*

$$L(\chi, s) = \prod_p \frac{1}{1 - \frac{\chi(p)}{p^s}}.$$

Dokaz. Dokaz ostavljamo za vježbu. □

Ako gornju formulu formalno logaritmiramo dobivamo

$$\begin{aligned}\ln(L(\chi, s)) &= \sum_p \ln(1 - \frac{\chi(p)}{p^s})^{-1} = \sum_p \sum_{k\in\mathbb{N}} \frac{\chi(p)}{kp^{sk}} \\ &= \sum_p \frac{\chi(p)}{p^s} + R(\chi, s).\end{aligned}$$

Kod druge jednakosti smo iskoristili formulu $\ln(1-x) = -\sum_{n\in\mathbb{N}} \frac{x^n}{n}$. Lako se vidi da $R(\chi, s)$ ograničena kad $s \to 1^+$

$$\begin{aligned}|R(\chi, 1)| &\leq \sum_{k\geq 2} \sum_p \frac{1}{kp^k} \leq \sum_p \sum_{k\geq 2} \frac{1}{p^k} \\ &= \sum_p \frac{1}{p^2} \frac{p}{p-1} \leq \sum_p \frac{1}{p^2} \cdot 2 \leq 2 \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{3}.\end{aligned}$$

Naravno, funkcija $\ln(L(\chi, s))$ nije dobro definirana, no ako definiramo $l(\chi, s) = \sum_p \sum_{k\in\mathbb{N}} \frac{\chi(p)}{kp^{sk}}$ može se pokazati da za $\Re(s) > 1$ vrijedi $e^{l(\chi,s)} = L(\chi, s)$, pa je formula koju smo dobili formalnim računom "točna".

Želimo funkciju $\mathcal{P}_a(s)$ izraziti pomoću funkcija $l(\chi, s)$ $(= \ln(L(\chi, s))$ i $R(\chi, s)$. Neka je $1_a(n)$ karakteristična funkcija podskupa prirodnih brojeva koji daju ostatak a pri djeljenju sa N. Ta funkcija se može izraziti pomoću karaktera.

Lema 6.24. *Vrijedi*

$$1_a(n) = \sum_{\chi\in\widehat{\mathbb{Z}/N\mathbb{Z}}} \frac{\chi(a)^{-1}}{\varphi(N)} \chi(n),$$

gdje je $\varphi(x)$ Eulerova φ-funkcija.

Dokaz. Dokaz slijedi direktno iz ortogonalnosti karaktera, vidi Zadatak 21. □

Iz prethodne leme slijedi

$$P_a(s) = \sum_{\chi\in\widehat{(\mathbb{Z}/N\mathbb{Z})^\times}} \frac{\chi(a)^{-1}}{\varphi(N)} \sum_p \frac{\chi(p)}{p^s},$$

odnosno

$$P_a(s) = \sum_{\chi \in \widehat{(\mathbb{Z}/N\mathbb{Z})^\times}} \frac{\chi(a)^{-1}}{\varphi(N)} \left(l(\chi, s) - R(\chi, s)\right)$$
$$= \sum_{\chi \in \widehat{(\mathbb{Z}/N\mathbb{Z})^\times}} \frac{\chi(a)^{-1}}{\varphi(N)} l(\chi, s) + O(1).$$

Preostaje nam još istražiti ponašanje funkcija $L(\chi, s)$ kad $s \to 1^+$.

Zadatak 23. Neka je χ trivijalan karakter modulo N. Tada

$$L(\chi, s) = \sum_{n \in \mathbb{N}, GCD(n,N)=1} \frac{1}{n^s}$$

ima pol u točki $s = 1$.

Sljedeći teorem zajedno sa prethodnim zadatkom implicira $\lim_{s\to 1^+} P_a(s) = \infty$ jer se može pokazati da $0 \neq L(\chi, 1) = \lim_{s\to 1} L(\chi, s) = \lim_{s\to 1} e^{l(\chi,s)}$ implicira ograničenost od $l(\chi, s)$ kad $s \to 1$.

Teorem 6.25. *Neka je $N \in \mathbb{N}$ i χ netrivijalan Dirichletov karakter modulo N. Tada je $L(\chi, s)$ definirana u točki $s = 1$ i vrijedi*

$$L(\chi, 1) \neq 0.$$

Najprirodniji dokaz gornjeg teorema koristi Dedekindove zeta funkcije.

Definicija 6.26. Neka je K polje algebarskih brojeva i neka je $\mathcal{O}_K$ prsten cijelih brojeva u K. Dedekindova zeta funkcija $\zeta_K(s)$ se definira formulom

$$\zeta_K(s) = \sum_{I \subset \mathcal{O}_K} \mathbb{N}(I)^{-s}, \qquad \text{gdje je } \Re(s) > 1.$$

gdje se sumira po svim idealima iz $\mathcal{O}_K$ koji su relativno prosti sa diskriminantom od $\mathcal{O}_K$. Standardno, $\mathbb{N}(I)$ označava normu ideala I.

Kao i kod Riemannove zeta funkcije, jedinstvena faktorizacija ideala na proste ideale implicira produktnu formulu.

$$\zeta_K(s) = \sum_{I \subset \mathcal{O}_K} \mathbb{N}(I)^{-s} = \prod_{\mathfrak{P} \subset \mathcal{O}_K} (1 + \mathbb{N}(\mathfrak{P})^{-s} + \mathbb{N}(\mathfrak{P})^{-2s} + \cdots)$$
$$= \prod_{\mathfrak{P} \subset \mathcal{O}_K} \frac{1}{1 - \mathbb{N}(\mathfrak{P})^{-s}}.$$

Nas će zanimati zeta funkcija ciklotomskih polja $K = \mathbb{Q}(\mu_N)$, gdje je μ_N primitivni N-ti korijen iz jedinice. U tom slučaju produktna formula ima sljedeći oblik.

Lema 6.27. *Neka je $K = \mathbb{Q}(\mu_N)$, tada je*

$$\zeta_K(s) = \prod_{p \nmid N} \frac{1}{\left(1 - \frac{1}{p^{f(p)s}}\right)^{g(p)}},$$

gdje je $f(p)$ red od p u $(\mathbb{Z}/N\mathbb{Z})^\times$ i $g(p) = \dfrac{\varphi(N)}{f(p)}$.

Dokaz. Neka je p prost broj relativno prost sa N i neka su $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ prosti ideali od $\mathcal{O}_K$ nad p. Dovoljno je dokazati da je $\mathbb{N}(\mathfrak{P}_i) = p^{f(p)}$. Kako se p ne račva u $\mathcal{O}_K$ (jer $p \nmid N$), znamo da je tada $r = \frac{\varphi(N)}{f(p)} = g(p)$ (jer je K stupnja $\varphi(N)$ nad $\mathbb{Q}$). Iz algebarske teorije brojeva znamo da je dovoljno dokazati da je $f(p)$ jednak stupnju proširenja konačnih polja $\mathbb{Z}/p\mathbb{Z} \subset \mathcal{O}_K/\mathfrak{P}_i$. Također znamo da je Galoisova grupa tog proširenja ciklička grupa reda f generirana s automorfizmom $x \mapsto x^p$. Ako fiksiramo neki prosti ideal $\mathfrak{P}$ nad p, tu grupu možemo identificirati s cikličkom podgrupom Galoisove grupe proširenja $K/\mathbb{Q}$, $\mathrm{Gal}(K/\mathbb{Q})$, koja je generirana automorfizmom σ_p (taj element se zove Frobenius nad p) koji djeluje na $\alpha \in K$ formulom $\sigma_p(\alpha) \equiv \alpha^p \pmod{\mathfrak{P}}$. Poznato je da je $\mathrm{Gal}(K/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/N\mathbb{Z})^\times$ i po tom izomorfizmu se σ_p preslikava u p pa slijedi da je $f = f(p)$. □

Veza između Dirichletovih i Dedekindovih L-funkcija je dana sljedećim identitetom.

Lema 6.28. *Neka je $K = \mathbb{Q}(\mu_N)$. Vrijedi*

$$\zeta_K(s) = \prod_{\chi \in \widehat{(\mathbb{Z}/N\mathbb{Z})^\times}} L(\chi, s) \quad \text{za} \quad \Re(s) > 1.$$

Dokaz. Dovoljno je dokazati da su Eulerovi produkti lijeve i desne strane jednakosti jednaki tj. da za svaki prost $p \nmid N$

$$\prod_{\chi \in \widehat{(\mathbb{Z}/N\mathbb{Z})^\times}} \left(1 - \frac{\chi(p)}{p^s}\right) = \left(1 - \frac{1}{p^{f(p)s}}\right)^{g(p)}.$$

Označimo sa H podgrupu od $(\mathbb{Z}/N\mathbb{Z})^\times$ (reda $f(p)$) generiranu s p. Budući da se svaki karakter od H može proširiti na $g(p)$ načina do karaktera od $(\mathbb{Z}/N\mathbb{Z})^\times$ vrijedi

$$\prod_{\chi \in \widehat{(\mathbb{Z}/N\mathbb{Z})^\times}} \left(1 - \frac{\chi(p)}{p^s}\right) = \prod_{\chi \in \widehat{H}} \left(1 - \frac{\chi(p)}{p^s}\right)^{g(p)}.$$

Kako $\chi(p)$ za $\chi \in \widehat{H}$ poprima kao vrijednosti sve $f(p)$-te korijene iz jedinice, tvrdnja leme slijedi iz sljedećeg polinomijalnog identiteta

$$\prod_{\omega} (1 - \omega T) = 1 - T^{f(p)}.$$

Ovdje se množi po svim ω za koje je $\omega^{f(p)} = 1$. □

Trebat će nam malo teorije Dirichletovih redova. Navest ćemo neke činjenice bez dokaza.

Definicija 6.29. Dirichletov red je red oblika

$$\sum_{n\geq 1} \frac{a_n}{n^s},$$

gdje je $(a_n)_{n\in\mathbb{N}}$ kompleksan niz i $s \in \mathbb{C}$.

Teorem 6.30. *Za svaki Dirichletov red postoji $\sigma \in [-\infty, +\infty]$ takav da red konvergira za svaki $\Re(s) > \sigma$ i divergira za svaki $\Re(s) < 0$. Takav σ nazivamo apcisa konvergencije.*

Teorem 6.31 (Landau)**.** *Neka je $F(s) = \sum_{n\geq 1} a_n n^{-s}$ Dirichletov red s $a_n \geq 0$ za sve $n \in \mathbb{N}$ čija je apcisa konvergencije $\sigma < +\infty$. Tada funkcija $F(s)$ ima singularitet u točki $s = \sigma$.*

Dokaz. □

Sad napokon možemo dokazati Teorem 6.25.

Dokaz. Neka je $K = \mathbb{Q}(\mu_N)$. Dovoljno je dokazati da

$$\zeta_K(s) = \prod_{\chi} L(\chi, s),$$

ima pol u točki $s = 1$. Po definiciji $\zeta_K(s)$ je Dirichletov red sa nenegativnim koeficijentima. Zato možemo primjeniti Landauov teorem: ako je σ apcisa konvergencije Dirichletovog reda $\zeta_K(s)$ onda $\zeta_K(s)$ ima singularitet u točki σ. Očito je $\sigma \leq 1$, pa ako $\zeta_K(s)$ nema singularitet u točki $s = 1$ onda Landauov teorem implicira da je $\sigma \leq 0$ jer su funkcije $L(\chi, s)$ holomorfne za $0 < \Re(s) < 1$. No to je nemoguće. Uzmimo $s \in (0, 1)$. Gruba ocjena p-tog Eulerovog faktora daje

$$\frac{1}{\left(1 - \frac{1}{p^{f(p)}}\right)^{g(p)}} = \left(1 + \frac{1}{p^{f(p)s} + \dots}\right)^{g(p)} \geq 1 + \frac{1}{p^{\varphi(N)s}} + \frac{1}{p^{2\varphi(n)s}} + \cdots.$$

Ako izmnožimo gornju nejednakost po svim $p \nmid N$, slijedi

$$\zeta_N(s) \geq \sum_{NZM(n,N)=1} \frac{1}{n^{\varphi(N)s}}.$$

Ako uvrstimo $s = \frac{1}{\varphi(N)}$ dobivamo

$$\zeta_K(s) \geq \sum_{NZM(n,N)=1} \frac{1}{n} = \infty.$$

□

Sada ćemo definirati analitičko proširenje Riemannove zeta funkcije na cijeli $\mathbb{C}$. Za početak ćemo definirati Gamma funkciju $\Gamma(s)$.

Definicija 6.32. Za $\Re(s) > 0$ definiramo

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

Zadatak 24. Dokažite:

a) $\Gamma(s+1) = s\Gamma(s)$,

b) $\Gamma(s)\Gamma(1-s) = \frac{\pi}{\sin(\pi s)}$,

c) $\Gamma(\frac{s}{2})\Gamma(\frac{s+1}{2}) = \sqrt(\pi)2^{1-s}\Gamma(s)$.

Prvi dio prethodnog zadatak implicira

Korolar 6.33. *$\Gamma(s)$ ima analitičko proširenje na $\mathbb{C}$ s jednostavnim polovima u točkama $s = 0, -1, -2, \ldots$.*

Dok iz drugog dijela slijedi

Korolar 6.34. *$\frac{1}{\Gamma(s)}$ je cijela funkcija na $\mathbb{C}$ (tj. nema polova).*

Gamma funkcija se pojavljuje na prirodan način kod prikaza Riemannove zeta funkcije pomoću Mellinove transformacije.

Definicija 6.35. Neka je $f(t)$ funkcija definirana za $t > 0$. Mellinova transformacija funkcije $f(t)$ je funkcija

$$g(t) = \int_0^\infty f(t) t^s \frac{t^s}{t}.$$

Zadatak 25. Neka je $c > 0$. Mellinova transformacija funkcije e^{-ct} je funkcija $c^{-s}\Gamma(s)$.

Prisjetimo se rezultata iz odjeljka 4.1. Theta funkcija

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

zadovolja funkcijsku jednadžbu

$$\theta\left(-\frac{1}{4\tau}\right) = \sqrt{-2i\tau}\theta(\tau).$$

Nas će zanimati ponašanje funkcije $\theta(\tau)$ na imaginarnoj osi pa uvodimo supstituciju $\tau \mapsto \frac{i}{2}t$ i definiramo $\tilde{\theta}(t) = \theta(\frac{i}{2}\tau)$ za $t > 0$. Vrijedi $\tilde{\theta}(t) = \frac{1}{\sqrt{t}}\tilde{\theta}(1/t)$.

Teorem 6.36. *$\zeta(s)$ ima analitičko proširenje na $\mathbb{C}$ s jednostavnim polom u točki $s = 1$ (reziduum je 1). Neka je*

$$\Lambda(s) = \pi^{-\frac{s}{2}}\Gamma(s/2)\zeta(s).$$

Tada je $\Lambda(s) = \Lambda(1-s)$.

Dokaz. Za $\Re(s) > 1$ vrijedi

$$\int_0^\infty \tilde{\theta}(t)t^{s/2}\frac{dt}{t} = \sum_{n\in\mathbb{Z}} \frac{1}{(\pi n^2)^{s/2}}\Gamma(s/2) = \Lambda(s).$$

Divergencije integrala za $\Re(s) \leq 1$ je posljedica ponašanja funkcije $\tilde{\theta}(t)$ kad $t \to 0^+$ i $t \to \infty$.

Lema 6.37. *$|\tilde{\theta}(t) - \frac{1}{\sqrt{t}}| < e^{-\frac{c}{t}}$ za neki $c \in \mathbb{R}$ kad $t \to 0^+$.*

Dokaz. Znamo da je $\tilde{\theta}(t) \to 1$ kad $t \to \infty$ (zbog toga što je nulti Foureirov koeficijent od $\theta(\tau)$ jednak jedan. Pa funkcijska jednadžba $\tilde{\theta}(t) = \frac{1}{\sqrt{t}}\tilde{\theta}(1/t)$ implicira $\tilde{\theta}(t) \sim \frac{1}{\sqrt{t}}$ kad $t \to \infty$. Pretpostavimo $\sqrt{t} > e^{-1/t}$ i $e^{-\frac{3\pi}{t}} < 1/2$. Računamo

$$\begin{aligned}
|\tilde{\theta}(t) - \frac{1}{\sqrt{t}}| &< \frac{1}{2}e^{1/t}\left(e^{-\pi/t} + e^{-4\pi/t} + \cdots\right) \\
&< \frac{1}{2}e^{1/t}e^{-\pi/t}\left(1 + e^{-3\pi/t} + \cdots\right) \\
&< \frac{1}{2}e^{-(\pi-1)/t}(1 + 1/2 + 1/4\cdots).
\end{aligned}$$

□

Izraz

$$\phi(s) = \int_1^\infty t^{s/2}\left(\tilde{\theta}(t) - 1\right)\frac{dt}{t} + \int_0^1 t^{s/2}\left(\tilde{\theta}(t) - \frac{1}{\sqrt{t}}\right)\frac{dt}{t}$$

definira holomorfnu funkciju za svaki $c \in \mathbb{C}$. Za $\Re(s) > 1$ integral $\int_0^\infty \tilde{\theta}(t)t^{s/2}\frac{dt}{t}$ konvergira pa vrijedi $\phi(s) = \Lambda(s) + \frac{1}{s} + \frac{1}{1-s}$. Dakle $\zeta(s) = \frac{\pi^{s/2}}{\Gamma(s/2)}\left(\frac{1}{2}\phi(s) - \frac{1}{s} - \frac{1}{1-s}\right)$ je analitičko proširenje od $\zeta(s)$ na cijeli $\mathbb{C}$ s mogućim polovima u točkama $s = 0$ i $s = 1$ (znamo da je $\frac{1}{\Gamma(s)}$ cijela funkcija). Iz Leme 6.37 slijedi da je točka $s = 1$ pol s reziduuom 1. Vrijedi $s\Gamma(s/2) = 2\Gamma(s/2 + 1) \to \neq 0$ kad $s \to 0$, pa $\zeta(s)$ nema pol u točki $s = 0$.

Preostaje nam još dokazati funkcijsku jednadžbu. Dovoljno je dokazati $\phi(s) = \phi(1-s)$. Zamjenom varijabli $t \mapsto 1/t$ dobivamo ($\frac{d(1/t)}{1/t} = -\frac{dt}{t}$)

$$\begin{aligned}
\phi(s) &= \int_0^1 t^{-s/2}\left(\tilde{\theta}(1/t) - 1\right)\frac{dt}{t} + \int_1^\infty t^{-s/2}\left(\tilde{\theta}(1/t) - \sqrt{t}\right)\frac{dt}{t} \\
&= \int_0^1 t^{-s/2}\left(\sqrt{t}\tilde{\theta}(t) - 1\right)\frac{dt}{t} + \int_1^\infty t^{-s/2}\left(\sqrt{t}\tilde{\theta}(t) - \sqrt{t}\right)\frac{dt}{t} \\
&= \int_0^1 t^{-s/2+1/2}\left(\tilde{\theta}(t) - 1/\sqrt{t}\right)\frac{dt}{t} + \int_0^\infty t^{-s/2+1/2}\left(\tilde{\theta}(t) - 1\right)\frac{dt}{t} \\
&= \phi(1-s)
\end{aligned}$$

□

6.5 Hasse-Weilova L-funkcija $L(E_n, s)$

Neka je $s \in \mathbb{C}$. Hasse-Weilovu L-funkciju $L(E_n, s)$ definirali smo formulom

$$L(E_n, s) = \frac{\zeta(s)\zeta(s-1)}{\prod_p Z(E_n/\mathbb{F}_p; p^{-s})}.$$

Zadatak 26. Neka je p prost broj koji dijeli $2n$. Dokažite da je

$$Z(E_n/\mathbb{F}_p) = \frac{1}{(1-T)(1-pT)}.$$

Produktna formula $\zeta(s) = \prod_p \frac{1}{1-p^{-s}}$ zajedno sa prethodnim zadatkom implicira

$$L(E_n, s) = \prod_{p \nmid 2n} \frac{1}{1 - 2a_{E_n,p}p^{-s} + p^{1-2s}},$$

gdje je (vidi Teorem 6.9)

$$(1-T)(1-pT)Z(E_n/F_p; T) = 1 - 2a_{E_n,p}T + T^2.$$

Zadnju jednakost možemo zapisati na malo drugačiji način koristeći proste ideal iz prstena $\mathbb{Z}[i]$. Prisjetimo se, ako je P prost ideal iz $\mathbb{Z}[i]$ tada je $\mathbb{N}P = p^{\deg P}$, ($p \in \mathbb{Z}$ prost), gdje je $\deg P$ je stupanj ideala P (stupanj proširenja od $\mathbb{Z}[i]/P$ nad $\mathbb{F}_p$). Kažemo da je P ideal nad p. Ako je P stupnja 2, onda je $P = (p)$ (i $p \equiv 3 \pmod 4$) i kažemo da je p inertan u $\mathbb{Z}[i]$. Ako je P stupnja jedan tada kažemo da se p cijepa u $\mathbb{Z}[i]$ (osim u slučaju kad je $P = (1+i)$, tada je $(2) = (1+i)^2$ i kažemo da se 2 ramificira u $\mathbb{Z}[i]$) i vrijedi $(p) = P\bar{P}$ (i $p \equiv 1 \pmod 4$). Ako sa α_P označimo generator ideala P određen kongruencijskim uvjetom iz Teorema 6.9 (definiramo $\alpha_P = 0$ za $P|2n$), onda vrijedi

$$(1-T)(1-pT)Z(E_n/F_p; T) = 1 - 2a_{E_n,p}T + T^2 = \prod_{P|(p)} (1 - (\alpha_P T)^{\deg P},$$

odnosno

$$L(E_n, s) = \prod_{P \nmid 2n} \frac{1}{1 - \alpha_P^{\deg P}(\mathbb{N}P)^{-s}}.$$

Definirajmo multiplikativno preslikavanje na $\mathbb{Z}[i]$ koje generatoru x prostog ideala P pridružuje $\alpha_P^{\deg P}$. Za $x \in \mathbb{Z}[i]$ relativno prost s 2, definiramo $\chi_1'(x) = i^j$ gdje je $i^j x \equiv 1 \pmod{2+2i}$. Neka je

$$\chi_n'(x) = \begin{cases} \chi_1'(x)\left(\frac{n}{\mathbb{N}x}\right), \text{ ako je } x \text{ relativno prost sa } 2n \\ 0, \text{ inače} \end{cases}$$

i $\tilde{\chi}_n(x) = x\chi_n'(x)$.

Dokaz sljedeće propozicije ostavljamo čitatelju.

Propozicija 6.38. *Preslikavanje $\tilde{\chi}_n$ je jedinstveno multiplikativno preslikavanje na $\mathbb{Z}[i]$ koje bilo koji generator prostog ideala P preslikava u $\alpha_P^{\deg P}$.*

Primjetimo da je χ_1' karakter od $\mathbb{Z}[i]/(2+2i)^\times$. Općenito kažemo da je ideal J konduktor karaktera $\chi : \mathbb{Z}[i]^\times \to \mathbb{C}^\times$ ako je J najveći ideal takav da $\chi(x)$ ovisi samo o x modulo J.

Propozicija 6.39. *Konduktor multiplikativnog karaktera χ_n' je jednak $(2+2i)n$ ako je n neparan, a $2n$ ako je n paran.*

Dokaz. Pretpostavimo da je n neparan. Slučaj n je paran ostavljamo čitatelju. Neka je $n = l_1 l_2 \cdots l_t$, gdje su l_i različiti neparni prosti brojevi (pretpostavljamo kao i uvijek da je n kvadratno slobodan). Prvo ćemo dokazati da $\chi_n'(x)$ ovisi samo o $x \bmod (2+2i)n$, gdje je $NZM(x, 2n) = 1$. Tada je $\mathbb{N}x = \prod p_i^{\alpha_i}$, gdje su p_i neparni prosti brojevi takvi da je $p_i \equiv 1 \pmod 4$ ako je α_i neparan (akoe je α_i neparan, onda se p_i cijepa u $\mathbb{Z}[i]$). Računamo

$$\left(\frac{n}{\mathbb{N}x}\right) = \prod_{j,k} \left(\frac{l_j}{p_k}\right) = \prod_{k,j} \left(\frac{p_k}{l_j}\right).$$

Druga jednakosti slijedi iz kvadratnog reciprociteta budući da brojevi p_i daju ostatako 1 pri djeljenju sa četiri. Iz definicije od χ_n' i prethodnog identiteta slijedi

$$\chi_n'(x) = \chi_1'(x) \prod_j \left(\frac{\mathbb{N}x}{l_j}\right) = \chi_1'(x)\left(\frac{\mathbb{N}x}{n}\right).$$

Pretpostavimo da je $x' = x + (2+2i)n\beta$, gdje je $\beta \in \mathbb{Z}[i]$. Tada $\mathbb{N}x' = (x + (2+2i)n\beta)(\bar{x} + (2+2i)n\bar{\beta}) \equiv x\bar{x} = \mathbb{N}x \pmod n$. Budući da je $\chi_1'(x') = \chi_1'(x)$ jer $x \equiv x' \pmod{2+2i}$ slijedi $\chi_n'(x) = \chi_n'(x')$.

Potrebno je još pokazati da ne postoji djeljitelj od $(2+2i)n$ takav da $\chi_n'(x)$ ovisi samo o x modulo taj djeljitelj (ovo svojstvo karaktera se naziva primitivnost). Pretpostavimo suprotno. Neke je $Q|(2+2i)n$ prost ideal sa traženim svojstvom. Posebno vrijedi da je $\chi_n'(x) = 0$ ili 1 za sve $x \equiv 1 \pmod{(2+2i)n/Q}$. Promotrimo tri slučaja

a) $Q = (2+2i)$. Neka je $x_0 = 1+2ni$. Po pretpostavci je $\chi'_n(x_0) \neq -1$, dok zbog $\mathbb{N}x_0 \equiv 1 \pmod{n}$ slijedi $\chi'_n(x_0) = \chi'_1(x_0) = -1$. Kontradikcija.

b) $Q = (a+bi)$ gdje je $\mathbb{N}Q = l \equiv 1 \pmod 4$ (Q je stupnja 1). Neka je $x_0 = 1+4kn(a-bi)/l$, za neki cijeli broj k. Po pretpostavci je $\chi'_n(x_0) \neq -1$. Očito $\chi'_1(x_0) = 1$ i $\mathbb{N}x \equiv 1+8akn/l \pmod n$, dakle $\chi'_n(x_0) = \left(\frac{1+8akn/l}{l}\right)$. Budući da je n kvadratno slobodan (i $l \nmid a$) $8an/l$ je relativno prost sa n pa postoji $k \in \mathbb{Z}$ takav da je $1+8akn/l$ kvadratni neostatak modulo l. Kontradikcija.

c) $Q = (l)$ gdje je $l \equiv 3 \pmod 4$ (Q je stupnja 2). Pretpostavljamo da je $\chi'_n(x_0) \neq -1$ za $x_0 \equiv 1 \pmod{(2+2i)n/l}$. Posebno za takav x_0 vrijedi $\chi'_1(x_0) = 1$. Kako je $(2+2i)n/l$ relativno prost sa l slijedi da brojevi oblika $1+\beta(2+2i)n/l$ za $\beta \in \mathbb{Z}[i]$, prolaze kroz sve klase ostataka od $\mathbb{Z}[i]$ modulo Q kad β prolazi kroz sve klase ostataka $\mathbb{Z}[i]$ modulo Q (dokaz: Dirichletov princip) pa možemo odrabrati β takav da $\mathbb{N}x_0 \in \mathbb{F}_l^\times$ nije kvadrat u $\mathbb{F}_l$, odnosno $\left(\frac{\mathbb{N}x}{l}\right) = -1$ (to je moguće jer je $\mathbb{Z}[i]/Q \cong \mathbb{F}_{l^2}$ i preslikavanje $\mathbb{N} : \mathbb{F}_{l^2} \to \mathbb{F}_l$ je surjektivno). Kontradikcija.

□

Za izvod funkcijske jednadžbe Hasse-Weilove L-funkcije $L(E_n, s)$ trebat će nam Gaussova suma karaktera $\chi'_n(x)$. Označimo sa n' konduktor karaktera χ'_n (iz prethodnog teorema). Lako se vidi da je

$$\psi(x) = e^{2\pi i \Re(x/n')}$$

aditivan karakter od $\mathbb{Z}[i]/n'$ koji je netrivijalan na višekratnicima pravih djeljitelja od n'. Gaussovu sumu $g(\chi'_n)$ definiramo formulom $g(\chi'_n) = \sum_{x \in \mathbb{Z}[i]/n'} \chi'_n(x)\psi(x)$. Vrijedi

Propozicija 6.40. $g(\chi'_n) = \begin{cases} \left(\frac{-2}{n}\right) n', & \textit{ako je } n \textit{ neparan} \\ \left(\frac{-1}{n_0}\right) in', & \textit{ako je } n = 2n_0 \textit{ paran.} \end{cases}$

Koristeći karaktere $\tilde{\chi}_n$ Hasse-Weilovu L-funkciju možemo zapisati kao

$$L(E_n, s) = \prod_{P \nmid 2n} \left(1 - \frac{\tilde{\chi}_n(P)}{(\mathbb{N}P)^s}\right)^{-1}.$$

Kao i kod Riemannove zeta funkcije, svaki Eulerov faktor možemo razviti u geometrijski red

$$\left(1 - \frac{\tilde{\chi}_n(P)}{(\mathbb{N}P)^s}\right)^{-1} = \sum_{k=0}^{\infty} \frac{\tilde{\chi}_n(P)^k}{(\mathbb{N}P)^{ks}},$$

pa koristeći multiplikativnost funkcija $\tilde{\chi}_n$ i $\mathbb{N}$ i jedinstvenu faktorizaciju ideala iz $\mathbb{Z}[i]$ na proste faktore dobivamo

$$L(E_n, s) = \sum_I \tilde{\chi}_n(I)(\mathbb{N}I)^{-s},$$

gdje sumiramo po svim idealima $I \subset \mathbb{Z}[i]$ koji su relativno prosti sa $2n$. Budući da $\tilde{\chi}_n$ poprima vrijednost 0 na idealima koji nisu relativno prosti sa $2n$, sumu možemo proširiti do sume po svim idealima.

Koristeći ovu formulaciju možemo lako vidjeti koja je veza između Dirichletovih redova $L(E_n, s)$ za različite n. Neka je

$$L(E_n, s) = \sum_{m=1}^{\infty} b_{m,n} m^{-s}.$$

Tada je $b_{m,n} = \sum_{\mathbb{N}I=m} \tilde{\chi}_n(I)$. Kako je $\tilde{\chi}_n(I) = \tilde{\chi}_1(I) \left(\frac{n}{\mathbb{N}I}\right)$, slijedi

$$b_{m,n} = \left(\frac{n}{m}\right) \sum_{\mathbb{N}I=m} \tilde{\chi}_1(I) = \left(\frac{n}{m}\right) b_{m,1}.$$

Dakle L-funkcija $L(E_n, s)$ je određena s $L(E_1, s)$ i karakterom $m \mapsto \left(\frac{n}{m}\right)$.

7 Analitičko proširenje i funkcijska jednadžba funkcije $L(E_n, s)$

U analogiji sa dokazom analitičkog proširenja Riemannove zeta funkcije tražimo funkciju $F(E_n, t)$ čija je Mellinova transformacija jednaka funkciji (svaki ideal $I \subset \mathbb{Z}[i]$ ima četiri generatora).

$$L(E_n, s) = \sum_I \tilde{\chi}_n(I)(\mathbb{N}I)^{-s} = \frac{1}{4} \sum_{x \in \mathbb{Z}[i]} \tilde{\chi}_n(x)(\mathbb{N}x)^{-s}.$$

Lako se vidi je tražena funkcija

$$F(E_n, t) = \frac{1}{4} \sum_{x \in \mathbb{Z}[i]} \tilde{\chi}_n(x) e^{-\pi t |x|^2}.$$

Cilj nam je pronaći funkcijsku jednadžbu za $F(E_n, t)$. Iz nje će direktno slijediti funkcijska jednadžba za $L(E_n, s)$. Zapisat ćemo $F(E_n, t)$ na način koji će uzeti u obzir činjenicu da je χ'_n karakter od $(\mathbb{Z}[i]/n')^{\times}$, gdje je $n' = (2+2i)n$ za n neparan, a $n' = 2n$ za n paran. Za $a + bi \in Z[i]$, označimo sa $u_1 + u_2 i = (a+bi)/n'$. Neka je $N' = |n'|^2$. Vrijedi

$$F(E_n, t) = \frac{n'}{4} \sum_{a+bi \in \mathbb{Z}[i]/n'} \chi'_n(a+bi) \sum_{m \in \mathbb{Z}^2} (m+u) \cdot (1,i) e^{-\pi N' t |m+u|^2}.$$

Ovdje je $u = (u_1, u_2)$ i $\cdot$ označava standardni skalarni produkt. Da bi analizirali funkciju $F(E_n, \frac{1}{N't})$ uvest ćemo dvije funkcije. Neka je $u = (u_1, u_2) \in \mathbb{R}^2$ takav da $u \notin \mathbb{Z}^2$, $w = (1, i)$ i neka je $t > 0$. Definiramo

$$\theta_u(t) = \sum_{m \in \mathbb{Z}^2} (m+u) \cdot w e^{-\pi t |m+u|^2}. \tag{18}$$

Tada je $F(E_n, \frac{1}{N't}) = \frac{n'}{4} \sum_{a+bi \in \mathbb{Z}[i]/n'} \chi'_n(a+bi)\theta_u(\frac{1}{t})$.

Za funkcijsku jednadžbu od $\theta_u(t)$, slično kao i kod klasične theta funkcije, primjenit ćemo Poissonovu sumacijsku formulu na funkciju $g(x) = (x+u) \cdot we^{-\pi t|x+u|^2}$ i njenu Fourierovu transformaciju $\hat{g}(y)$. Trebat će na slijedeća lema čiji dokaz ostavljamo čitatelju.

Lema 7.1.

$$\hat{g}(y) = -it^{-2}w \cdot ye^{2\pi iu\cdot y}e^{-(\pi/t)|y|^2}.$$

Definirajmo

$$\theta^u(t) = \sum_{m\in\mathbb{Z}^2} m \cdot we^{2\pi im\cdot u}e^{-\pi t|m|^2}.$$

Tada vrijedi iz Poissonove sumacije slijedi

$$\theta_u(t) = \sum_{m\in\mathbb{Z}^2} g(m) = \sum_{m\in\mathbb{Z}^2} \hat{g}(m) = \frac{-i}{t^2}\theta^u\left(\frac{1}{t}\right). \tag{19}$$

8 Heckeovi operatori

U ovom odjeljku ćemo definirati Heckeove operatore - linearne operatore koji djeluju na modularne formame, koji nam omogućuju nalaženje kanonske baze prostora modularnih formi (koja se sastoji od zajedničkih karakterističnih formi svih operatora). L-funkcije tih karakterističnih formi (Heckeove eigenforme) možemo definirati preko Mellinove transformacije (slično kao u dokazu analitičkog proširenja Riemannove zeta funkcije) i tako definirane L-funkcije imaju Eulerov produkt i zadovoljavaju funkcijsku jednadžbu pa su prirodna generalizacija Hasse-Weilovih L-funkcija koje su prema teoremu o modularnosti (koji implicira posljednji Fermatov teorem) Mellinova tranformacija Heckeovih eigenformi težine dva za $\Gamma_0(N)$ (za neki $N \in \mathbb{N}$) sa racionalnim Fourierovim koeficijentima.

Heckeovi operatori objašnjavaju razne zanimljive relacije između Fourierovih koeficijenata modularnih formi. Klasičan primjer je Ramanujanova Δ-funkcija. Ramanujanova Δ-funkcija se definira formulom

$$\Delta(\tau) = q\prod_{i=1}^{\infty}(1-q^i)^{24} = \sum_{n=1}^{\infty}\tau(n)q^n, \quad \text{gdje je } q = e^{2\pi i\tau}, \tau \in \mathbb{H}.$$

Poznato je da je $\Delta(\tau)$ baza prostora $S_{12}(\Gamma(1))$, a time je automatski karakteristična forma za djelovanje svih Heckeovih operatora. Iz formula za djelovanja Heckeovih operatora na Fourierove koeficijente modularnih formi (Propozicija 8.4) slijede sljedeća svojstva τ-funkcije:

- $\tau(mn) = \tau(m)\tau(n)$ za $NZM(m,n) = 1$,
- $\tau(p^{r+1}) = \tau(p)\tau(p^r) - p^{11}\tau(p^{r-1})$, za prost broj p,

koja je direktno iz definicije τ funkcije vrlo teško dokazati.

8.1 Dvostruki slash operatori

Neka su Γ_1 i Γ_2 kongruencijske podgrupe od $\mathrm{SL}_2(\mathbb{Z})$ i neka je $\mathrm{GL}_2(\mathbb{Q})^+ < \mathrm{GL}_2(\mathbb{Q})$ podgrupa matrica pozitivne determinante. U ovom odjeljku ćemo za $\alpha \in \mathrm{GL}_2(\mathbb{Q})^+$ definirati operator $[\Gamma_1 \alpha \Gamma_2]_k$ (dvostruki slash operator) koji preslikava modularne formu težine k za Γ_1 u modularne forme težine k za Γ_2.

Neka je $f : \mathbb{H} \to \mathbb{C}$ funkcija. Za $\alpha \in \mathrm{GL}_2(\mathbb{Q})^+$ definiramo slash operator težine k formulom

$$(f[\alpha]_k)(\tau) = (\det \alpha)^{k-1} j(\alpha, \tau)^{-k} f(\alpha(\tau)), \text{ za } \tau \in \mathbb{H},$$

gdje je $j(\alpha, \tau) = c\tau + d$, za $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Slash operator definira djelovanje grupe $\mathrm{GL}_2(\mathbb{Q})^+$ na funkcijama, tj. vrijedi $f[\alpha]_k[\beta]_k = f[\alpha\beta]_k$ za svaki $\alpha, \beta \in \mathrm{GL}_2(\mathbb{Q})^+$ (vidi Lemu 3.2 za svojstva slash operatora).

Definicija 8.1. Dvostruki slash operator $[\Gamma_1 \alpha \Gamma_2]_k$ težine k definiramo na modularnim formama $f \in M_k(\Gamma_1)$ formulom

$$f[\Gamma_1 \alpha \Gamma_2]_k = \sum_j f[\beta_j]_k,$$

gdje je $\{\beta_j\}$ (konačan skup) takav da je $\Gamma_1 \alpha \Gamma_2 = \cup_j \Gamma_1 \beta_j$.

Napomena. Preslikavanje je dobro definirano zbog invarijantnosti od f na djelovanje od $[\gamma]_k$ za $\gamma \in \Gamma_1$.

Pokazat ćemo da je skup predstavnika $\{\beta_j\}$ konačan. Pogledajmo djelovanje operatora $[\Gamma_1 \alpha \Gamma_2]_k$ u tri specijalna slučaja

1) Ako je $\Gamma_2 \subset \Gamma_1$ i $\alpha = I$, onda je operator identiteta, $f[\Gamma_1 \alpha \Gamma_2]_k = f$.

2) Ako je $\Gamma_1 \subset \Gamma_2$ i $\alpha = I$, onda operator definiramo kao trag, $f[\Gamma_1 \alpha \Gamma_2]_k = \sum f[\gamma_j]_k$, gdje sumiramo po predstavnicima klasa $\{\gamma_j\}$ od $\Gamma_1 \backslash \Gamma_2$.

3) Ako je $\alpha^{-1} \Gamma_1 \alpha = \Gamma_2$, onda je operator djeluje kao običan slash operator $[\alpha]_k$, $f[\Gamma_1 \alpha \Gamma_2]_k = f[\alpha]_k$.

Općenito slučaj možemo prikazati kao kompoziciju ova tri specijalna slučaja. Neka je $\Gamma_3 = \Gamma_2 \cap \alpha^{-1} \Gamma_1 \alpha$ i $\Gamma_3' = \Gamma_1 \cap \alpha \Gamma_2 \alpha^{-1}$. Tada je

$$[\Gamma_1 \alpha \Gamma_2]_k = [\Gamma_3 I \Gamma_2]_k \circ [\Gamma_3' \alpha \Gamma_3]_k \circ [\Gamma_1 I \Gamma_3']_k, \tag{20}$$

odnosno $f \mapsto f \mapsto f[\alpha]_k \mapsto \sum f[\alpha\gamma_j]_k$. Vidimo da su predstavnici $\{\beta_j\}$ iz definicije jednaki $\{\alpha\gamma_j\}$, gdje su $\{\gamma_j\}$ predstavnici klasa od $\Gamma_3 \backslash \Gamma_2$ pa konačnost skupa $\{\gamma_j\}$ slijedi iz sljedećeg zadatka.

Zadatak 27. a) Ako je $\Gamma < \mathrm{SL}_2(\mathbb{Z})$ kongruencijska podgrupa i $\alpha \in \mathrm{GL}_2(\mathbb{Q})^+$, tada je $\alpha^{-1} \Gamma \alpha$ također kongruencijska podgrupa.

b) Ako su Γ i $\tilde{\Gamma}$ kongruencijske podgrupe, tada je indeks $[\Gamma : \Gamma \cap \tilde{\Gamma}]$ konačan.

Budući da dvostruki slash operator u gornja tri specijalna slučaja preslikava modularne (kasp) forme u modularne (kasp) forme, isto možemo zaključiti i za njihovu kompoziciju, dakle općenito vrijedi

$$[\Gamma_1 \alpha \Gamma_2]_k : M_k(\Gamma_1) \to M_k(\Gamma_2),$$

odnosno

$$[\Gamma_1 \alpha \Gamma_2]_k : S_k(\Gamma_1) \to S_k(\Gamma_2).$$

8.2 Hecke operatori na $\Gamma_1(N)$

Postoje dvije vrste Hecke operatora na $\Gamma_1(N)$, oboje su specijalni slučajevi dvostrukih slash operatora. Za prvu vrstu uzmimo $\alpha \in \Gamma_0(N)$.

Prisjetimo se: $\Gamma_1(N)$ je normalna podgrupa od $\Gamma_0(N)$ ($\Gamma_1(N)$ je jezgra preslikavanja $\Gamma_0(N) \to (\mathbb{Z}/N\mathbb{Z})^\times$, $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto d \bmod N$) i vrijedi $\Gamma_0(N)/\Gamma_1(N) \cong (\mathbb{Z}/N\mathbb{Z})^\times$. Prema tome za $f \in M_k(\Gamma_1(N))$

$$f[\Gamma_1(N)\alpha\Gamma_1(N)]_k = f[\alpha]_k, \quad \alpha \in \Gamma_0(N),$$

je element od $M_k(\Gamma_1(N))$, odnosno $\Gamma_0(N)$ djeluje na $M_k(\Gamma_1(N))$. Budući da podgrupa $\Gamma_1(N)$ djeluje trivijalno dobivamo djelovanje kvocijenta $\Gamma_0(N)/\Gamma_1(N) \cong (\mathbb{Z}/N\mathbb{Z})^\times$. Prema tome operator $[\alpha]_k$ za $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$ ovisi jedino o $d \bmod N$ pa koristimo oznaku $\langle d \rangle = [\alpha]_k$ i pišemo $\langle d \rangle f = f[\alpha]_k$. Ovo je prva vrsta Hecke operatora, naziva je još i dijamantni operator (diamond operator).

Dijamantni operatori međusobno komutiraju pa se mogu istovremeno dijagonalizirati u nekoj bazi od $M_k(\Gamma_1(N))$. Tada svaki element f te baze definira Dirichletov karakter $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}$ prema formuli

$$\langle d \rangle f = \chi(d) f,$$

i vrijedi $M_k(\Gamma_1(N)) = \bigoplus_\chi M_k(N, \chi)$, gdje je

$$M_k(N, \chi) = \{f \in M_k(\Gamma_1(N)) : \langle d \rangle f = \chi(d) f \text{ za sve } d \in (\mathbb{Z}/N\mathbb{Z})^\times\}.$$

Druga vrsta Heckeovih operatora su dvostruki slash operatori za koje je također $\Gamma_1 = \Gamma_2 = \Gamma_1(N)$, ali sada je $\alpha = \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)$, gdje je p prost. Ovaj operator označavamo sa T_p i preslikavanje

$$T_p : M_k(\Gamma_1(N)) \to M_k(\Gamma_1(N))$$

je dano formulom

$$T_p f = f[\Gamma_1(N) \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right) \Gamma_1(N)]_k.$$

Pokažimo prvo da T_p i $\langle d \rangle$ komutiraju. Trebat će nam sljedeća činjenica.

Zadatak 28. Neka je $N \in \mathbb{N}$ i p prost. Dokažite

$$\Gamma_1(N) \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right) \Gamma_1(N) = \left\{\gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \equiv \left(\begin{smallmatrix} 1 & * \\ 0 & p \end{smallmatrix}\right) \pmod N, \det \gamma = p\right\}.$$

Propozicija 8.2. *Neka je p prost i $d \in \mathbb{N}$. Operatori $\langle d \rangle$ i T_p komutiraju na $M_k(\Gamma_1(N))$, za sve $k, N \in \mathbb{N}$.*

Dokaz. Neka je $\alpha = \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)$ i $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$. Direktnim računom se provjeri da je $\gamma\alpha\gamma^{-1} \equiv \left(\begin{smallmatrix} 1 & * \\ 0 & p \end{smallmatrix}\right) \pmod N$ pa je prema prethodnom zadatku $\Gamma_1(N)\alpha\Gamma_1(N) = \Gamma_1(N)\gamma\alpha\gamma^{-1}\Gamma_1(N)$. Budući da je $\Gamma_1(N)$ normalna podgrupa od $\Gamma_0(N)$ slijedi $\Gamma_1(N)\gamma\alpha\gamma^{-1}\Gamma_1(N) = \gamma\Gamma_1(N)\alpha\Gamma_1(N)\gamma^{-1}$. Ako sa $\{\beta_i\}$ označimo predstavnike orbita djelovanja od $\Gamma_1(N)$ na $\Gamma_1(N)\alpha\Gamma_1(N)$, tj. $\Gamma_1(N)\alpha\Gamma_1(N) = \cup_j \Gamma_1(N)\beta_j$, tada je

$$\gamma\Gamma_1(N)\alpha\Gamma_1(N)\gamma^{-1} = \gamma\bigcup_j \Gamma_1(N)\beta_j\gamma^{-1} = \bigcup_j \Gamma_1(N)\gamma\beta_j\gamma^{-1}.$$

Dakle, dokazali smo $\cup_j \Gamma_1(N)\beta_j\gamma = \cup_j \Gamma_1(N)\gamma\beta_j$, odnosno $T_p\langle d\rangle = \langle d\rangle T_p$. □

Odredimo sada predstavnike $\Gamma_1(N)$ orbita od $\Gamma_1(N)\alpha\Gamma_1(N)$, za $\alpha = \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)$. Prema (20) treba odrediti predstavnike klasa od $\Gamma_3 = \alpha^{-1}\Gamma_1(N)\alpha$ u $\Gamma_1(N)$. Iz direktnog računa slijedi $\Gamma_3 = \Gamma_1(N) \cap \Gamma^0(p)$, gdje je

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

Propozicija 8.3. *Predstavnici klasa od $\Gamma_3 = \Gamma^0(p) \cap \Gamma_1(N)$ u $\Gamma_1(N)$ su $\left(\begin{smallmatrix} 1 & j \\ 0 & 1 \end{smallmatrix}\right)$ za $0 \le j < p$ ako $p|N$, odnosno $\left(\begin{smallmatrix} 1 & j \\ 0 & 1 \end{smallmatrix}\right)$ za $0 \le j < p$ i $\left(\begin{smallmatrix} mp & n \\ N & 1 \end{smallmatrix}\right)$ (za neke $m, n \in \mathbb{Z}$, gdje je $mp - nN = 1$) ako $p \nmid N$.*

Dokaz. Pretpostavimo da $p|N$. Tada je Γ_3 nivoa N. Označimo sa $\tilde{\Gamma}_3$ i $\tilde{\Gamma}_1(N)$ redukcije grupa mod N. Dovoljno je odrediti predstavnike klasa od $\tilde{\Gamma}_3$ u $\tilde{\Gamma}_1(N)$ (vidi Zadatak 1). Lako se vidi da je $\tilde{\Gamma}_1(N) \cong \mathbb{Z}/N\mathbb{Z}$ i $\tilde{\Gamma}_3 \cong p\mathbb{Z}/N\mathbb{Z}$ pa su predstavnici od $\tilde{\Gamma}_3$ u $\tilde{\Gamma}_1(N)$ elementi $\{0, 1, \ldots p-1\}$, odnosno predstavnici od Γ_3 u $\Gamma_1(N)$ su $\left(\begin{smallmatrix} 1 & j \\ 0 & 1 \end{smallmatrix}\right)$ za $0 \le j < p$. Slučaj $p \nmid N$ ostavljamo čitatelju. □

Sad možemo odrediti djelovanje od T_p na Fourierovim koeficijentima.

Propozicija 8.4. *Neka je $f \in M_k(\Gamma_1(N))$. Budući da je $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma_1(N)$, f ima period 1 i Fourierov razvoj*

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

Tada vrijedi

a)

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

(Ovdje $a_{n/p} = 0$ ako $p \nmid n$ i $1_n : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ je trivijalan karakter modulo N.)

b) Neka je $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ *karakter. Ako je* $f \in M_k(\Gamma_1(N), \chi)$ *tada* $T_p f \in M_k(\Gamma_1(N), \chi)$ *i vrijedi*

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

Dokaz. □

8.3 Glavna lema i newforme

Neka je $M|N$ i $d|\frac{N}{M}$, $d > 1$. Normalizirajmo preslikavanje $[\alpha_d]$ iz prethodnog odjeljka formulom

$$\iota_d = d^{1-k}[\alpha_d]_k : S_k(\Gamma_1(M)) \to S_k(\Gamma_1(N)), \quad (\iota_d f)(\tau) = f(d\tau),$$

gdje je $\alpha_d = \left(\begin{smallmatrix} d & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Tada ι_d djeluje na Fourierov razvoj formulom

$$\iota_d : \sum_{n=1}^{\infty} a_n q^n \mapsto \sum_{n=1}^{\infty} a_n q^{dn}, \qquad \text{gdje je } q = e^{2\pi i \tau}.$$

Teorem 8.5 (Glavna lema)**.** *Neka* $f \in S_k(\Gamma_1(N))$ *ima Fourierov razvoj* $f(\tau) = \sum a_n(f) q^n$*, tako da je* $a_n(f) = 0$ *za* $NZM(n, N) = 1$*. Tada je* f *oblika* $f = \sum_{p|N} \iota_p f_p$*, gdje su* $f_p \in S_k(\Gamma_1(N/p))$*.*

Glavnu lemu su originalno dokazali Atkin i Lehner. Mi ćemo prezentirati elegantan dokaz Davida Carltona koji koristi neke osnovne rezultate o reprezentacijama konačnih grupa.

Prvo ćemo u nekoliko koraka preformulirati lemu u terminima linearne algebre.

Definicija 8.6. Za prirodan broj m definiramo

$$\Gamma^1(m) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) \middle| \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} 1 & 0 \\ * & 1 \end{smallmatrix}\right) \pmod{m} \right\}.$$

Iz direktnog računa slijedi:

Lema 8.7. *Neka je* M *prirodan broj. Vrijedi* $\alpha_M \Gamma_1(M) \alpha_M^{-1} = \Gamma^1(M)$*.*

Prema tome, za $M \in \mathbb{N}$, preslikavanje $M^{k-1}[\alpha_M^{-1}]_k : S_k(\Gamma_1(M)) \to S_k(\Gamma^1(M))$ je izomorfizam koji preslikava $f(\tau)$ u $f(\tau/M)$, odnosno $\sum a_n q^n \mapsto \sum a_n q_M^n$, gdje je $q_M = q^{1/M}$. Ako odaberemo $d = N/M$, onda preslikavanju $\iota_d : S_k(\Gamma_1(M)) \to S_k(\Gamma_1(N))$ po gornjem izomorfizmu odgovara inkluzija $S_k(\Gamma^1(M)) \to S_k(\Gamma^1(N))$ što nam daje drugu verziju Glavne leme.

Teorem 8.8 (Glavna lema, druga verzija)**.** *Ako* $f \in S_k(\Gamma^1(N))$ *ima Fourierov razvoj* $f(\tau) = \sum a_n(f) q_N^n$*, gdje je* $a_n(f) = 0$ *za* $NZM(n, N) = 1$*. Tada je* $f = \sum_{p|N} f_p$*, gdje je* $f_p \in S_k(\Gamma^1(N/p))$*.*

Sada ćemo uvjet na f iz Glavne leme opisati pomoću linearnih operatora. Trebat će nam sljedeća definicija.

Definicija 8.9. Neka je $m \in \mathbb{N}$. Definirajmo

$$\Gamma^0(m) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) | \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} * & 0 \\ * & * \end{smallmatrix}\right) \pmod{m} \right\} \text{ i}$$

$\Gamma_d = \Gamma_1(N) \cap \Gamma^0(N/d)$.

Lema 8.10. *Predstavnici klasa kvocijentnog prostora* $\Gamma(N)\backslash\Gamma_d$ *su*

$$\left\{ \left(\begin{smallmatrix} 1 & bN/d \\ 0 & 1 \end{smallmatrix}\right) | 0 \leq b < d \right\}.$$

Dokaz. Slika od Γ_d u $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ se sastoji od matrica $\left(\begin{smallmatrix} 1 & bN/d \\ 0 & 1 \end{smallmatrix}\right)$ za $b = 0, 1, \ldots, d-1$ odakle slijedi tvrdnja. □

Usrednjivanjem po predstavnicima klasa iz prethodne leme definiramo operator traga

$$\pi_d : S_k(\Gamma(N)) \to S_k(\Gamma(N)), \pi_d(f) = \frac{1}{d} \sum_{b=0}^{d-1} f[\left(\begin{smallmatrix} 1 & bn/d \\ 0 & 1 \end{smallmatrix}\right)]_k.$$

Operator π_d je projekcija na $S_k(\Gamma_d)$ (vrijedi $\pi_d^2 = \pi_d$). Slično kao i kod Hecke operatora, može se vidjeti da π_d djeluje na Fourierove koeficijente formulom

$$\pi_d : \sum_{n=1}^{\infty} a_n q_N^n \mapsto \sum_{n:d|n} a_n q_N^n.$$

Iz toga slijedi da $\pi_{d_1 d_2} = \pi_{d_1}\pi_{d_2} = \pi_{d_2}\pi_{d_1}$, za $d_1 d_2 | N$.

Definirajmo $\pi : S_k(\Gamma(N)) \to S_k(\Gamma(N))$ formulom $\pi = \prod_{p|N}(1 - \pi_p)$. Budući da operatori π_d komutiraju, vrijedi

$$\pi : \sum_{n=1}^{\infty} a_n q_N^n \mapsto \sum_{n:NZM(n,N)=1} a_n q_N^n.$$

Prema tome $f(\tau)$ iz Teorema 8.8 se nalazi u prostoru $S_k(\Gamma^1(N)) \cap \ker(\pi)$. Budući da su π_d komutirajući projektori vrijedi

$$\ker(\pi) = \ker\left(\prod_{p|N}(1 - \pi_p)\right) = \sum_{p|N} \ker(1 - \pi_p) = \sum_{p|N} \mathrm{Im}(\pi_p).$$

Po definicije je π_p projekcija na $S_k(\Gamma_p)$ pa je

$$\mathrm{Im}(\pi_p) = S_k(\Gamma_1(N) \cap \Gamma^0(N/p)),$$

odnosno

$$\ker(\pi) = \sum_{p|N} S_k(\Gamma_1(N) \cap \Gamma^0(N/p)).$$

Prema tome, Glavna lema je ekvivalentna sljedećoj tvrdnji.

Teorem 8.11 (Glavna lema, treća verzija)**.**

$$S_k(\Gamma^1(N)) \cap \sum_{p|N} S_k(\Gamma_1(N) \cap \Gamma^0(N/p)) = \sum_{p|N} S_k(\Gamma^1(N/p)).$$

Prostore modularnih formi koji se javljaju u iskazu Teorema 8.11 čemo opisati preko djelovanja grupa. Znamo da grupa $\mathrm{SL}_2(\mathbb{Z})$ djeljuje na $S_k(\Gamma(N))$ preko slash operatora težine k tako da (po definiciji) njena normalna grupa $\Gamma(N)$ djeluje trivijalno što inducira djelovanje konačne grupe $\mathrm{SL}_2(\mathbb{Z})/\Gamma(N) \cong \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Ako je $N = \prod_{i=1}^n p_i^{e_i}$ faktorizacija na proste djeljitelje broja N, onda kineski teorem o ostacima povlači

$$G := \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) = \prod_{i=1}^n G_i, \text{ gdje je } G_i = \mathrm{SL}_2(\mathbb{Z}/p_i^{e_i}\mathbb{Z}).$$

Definirajmo

$$H_i = \Gamma^1(p_i^{e_i})/\Gamma(p_i^{e_i}),$$
$$K_i = (\Gamma_1(p_i^{e_i}) \cap \Gamma^0(p_i^{e_i-1}))/\Gamma(p_i^{e_i}).$$

Zadatak 29. Za prosti broj p i $e \geq 1$ vrijedi

$$\left\langle \Gamma^1(p^e), \Gamma_1(p^e) \cap \Gamma^0(p^{e-1}) \right\rangle = \Gamma^1(p^{e-1}),$$

gdje je $\langle A, B \rangle$ oznaka za grupu generiranom grupama A i B.

Općenito, za vektorski prostor V na koji djeluje grupa G, sa $V^G \subset V$ ćemo označavati potprostor vektora koje G fiksira. Koristeći tu oznaku i prethodni zadatak Teorem 8.11 možemo iskazati formulom

$$S_k(\Gamma(N))^H \cap \sum_{i=1}^n S_k(\Gamma(N))^{K_i} = \sum_{i=1}^n S_k(\Gamma(N))^{\langle H, K_i \rangle}$$

Ova tvrdnja direktno slijedi iz sljedećeg rezultata iz teorije reprezentacija konačnih grupa.

Propozicija 8.12. *Neka je V ireducibilna reprezentacija grupe $G = \prod_{i=1}^n G_i$ i neka su $H = \prod_{i=1}^n H_i$ i $K = \prod_{i=1}^n K_i$ podgrupe od G. Tada*

$$V^H \cap \sum_{i=1}^n V^{K_i} = \sum_{i=1}^n V^{\langle H, K_i \rangle}.$$

Dokaz ove propozicije (zajedno sa pregledom osnovnih pojmova iz teorije reprezentacija konačnih grupa) se nalazi u dodatku.

9 Dodatak: Reprezentacije konačnih grupa

U ovom odjeljku pretpostavljamo da su svi vektorski prostori nad $\mathbb{C}$.

Definicija 9.1. Neka je G grupa i V vektorski prostor. Reprezentacija grupe G je par (π, V), gdje je $\pi : G \to GL(V)$ homomorfizam grupa ($\mathrm{GL}(V)$ označava grupu linearnih invertibilnih operatora na V). Dimenzija reprezentacije se definira kao dimenzija vektorskog prostora V.

Prirodna preslikavanja između reprezentacija su linearni operatori koji čuvaju djelovanje grupe.

Definicija 9.2. Neka su (π_1, V_1) i (π_2, V_2) reprezentacije grupa G. Kažemo da linearni operator $L : V_1 \to V_2$ ispreplićе reprezentacije π_1 i π_2 (odnosno da je L operator isprepliranja) ako vrijedi

$$L(\pi_1(g)v) = \pi_2(g)L(v),$$

za sve $v \in V_1$ i $g \in G$. Operatori ispreplitanja čine vektorski prostor koji označavamo sa $\mathrm{Hom}_G(\pi_1, \pi_2)$ (ili $\mathrm{Hom}_G(V_1, V_2)$). Kažemo da su reprezentacije (π_1, V_1) i (π_2, V_2) ekvivalentne, ako $\mathrm{Hom}_G(\pi_1, \pi_2)$ sadrži izomorfizam. Pišemo $\pi_1 \cong \pi_2$.

Zadatak 30. Neka je $f \in \mathrm{Hom}_G(V_1, V_2)$ operator ispreplitanja reprezentacija π_1 i π_2 grupe G. Dokažite da su $\mathrm{Ker}\, f$ i $\mathrm{Im}\, f$ podreprezentacije od π_1 i π_2.

Definicija 9.3. Neka je (π, V) reprezentacija grupe G. Za potprostor $W < V$ kažemo da je G-invarijantan ako je $\pi(g)w \in W$ za sve $g \in G$ i $w \in W$ (kad nema zabune pišemo gw umjesto $\pi(g)w$). Kažemo da je reprezentacija ireducibilna ako su $\{0\}$ i V jedini G-invarijantni potprostori od V.

Lema 9.4 (Schurov lema)**.** *Neka je (π, V) ireducibilna, konačno dimenzionalna reprezentacija grupe G. Tada se* $\mathrm{Hom}_G(V, V)$ *sastoji od operatora oblika λI, za svaki $\lambda \in \mathbb{C}$ (I je identiteta).*

Dokaz. Neka je $A \in \mathrm{Hom}_G(V, V)$ i neka je λ svojstvena vrijednost od A. Lako se vidi da je $A - \lambda I \in \mathrm{Hom}_G(V, V)$. S druge strane, svi ne nul operatori u $\mathrm{Hom}_G(V, V)$ su izomorfizmi (prema prethodnom zadatku $\mathrm{Ker}\, A$ je podreprezentacija ireducibilne reprezentacije π pa je $\mathrm{Ker}\, A = V$ ili 0). Kako $A - \lambda I$ nije injekcija, slijedi da je $A = \lambda I$. □

Ako su (π_1, V_1) i (π_2, V_2) reprezentacije grupa G_1 i G_2, tada je njihov tenzorski produkt $(\pi_1 \otimes \pi_2, V_1 \otimes V_2)$ reprezentacija grupe $G_1 \times G_2$ definirana formulom

$$(\pi_1 \otimes \pi_2)(g_1, g_2)(v_1 \otimes v_2) = \pi_1(g_1)v_1 \otimes \pi_2(g_2)v_2,$$

za sve $(g_1, g_2) \in G_1 \times G_2$.

Propozicija 9.5. *Neka je (π, V) ireducibilna konačno dimenzionalna reprezentacija od $G_1 \times G_2$. Tada postoje ireducibilne reprezentacije π_1 i π_2 od G_1 i G_2 takve da je $\pi \cong \pi_1 \otimes \pi_2$.*

Dokaz. Neka su π_1' i π_2' reprezentacije od G_1 i G_2 na V definirane formulama $\pi_1'(g_1)v = \pi((g_1,1))v$, odnosno $\pi_2'(g_2)v = \pi((1,g_2))v$ za $g_1 \in G_1$, $g_2 \in G_2$ i $v \in V$. Neka je V_1 G_1-invarijantan potprostor od V takav da je reprezentacija $\pi_1'|V_1$ ireducibilna. Neka je $v_0 \in V$ i $V_2 = \langle \pi_2'(g_2)v_0 | g_2 \in G_2 \rangle$ G_2-invarijantan potprostor od V generiran s v_0. Definirajmo $G_1 \times G_2$ ekvivarijantno preslikavanje $A : V_1 \otimes V_2 \to V$ tako da je $A(v_0 \otimes v_0) = v_0$. Tada je $A(\pi_1'(g_1)v_0 \otimes \pi_2'(g_2)v_0) = \pi(g_1,g_2)v_0$ za $g_1 \in G_1$ i $g_2 \in G_2$. Kako vektori $\pi_1'(g_1)v_0 \otimes \pi_2'(g_2)v_0$ razapinju $V_1 \otimes V_2$, lako se vidi da je preslikavanje A dobro definirano. Preslikavanje je surjektivno zato što je π ireducibilna (pa vektori $\pi(g_1,g_2)v_0$ generiraju V za $(g_1,g_2) \in G_1 \times G_2$). Ako je A bijekcija onda smo dokazali $\pi_1 \otimes \pi_2 \cong \pi$. Pretpostavimo da A nije injekcija. Tada je $\operatorname{Ker} A$ $G_1 \times G_2$ invarijantan potprostor od $V_1 \otimes V_2$, pa je specijalno kvocijentna reprezentacija $(\pi_1 \otimes \pi_2, V_1 \otimes V_2/\operatorname{Ker} A)$ ekvivalentna s (V,π). Treba još pokazati da je kvocijentna reprezentacija ekvivalentna tenzorskom produktu reprezentacija.

Lema 9.6. *Vrijedi*

$$(\pi_1 \otimes \pi_2, \operatorname{Ker} A) \cong (\pi_1 \otimes \pi_2, V_1 \otimes W),$$

za neki $W < V_2$.

Dokaz. Pokažimo prvo da je linearno preslikavanje B

$$V_1 \otimes \operatorname{Hom}_{G_1}(V_1, \operatorname{Ker} A) \to \operatorname{Ker} A,$$

određeno formulom $v_1 \otimes f \mapsto f(v_1)$, za sve $v_1 \in V_1$ i $f \in \operatorname{Hom}_{G_1}(V_1, \operatorname{Ker} A)$ ekvivalencija $G_1 \times G_2$ reprezentacija ($g \in G_2$ djeluje na $f \in \operatorname{Hom}_{G_1}(V_1, \operatorname{Ker} A)$ formulom $(gf)(v) = \pi_2(g)f(v)$). Vrijedi

$$(g_1,g_2)(v_1 \otimes f) \mapsto (g_2 f)(g_1 v_1) = g_1 g_2 f(v_1) = (g_1,g_2)f(v_1),$$

iz čega slijedi da je B operator ispreplitanja $G_1 \times G_2$ reprezentacija. Iz definicije tenzorskog produkta slijedi da je $V_1 \times V_2$ kao reprezentacija grupe G_1 ekvivalentna direktnoj sumi reprezentacija V_1^m, gdje je $m = \dim V_2$. Prema tome $\operatorname{Ker} A$ je kao G_1 podreprezentacija od V_1^m ekvivalentna direktnoj sumi V_1^k za neki $k \in \mathbb{N}$ (jer je V_1 ireducibilna), iz čega slijedi da je

$$V_1 \otimes \operatorname{Hom}_{G_1}(V_1, \operatorname{Ker} A) \cong \operatorname{Ker} A.$$

□

Prema prethodnoj lemi kvocijentna reprezentacija $(\pi_1 \otimes \pi_2, V_1 \otimes V_2/\operatorname{Ker} A)$ je ekvivalentna reprezentaciji $(\pi_1 \otimes \pi_2, V_1 \otimes V_2/(V_1 \otimes W))$, za neki $W < V_2$. Lako vidi da su reprezentacije $(\pi_1 \otimes \pi_2, V_1 \otimes V_2/(V_1 \otimes W))$ i $(\pi_1 \otimes \pi_2, V_1 \otimes (V_2/W))$ ekvivalentne. Primjetimo da je $\operatorname{Hom}_{G_1}(V_1, \operatorname{Ker} A)$ podreprezentacija od $\operatorname{Hom}_{G_1}(V_1, V_1 \otimes V_2) \cong V_2$ (ovo je ekvivalencija $G_1 \times G_2$ reprezentacija) pa tvrdnja slijedi.

□

Sad možemo dokazati Propoziciju 8.12.

Dokaz Propozicije 8.12. Prema Propoziciji 9.5 V možemo dekomponirati kao tenzorski produkt $V = \otimes_{i=1}^{n} V_i$, gdje G_i djeluje na V_i. Za svaki V_i postoje tri, u parovima linearno disjunktna, potprostora V_{i1}, V_{i2} i V_{i3} (tj. suma $V_{i1}+V_{i2}+V_{i3}$ je direktna) takva da je

$$V_i^{\langle H_i, K_i \rangle} = V_{i1}, \qquad V_i^{H_i} = V_{i1} \oplus V_{i2}, \qquad V_i^{K_i} = V_{i1} \oplus V_{i3}.$$

(Budući da je $V^{K_i} \cap V^{H_i} = V^{\langle H_i, K_i \rangle}$.) Prema tome vrijedi

$$\begin{aligned} V^H &= (V_{11} \oplus V_{12}) \otimes \cdots (V_{n1} \oplus V_{n2}), \\ \sum_{i=1}^{n} V^{K_i} &= \sum_{i=1}^{n} V_1 \otimes \cdots (V_{i1} \oplus V_{i3}) \otimes \cdots V_n, \\ \sum_{i=1}^{n} V^{\langle H, K_i \rangle} &= \sum_{i=1}^{n} (V_{11} \oplus V_{12}) \otimes \cdots \otimes V_{i1} \otimes \cdots \otimes (V_{n1} \oplus V_{n2}). \end{aligned}$$

Tvrdnja sada slijedi iz distributivnosti tenzorskog produkta i direktnih suma. Argument ćemo raspisati za $n = 2$, dok opći slučaj ostavljamo čitatelju. Umjesto $U \otimes V$ radi jednostavnosti pišemo UV.

Za $n = 2$ vrijedi, $V^H = V_{11}V_{21} + V_{11}V_{22} + V_{12}V_{21} + V_{12}V_{22}$ i $V^{K_1} + V^{K_2} = V_1V_{21} + V_1V_{13} + V_{11}V_2 + V_{13}V_2$. Budući da je $(V_{11}+V_{13}) \cap V_{12}$ trivijalan slijedi da je presjek jedanak $V_{11}V_{21}+V_{11}V_{22}+V_{12}V_{21}$. S druge strane, $V^{\langle H, K_1 \rangle} + V^{\langle H, K_2 \rangle} = (V_{11} + V_{12})V_{21} + V_{11}(V_{21} + V_{22}) = V_{11}V_{21} + V_{12}V_{21} + V_{11}V_{22} + V_{11}V_{21}$ pa tvrdnja slijedi.

□

Literatura

[1] F. Diamond and J. Shurman, A First Course in Modular Forms, Springer, 2005.

[2] L. E. Dickson, History of the Theory of Numbers, Vol. II, Chelsea, New York, 1952.

[3] N. Koblitz, Introduction to elliptic curves and modular forms, Second edition, Graduate Texts in Mathematics, 97. Springer-Verlag, New York, 1993.

[4] K. Tasaka, On a conjecture for representations of integers as sums of squares and double shuffle relations, Ramanujan J., 33(1) (2014), 1–21.