Master's Thesis

Rankin L-functions and the Birch and Swinnerton-Dyer Conjecture

Author:
Reza Sadoughian

Supervisor:
Henri Darmon

Academic year 2011-2012

Concordia University
Department of Mathematics & Statistics

University of Padova
Department of Mathematics

Abstract

In this thesis we use Rankin's method to evaluate the central critical value of the L-series attached to an elliptic curve E over $\mathbb{Q}$ and certain odd irreducible 2-dimensional Artin representation $\tau : G_{\mathbb{Q}} \to GL_2(\mathbb{C})$. The motivation for this study is the twisted Birch and Swinnerton-Dyer conjecture.

Let K be a number field and $E(K)$ be the abelian group of K-rational points on E. Consider the natural representation of $\mathrm{Gal}(K/\mathbb{Q})$ on $\mathbb{C} \otimes_{\mathbb{Z}} E(K)$, i.e. for any point $P = (x, y) \in E(\overline{\mathbb{Q}})$, an element $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts as

$$\begin{array}{rcl} \mathrm{Gal}(K/\mathbb{Q}) \times E(K) & \to & E(K) \\ (\sigma, P) & \mapsto & P^{\sigma} = (\sigma(x), \sigma(y)). \end{array}$$

Let ρ_E be the 2-dimensional ℓ-adic Galois representation attached to the elliptic curve E, namely, the p-adic Tate module of E.

Twisted form of the Birch and Swinnerton-Dyer conjecture: Let τ be a continuous and irreducible finite dimensional complex representation of $\mathrm{Gal}(K/\mathbb{Q})$. Then

$$\mathrm{ord}_{s=1} L(\tau \otimes \rho_E, s) = \langle \tau, \mathbb{C} \otimes_{\mathbb{Z}} E(K) \rangle = \text{multiplicity of } \tau \text{ in } \mathbb{C} \otimes_{\mathbb{Z}} E(K).$$

This conjecture is a natural strengthening of the Birch and Swinnerton-Dyer conjecture. In fact, if we replace τ by the trivial representation, then we recover this conjecture. We explain it briefly. Let K be a number field and consider $E(K)$ the abelian group of K-rational points on E. The Mordell-Weil theorem tells us that $E(K)$ has the form

$$E(K) \cong E(K)_{\mathrm{tors}} \oplus \mathbb{Z}^r$$

where the torsion subgroup $E(K)_{\mathrm{tors}}$ is finite and the *rank* r of $E(K)$ is a nonnegative integer. It is relatively easy to compute the torsion subgroup but there is no known procedure that is guaranteed to yield the rank $r_K(E)$.

The *Hasse-Weil L-function of E* is:

$$L(E, s) = \prod_p \frac{1}{1 - a_p p^s + \mathbf{1}_E(p) p^{1-2s}}$$

where $\mathbf{1}_E$ is the trivial character modulo the conductor N_E and

$$a_p(E) = p - (\text{the number of solutions (x,y) of equation E working modulo p}).$$

More generally, for any number field K, one can associate to E an L-series $L(E/K, s)$. The product defining $L(E/K, s)$ converges and gives an analytic function for all $\mathcal{R}(s) > \frac{3}{2}$. Its analytic continuation is conjectured as follows:

Conjecture: The L-series $L(E/K, s)$ has an analytic continuation to the entire complex plane and satisfies a functional equation relating its values at s and $2 - s$.

The original half plane of convergence of $L(E/K, s)$ is the half plane $\mathcal{R}(s) > \frac{3}{2}$ and the functional equation then determines $L(E/K, s)$ for $\mathcal{R}(s) < \frac{1}{2}$, but the behaviour of $L(E/K, s)$ at the center of the remaining strip $\{\frac{1}{2} < \mathcal{R}(s) < \frac{3}{2}\}$ is what conjecturally determines the rank of $E(K)$. Birch and Swinnerton-Dyer conjectures

that the rank of E over K is equal to the order of vanishing of $L(E/K, s)$ at $s = 1$:

Birch and Swinnerton-Dyer Conjecture: The order of vanishing of $L(E/K, s)$ at $s = 1$ is the rank of $E(K)$. That is, if $E(K)$ has rank r then: [1]

$$L(E/K, s) = (s-1)^r g(s) \quad , \; g(1) \neq 0, \infty.$$

This conjecture relates the algebraic group of an elliptic curve E to analytic properties of $L(E, s)$.

Let τ be a continuous and irreducible finite-dimensional complex representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. One can associate to τ an L-series $L(\tau, s)$. On the other hand, there is a representation ρ_E of the elliptic curve E, namely, the p-adic Tate module of E, such that its associated L-series $L(\rho_E, s)$ is equal to $L(E, s)$. One can construct an L-series $L(\rho_E \otimes \tau, s)$ which corresponds to the tensor product of two representations ρ_E and τ. By Rankin method, one can show that if τ is arising from a modular form, then the L-series $L(\rho_E \otimes \tau, s)$ admits analytic continuation to $\mathbb{C}$. (see chapter 2.1)

In this thesis, we provide some numerical evidence for the twisted form of the Birch and Swinnerton-Dyer conjecture using the Deligne-Serre theorem and Rankin's method. Deligne and Serre proved a correspondence between the modular forms of weight 1 and certain 2-dimensional Galois representations. Given a cusp form $g = \sum_{n=0}^{\infty} b_n q^n \in \mathcal{S}_1(\Gamma_0(N), \chi)$, one gets an irreducible 2-dimensional complex representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$:

$$\rho_g : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{C})$$

with the property that

$$\mathrm{char}(\rho_g(\mathrm{Frob}_p)) = X^2 - b_p X + \chi(p) \quad \text{for all } p \nmid N.$$

The image of ρ_g in projective space $\mathrm{PGL}_2(\mathbb{C}) = \mathrm{GL}_2(\mathbb{C})/\mathbb{C}^*$ is a dihedral group D_n or one of the groups A_4, S_4 or A_5.

For a given cusp form $g \in \mathcal{S}_1(\Gamma_0(N), \chi)$, we apply the twisted form of Birch and Swinnerton-Dyer conjecture to $\tau = \rho_g$:

$$\mathrm{ord}_{s=1} L(\rho_g \otimes \rho_E, s) = \text{multiplicity of } \rho_g \text{ in } \mathbb{C} \otimes_{\mathbb{Z}} E(K).$$

Then for some elliptic curve E of conductor M with $N|M$, we computed $L(\rho_E \otimes \rho_g, 1)$ and verified if it vanishes. Assuming the BSD conjecture, one can say

$$L(\rho_g \otimes \rho_E, 1) = 0 \quad \Leftrightarrow \quad \rho_g \text{ occurs in the representation } \mathbb{C} \otimes_{\mathbb{Z}} E(K).$$

where K denotes the finite extension of Q which is fixed by the kernel ρ_g. As a consequence, if $L(\rho_g \otimes \rho_E, 1) = 0$, then the rank $r_K(E)$ of elliptic curve E over K is $\geqslant 2$.

In chapter one, we introduce some background about modular forms and Eisenstein series of weight 1. Chapter two introduces the Rankin convolution L-series $L(f \otimes g, s)$ attached to two modular forms f and g. Then its analytic continuation

[1] In 2000, this Conjecture was declared a million dollar millennium prize problem by the Clay Mathematics Institute.

is discussed via the Rankin-Selberg method and some applications of this method is presented. In chapter three, we state and prove the Deligne-Serre theorem. Finally in chapter four, we discuss the conjecture of Birch and Swinnerton-Dyer. Then we present a twisted form of it. One interesting case is when we twist an elliptic curve with a cusp form of weight 1. We develop techniques to compute the constant term of the twisted L-series $L(\rho_E \otimes \rho_g, s)$ at $s = 1$. We perform some computations for certain elliptic curves with small conductor N using the database Sage. We presented these computations in tables 1 to 14.

Acknowledgements

I would first of all like to thank my thesis advisor Professor Henri Darmon for his help and his will to teach me. I appreciate all the time he spent showing me new, interesting and important aspects in the world of Number Theory.

Special thanks to my friends in the Mathematics Department of Concordia and in particular, to Rodrigo Matias for his permanent support and encouragement.

Contents

1 Modular forms of weight 1

In this chapter, we introduce the non-holomorphic Eisenstein series of weight 1 and characters ψ and χ with parameter s. Since it can be analytically extended to a meromorphic function such that it is holomorphic on $\mathcal{R}(s) > \frac{-1}{2}$, one obtain a modular form of weight 1 at $s = 0$. Then we present theta series and give some examples of cusp forms of weight 1 arising from theta series.

1.1 Eisenstein series of weight 1

Let ψ and χ be Dirichlet characters mod M and mod N, respectively. For any integer $k \geqslant 1$ and $z \in \mathcal{H}$, we put:

$$\widetilde{E}_k(z; \psi, \chi) = \sum_{(m,n)\in\mathbb{Z}\times\mathbb{Z}}{}' \frac{\psi(m)\chi(n)}{(mz+n)^k}.$$

Here the summation $\sum'$ is over all integers $(m, n) \neq (0, 0)$. This series is absolutely convergent for $k \geqslant 3$. Therefore we need some modification to discuss the case $k = 1$.

We define a new kind of Eisenstein series in two variables z and s such that it is holomorphic as a function of s but it is not holomorphic as a function of z.

Definition 1. *For $z = x + iy \in \mathcal{H}$, $s \in \mathbb{C}$ and $k \in \mathbb{Z}$, define*

$$\widetilde{E}_k(z, s; \psi, \chi) = \sum_{(m,n)\in\mathbb{Z}\times\mathbb{Z}}{}' \frac{\psi(m)\chi(n)}{(mz+n)^k} \frac{y^s}{|mz+n|^{2s}}. \tag{1}$$

This function is called non-holomorphic Eisenstein series or Epstein zeta function of weight k and characters ψ and χ.

The right hand side of the formula is uniformly and absolutely convergent for $k + 2\mathcal{R}(s) \geqslant 2 + \varepsilon$ for any $\varepsilon > 0$. Therefore it is holomorphic on $\mathcal{R}(s) > \frac{2-k}{2}$. However, it is not holomorphic as a function of z. Put:

$$\Gamma_0(M, N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) |\ c \equiv 0 \bmod \mathrm{N}, \quad b \equiv 0 \bmod \mathrm{M} \right\}.$$

Then $\Gamma_0(M, N)$ is a modular group. For any $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(M, N)$, we have:

$$E_k(\gamma z, s; \psi, \chi) = \psi(d)\overline{\chi(d)}(cz + d)^k |cz + d|^{2s} \widetilde{E}_1(z, s; \psi, \chi).$$

We easily see that if $\psi(-1)\chi(-1) \neq (-1)^k$, then $\widetilde{E}_1(z, s; \psi, \chi) = 0$. So we assume:

$$\psi(-1)\chi(-1) = (-1)^k \tag{2}$$

throughout this section.

We wish to study the case $k = 1$. The series $\widetilde{E}_1(z, s; \psi, \chi)$ is not convergent at $s = 0$. But if $\widetilde{E}_1(z, s; \psi, \chi)$ is continued analytically to $s = 0$ and holomorphic at $s = 0$, then we will obtain a modular form of weight 1.

Theorem 2. *The Eisenstein series $\widetilde{E}_1(z,s;\psi,\chi)$ is analytically continued to a meromorphic function on the whole s-plane. If χ is non-trivial, then $\widetilde{E}_1(z,s;\psi,\chi)$ is an entire function of s. If χ is trivial, then it is holomorphic for $\mathcal{R}(s) > \frac{-1}{2}$. At $s=0$, we get a modular form of weight 1 for the modular group $\Gamma_0(M,N)$. Its Fourier expansion is given by:*

$$\widetilde{E}_1(z,s;\psi,\chi) = C + D + A\sum_{n=0}^{\infty} a_n q_N^n.$$

Here

$$C = \begin{cases} 0 & \text{if} \quad \psi \text{ is the principal character} \\ 2L(\chi,1) & \text{if} \quad \psi \text{ is not the principal character} \end{cases},$$

$$D = \begin{cases} 0 & \text{if} \quad \chi \text{ is non-trivial} \\ -2\pi i L(\psi,0)\prod_{p|M}(1-p^{-1}) & \text{if} \quad \chi \text{ is trivial} \end{cases},$$

$$A = \frac{-4\pi i\tau(\chi')}{N},$$

$$a_n = \sum_{0<c|n}\psi(\tfrac{n}{c})\sum_{0<d|gcd(l,c)} d\mu(\tfrac{l}{d})\chi'(\tfrac{l}{d})\overline{\chi'}(\tfrac{c}{d}),$$

$$q_N = e^{2\pi i/N}$$

where χ' is the primitive character of mod N' associated with χ,

$$\tau(\chi') = \sum_{a=1}^{N'}\chi'(a)e^{2\pi i a/N'}$$

is the Gauss sum attached to χ'; μ is the Mobius function and $l = \frac{N}{N'}$.

Proof: See [11] Theorem 7.29, Corollary 7.2.10 and Theorem 7.2.13. ■

In the next sections, we will need a more general kind of Eisenstein series.

Definition 3. *Let χ be a character mod N with $\chi(-1) = -1$ and* **1** *the trivial character mod N. Assume M is an integer with $N|M$. Then:*

$$\widetilde{E}_1(z,s;\chi;M) := \sum_{(m,n)\in\mathbb{Z}\times\mathbb{Z}}{}' \frac{\chi(n)}{Mmz+n}\frac{y^s}{|Mmz+n|^{2s}} \tag{3}$$

is called the non-holomorphic Eisenstein series of weight 1, character χ and level M.

When $M=1$, $\widetilde{E}_1(z,s;\chi;M)$ is the non-holomorphic Eisenstein series with characters **1** *and χ:*

$$\widetilde{E}_1(z,s;\chi;1) = \widetilde{E}_1(z,s;\mathbf{1},\chi).$$

We will need the q-expansion of $\widetilde{E}_1(z,\chi,M)$ for the next sections. The case $M=N$ is easier to handle:

$$\begin{aligned}\widetilde{E}_1(z,s;\chi;N) &= \sum_{(m,n)\in\mathbb{Z}\times\mathbb{Z}}{}' \frac{\chi(n)}{Nmz+n}\frac{y^s}{|Nmz+n|^{2s}}\\ &= \sum_{(m,n)\in N\mathbb{Z}\times\mathbb{Z}}{}' \frac{\chi(n)}{mz+n}\frac{y^s}{|mz+n|^{2s}}\\ &= \frac{1}{N^s}\widetilde{E}_1(Nz,s;\mathbf{1},\chi).\end{aligned}$$

Define:

$$\widetilde{E}_1(z;\chi;N) := \widetilde{E}_{1,}(z;0,\chi;N). \tag{4}$$

This is an Eisenstein series of weight 1 and character χ. It belongs to $\mathcal{M}_1(\Gamma_0(N),\chi)$. Its q-expansion is given by:

$$\widetilde{E}_1(z;\chi;N) = 2L_N(\chi,1) - \frac{4\pi i\tau(\chi)}{N}\sum_{n=0}^{\infty}\sigma_{\overline{\chi}}(n)q^n \tag{5}$$

where $\sigma_{\overline{\chi}}(n) = \sum_{d|n}\overline{\chi}(d)$. Since χ is a character mod N, for any $p|N$, the factor $1-\frac{\chi(p)}{p^s}$ is one. Therefore

$$L(\chi,s) = L_N(\chi,s).$$

Assume that χ is a primitive character. The functional equation satisfied by $L(\chi,s)$ is:

$$\pi^{-(s+1)/2}\Gamma(\tfrac{s+1}{2})N^sL(\chi,s) = -i\pi^{-(2-s)/2}\Gamma(\tfrac{2-s}{2})\tau(\chi)L(\overline{\chi},1-s).$$

Specializing the above equation at $s=1$ and by using $\Gamma(1/2)=\sqrt{\pi}$ we get:

$$\begin{aligned}L(\overline{\chi},0) &= \frac{-i\Gamma(1)N}{\sqrt{\pi}\Gamma(1/2)\tau(\chi)}L(\chi,1)\\ &= \frac{-iN}{\pi\tau(\chi)}L(\chi,1).\end{aligned}$$

There is a nice formula (see [20]) for computing $L(\chi,0)$ where χ is any character of mod N:

$$L(\chi,0) = \frac{-1}{N}\sum_{i=1}^{N} i\chi(i).$$

We can rewrite the q-expansion of $\widetilde{E}_1(z;\chi;N)$:

$$\widetilde{E}_1(z;\chi;N) = \frac{-2\pi i\tau(\chi)}{N}L(\overline{\chi},0) - \frac{4\pi i\tau(\chi)}{N}\sum_{n=0}^{\infty}\sigma_{\overline{\chi}}(n)q^n.$$

We introduce the *normalised Eisenstein series* $E_1(z;\chi;N)$, related to $\widetilde{E}_1(z;\chi;N)$ by the equation

$$\widetilde{E}_1(z,s;\chi;N) = \frac{-4\pi i\tau(\chi)}{N}E_1(z,s;\chi;N). \tag{6}$$

Thus the q-expansion of $E_1(z;\chi;N)$ is given by

$$E_1(z;\chi;N) = \frac{1}{2}L(\overline{\chi},0) + \sum_{n=0}^{\infty} \sigma_{\overline{\chi}}(n)q^n. \tag{7}$$

Define:

$$\begin{aligned} \widetilde{E}_1'(z,s;\chi;N) &= \sum_{\substack{(m,n)\in\mathbb{Z}\times\mathbb{Z} \\ gcd(m,n)=1}} \frac{\chi(n)}{Nmz+n}\frac{y^s}{|Nm'z+n'|^{2s}} \\ &= \sum_{\substack{(m,n)\in\mathbb{Z}\times\mathbb{Z} \\ gcd(Nm,n)=1}} \frac{\chi(n)}{Nmz+n}\frac{y^s}{|Nm'z+n'|^{2s}}. \end{aligned} \tag{8}$$

(the last equality holds since $\chi(n) = 0$ for any $p|\gcd(n,N)$) We want to find the q-expansion of the following Eisenstein series:

$$\widetilde{E}_1'(z;\chi;N) := \widetilde{E}_1'(z,0;\chi;N). \tag{9}$$

If $\mathcal{R}(s) > \frac{1}{2}$, the Eisenstein series $\widetilde{E}_1(z,s;\chi;N)$ is absolutely convergent and thus we can rearrange it and write

$$\begin{aligned} \widetilde{E}_1(z,s;\chi;N) &= \sideset{}{'}\sum_{(m,n)\in\mathbb{Z}\times\mathbb{Z}} \frac{\chi(n)}{Nmz+n}\frac{y^s}{|Nmz+n|^{2s}} \\ &= \sum_{k=1}^{\infty} \sum_{\substack{(m,n)\in\mathbb{Z}\times\mathbb{Z} \\ gcd(m,n)=k}} \frac{\chi(n)}{Nmz+n}\frac{y^s}{|Nmz+n|^{2s}} \\ &= \sum_{k=1}^{\infty} \frac{\chi(k)}{k^{1+2s}} \sum_{\substack{(m',n')\in\mathbb{Z}\times\mathbb{Z} \\ gcd(m',n')=1}} \frac{\chi(n')}{Nm'z+n'}\frac{y^s}{|Nm'z+n'|^{2s}} \\ &= L(\chi,1+2s)\widetilde{E}_1'(z,s;\chi;N). \end{aligned}$$

Both $\widetilde{E}_1(z,s;\chi;N)$ and $\widetilde{E}_1'(z,s;\chi;N)$ are holomorphic on $\mathcal{R}(s) > \frac{-1}{2}$. So we can set $s = 0$ in the above equation and get

$$\widetilde{E}_1(z;\chi;N) = L(\chi,1)\widetilde{E}_1'(z;\chi;N). \tag{10}$$

Now we consider a more general situation where $N|M$. As before, one can show that:

$$\widetilde{E}_1(z,s;\chi;M) = L(\chi,1+2s)\widetilde{E}_1'(z,s;\chi;M) \tag{11}$$

where $\widetilde{E}_1'(z,s,\chi,M) = \sum_{\substack{(m,n)\in\mathbb{Z}\times\mathbb{Z} \\ gcd(m,n)=1}} \frac{\chi(n)}{Mmz+n}\frac{y^s}{|Mmz+n|^{2s}}$.

Define:

$$\widetilde{E}_1(z;\chi;M) \;:=\; \widetilde{E}_1(z,0;\chi;M). \tag{12}$$

Then:

$$\widetilde{E}_1(z;\chi;M) = L(\chi,1)\widetilde{E}_1'(z;\chi;M)$$

where $\widetilde{E}_1'(z;\chi;M) = \widetilde{E}_1'(z,0;\chi;M)$. By an example, we show how to compute Fourier coefficients of $\widetilde{E}_1(z,\chi,M)$.

Example 4. *Let χ be a primitive character mod N and let $M = pN$ where p is relatively prime to N. We want to compute the q-expansion of $\widetilde{E}_1(z;\chi;M)$. It is enough to do it for $\widetilde{E}_1'(z;\chi;M)$. For $\mathcal{R}(s) > \frac{-1}{2}$, the series $\widetilde{E}_1'(z,s;\chi,M)$ is holomorphic and one can write*

$$\begin{aligned}
\frac{1}{p^s}\widetilde{E}_1'(pz,s;\chi;N) &= \frac{1}{p^s}\sum_{\substack{(m,n)\in\mathbb{Z}\times\mathbb{Z}\\ gcd(m,n)=1}} \frac{\chi(n)}{Npmz+n}\frac{(py)^s}{|Npmz+n|^{2s}} \\
&= \sum_{\substack{(m,n)\in\mathbb{Z}\times\mathbb{Z}\\ gcd(m,n)=1\\ p\nmid n}} \frac{\chi(n)}{Npmz+n}\frac{y^s}{|Npmz+n|^{2s}} + \sum_{\substack{(m,n)\in\mathbb{Z}\times\mathbb{Z}\\ gcd(m,n)=1\\ p\mid n}} \frac{\chi(n)}{Npmz+n}\frac{y^s}{|Npmz+n|^{2s}} \\
&= \sum_{\substack{(m,n)\in\mathbb{Z}\times\mathbb{Z}\\ gcd(pm,n)=1}} \frac{\chi(n)}{Npmz+n}\frac{y^s}{|Npmz+n|^{2s}} + \frac{\chi(p)}{p^{1+2s}}\sum_{\substack{(m,n')\in\mathbb{Z}\times\mathbb{Z}\\ gcd(m,n')=1}} \frac{\chi(n')}{Nmz+n'}\frac{y^s}{|Nmz+n'|^{2s}} \\
&= \widetilde{E}_1'(z,s;\chi;Np) + \frac{\chi(p)}{p^{1+2s}}\widetilde{E}_1'(z,s;\chi,N).
\end{aligned}$$

Setting $s = 0$ in the above equation gives:

$$\begin{aligned}
\widetilde{E}_1'(z;\chi;Np) &= \widetilde{E}_1'(pz;\chi;N) - \frac{\chi(p)}{p}\widetilde{E}_1'(z;\chi;N) &(13)\\
&= \frac{1}{2}(1-\tfrac{\chi(p)}{p})L(\overline{\chi},0) + \sum_{n=0}^{\infty}\left(\sigma_{\overline{\chi}}(\tfrac{n}{p}) - \tfrac{\chi(p)}{p}\sigma_{\overline{\chi}}(n)\right)q^n &(14)
\end{aligned}$$

where $\sigma_{\overline{\chi}}(\frac{n}{p}) = 0$ if $p \nmid n$.

By similar computation, we can get a more general formula. Assume $N = \prod_{i=1}^{v} p_i^{\alpha_i}$ and $M = \prod_{i=1}^{v} p_i^{\beta_i}\prod_{j=1}^{w} q_j^{\gamma_j}$ where p_i's and q_i's are distinct prime numbers and $\beta_i \geqslant \alpha_i$ for any $i = 1,...,v$ (thus $N|M$). Set $Q = \{q_1, q_2, ..., q_w\}$. We have

$$\begin{aligned}
\widetilde{E}_1'(z;\chi;M) &= \widetilde{E}_1'(Mz;\chi;N)\\
&\quad -\sum_{q_i\in Q}\frac{\chi(q_i)}{q_i}\widetilde{E}_1'(\tfrac{M}{q_i}z;\chi;N)\\
&\quad +\sum_{\substack{q_i,q_j\in Q\\ q_i\neq q_j}}\frac{\chi(q_iq_j)}{q_iq_j}\widetilde{E}_1'(\tfrac{M}{q_iq_j}z;\chi;N)\\
&\quad \pm\cdots\\
&\quad +(-1)^w\frac{\chi(q_1q_2...q_w)}{q_1q_2...q_w}\widetilde{E}_1'(\tfrac{M}{q_1q_2...q_w}z;\chi;N).
\end{aligned}$$

Since we already computed the q-expansion of $\widetilde{E}_1'(z;\chi;N)$, we obtain the q-expansion of $\widetilde{E}_1'(z,\chi,M)$ using the above equation.

1.2 Theta series

We give a brief description of theta series and provide some examples. For more details, see [19]. Let $Q:\mathbb{Z}^r\to\mathbb{Z}$ be any positive definite integer-valued quadratic form in r variables, r even. Define the *theta series* associated to Q as

$$\Theta_Q(\tau)=\sum_{x\in\mathbb{Z}^r} q^{Q(x)}.$$

Θ_Q belongs to $\mathcal{M}_{\frac{r}{2}}(\Gamma_0(N),\chi)$. The level N is determined as follows: write $Q(x)=\frac{1}{2}x^tAx$ where A is an even symmetric $r\times r$ matrix, i.e. $A=(a_{ij}),\ a_{ii}\in 2\mathbb{Z}$; then N is the smallest positive integer such that NA^{-1} is again even. The character χ is the Kronecker symbol $\chi=\left(\frac{D}{\cdot}\right)$ with $D=(-1)^{\frac{r}{2}}\det A$. With some examples, we explain how to get cusp forms of weight 1 arising from theta series.

Example 5. *The following quadratic forms $Q_1(x_1,x_2)=x_1^2+x_1x_2+6x_2^2$ and $Q_2(x_1,x_2)=2x_1^2+x_1x_2+3x_2^2$ have level $N=23$ and character $\chi(d)=\left(\frac{-23}{d}\right)=\left(\frac{d}{23}\right)$. Put*

$$\begin{aligned} f &= \tfrac{1}{2}(\Theta_{Q_1}-\Theta_{Q_2})\\ &= q-q^2-q^3+q^6+q^8-q^{13}+\cdots \quad . \end{aligned}$$

Then f is a cusp form of weight 1 and character χ. Further:

$$f=\eta(z)\eta(23z)=q\prod_{n=1}^{\infty}(1-q^n)(1-q^{23n}),$$

where η is the Dedekind's η-function.
More generally, for any prime number p with $p\equiv -1$ (mod 24) set $Q_1(x_1,x_2)=6x_1^2+x_1x_2+\frac{p+1}{24}x_2^2$ and $Q_2(x_1,x_2)=6x_1^2+5x_1x_2+\frac{p+25}{24}x_2^2$. Put

$$\begin{aligned} g &= \frac{1}{2}(\Theta_{Q_1}-\Theta_{Q_2})\\ &= q^{\frac{p+1}{24}}(1-q-q^2+q^5+q^7-q^{12}+\cdots) \end{aligned}$$

One has

$$g(z)=\eta(z)\eta(pz)=q^{\frac{p+1}{24}}\prod_{n=1}^{\infty}(1-q^n)(1-q^{pn}),$$

g is a cusp form of weight 1 and level p. For more details, see [16]

Example 6. *We can define in a similar way a cusp form of weight 1 and level 31. Let $Q_1(x_1,x_2)=x_1^2+x_1x_2+8x_2^2$ and $Q_2(x_1,x_2)=2x_1^2+x_1x_2+4x_2^2$. Set*

$$\begin{aligned} f &= \frac{1}{2}(\Theta_{Q_1}-\Theta_{Q_2})\\ &= q-q^2-q^5-q^7+q^8+q^9+q^{10}+\cdots \quad . \end{aligned}$$

Then $f\in\mathcal{S}_1(\Gamma_0(31),\left(\frac{-31}{\cdot}\right))$.

2 The Rankin-Selberg method and applications

The 2-dimensional representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ which are geometric are all expected to arise from modular forms, i.e. we expect that if ρ is an odd 2-dimensional compatible system of ℓ-adic representations, then there is a modular form f and integer j such that:

$$L(\rho, s) = L(f, s+j).$$

We can construct representations of higher dimension built up from those arising from modular forms. For example, given 2 representations V_1 and V_2, we have:

$$L(V_1 \oplus V_2) = L(V_1, s).L(V_2, s).$$

This L-function inherits its analytic properties from $L(V_1, s)$ and $L(V_2, s)$ so it is not interesting. However, one can try to construct an L-series corresponding to the representation $V_1 \otimes V_2$. In this chapter, we study the representation associated to $V_1 \otimes V_2$ where V_1 and V_2 are modular, i.e. they arise from modular forms.

2.1 Rankin convolution L-series

Let

$$f = \sum_{n=1}^{\infty} a_n q^n \in \mathcal{S}_k(\Gamma_0(N), \chi_f)$$

and

$$g = \sum_{n=1}^{\infty} b_n q^n \in \mathcal{S}_\ell(\Gamma_0(N), \chi_g)$$

be normalized eigenforms of level N (we assume also the case $N = 1$). We do not assume that they are new of this level, but we do assume that they are simultaneous eigenvectors for the Hecke operators T_r with $\gcd(r, N) = 1$ as well as the operators U_r attached to the primes r dividing N. Then their associated L-functions have an Euler product expansion:

$$\begin{aligned} L(f, s) &= \sum_{n=1}^{\infty} \frac{a_n}{n^s} \\ &= \prod_{p|N} \left(1 - a_p p^{-s}\right)^{-1} \prod_{p\nmid N} (1 - a_p p^{-s} + \chi_f(p) p^{k-1-2s})^{-1}. \end{aligned}$$

We define:

$$L_N(f, s) := \prod_{p\nmid N} \left(1 - a_p p^{-s} + \chi_f(p) p^{k-1-2s}\right)^{-1}.$$

For each prime p, let α_p and $\alpha_p^{'}$ be the roots of the Hecke polynomials $x^2 - a_p x + \chi_f(p) p^{k-1}$, choosing $(\alpha_p, \alpha_p^{'}) = (a_p, 0)$ when $p|N$. It follows:

$$L_N(f, s) = \prod_{p\nmid N} \left(1 - \alpha_p p^{-s}\right)^{-1} (1 - \alpha_p^{'} p^{-s})^{-1}.$$

For each prime p, let α_p and $\alpha_p^{'}$ be the roots of the Hecke polynomials $x^2 - a_p x + \chi_f(p)p^{k-1}$, choosing $(\alpha_p, \alpha^{'}) = (a_p, 0)$ when $p|N$. Hence for each prime $p|N$, we have $L_{(p)}(f,s) = (1 - a_p p^{-s})^{-1}$. Therefore we can simply write:

$$L(f,s) = \prod_{p \in \mathcal{P}} L_{(p)}(f,s).$$

We do the same for g. For each prime p, let β_p and $\beta_p^{'}$ be the roots of the Hecke polynomials $x^2 - b_p x + \chi_g(p)p^{\ell-1}$, choosing $(\beta_p, \beta_p^{'}) = (b_p, 0)$ when $p|N$. We write

$$L(g,s) = \prod_{p \in \mathcal{P}} L_{(p)}(g,s),$$

where

$$L_{(p)}(g,s) = \left(1 - \beta_p p^{-s}\right)^{-1} (1 - \beta_p^{'} p^{-s})^{-1}.$$

We want to define an L-series attached to both modular forms f and g. For it, we can use their product expansion:

Definition 7. *The Rankin L-series or Rankin convolution L-series attached to (f,g) is defined as:*

$$L(f \otimes g, s) = \prod_{p \in \mathcal{P}} L_p(f \otimes g, s) \tag{15}$$

where:

$$L_{(p)}(f \otimes g, s) := (1 - \alpha_p \beta_p p^{-s})^{-1}(1 - \alpha_p \beta_p^{'} p^{-s})^{-1}(1 - \alpha_p^{'} \beta_p p^{-s})^{-1}(1 - \alpha_p^{'} \beta_p^{'} p^{-s})^{-1}.$$

$V_f \otimes V_g$ is the tensor product of the two representations which is 4-dimensional so that $L(f \otimes g, s)$ is defined by an Euler product with factors of degree 4.

We study the analytic continuation of $L(f \otimes g, s)$ and try to find a functional equation for it. First, we would like to write $L(f \otimes g, s) = \displaystyle\sum_{n=1}^{\infty} \frac{A_n}{n^s}$ and compute the coefficients A_n. We have:

$$\begin{aligned} L_{(p)}(f \otimes g, s) &= (1 - \alpha_p \beta_p p^{-s})^{-1}(1 - \alpha_p \beta_p^{'} p^{-s})^{-1}(1 - \alpha_p^{'} \beta_p p^{-s})^{-1}(1 - \alpha_p^{'} \beta_p^{'} p^{-s})^{-1} \\ &= (1 + \alpha_p \beta_p p^{-s} + (\alpha_p \beta_p)^2 p^{-2s} + ...)(1 + \alpha_p \beta_p^{'} p^{-s} + (\alpha_p \beta_p^{'})^2 p^{-2s} + ...) \\ &\quad (1 + \alpha_p^{'} \beta_p p^{-s} + (\alpha_p^{'} \beta_p)^2 p^{-2s} + ...)(1 + \alpha_p^{'} \beta_p^{'} p^{-s} + (\alpha_p^{'} \beta_p^{'})^2 p^{-2s} + ...). \end{aligned}$$

It follows that:

$$\begin{aligned} A_p &= \alpha_p \beta_p + \alpha_p \beta_p^{'} + \alpha_p^{'} \beta_p + \alpha_p^{'} \beta_p^{'} \\ &= (\alpha_p + \alpha_p^{'})(\beta_p + \beta_p^{'}) \\ &= a_p b_p. \end{aligned}$$

$$\begin{aligned}
A_{p^2} &= (\alpha_p\beta_p)^2 + (\alpha_p\beta_p^{'})^2 + (\alpha_p^{'}\beta_p)^2 + (\alpha_p^{'}\beta_p^{'})^2 \\
&\quad + (\alpha_p\beta_p)(\alpha_p\beta_p^{'}) + (\alpha_p\beta_p)(\alpha_p^{'}\beta_p) + (\alpha_p\beta_p)(\alpha_p^{'}\beta_p^{'}) \\
&\quad + (\alpha_p\beta_p^{'})(\alpha_p^{'}\beta_p) + (\alpha_p\beta_p^{'})(\alpha_p^{'}\beta_p^{'}) + (\alpha_p^{'}\beta_p)(\alpha_p^{'}\beta_p^{'}) \\
&= \frac{1}{2}\Big((\alpha_p^2 + \alpha_p^{'2})(\beta_p^2 + \beta_p^{'2}) + (\alpha_p\beta_p + \alpha_p\beta_p^{'} + \alpha_p^{'}\beta_p + \alpha_p^{'}\beta_p^{'})(\alpha_p\beta_p + \alpha_p\beta_p^{'} + \alpha_p^{'}\beta_p + \alpha_p^{'}\beta_p^{'})\Big) \\
&= \frac{1}{2}\Big((a_p^2 - 2\chi_f(p)p^{k-1})(b_p^2 - 2\chi_g(p)p^{\ell-1}) + A_p^2\Big) \\
&= a_p^2 b_p^2 - a_p^2\chi_g(p)p^{\ell-1} - b_p^2\chi_f(p)p^{k-1} + 2\chi_f(p)p^{k-1}\chi_g(p)p^{\ell-1} \\
&= (a_p^2 - \chi_f(p)p^{k-1})(b_p^2 - \chi_g(p)p^{\ell-1}) + \chi_f(p)p^{k-1}\chi_g(p)p^{\ell-1} \\
&= a_{p^2}b_{p^2} + \chi_f(p)\chi_g(p)p^{k+\ell-2}.
\end{aligned}$$

We see that $A_{p^2} \neq a_{p^2}b_{p^2}$. This motivates us to consider the following "modified Rankin L-series" as an approximation of the Rankin convolution L-series.

Definition 8. *The modified Rankin function attached to f and g is defined by:*

$$\mathcal{D}(f,g,s) = \sum_{n=1}^{\infty} \frac{a_n b_n}{n^s}.$$

The function $a_n b_n$ is weakly multiplicative and therefore we can write:

$$\mathcal{D}(f,g,s) = \prod_p (1 + a_p b_p p^{-s} + a_{p^2} b_{p^2} p^{-2s} + ...).$$

Define

$$\mathcal{D}_{(p)}(f,g,s) = \sum_{n=0}^{\infty} a_{p^n} b_{p^n} p^{-ns}.$$

The series of $\mathcal{D}(f,g,s)$ is absolutely convergent if $\mathcal{R}(s) > \frac{k+\ell}{2}$. Hence we can rearrange it and write:

$$\mathcal{D}(f,g,s) = \prod_p \mathcal{D}_{(p)}(f,g,s). \qquad (16)$$

We study $\mathcal{D}(f,g,s)$ locally, i.e. prime by prime. We try to find a formula relating $\mathcal{D}_p(f,g,s)$ to $L_{(p)}(f \otimes g, s)$. We give two preliminary lemmas.

Lemma 9. *Let $\left(B_{p^j}\right)_{j=1,2,...}$ be a sequence of complex numbers satisfying an r-term linear recurrence of the form*

$$\begin{aligned}
B_{p^0} &= 1 \\
B_{p^{j+r}} &= \lambda_1 B_{p^{j+r-1}} + \lambda_2 B_{p^{j+r-2}} + ... + \lambda_r B_{p^j}
\end{aligned}$$

for all $j \geqslant 0$. Then:

$$\sum_{n=0}^{\infty} B_{p^n} x^n = \frac{Q(x)}{1 - \lambda_1 x - \lambda_2 x^2 - ... - \lambda_r x^r}$$

for some $Q(x) \in \mathbb{C}[x]$ of degree strictly less than r.

Proof: If we compute the product $(1+B_p x+B_{p^2}x^2+...)(1-\lambda_1 x-\lambda_2 x^2-...-\lambda_r x^r) = Q(x)$, we see that the term of degree $t \geqslant r$ is $B_{p^t} - \lambda_1 B_{p^{t-1}} - \lambda_2 B_{p^{t-2}} - ... - \lambda_{t-r} B_{p^r} = 0$ by the recurrence formula. Hence it has no terms of degree $\geqslant r$. ■

In the above lemma, put $B_{p^i} = a_{p^i} b_{p^i}$. We try to find a recurrence formula for B_{p^i}.

Lemma 10. *The sequence $B_{p^i} = a_{p^i} b_{p^i}$ satisfies a recurrence formula of the form*

$$B_{p^{j+4}} = \lambda_1 B_{p^{j+3}} + \lambda_2 B_{p^{j+2}} + \lambda_3 B_{p^{j+1}} + \lambda_4 B_{p^j},$$

where

$$(1-\lambda_1 x-\lambda_2 x^2-\lambda_3 x^3-\lambda_4 x^4) = (1-\alpha_p\beta_p x)(1-\alpha_p\beta_p^{'} x)(1-\alpha_p^{'}\beta_p x)(1-\alpha_p^{'}\beta_p^{'} x).$$

Proof: a_{p^i} satisfies a two term recurrence formula:

$$a_{p^{i+2}} = a_p a_{p^{i+1}} - \chi_f(p)p^{k-1}a_{p^i} \quad \forall i \geqslant 0.$$

Let

$$W = \left\{(x_i)_{i\geqslant 0} : \ x_{i+2} = a_p x_{i+1} - \chi_f(p)p^{k-1}x_i\right\}.$$

We claim that $\dim(W) = 2$ and a basis for this vector space is given by $(\alpha_p^j)_{j=1,2,...}$ and $(\alpha_p^{'j})_{j=1,2,...}$. To prove it, consider the following linear transformation on W:

$$\begin{aligned} \varphi : \quad & W && \to W \\ & (x_0, x_1, ...) && \mapsto (x_1, x_2, ...). \end{aligned}$$

φ is an invertible map, since x_0 can be determined by x_1 and x_2. The eigenvalues of this transformations are geometric progressions. Suppose $\varphi((x_0,x_1,...)) = \lambda(x_0,x_1,...)$. Then $x_2 = \lambda x_1 = \lambda^2 x_0$. From $x_2 = a_p x_1 - \chi_f(p)p^{k-1}x_0$ we get $\lambda^2 x_0 = a_p\lambda x_0 - \chi_f(p)p^{k-1}x_0$ therefore $\lambda^2 = a_p\lambda - \chi_f(p)p^{k-1}$, i.e. λ is a root of $x^2 = a_p x - \chi_f(p)p^{k-1}$ so is equal to α_p or $\alpha_p^{'}$. Hence $\left(a_{p^i}\right)_i$ is a linear combination of α_p^i and $\alpha_p^{'i}$. Likewise, $\left(b_{p^i}\right)_i$ is a linear combination of β_p^i and $\beta_p^{'i}$. It follows that $\left(B_{p^i}\right) = a_{p^i}b_{p^i}$ is a linear combinations of the four geometric progressions $(\alpha_p\beta_p)^i$, $(\alpha_p\beta_p^{'})^i$, $(\alpha_p^{'}\beta_p)^i$ and $(\alpha_p^{'}\beta_p^{'})^i$ and they satisfy the desired recurrence formula.

Corollary 1. *We have:*

$$\sum_{n=0}^{\infty} a_{p^n} b_{p^n} p^{-ns} = \frac{1-\chi(p)p^{k+\ell-2}}{1-\alpha_p\beta_p p^{-s} - \alpha_p^{'}\beta_p p^{-2s} - \alpha_p\beta_p^{'}p^{-s} - \alpha_p^{'}\beta_p^{'}p^{-s}}$$

where $\chi = \chi_f\chi_g$. In other words:

$$\mathcal{D}_{(p)}(f,g,s) = (1-\chi(p)p^{k+\ell-2}p^{-2s})L_{(p)}(f\otimes g, s). \tag{17}$$

Proof: By the lemma 9:

$$\sum_{n=0}^{\infty} a_{p^n} b_{p^n} p^{-ns} = \frac{Q(p^{-s})}{1-\alpha_p\beta_p p^{-s} - \alpha_p^{'}\beta_p p^{-2s} - \alpha_p\beta_p^{'}p^{-s} - \alpha_p^{'}\beta_p^{'}p^{-s}}$$

for $Q(x)$ a polynomial of degree $\leqslant 3$. We have:

$$
\begin{aligned}
&1-a_p\beta_p p^{-s}-a_p^{'}\beta_p p^{-2s}-\alpha_p\beta_p^{'}p^{-s}-\alpha_p^{'}\beta_p^{'}p^{-s}\\
&\quad=(1-\alpha_p\beta_p p^{-s}+\beta_p^2\chi_f(p)p^{k-1-2s})(1-\alpha_p\beta_p^{'}p^{-s}+\beta_p^{'2}\chi_f(p)p^{k-1-2s})\\
&\quad=1-a_pb_pp^{-s}+[\beta_p^{'2}\chi_f(p)p^{k-1}+a_p^2\chi_g(p)p^{\ell-1}+\beta_p^2\chi_f(p)p^{k-1}]p^{-2s}\\
&\quad-[a_pb_p\chi(p)p^{k+\ell-2}]p^{-3s}+\chi(p)p^{2(k+\ell-2)}p^{-4s}. \qquad (18)
\end{aligned}
$$

Using $\beta_p^2+\beta_p^{'2}=(\beta_p+\beta_p^{'})^2-2\beta_p\beta_p^{'}=b_p^2-2\chi_g(p)p^{\ell-1}$ we get:

$$
\begin{aligned}
(18) &= 1-a_pb_pp^{-s}+[b_p^2\chi_f(p)p^{k-1}+a_p^2\chi_g(p)p^{\ell-1}-2\chi(p)p^{k+\ell-2}]p^{-2s} \qquad (19)\\
&\quad -[a_pb_p\chi(p)p^{k+\ell-2}]p^{-3s}+\chi(p)p^{2(k+\ell-2)}p^{-4s}. \qquad (20)
\end{aligned}
$$

One can show:

$$
\begin{aligned}
Q(p^{-s}) &= (1+a_pb_pp^{-s}+a_{p^2}b_{p^2}p^{-2s}+....)\\
&\quad\times(1-a_pb_pp^{-s}+[\beta_p^{'2}\chi_f(p)p^{k-1}+a_p^2\chi_g(p)p^{\ell-1}+\beta_p^2\chi(p)p^{k-1}]p^{-2s}\\
&\quad-[a_pb_p\chi(p)p^{k+\ell-2}]p^{-3s}+\chi(p)p^{2(k+\ell-2)}p^{-4s})\\
&= 1-\chi(p)p^{k+\ell-2}p^{-2s}.
\end{aligned}
$$

Hence the corollary holds. ■

Theorem 11. *Let $f\in\mathcal{S}_k(\Gamma_0(N),\chi_f)$ and $g\in\mathcal{S}_\ell(\Gamma_0(N),\chi_g)$. Then*

$$L(f\otimes g,s)=L(\chi,2s-k-\ell+2)\mathcal{D}(f,g,s). \qquad (21)$$

In particular, if $f\in\mathcal{S}_k(SL_2(\mathbb{Z}))$ and $g\in\mathcal{S}_\ell(SL_2(\mathbb{Z}))$ ($N=1$ and χ_f,χ_g are trivial characters) we have:

$$L(f\otimes g,s)=\zeta(2s-k-\ell+2)\mathcal{D}(f,g,s). \qquad (22)$$

Proof: Using (17) , (15), (16), we get (21). For the case $N=1$, as $L(\mathbf{1},2s-k-\ell+2)=\zeta(2s-k-\ell+2)$, we get (22). ■

We study the analytic properties of $\mathcal{D}(f,g,s)$ for $N=1$, then we can get a formula for $\mathcal{D}(f,g,k-1)$ when $k>\ell+2$.

As for the case of weight 1, we can define an Eisenstein series of weight k and level 1:

$$\widetilde{E}_k(z)=\sum_{(m,n)\in\mathbb{Z}\times\mathbb{Z}}{}^{'}\frac{1}{|mz+n|^k}$$

and

$$\widetilde{E}_k^{'}(z):=\sum_{\substack{(m,n)\in\mathbb{Z}\times\mathbb{Z}\\ gcd(m,n)=1}}\frac{1}{(mz+n)^k}.$$

Similarly, we define the non-holomorphic Eisenstein series of weight k:

$$\widetilde{E}_k(z,s)=\sum_{(m,n)\in\mathbb{Z}\times\mathbb{Z}}{}^{'}\frac{1}{(mz+n)^k}\frac{y^s}{|mz+n|^{2s}}.$$

- $\widetilde{E}_k(z,s)$ is convergent for $\mathcal{R}(s) \gg 0$ and for any k. It is holomorphic as a function of s.
- $\widetilde{E}_k(\frac{az+b}{cz+d}, s) = (cz+d)^k \widetilde{E}_k(z,s)$ so it behaves like a modular form as a function of z however it is not holomorphic as a function of z.

Define analogously:

$$\widetilde{E}'_k(z,s) := \sum_{\substack{(m,n)\in\mathbb{Z}\times\mathbb{Z} \\ gcd(m,n)=1}} \frac{1}{(mz+n)^k} \frac{y^s}{(mz+n)^{2s}}.$$

Then

$$\widetilde{E}_k(z,s) = \zeta(2z)\widetilde{E}'_k(z,s).$$

We need the following preliminary lemma.

Lemma 12. *Put* $(\mathbb{Z}\times\mathbb{N})' := \{(a,b) \in \mathbb{Z}\times\mathbb{N} | \; gcd(a,b)=1\}$. *Define* $\Gamma_\infty := \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \mid n \in \mathbb{Z} \right\}$ *which is a subgroup of* $SL_2(\mathbb{Z})$. *Then the map*

$$\begin{array}{ccc} \Gamma_\infty \backslash SL_2(\mathbb{Z}) & \to & (\mathbb{Z}\times\mathbb{N})' \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} & \mapsto & (c,d) \end{array}$$

is a bijection.

Proof: The map obviously surjects. Moreover, it is left unchanged by multiplying by any matrix in Γ_∞, so Γ_∞ is inside the kernel. We can easily see that Γ_∞ is all the kernel hence we have the injectivity. ■

Proposition 13. *Let* $f \in \mathcal{S}_k(SL_2(\mathbb{Z}))$ *and* $g \in \mathcal{S}_\ell(SL_2(\mathbb{Z}))$. *For* $\mathcal{R}(s) > 2 - \frac{k-\ell}{2}$ *we have:*

$$\left\langle \widetilde{E}'_{k-\ell}(z,s)g(z), f^*(z) \right\rangle_k = \frac{2\Gamma(k+s-1)}{(4\pi)^{k+s-1}} \mathcal{D}(f,g,k+s-1) \tag{23}$$

where $f^* \in \mathcal{S}_k(SL_2(\mathbb{Z}))$ *is the modular form satisfying* $a_n(f^*) = \overline{a_n}$. *In particular, if* $s=0$, *then*

$$\left\langle \widetilde{E}'_{k-\ell}(z)g(z), f^*(z) \right\rangle_k = \frac{2\Gamma(k-1)}{(4\pi)^{k-1}} \mathcal{D}(f,g,k-1). \tag{24}$$

Proof: We can easily see that:

$$\begin{aligned} y(\gamma z)^{k+s} g(\gamma z) f(\gamma(-\bar{z})) &= \frac{y^{k+s}}{|mz+n|^{2(k+s)}} (mz+n)^\ell g(z) \overline{(mz+n)^k} f(-\bar{z}) \\ &= \frac{y^{k+s}}{(mz+n)^{k-\ell} |mz+n|^{2s}} g(z) f(-\bar{z}) \end{aligned}$$

for any $\gamma = \begin{pmatrix} * & * \\ m & n \end{pmatrix}$. Remark that $f^*(z) = \overline{f(-\bar{z})}$. Then we compute:

$$
\begin{aligned}
\left\langle \widetilde{E}'_{k-\ell}(z,s)g(z), f^*(z)\right\rangle_k &= \int_{\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}} y^k \widetilde{E}'_{k-\ell}(z,s)g(z)f(-\bar{z})\frac{dx\ dy}{y^2} \\
&= \int_{\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}} y^k \sum_{\substack{(m,n)\in\mathbb{Z}\times\mathbb{Z}\\ gcd(m,n)=1}} \frac{y^s}{(mz+n)}\cdot\frac{g(z)f(-\bar{z})}{|mz+n|^{2s}}\frac{dx\ dy}{y^2} \\
&= \int_{\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}} \sum_{\substack{(m,n)\in\mathbb{Z}\times\mathbb{N}\\ gcd(m,n)=1}} \frac{y^{k+s}}{(mz+n)}\cdot\frac{g(z)f(-\bar{z})}{|mz+n|^{2s}}\frac{dx\ dy}{y^2} \\
&= 2\int_{\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}} \sum_{\gamma\in\Gamma_\infty\backslash\mathrm{SL}_2(\mathbb{Z})} y(\gamma z)^{k+s}g(\gamma z)f(-\gamma\bar{z})\frac{dx(\gamma z)\ dy(\gamma z)}{y^2(\gamma z)} \\
&= 2\sum_{\gamma\in\Gamma_\infty\backslash\mathrm{SL}_2(\mathbb{Z})} \int_{\gamma(\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H})} y(z)^{k+s}g(z)f(-\bar{z})\frac{dx\ dy}{y^2}. \qquad (25)
\end{aligned}
$$

The different translates $\gamma(\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H})$ of the original fundamental domain $\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}$ are disjoint and they fit together exactly to form a fundamental domain for the action of Γ_∞ on $\mathcal{H}$. This is called Rankin's unfolding trick. Hence:

$$
\begin{aligned}
(25) &= 2\int_{\Gamma_\infty\backslash\mathcal{H}} y^{k+s}g(z)f(-\bar{z})\frac{dx\ dy}{y^2} \\
&= 2\int_{y=0}^{\infty}\int_{x=0}^{1} y^{k+s}\left(\sum_{n\geqslant 1} b_n e^{2\pi i n z}\right)\left(\sum_{m\geqslant 1} a_m e^{-2\pi i m\bar{z}}\right)\frac{dxdy}{y^2} \\
&= 2\int_{y=0}^{\infty}\int_{x=0}^{1} y^{k+s}\sum_{n,m\geqslant 1} b_n a_m e^{2\pi i n(x+iy)}e^{-2\pi i m(x-iy)}\frac{xdy}{y^2} \\
&= 2\int_{y=0}^{\infty} y^{k+s}\sum_{n,m\geqslant 1} b_n a_m e^{-2\pi(n+m)y}\left(\int_{x=0}^{1} e^{2\pi i(n-m)x}dx\right)\frac{dy}{y^2}.
\end{aligned}
$$

The integral in the parenthesis is equal to the Kronecker delta $\delta_{(n,m)}$. So the last line is equal to:

$$
\begin{aligned}
&= 2\int_{y=0}^{\infty} y^{k+s}\sum_{n\geqslant 1} a_n b_n e^{-2\pi(n+n)y}\frac{dy}{y^2} \\
&= 2\sum_{n\geqslant 1} a_n b_n\int_{y=0}^{\infty} y^{k-1+s}e^{-4\pi n y}\frac{dy}{y} \\
&= 2\left(\sum_{n\geqslant 1}\frac{a_n b_n}{(4\pi n)^{k-1+s}}\right)\int_0^{\infty} u^{k-1+s}e^{-u}\frac{du}{u} \\
&= \frac{2\Gamma(k-1+s)}{(4\pi)^{k-1+s}}\mathcal{D}(f,g,k-1+s)
\end{aligned}
$$

where we have made the change of variable $u = 4\pi n y$ for each integral in the sum. ■

The formula (23) makes sense even when $k \not> \ell + 2$. In particular, it makes sense when $k = \ell$. Consider the following Eisenstein series

$$\begin{aligned}\widetilde{E}(z,s) &= \widetilde{E}_0(z,s) \\ &= \sum_{(m,n)\in\mathbb{Z}\times\mathbb{Z}}{}' \frac{y^s}{|mz+n|^{2s}}\end{aligned}$$

which converges for $\mathcal{R}(s) > 1$. Define

$$\begin{aligned}\widetilde{E}'(z,s) &:= \widetilde{E}'_0(z,s) \\ &= \sum_{\substack{(m,n)\in\mathbb{Z}\times\mathbb{Z}\\ gcd(m,n)=1}} \frac{y^s}{|mz+n|^{2s}}.\end{aligned}$$

Then

$$\widetilde{E}(z,s) = \zeta(2s)\widetilde{E}'(z,s).$$

So $\widetilde{E}(z,s)$ is a nonholomorphic Eisenstein series of weight 0. As a function of s, with z fixed, we write:

$$\widetilde{E}'(z,s) = \sum_{\substack{(m,n)\in\mathbb{Z}\times\mathbb{Z}\\ gcd(m,n)=1}} \frac{1}{Q_z^s(m,n)}$$

where $Q_z^s(m,n) = \dfrac{|mz+n|^2}{y}$ is a quadratic form in two variables with $\operatorname{disc}(Q_z) = -4$.

$\widetilde{E}'(z,s)$ is a non-holomorphic Eisenstein series of weight zero attached to Q_z when considered as a function of s.

Lemma 14. *Let $f, g \in \mathcal{S}_k(SL_2(\mathbb{Z}))$ be two modular forms of the same weight. Then:*

$$\left\langle \widetilde{E}(z,s)g(z), f(z)\right\rangle_k = \frac{2\Gamma(s+k-1)}{(4\pi)^{s+k-1}} L(f\otimes g, s+k-1).$$

Proof: We have:

$$\begin{aligned}\left\langle \widetilde{E}_k(z,s)g(z), f(z)\right\rangle_k &= \zeta(2s)\left\langle \widetilde{E}'_k(z,s)g(z), f(z)\right\rangle_k \\ &= \zeta(2s)\frac{2\Gamma(s+k-1)}{(4\pi)^{s+k-1}}\mathcal{D}(f,g,s+k-1) \\ &= \zeta(2s)\frac{2\Gamma(s+k-1)}{(4\pi)^{s+k-1}}L(f\otimes g, s+k-1)\zeta(2(s+k-1)+2-2k)^{-1} \\ &= \frac{2\Gamma(s+k-1)}{(4\pi)^{s+k-1}}L(f\otimes g, s+k-1). \quad \blacksquare\end{aligned}$$

Theorem 15. *Let $z \in \mathcal{H}$ be fixed. Then*
1) The function $\widetilde{E}(z,s)$ has a meromorphic continuation to $s \in \mathbb{C}$ and is entire except for a simple pole with residue π at $s = 1$.

2) The function $G(z,s) := \dfrac{\Gamma(s)}{\pi^s}\widetilde{E}(z,s)$ *is holomorphic except for simple poles at* $s=1$ *and* $s=0$ *with residue 1 and -1 repectively. Moreover*

$$G(z,s) = G(z,1-s).$$

Proof: Consider

$$\theta_z(t) = \sum_{(m,n)\in\mathbb{Z}^2} e^{-\pi Q_z(m,n)t}.$$

We compute its Mellin transform and get:

$$\begin{aligned} G(z,s) &= \Gamma(s) \sum_{(m,n)\in\mathbb{Z}\times\mathbb{Z}}{}' [\pi Q_z(m,n)]^{-s} \\ &= \int_0^\infty (\theta_z(t)-1)t^s \frac{dt}{t}. \end{aligned}$$

The Poisson summation formula implies that

$$\theta_z(\tfrac{1}{t}) = t\theta_z(t).$$

Then we can write for $\mathcal{R}(s) > 1$:

$$\begin{aligned} G(z,1-s) &= \int_0^\infty (\theta_z(t)-1)t^{1-s}\frac{dt}{t} \\ &= \int_0^\infty (\frac{1}{t}\theta_z(\frac{1}{t})-1)t^{1-s}\frac{dt}{t} \\ &= \int_0^\infty \left(\frac{1}{t}(\theta_z(\frac{1}{t})-1)-1+\frac{1}{t}\right)t^{1-s}\frac{dt}{t} \\ &= \int_0^\infty (t(\theta_z(t)-1)-1+t)\, t^{s-1}\frac{dt}{t} \\ &= \int_0^\infty (\theta_z(t)-1)t^s\frac{dt}{t} + \int_0^\infty (-1+t)\, t^{s-1}\frac{dt}{t} \\ &= G(z,s) + \frac{1}{1-s} + \frac{1}{s}. \end{aligned}$$

(in the fourth line, we make the change of variable $s = \frac{1}{u}$) Hence $G(z,s)$ is invariant under the change $s \to 1-s$. It is entire except for simple poles at $s=1$ and $s=0$ with residue 1 and -1, respectively.

We compute the residue of $\widetilde{E}(z,s)$ at $s=1$:

$$\begin{aligned} \mathrm{Res}_{s=1}\widetilde{E}(z,s) &= \mathrm{Res}_{s=1}\frac{\pi^s}{\Gamma(s)}G(z,s) \\ &= \frac{\pi}{\Gamma(1)}\mathrm{Res}_{s=1}G(z,s) \\ &= \pi. \end{aligned}$$

Since the Gamma function $\Gamma(s)$ has a simple pole at $s=0$, then $\widetilde{E}(z,s)$ it holomorphic at this point. ■

In the lemma 14, we obtained an integral representation for $L(f \otimes g, s+k-1)$. Now define

$$\begin{aligned} \Lambda(f \otimes g, s) &:= \langle G(z, s-k+1)g, f \rangle_k \\ &= \frac{2\Gamma(s-k+1)\Gamma(s)}{4^s \pi^{s-k+1}} L(f \otimes g, s). \end{aligned} \tag{26}$$

This function has some nice properties.

Proposition 16. *Let $f, g \in \mathcal{S}_k(SL_2(\mathbb{Z}))$ be two modular forms of the same weight. The function $\Lambda(f \otimes g, s)$ extends to a meromorphic function of s. It is holomorphic except at $s = k-1$ and $s = k$ where it has simple poles with residues $-\langle g, f \rangle$ and $\langle g, f \rangle$ respectively.*

Proof: We have seen that $G(z, s)$ is an entire function except at $s = 0$ and $s = 1$ where it has simple poles with residue 1 and -1 respectively. So $\Lambda(f \otimes g, s)$ extends to a meromorphic function with two poles at points $s = k-1$ and $s = k$. We compute the residue of $\Lambda(f \otimes g, s)$ at $s = 0$:

$$\begin{aligned} \mathrm{Res}_{s=k-1}\Lambda(f \otimes g, s) &= \mathrm{Res}_{s=k-1} \langle G(z, s-k+1)g, f \rangle_k \\ &= \langle \mathrm{Res}_{s=0} G(z, s) g, f \rangle_k \\ &= -\langle g, f \rangle . \end{aligned}$$

Similarly, $\mathrm{Res}_{s=k}\Lambda(f \otimes g, s) = \langle g, f \rangle$. ■

Corollary 2. *Let $f, g \in \mathcal{S}_k(SL_2(\mathbb{Z}))$ be two modular forms of the same weight. $L(f \otimes g, s)$ extends to a meromorphic function of $s \in \mathbb{C}$. It has a simple pole at $s = k$ if and only if $\langle f, g \rangle \neq 0$.*

Proof: Write $L(f \otimes g, s) = \dfrac{4^s \pi^{2(s-k+1)}}{2\Gamma(s)\Gamma(s-k+1)} \Lambda(f \otimes g, s)$. The function $\Gamma(s)$ has simple pole at all points $s = 0, -1, -2, ...$ with residue $\mathrm{Res}_{s=n}\Gamma(s) = \frac{(-1)^n}{n}$ for $n = 0, -1, -2, ...$. So $\dfrac{1}{\Gamma(s)}$ has zeros at points $s = 0, -1, -2, ...$. Hence $L(f \otimes g, s)$ cannot have a pole at $s = k-1$ and it has a pole at $s = k$ if and only if $\langle f, g \rangle = 0$. ■

We can also find similar formulas for modular forms of level $N > 1$. Let $\chi : (\mathbb{Z}/N\mathbb{Z}) \to \mathbb{C}^*$ be a character modulo N. Put:

$$\begin{aligned} \widetilde{E}(z, s; \chi; N) &:= \widetilde{E}_0(z, s; \chi; N) \\ &= \sum_{(m,n) \in \mathbb{Z} \times \mathbb{Z}}{}' \frac{\chi(n) y^s}{(Nmz+n)^{2s}} \end{aligned} \tag{27}$$

and

$$\begin{aligned} \widetilde{E}'(z, s; \chi; N) &:= \widetilde{E}'_0(z, s; \chi; N) \\ &= \sum_{\substack{(m,n) \in \mathbb{Z} \times \mathbb{Z} \\ gcd(Nm,n)=1}} \frac{\chi(n) y^s}{(Nmz+n)^{2s}}. \end{aligned} \tag{28}$$

It follows that:

$$\widetilde{E}(z,s;\chi;N) = L(\chi,2s)\widetilde{E}^{'}(z,s;\chi;N). \tag{29}$$

As before, set:

$$\begin{aligned} \widetilde{E}(z;\chi;N) &:= \widetilde{E}(z,0;\chi;N) \qquad (30)\\ \widetilde{E}^{'}(z;\chi;N) &:= \widetilde{E}^{'}(z,0;\chi;N). \qquad (31)\end{aligned}$$

Proposition 17. *Let $f \in \mathcal{S}_k(\Gamma_0(N),\chi_f)$ and $g \in \mathcal{S}_\ell(\Gamma_0(N),\chi_g)$. For $\mathcal{R}(s) > 2 - \frac{k-\ell}{2}$ we have:*

$$\left\langle \widetilde{E}^{'}_{k-\ell}(z,s;\chi^{-1};N)g(z), f^*(z)\right\rangle_{k,N} = \frac{2\Gamma(k+s-1)}{(4\pi)^{k+s-1}}\mathcal{D}(f,g,k+s-1) \tag{32}$$

where $\chi = \chi_f\chi_g$ and $f^* \in \mathcal{S}_k(\Gamma_0(N),\overline{\chi_f})$ is the modular form satisfying $a_n(f^*) = \overline{a_n}$. In particular, if $s=0$, then

$$\left\langle \widetilde{E}^{'}_{k-\ell}(z;\chi^{-1};N)g(z), f^*(z)\right\rangle_{k,N} = \frac{2\Gamma(k-1)}{(4\pi)^{k-1}}\mathcal{D}(f,g,k-1). \tag{33}$$

Proof: The proof is similar to the proposition 13. ■

Lemma 18. *Let $f \in \mathcal{S}_k(\Gamma_0(N),\chi_f)$ and $g \in \mathcal{S}_\ell(\Gamma_0(N),\chi_g)$ be two modular forms. Then:*

$$\left\langle \widetilde{E}_{k-\ell}(z,s;\chi^{-1};N)g(z), f^*(z)\right\rangle_{k,N} = \frac{2\Gamma(s+k-1)}{(4\pi)^{s+k-1}}\frac{L(\chi^{-1},2s+k-\ell)}{L(\chi,2s+k-\ell)}L(f\otimes g,s+k-1) \tag{34}$$

where $\chi = \chi_f\chi_g$. In particular, if $\chi_f = \chi_g^{-1}$, then

$$\left\langle \widetilde{E}_{k-\ell}(z,s;\mathbf{1};N)g(z), f^*(z)\right\rangle_{k,N} = \frac{2\Gamma(s+k-1)}{(4\pi)^{s+k-1}}L(f\otimes g,s+k-1). \tag{35}$$

Proof: We have:

$$\begin{aligned}\left\langle \widetilde{E}_{k-\ell}(z,s;\chi^{-1};N)g(z), f^*(z)\right\rangle_{k,N} &= L(\chi^{-1},2s+k-\ell)\left\langle \widetilde{E}^{'}_{k-\ell}(z,s;\chi^{-1};N)g(z), f^*(z)\right\rangle_{k,N}\\ &= L(\chi^{-1},2s+k-\ell)\frac{2\Gamma(s+k-1)}{(4\pi)^{s+k-1}}\mathcal{D}(f,g,s+k-1)\\ &= L(\chi^{-1},2s+k-\ell)\frac{2\Gamma(s+k-1)L(f\otimes g,s+k-1)}{(4\pi)^{s+k-1}L(\chi,2(s+k-1)+2-k-\ell)}\\ &= \frac{2\Gamma(s+k-1)}{(4\pi)^{s+k-1}}\frac{L(\chi^{-1},2s+k-\ell)}{L(\chi,2s+k-\ell)}L(f\otimes g,s+k-1).\end{aligned}$$

In particular, if $\chi_f = \chi_g^{-1}$ or equivalently if $\chi = \mathbf{1}$, then $L(\chi^{-1},2s+k-\ell) = L(\chi,2s+k-\ell) = \zeta_N(2s+k-\ell)$, so (35) holds. ■

For two arbitrary modular forms f and g, one has the following more general result:

Theorem 19. *Let $f \in \mathcal{S}_k(\Gamma_0(N_f), \chi_f)$ and $g \in \mathcal{S}_\ell(\Gamma_0(N_g), \chi_g)$. Assume that χ_f and χ_f are primitive characters modulo N_f and N_g, respectively. Moreover, $\chi_f \chi_g^{-1}$ is primitive modulo $M = gcd(N_f, N_g)$. As before, set*

$$\Lambda(f \otimes g, s) = \frac{2\Gamma(s-k+1)\Gamma(s)}{4^s \pi^{s-k+1}} L(f \otimes g, s).$$

Then $\Lambda(f \otimes g, s)$ is an entire function of s unless $f = g^*$. If $f = g^*$, then $\Lambda(f \otimes f^*, s)$ has two simple poles at $s = k$ and $s = k-1$.

Proof: See [10]. ■

2.2 Some applications of the Rankin-Selberg method

In this section, we apply the Rankin-Selberg method to compute the norm of a modular form whose fourier coefficients are real:

$$||f|| = \sqrt{\langle f, f \rangle}.$$

As a second application of the Rankin-Selberg method, we state and prove an estimate for $\sum_{p \nmid N} |a_p|^2 p^{-s}$.

We need the following lemma:

Lemma 20. ***(Landau)*** *Let $f(s) = \sum_{n=0}^{\infty} \frac{a_n}{n^s}$ be a Dirichlet series with real coefficients $a_n \geqslant 0$. Suppose that the series defining f(s) converges for $\mathcal{R}(s) > \sigma_0$. Suppose further that the function f extends to a function holomorphic in a neighborhood of $s = \sigma_0$. Then, in fact, the series defining $f(s)$ converges for $\mathcal{R}(s) > \sigma_0 - \varepsilon$ for some $\varepsilon > 0$.*

Proof: See [15]. ■

Proposition 21. *Let $f = \sum_{n=0}^{\infty} a_n q^n \in \mathcal{S}_k(SL_2(\mathbb{Z}))$ be a normalised Hecke eigenform. Then:*
(a)

$$\sum_{n=0}^{\infty} a_n^2 n^{-s} = \zeta(s-k+1) \sum_{n=0}^{\infty} a_{n^2} n^{-s}. \tag{36}$$

(b)

$$\langle f, f \rangle_k = \frac{\pi (k-1)!}{3(4\pi)^k} \sum_{n=0}^{\infty} \frac{a_{n^2}}{n^k}. \tag{37}$$

Proof: Being f a normalised Hecke eigenform, its fourier coefficients satisfy:
1. $a_1 = 1$,

2. $a_{p^n} = a_p a_{p^{n-1}} - p^{k-1} a_{p^{n-2}}$ for all p prime and $n \geqslant 2$ (38)

3. $a_{mn} = a_m a_n$ when $\gcd(m, n) = 1$.

We compute the product expansion of two series $\sum_{n=0}^{\infty} a_n^2 n^{-s}$ and $\sum_{n=0}^{\infty} a_{n^2} n^{-s}$.
Define $b_n := a_n^2$. Then from (38), we have:

$$\begin{aligned}
b_{p^n} &= (a_p a_{p^{n-1}} - p^{k-1} a_{p^{n-2}})^2 \\
&= a_p^2 b_{p^{n-1}} + p^{2(k-1)} b_{n-2} - 2a_p p^{k-1} a_{p^{n-1}} a_{p^{n-2}} \\
&= a_p^2 b_{p^{n-1}} + p^{2(k-1)} b_{p^{n-2}} - 2a_p p^{k-1} (a_p a_{p^{n-2}} - p^{k-1} a_{p^{n-3}}) a_{p^{n-2}} \\
&= a_p^2 b_{p^{n-1}} + p^{k-1}(p^{k-1} - 2a_p^2) b_{p^{n-2}} + 2a_p p^{2(k-1)} a_{p^{n-2}} a_{p^{n-3}}.
\end{aligned}$$

Now, we can replace n by $n-1$ in the equation (38) and then replace $a_{p^{n-2}} a_{p^{n-3}}$ by its equivalent in the above equation. So we get

$$b_{p^n} = (a_p^2 - p^{k-1}) b_{p^{n-1}} + p^{k-1}(p^{k-1} - a_p^2) b_{p^{n-2}} + p^{3(k-1)} b_{p^{n-3}}.$$

Using the lemma 9, we have the following product expansion:

$$\sum_{i=0}^{\infty} b_{p^i} p^{-is} = \frac{1 + p^{k-1} p^{-s}}{1 - (a_p^2 - p^{k-1}) p^{-s} - p^{k-1}(p^{k-1} - a_p^2) p^{-2s} - p^{3(k-1)} p^{-3s}}.$$

The series $\sum_{n=0}^{\infty} a_n^2 n^{-s}$ is absolutely convergent for $\mathcal{R}(s) > k$. On the other hand, $b_1 = 1$ and $b_{mn} = b_m b_n$ when $\gcd(m,n) = 1$. So we can rearrange the series and write:

$$\begin{aligned}
\sum_{n=0}^{\infty} a_n^2 n^{-s} &= \prod_p \sum_{i=0}^{\infty} b_{p^i} p^{-is} \\
&= \prod_p \frac{1 + p^{k-1} p^{-s}}{1 - (a_p^2 - p^{k-1}) p^{-s} - p^{k-1}(p^{k-1} - a_p^2) p^{-2s} - p^{3(k-1)} p^{-3s}} \quad , \mathcal{R}(s) > k.
\end{aligned}$$

Define $c_n = a_{n^2}$. For a prime number p, we have:

$$\begin{aligned}
c_{p^n} &= a_p a_{p^{2n-1}} - p^{k-1} a_{p^{2n-2}} \\
&= a_p (a_p a_{p^{2n-2}} - p^{k-1} a_{p^{2n-3}}) - p^{k-1} a_{p^{2n-2}} \\
&= (a_p^2 - p^{k-1}) c_{p^{n-1}} - p^{k-1} a_p a_{p^{2n-3}} \\
&= (a_p^2 - p^{k-1}) c_{p^{n-1}} - p^{k-1} (a_{p^{2n-2}} + p^{k-1} a_{p^{2n-4}}) \\
&= (a_p^2 - 2p^{k-1}) c_{p^{n-1}} - p^{2(k-1)} c_{p^{n-2}}.
\end{aligned}$$

Clearly $c_1 = 1$ and $c_{mn} = c_m c_n$ when $\gcd(m,n) = 1$. The series $\sum_{n=0}^{\infty} a_{n^2} n^{-s}$ is absolutely convergent when $\mathcal{R}(s) > k$. By the same argument as for b_n, we can write:

$$\sum_{n=0}^{\infty} a_{n^2} n^{-s} = \prod_p \frac{1 + p^{k-1} p^{-s}}{1 - (a_p^2 - 2p^{k-1}) p^{-s} + p^{2(k-1)} p^{-2s}}.$$

We can easily see that:

$$1 - (a_p^2 - p^{k-1}) p^{-s} - p^{k-1}(p^{k-1} - a_p^2) p^{-2s} - p^{3(k-1)} p^{-3s} = (1 - p^{k-1} p^{-s})(1 - (a_p^2 - 2p^{k-1}) p^{-s} + p^{2(k-1)} p^{-2s}).$$

Hence the part (a) is proved. For the second part, consider

$$\begin{aligned}\left\langle \widetilde{E}(z,s)f(z), f^*(z)\right\rangle_k &= \frac{\Gamma(s+k-1)}{(4\pi)^{s+k-1}}L(f\otimes f, s+k-1)\\ &= \frac{\Gamma(s+k-1)\zeta(2s)}{(4\pi)^{s+k-1}}D(f,f,s+k-1).\end{aligned}$$

Since f is a Hecke eigenform, its fourier coefficients a_n are real. Thus $f^*(z) = f(z)$ and

$$D(f,f,s+k-1) = \sum_{n=0}^{\infty}\frac{a_n^2}{n^{s+k-1}} = \zeta(s)\sum_{n=0}^{\infty}\frac{a_{n^2}}{n^{s+k-1}}.$$

The series $f(s) := \sum_{n=0}^{\infty}\frac{a_{n^2}}{n^{s+k-1}}$ is absolutely convergent for $\mathcal{R}(s) > 1$. Since $\zeta(s)$ and $D(f,f,s+k-1)$ are meromorphic functions over $\mathbb{C}$ and have simple pole at $s=1$, by Landau's lemma, then $f(s)$ is holomorphic in a neighborhood of $s=1$ and the series $f(s) = \sum_{n=0}^{\infty}\frac{a_{n^2}}{n^{s+k-1}}$ is convergent at $s=1$.
We compute:

$$\begin{aligned}\mathrm{Res}_{s=1}\langle G(z,s)f(z), f(z)\rangle_k &= \mathrm{Res}_{s=1}\left\langle \frac{\Gamma(s)}{\pi^s}\widetilde{E}(z,s)f(z), f(z)\right\rangle_k\\ &= \mathrm{Res}_{s=1}\frac{2\Gamma(s)\Gamma(s+k-1)\zeta(2s)}{\pi^s(4\pi)^{s+k-1}}D(f,f,s+k-1)\\ &= \mathrm{Res}_{s=1}\frac{2\Gamma(s)\Gamma(s+k-1)\zeta(2s)}{\pi^s(4\pi)^{s+k-1}}\zeta(s)\sum_{n=0}^{\infty}\frac{a_{n^2}}{n^{s+k-1}}\\ &= \frac{2\Gamma(1)\Gamma(k)\zeta(2)}{\pi(4\pi)^k}\left(\sum_{n=0}^{\infty}\frac{a_{n^2}}{n^k}\right)\mathrm{Res}_{s=1}\zeta(s)\\ &= \frac{\pi(k-1)!}{3(4\pi)^k}\sum_{n=0}^{\infty}\frac{a_{n^2}}{n^k}.\end{aligned}$$

On the other hand:

$$\begin{aligned}\mathrm{Res}_{s=1}\langle G(z,s)f(z), f(z)\rangle_k &= \langle \mathrm{Res}_{s=1}G(z,s)f(z), f(z)\rangle_k\\ &= \langle f(z), f(z)\rangle_k.\end{aligned}$$

Thus we have the required result. ■

We can also find similar formula for a modular form of level $N > 1$ for the case when the fourier coefficients of f are real.

Proposition 22. *Let $f = \sum_{n=0}^{\infty} a_n q^n \in \mathcal{S}_k(\Gamma_0(N))$ be a normalised Hecke eigenform with real fourier coefficients where $N = \prod_{i=1}^{r} p_i^{\alpha_i}$ (p_i's are distinct prime numbers and*

$\alpha_i \geqslant 1$). Then:
(a)

$$\begin{aligned}\sum_{n=0}^{\infty}\frac{a_n^2}{n^s} &= L(\mathbf{1}, s-k+1)\sum_{n=0}^{\infty}\frac{a_{n^2}}{n^s} \\ &= \zeta(s-k+1)\prod_{p|N}(1-\frac{1}{p})\sum_{n=0}^{\infty}\frac{a_{n^2}}{n^s}.\end{aligned}$$

where $\mathbf{1}$ is the trivial character of mod N.
(b)

$$\langle f, f\rangle_{k,N} = \frac{N\pi(k-1)!}{3(4\pi)^k}\sum_{n=0}^{\infty}\frac{a_{n^2}}{n^k}. \tag{39}$$

Proof: In the proposition (17), we put $g = f$ and so $\chi = \mathbf{1}$. We then have

$$\begin{aligned}\left\langle \widetilde{E}'(z, s; \mathbf{1}; N)f(z), f^*(z)\right\rangle_{k,N} &= \left\langle \widetilde{E}'(z, s; \mathbf{1}; N)f(z), f(z)\right\rangle_{k,N} \\ &= \frac{2\Gamma(s+k-1)}{(4\pi)^{s+k-1}}\mathcal{D}(f, f, s+k-1).\end{aligned}$$

Let $N = \prod_{i=1}^{v} p_i^{\alpha_i}$ where p_i's are distinct prime numbers and $\alpha_i \geqslant 1$ and set $P = \{p_1, p_2, ..., p_r\}$. Then:

$$\begin{aligned}\frac{1}{N^s}\widetilde{E}_1'(Nz, s) &= \frac{1}{N^s}\sum_{\substack{(m,n)\in\mathbb{Z}\times\mathbb{Z}\\ gcd(m,n)=1}}\frac{(Ny)^s}{(Nmz+n)^{2s}} \\ &= \sum_{\substack{(m,n)\in\mathbb{Z}\times\mathbb{Z}\\ gcd(m,n)=1}}\frac{y^s}{(Nmz+n)^{2s}} \\ &= \sum_{\substack{(m,n)\in\mathbb{Z}\times\mathbb{Z}\\ gcd(Nm,n)=1}}\frac{y^s}{(Nmz+n)^{2s}} + \sum_{p_i\in P}\sum_{\substack{(m,n)\in\mathbb{Z}\times\mathbb{Z}\\ gcd(m,n)=1\\ p_i|n}}\frac{y^s}{(Nmz+n)^{2s}} \\ &\quad - \sum_{\substack{p_i,p_j\in P\\ p_i\neq p_j}}\sum_{\substack{(m,n)\in\mathbb{Z}\times\mathbb{Z}\\ gcd(m,n)=1\\ p_ip_j|n}}\frac{y^s}{(Nmz+n)^{2s}} + \cdots - (-1)^v\sum_{\substack{(m,n)\in\mathbb{Z}\times\mathbb{Z}\\ gcd(m,n)=1\\ p_1p_2...p_v|n}}\frac{y^s}{(Nmz+n)^{2s}} \\ &= \widetilde{E}'(z, s; \mathbf{1}; N) + \sum_{p_i\in P}\frac{1}{p_i^{2s}}\sum_{\substack{(m,n)\in\mathbb{Z}\times\mathbb{Z}\\ gcd(m,n)=1}}\frac{y^s}{(\frac{N}{p_i}mz+n)^{2s}} \\ &\quad - \sum_{\substack{p_i,p_j\in P\\ p_i\neq p_j}}\frac{1}{(p_ip_j)^{2s}}\sum_{\substack{(m,n)\in\mathbb{Z}\times\mathbb{Z}\\ gcd(m,n)=1}}\frac{y^s}{(\frac{N}{p_ip_j}mz+n)^{2s}} + \cdots \\ &\quad -(-1)^v\frac{1}{(p_1...p_v)^{2s}}\sum_{\substack{(m,n)\in\mathbb{Z}\times\mathbb{Z}\\ gcd(m,n)=1}}\frac{y^s}{(\frac{N}{p_1...p_v}mz+n)^{2s}}.\end{aligned}$$

Since for any M:

$$\sum_{\substack{(m,n)\in\mathbb{Z}\times\mathbb{Z}\\ gcd(m,n)=1}} \frac{y^s}{(Mmz+n)^{2s}} = \frac{1}{M^s} \sum_{\substack{(m,n)\in\mathbb{Z}\times\mathbb{Z}\\ gcd(m,n)=1}} \frac{(My)^s}{(Mmz+n)^{2s}} = \frac{1}{M^s} E^{'}(Mz,s),$$

it follows

$$\begin{aligned}
\widetilde{E}^{'}(z,s;\mathbf{1};N) &= \frac{1}{N^s}\widetilde{E}^{'}_1(Nz,s) - \sum_{p_i\in P} \frac{1}{N^s p_i^s} E^{'}(\tfrac{N}{p_i}z,s) \\
&+ \sum_{\substack{p_i,p_j\in P\\ p_i\neq p_j}} \frac{1}{N^s(p_ip_j)^s} E^{'}(\tfrac{N}{p_ip_j}z,s) \\
&- \cdots \\
&+ (-1)^v \frac{1}{N^s(p_1...p_v)^s} E^{'}(\tfrac{N}{p_1p_2...p_v}z,s).
\end{aligned}$$

One can compute the residue of $E^{'}(Mz,s)$ at $s=1$ for any M. In fact:

$$\mathrm{Res}_{s=1}E^{'}(Mz,s) = \mathrm{Res}_{s=1}\frac{E(Mz,s)}{\zeta(2s)} = \mathrm{Res}_{s=1}\frac{\pi^s G(Mz,s)}{\Gamma(s)\zeta(2s)} = \frac{\pi}{\Gamma(1)\zeta(2)}\mathrm{Res}_{s=1}G(Mz,s) = \frac{6}{\pi}.$$

Therefore

$$\begin{aligned}
\mathrm{Res}_{s=1}\widetilde{E}^{'}(z,s;\mathbf{1};N) &= \frac{6}{N\pi}\left(1 - \sum_{p_i\in P}\frac{1}{p_i} + \sum_{\substack{p_i,p_j\in P\\ p_i\neq p_j}} \frac{1}{p_ip_j} + \cdots + (-1)^v\frac{1}{p_1...p_v}\right) \\
&= \frac{6}{N\pi}\prod_{p|N}(1-\tfrac{1}{p}).
\end{aligned}$$

We compute then the residue of both sides of the formula (2.2) at $s=1$:

$$\mathrm{Res}_{s=1}\left\langle \widetilde{E}^{'}_{k-\ell}(z,s;\mathbf{1};N)f(z),f(z)\right\rangle_{k,N} = \frac{6}{N\pi}\left(\prod_{p|N}(1-\tfrac{1}{p})\right)\langle f(z),f(z)\rangle_{k,N}$$

and

$$\begin{aligned}
\mathrm{Res}_{s=1}\left(\frac{2\Gamma(s+k-1)}{(4\pi)^{s+k-1}}\mathcal{D}(f,f,s+k-1)\right) &= \frac{2\Gamma(k)}{(4\pi)^k}\mathrm{Res}_{s=1}\mathcal{D}(f,f,s+k-1) \\
&= \frac{2\Gamma(k)}{(4\pi)^k}\prod_{p|N}(1-\frac{1}{p})\left(\sum_{n=0}^{\infty}\frac{a_{n^2}}{n^k}\right)\mathrm{Res}_{s=1}\zeta(s) \\
&= \frac{2(k-1)!}{(4\pi)^k}\prod_{p|N}(1-\frac{1}{p})\left(\sum_{n=0}^{\infty}\frac{a_{n^2}}{n^k}\right).
\end{aligned}$$

So we have obtained the formula (39). ■

Remark 23. *The series* $\sum_{n=0}^{\infty} \frac{a_{n^2}}{n^k}$ *in the formulas (37) and (39) does not converge fast. However, there are faster methods to compute numerically the norm of a modular form. For example, let* $f \in \mathcal{S}_k(SL_2(\mathbb{Z}))$ *be a normalised Hecke eigenform. Then*

$$\langle f, f\rangle_k = \frac{2}{\pi}\frac{(k-1)!}{(4\pi)^k}\sum_{n\geqslant 1}\frac{A(n)}{n^k}$$

where $A(n) = \sum_{m|n}(-1)^{\Omega(m)}m^{k-1}(a_{n/m})^2$ *while* $\Omega(m)$ *is the number of prime divisors of* m *counted with multiplicity. For more details, see [4].*

As a second application of the Rankin-Selberg method, we give an estimate for $\sum_{p\nmid N}\frac{|a_p|^2}{p^s}$.

Theorem 24. *Let* $f \in \mathcal{S}_k(\Gamma_0(N), \chi)$. *Suppose* f *is an normalized eigenform for the* T_p *operator with* $p \nmid N$. *Then the series* $\sum_{p\nmid N}\frac{|a_p|^2}{p^s}$ *converges for all* $\mathcal{R}(s) > k$ *and we have:*

$$\sum_{p\nmid N}\frac{|a_p|^2}{p^s} \leqslant log\left(\frac{1}{s-k}\right) + O(1) \quad \text{as } s \to k^+. \tag{40}$$

To prove this theorem, we need two preliminary results:

Theorem 25.

$$\sum_p p^{-s} \leqslant log\left(\frac{1}{s-1}\right) + O(1) \quad \text{as } s \to 1^+. \tag{41}$$

Proof: Recall that the zeta function $\zeta(s) = \prod_p (1-p^{-s})^{-1}$ has a simple pole at $s = 1$. Taking logarithms of both sides and using the Taylor expansion for the logarithms, we obtain:

$$\begin{aligned}
\log\zeta(s) &= \sum_p -\log(1-p^{-s}) \\
&= \sum_p \sum_{m=1}^{\infty} \frac{p^{-ms}}{m} \\
&= \sum_{m=1}^{\infty} \sum_p \frac{p^{-ms}}{m} \\
&= \sum_{m=1}^{\infty} g_m(s)
\end{aligned}$$

where $g_m(s) = \sum_p \frac{p^{-ms}}{m}$. Notice that $g_1(s) = \sum_p p^{-s}$. We know that the residue of $\zeta(s)$ at s=1 is equal to 1:

$$\mathrm{Res}_{s=1}\zeta(s) = 1$$

or equivalently

$$\lim_{s\to 1}(s-1)\zeta(s) = 1\ .$$

Taking logarithm gives:

$$\lim_{s\to 1^+}[\log(s-1) + \log\zeta(s)] = 0.$$

We claim that the series $\sum_{m=2}^{\infty} g_m(s)$ converges for $s = 1$. Indeed,

$$\begin{aligned}
\sum_{m=2}^{\infty} g_m(s) &= \sum_p \sum_{m=2}^{\infty} \frac{p^{-ms}}{m} \\
&= \sum_p \sum_{n=1}^{\infty} \left(\frac{p^{-2ns}}{2n} + \frac{p^{-(2n+1)s}}{2n+1}\right) \\
&\leqslant \sum_p \sum_{n=1}^{\infty} \left(\frac{p^{-2ns}}{2n} + \frac{p^{-2ns}}{2n}\right) \\
&\leqslant \sum_p \sum_{n=1}^{\infty} \frac{p^{-2ns}}{n} \\
&= \log\zeta(2s).
\end{aligned}$$

Then

$$\sum_p p^{-s} + \sum_{m=2}^{\infty} g_m(s) = \log\zeta(s) = \log\frac{1}{s-1}.$$

This completes the proof. ■

Proof of the theorem [24]: Using Deligne's inequality, i.e. $|a_n| \leqslant Cn^{\frac{k-1}{2}}$. We see that the series $\sum_{n=1}^{\infty} \frac{|a_n|^2}{n^s}$ converges for $\mathcal{R}(s) > \frac{k+1}{2}$. Denote $\alpha_{p,1}$ and $\alpha_{p,2}$ for the roots of $x^2 - a_p x - \chi(p)p^{k-1}$. Consider

$$L_N(f\otimes f^*, s) = \prod_{p\nmid N} L_p(f\otimes f^*, s) \tag{42}$$

where

$$L_p(f\otimes f^*, s) = \prod_{i,j=1}^{2}(1-\alpha_{p,i}\overline{\alpha_{p,j}}p^{-s})^{-1}.$$

Recall that $D_N(f, f^*, s) = \sum_{(n,N)=1} \frac{|a_n|^2}{n^s}$. Then

$$L_N(f\otimes f^*, s) = D_N(f, f^*, s)\zeta_N(2s+2-2k)$$

where
$$\zeta_N(s) = \prod_{p\nmid N}(1-p^{-s})^{-1}.$$

Then
$$L_N(f\otimes f^*, s) = H(s)D(f, f^*, s)\zeta(2s+2-2k)$$
where $H(s) = \prod_{p\nmid N}\Big((1-p^{-2s+2k-2})(1-|a_p^2|p^{-s})\Big)$. We claim that $H(s)\neq 0$ in the half plane $\mathcal{R}(s)\geqslant k$:
For any $p|N$, one has $a_{p^m} = a_p^m$ for any $m\in\mathbb{N}$. By the Deligne's inequality, one has $|a_{p^m}|\leqslant C(p^m)^{\frac{k-1}{2}}$. Therefore $|a_p|\leqslant C^{\frac{1}{m}}p^{\frac{k-1}{2}}$. Taking limit $m\to\infty$, we get $|a_p|\leqslant p^{\frac{k-1}{2}} < p^k$. Then for $\mathcal{R}(s)\geqslant k$, $1-|a_p^2|p^{-s}\neq 0$, and so $H(s)\neq 0$ in the half plane $\mathcal{R}(s)\geqslant k$.

Since $\langle f, f^*\rangle\neq 0$, by the corollary [2], we see that $L(f\otimes f^*, s) = D(f, f^*, s)\zeta(2s+2-2k)$ extends to a meromorphic function with a unique simple pole at $s=k$. We conclude that $L_N(f\otimes f^*, s) = H(s)L(f\otimes f^*, s)$ is holomorphic for $\mathcal{R}(s)\geqslant k$ and has a unique simple pole at $s=k$.

We have $\lim_{s\to k}(s-k)L_N(f\otimes f^*, s) = O(1)$. Hence:
$$\lim_{s\to k^+}\log(s-k) + \lim_{s\to k^+}\log L_N(f\otimes f^*, s) = O(1).$$

Taking logarithm of both sides of the formula (42) gives:
$$\begin{aligned}
\log L_N(f\otimes f^*, s) &= -\sum_{p\nmid N}\left[\sum_{i,j=1}^{2}\log(1-\alpha_{p,i}\overline{\alpha_{p,j}}p^{-s})\right]\\
&= \sum_{p\nmid N}\sum_{m=1}^{\infty}\left(\frac{(\alpha_{p,1}\overline{\alpha_{p,1}})^m}{mp^{ms}}+\frac{(\alpha_{p,1}\overline{\alpha_{p,2}})^m}{mp^{ms}}+\frac{(\alpha_{p,2}\overline{\alpha_{p,1}})^m}{mp^{ms}}+\frac{(\alpha_{p,2}\overline{\alpha_{p,2}})^m}{mp^{ms}}\right)\\
&= \sum_{p\nmid N}\left(\sum_{m=1}^{\infty}\frac{(\alpha_{p,1}^m+\alpha_{p,2}^m)(\overline{\alpha_{p,1}}^m+\overline{\alpha_{p,2}}^m)}{mp^{ms}}\right)\\
&= \sum_{m=1}^{\infty}\left(\sum_{p\nmid N}\frac{(\alpha_{p,1}^m+\alpha_{p,2}^m)(\overline{\alpha_{p,1}}^m+\overline{\alpha_{p,2}}^m)}{mp^{ms}}\right)\\
&= \sum_{m=1}^{\infty}g_m(s)
\end{aligned}$$

where $g_m(s) = \sum_{p\nmid N}\frac{(\alpha_{p,1}^m+\alpha_{p,2}^m)(\overline{\alpha_{p,1}}^m+\overline{\alpha_{p,2}}^m)}{mp^{ms}}$. Remark that
$$g_1(s) = \sum_{p\nmid N}\frac{(\alpha_{p,1}+\alpha_{p,2})(\overline{\alpha_{p,1}}+\overline{\alpha_{p,2}})}{p^s} = \sum_{p\nmid N}\frac{|\alpha_{p,1}+\alpha_{p,2}|^2}{p^s} = \sum_{p\nmid N}\frac{|a_p|^2}{p^s}\ .$$

It follows that

$$g_1(s) \leqslant \sum_{m=1}^{\infty} g_m(s) = L_N(f \otimes f^*, s).$$

Taking limit $s \to k^+$ gets:

$$g_1(s) = \lim_{s \to k^+} \sum_{p \nmid N} \frac{|a_p|^2}{p^s} \leqslant \log\left(\frac{1}{s-k}\right).$$

This completes the proof. ■

The theorem above suggests us to give the following definition:

Definition 26. *Let $\mathcal{P}$ be the set of natural primes and let $X \subseteq \mathcal{P}$. Define the **superior density of** X to be*

$$dens.sup(X) = \limsup_{s \to 1^+} \frac{\sum_{p \in X} p^{-s}}{log \frac{1}{s-1}}.$$

Remark 27. *Let $X \subset \mathcal{P}$ be a subset of natural primes such that $dens.sup(X)$ exists. Since $\sum_{p \in \mathcal{P}} p^{-s} \leqslant log\left(\frac{1}{s-1}\right) + O(1)$ as $s \to 1^+$, we have $dens.sup(X) \in [0,1]$.*

Remark 28. *Let $X \subset \mathcal{P}$ be a finite subset of primes. Then $dens.sup(X) = 0$. But the converse is not true. For example, assume $X = \{p_1, p_2, p_3, ...\}$ is any ordered subset of primes such that $2p_i < p_{i+1}$ for any $i \geqslant 1$. Then*

$$\sum_{i=1}^{\infty} p_i^{-s} < p_1^{-s} \sum_{i=1}^{\infty} 2^{-(i-1)s} = 2p_1^{-s}.$$

Therefore $dens.sup(X)$=0.

Remark 29. ***(Dirichlet's Theorem on Primes in Arithmetic Progressions)*** *Let m be a positive integer and a be an integer for which $gcd(m,a) = 1$. If X=$\{p \in \mathcal{P} : p \equiv a \bmod m\}$, then $dens.sup(X) = \frac{1}{\varphi(m)}$ where φ is the Euler totient function, i.e. $\varphi(m)$ is the number of integers k in the range $1 \leqslant k \leqslant n$ for which $gcd(n,k) = 1$.*

In particular, there are infinitely many primes p satisfying $p \equiv a \bmod m$.

Proposition 30. *Let $f \in \mathcal{S}_1(\Gamma_0(N), \chi)$ be a normalized newform. Then for each $\eta > 0$, there exists sets $X_\eta, Y_\eta \in \mathbb{C}$ such that:*
- $|Y_\eta| < \infty$
- $dens.sup(X) \leqslant \eta$
- $a_p \in Y_\eta$ if $p \notin X_\eta$.

We need the following result in order to prove the proposition above.

Proposition 31. *Let $f = \sum_{n \geqslant 1} a_n q^n \in \mathcal{M}_k(\Gamma_0(N), \chi)$ be a normalised newform. Then*

1. The field $K = \mathbb{Q}(a_n : n \in \mathbb{N})$ is a finite extension of $\mathbb{Q}$ and each a_n is an algebraic integer.

2. For any embedding $\sigma : K_f \hookrightarrow \mathbb{C}$, we have

$$\sigma(f) := \sum \sigma(a_n) q^n \in \mathcal{M}_k(\Gamma_0(N), \chi \circ \sigma).$$

Proof: See [16]. ■

Proof of the proposition 30: Let $K = \mathbb{Q}(a_1, a_2, ...)$ be the number field containing all fourier coefficients of f. Fix $c > 0$ and let

$$Y(c) := \left\{ \alpha \in \mathcal{O}_K : |\sigma(\alpha)|^2 < c \text{ for all } \sigma \in \mathrm{Hom}(K, \mathbb{C}) \right\}.$$

We claim that the set $Y(c)$ is finite: Let $x \in \mathcal{O}_K$ with minimal polynomial of degree m over $\mathbb{Z}$:

$$X^m + b_{m-1} X^{m-1} + ... + b_0 \quad , b_i \in \mathbb{Z}.$$

The j-th coefficient b_j can be given by

$$b_j = \sum_{\substack{i_1, ..., i_{m-j} \\ i_k \neq i_l \text{ for } k \neq l}} \sigma_{i_1}(a) ... \sigma_{i_{m-j}}(a)$$

and therefore one has:

$$|b_j| \leqslant \sum_{\substack{i_1, ..., i_{m-j} \\ i_k \neq i_l \text{ for } k \neq l}} |\sigma_{i_1}(a)| ... |\sigma_{i_{m-j}}(a)| \leqslant \binom{m}{m-j} \sqrt{c}.$$

Since the coefficients b_j are integers, this means that the minimal polynomials of the elements of $Y(c)$ are just a finite number. Therefore $Y(c)$ must be finite.
Now set

$$X(c) = \{ p \in \mathcal{P} : a_p \notin Y(c) \}.$$

By proposition (31), for each embedding $\sigma : K \to \mathbb{C}$, $\sigma(f) = \sum_{n=1}^{\infty} \sigma(a_n) q^n$ is a normalised newform which lies in $\mathcal{S}_k(\Gamma_0(N), \chi \circ \sigma)$. Applying the theorem 24 to $\sigma(f)$ gives:

$$\sum_{p \nmid N} \frac{|\sigma(a_p)|^2}{p^s} \leqslant \log \left(\frac{1}{s-1} \right) + O(1).$$

Doing summation over all embeddings $\sigma : K \to \mathbb{C}$ gives:

$$\sum_{\sigma \in \mathrm{Hom}(K, \mathbb{C})} \left(\sum_{p \nmid N} \frac{|\sigma(a_p)|^2}{p^s} \right) \leqslant [K : \mathbb{Q}] \log \left(\frac{1}{s-1} \right) + O(1).$$

For any $p \in X(c)$, there is an embedding σ such that $|\sigma(a_p)|^2 \geqslant c$, so $\sum_{\sigma \in \mathrm{Hom}(K,\mathbb{C})} |\sigma(a_p)|^2 \geqslant c$. It follows

$$\begin{aligned} c \sum_{p \in X(c)} p^{-s} &\leqslant \sum_{p \in X(c)} \left(\sum_{\sigma \in \mathrm{Hom}(K,\mathbb{C})} |\sigma(a_p)|^2 \right) p^{-s} \\ &\leqslant [K:\mathbb{Q}] \log \left(\frac{1}{s-1} \right) + O(1) \end{aligned}$$

and so dens.sup$(X(c)) \leqslant \dfrac{[K:\mathbb{Q}]}{c}$. It follows that if $\eta \geqslant \dfrac{[K:\mathbb{Q}]}{c}$, then $X_\eta = X(c)$ and $Y_\eta = Y(c)$ satisfy the necessary conditions of the proposition and we are done. ■

3 Artin representations attached to modular forms of weight 1

3.1 The Deligne-Serre theorem

There is a correspondence between the modular forms of weight 1 and certain representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ in $\mathrm{GL}_2(\mathbb{C})$. The existence of this correspondence is conjectured by Langlands and then constructed by Serre and Deligne.

Theorem 32. ***(Deligne-Serre)*** *Given a normalised eigenform $f = \sum_{n=1}^{\infty} a_n n^{-s} \in \mathcal{S}_1(\Gamma_0(N), \chi)$ with χ an odd character mod N, there exists a continuous Galois representation $\rho_f : G_{\mathbb{Q}} \to GL_2(\mathbb{C})$ with the property that*

$$char(\rho_f(Frob_p)) = X^2 - a_p X + \chi(p) \quad \textit{for all } p \nmid N \quad .$$

In addition, ρ_f is irreducible if and only if f is a cusp form.

Assuming the theorem, we can restrict the image of ρ_f by conjugating it.

Lemma 33. *Let $K_f = \mathbb{Q}(a_1, a_2, ...)$ be the number field generated by the Fourier coefficients of f. If the Deligne-Serre representation ρ_f exists, then it is realisable over K_f, i.e. one can conjugate it in such a way that it takes values on $GL_2(K_f)$.*

Proof: Let $C \in G_{\mathbb{Q}}$ be the complex conjugation. As the order of C is two, i.e $C \circ C = 1$, the eigenvalues of $\rho_f(C)$ are 1 or/and -1. Let φ_N be the mod N cyclotomic character. By the isomorphism $\mathrm{Gal}(\mathbb{Q}(\xi_N)/\mathbb{Q})$ with $(\mathbb{Z}/N\mathbb{Z})^*$, we can consider $\varphi_N : G_{\mathbb{Q}} \to (\mathbb{Z}/N\mathbb{Z})^* \cong \mathrm{Gal}(\mathbb{Q}(\xi_N)/\mathbb{Q})$ which takes $g \in G_{\mathbb{Q}}$ to the automorphism induced by g on the Nth cyclotomic extension $\mathbb{Q}(\xi_N)$ of $\mathbb{Q}$. We can compose two maps φ_N and χ:

$$G_{\mathbb{Q}} \xrightarrow{\varphi_N} (\mathbb{Z}/N\mathbb{Z})^* \xrightarrow{\chi} \mathbb{C}^*.$$

We abuse the language and use χ in place of $\varphi_N \circ \chi$ and call it *Galois character*. Consider $\det \rho_f : G_{\mathbb{Q}} \to \mathbb{C}^*$. By the Deligne-Serre theorem, we have $\det(\rho_f) = \chi$. Hence

$$\det(\rho_f)(C) = \chi(-1) = -1$$

since χ is an odd character (in fact, if we had $\chi(1) = 1$, then $f = 0$). So the two eigenvalues of $\det(\rho_f)$ are 1 and -1. So we may assume, by conjugating if necessary, that

$$\rho_f(C) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Write

$$\rho_f(\sigma) = \begin{pmatrix} a(\sigma) & b(\sigma) \\ c(\sigma) & d(\sigma) \end{pmatrix} \quad \text{for } \sigma \in G_{\mathbb{Q}}$$

where $a, b, c, d : G_{\mathbb{Q}} \to \mathbb{C}$ such that $a(C) = 1,\ b(C) = c(C) = 0,\ d(C) = -1$.

We claim that $a(\sigma), d(\sigma) \in K_f$ for all $\sigma \in G_{\mathbb{Q}}$. In fact by the theorem of Deligne-Serre we have $\mathrm{Tr}(\sigma) = a(\sigma) + d(\sigma) \in K_f$ for all $\sigma \in G_{\mathbb{Q}}$. On the other hand

$$\begin{pmatrix} a(\sigma) & b(\sigma) \\ c(\sigma) & d(\sigma) \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} a(\sigma) & -b(\sigma) \\ c(\sigma) & -d(\sigma) \end{pmatrix} \in G_{\mathbb{Q}}.$$

Thus $a(\sigma) - d(\sigma) \in K_f$ for all $\sigma \in G_{\mathbb{Q}}$. Hence $a(\sigma), d(\sigma) \in K_f$.
Consider

$$\begin{pmatrix} a(\sigma) & b(\sigma) \\ c(\sigma) & d(\sigma) \end{pmatrix} \begin{pmatrix} a(\tau) & b(\tau) \\ c(\tau) & d(\tau) \end{pmatrix} = \begin{pmatrix} a(\sigma)a(\tau) + b(\sigma)c(\tau) & \cdot \\ \cdot & \cdot \end{pmatrix}.$$

This implies $a(\sigma)a(\tau) + b(\sigma)c(\tau) \in K_f$. Therefore $b(\sigma)c(\tau) \in K_f$ for all $\sigma, \tau \in G_{\mathbb{Q}}$. There are two possible cases for $c : G_{\mathbb{Q}} \to \mathbb{C}$.

Case 1: c is identically zero: In this case, ρ_f is reducible hence by semi-simplicity $\rho_f = \chi_1 \bigoplus \chi_2$ where χ_1, χ_2 are one-dimensional representations. We can write:

$$\rho_f = \begin{pmatrix} \chi_1 & 0 \\ 0 & \chi_2 \end{pmatrix}.$$

Hence the image of ρ_f is in $\mathrm{GL}_2(K_f)$ in this case.

Case 2: $c \neq 0$: There exists σ_0 such that $\rho_f(\sigma_0) = \begin{pmatrix} a(\sigma_0) & b(\sigma_0) \\ c(\sigma_0) & d(\sigma_0) \end{pmatrix}$ with $c(\sigma_0) \neq 0$. Let $\lambda \in \mathbb{C}$ be such that $\lambda^2 = c(\sigma_0)$. We can conjugate $\rho_f(\sigma_0)$ by A=$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$ and get $A\rho_f(\sigma_0)A^{-1} = \begin{pmatrix} a(\sigma_0) & b(\sigma_0)c(\sigma_0) \\ 1 & d(\sigma_0) \end{pmatrix}$. Since $b(\sigma)c(\tau) \in K_f$, for $\tau = \sigma_0$ we get $b(\sigma) \in K_f$ for any $\sigma \in G_{\mathbb{Q}}$.

Consider the function $b : G_{\mathbb{Q}} \to \mathbb{C}$. If b is identically zero, then ρ_f will be reducible and like before, we have the result in this case. So assume $b \neq 0$ therefore there exists σ' such that $b(\sigma') \neq 0$, then $b(\sigma') \in K_f^*$. As $b(\sigma)c(\tau) \in K_f$, this implies $c(\tau) \in K_f$ for all $\tau \in G_{\mathbb{Q}}$. ■

Proposition 34. *Let $\rho : G_{\mathbb{Q}} \to GL_d(K)$ be a Galois representation where K is a number field. Then ρ is similar to a Galois representation $\rho' : G_{\mathbb{Q}} \to GL_d(\mathcal{O}_K)$, i.e. it can be conjugated in such a way that it takes values on $GL_d(\mathcal{O}_K)$.*

Proof: For a proof, See [6] Proposition 9.3.5 . ■

As a consequence, if we have a Deligne-Serre representation ρ_f, we can conjugate it so that

$$\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathcal{O}_{K_f}).$$

3.2 The proof of the Deligne-Serre theorem

The steps of the proof of Deligne-Serre's theorem are as follows. Our purpose is to construct a representation with $\mathrm{Tr}(\mathrm{Frob}_p) = a_p$ and $\det(\mathrm{Frob}_p) = \chi(p)$.

Step 1: Starting with a modular form f of weight 1, we may multiply it with a certain Eisenstein series E of weight $\geqslant 1$, whose q-expansion is congruent to 1 modulo ℓ. So we obtain a modular form $E.f$ of weight $\geqslant 2$ whose q-expansion is congruent to that of f modulo ℓ. The representations attached to eigenforms of weight $\geqslant 2$ are pretty well understood and arise from the ℓ-adic representations. They may be reduced modulo ℓ to obtain representations in $\mathrm{Gl}_2(\mathbb{F}_\ell)$. We construct a representation $\overline{\rho}_\lambda : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_\ell)$ attached to $E.f$ (where λ is a prime above ℓ) satisfying $\mathrm{Tr}(\mathrm{Frob}_p) = a_p \bmod \ell$ and $\det(\mathrm{Frob}_p) = \chi(p) \bmod \ell$. We can do this step for almost all primes ℓ.

Step 2: We use an analytic result of Rankin to show that the a_p's are finite in number if we exclude a set of primes p of small density. Then we can get a uniform bound (independent of ℓ on the image of $\overline{\rho}_\ell$.)

Step 3: We glue the $\overline{\rho}_\lambda$'s to obtain a preresentation ρ into $\mathrm{GL}_2(\mathcal{O}_L)$ for some ring of integers $\mathcal{O}_L$ which would reduce to $\overline{\rho}_\lambda$ for infinitely many ℓ. This is possible thanks to the bound on the image of $\overline{\rho}_\lambda$ obtained in the third step. The representation ρ has the desired properties.

3.2.1 Step 1: Construction ℓ-adic representations $\overline{\rho}_\lambda : G_{\mathbb{Q}} \to \mathbf{GL}_2(\mathbb{F}_\ell)$

Theorem 35. *Let $0 \neq f \in M_k(\Gamma_0(N), \chi)$ with $k \geqslant 2$. Suppose that f is a normalised eigenform for all T_p with $p \nmid N$. Let K be a number field which contains all the a_p and all the $\chi(p)$. Let λ be a finite place of K of residual characteristic ℓ and let K_λ be the completion of K with respect to it. Then there exists a semi- simple Galois representation*

$$\rho_\lambda : G_{\mathbb{Q}} \to GL_2(K_\lambda)$$

which is unramified at all primes that don't divide Nl and such that:

$$\begin{aligned} Tr(Frob_p) &= a_p \\ det(Frob_p) &= \chi(p)p^{k-1} \quad \text{if } p \nmid Nl. \end{aligned}$$

After the lemma below, such a representation is unique up to isomorphism.

Lemma 36. *Let ρ, ρ' : $G_{\mathbb{Q}} \to GL_2(\mathbb{C})$ be two Galois representations and X be a subset of rational prime numbers with density 1. Assume that for all $p \in X$, we have $char(\rho(Frob_p)) = char(\rho'(Frob_p))$. Then $\rho = \rho'$.*

Proof: See [7].■

Remark 37. *If f is an Eisenstein series, the attached representation to it is the direct sum of two 1-dimensional representations and is therefore reducible. We show how one can construct this representation. Let $N \in \mathbb{N}$ and let ψ and φ be primitive characters modulo u and v respectively such that $(\psi\varphi)(-1) = -1$ and $uv|N$. Set*

$$E_1^{\psi,\varphi}(z) := \delta(\varphi)L(\psi, 0) + \delta(\psi)L(\varphi, 0) + 2\sum_{n=1}^{\infty} \sigma_0^{\psi,\varphi}(n)q^n$$

where $q = e^{2\pi iz}$, $\delta(\varphi) = 1$ *iff* $\varphi = \mathbf{1}$ *and* 0 *otherwise, while* $\sigma_0^{\psi,\varphi} = \sum_{\substack{m|n \\ m>0}} \psi(\frac{n}{m})\varphi(m)$ *and* $L(\varphi, s)$ *(resp.* $L(\psi, s)$*) is the function associated to* φ *(resp.* ψ*). Set* $\chi = \psi\varphi$ *which is a character modulo* N*. Consider* ψ *and* φ *as characters of* $G_{\mathbb{Q}}$*. Then the representation*

$$\begin{aligned} \rho: \ G_{\mathbb{Q}} &\to \ GL_2(\mathbb{C}) \\ \sigma &\mapsto \begin{pmatrix} \psi(\sigma) & 0 \\ 0 & \varphi(\sigma) \end{pmatrix} \end{aligned}$$

is reducible with the desired properties.(see [6] and [7])

In the theorem above, the weight of modular form f is assumed to be $\geqslant 2$, so for the case weight 1, we will need a different construction.

From here to the end of the theorem 39, assume that $K \subseteq \mathbb{C}$ is the number field containing all the coefficients of f, λ is a finite place of K, $\mathcal{O}_\lambda$ is its valuation ring and m_λ its maximal ideal. Furthermore, $k_\lambda = \mathcal{O}_\lambda/m_\lambda$ is the residue field and l its characteristic.

Definition 38. *Let* $K \subset \mathbb{C}$ *be a number field,* λ *a finite place of* K*,* $\mathcal{O}_\lambda$ *is the valuation ring and* m_λ *its maximal ideal. Furthermore,* $k_\lambda = \mathcal{O}_\lambda/m_\lambda$ *is the residue field and* ℓ *is its characteristic.*

Let $f \in M_k(N, \chi)$*,* $k \geqslant 1$*. We say that* f *is* λ*-integral (resp. that* $f \equiv 0$ *mod* m_λ*) if all the coefficients of* f *lie in* $\mathcal{O}_\lambda$ *(resp. in* m_λ*).*

If f *is* λ*-integral, we say that* f *is an eigenform mod* m_λ *of the Hecke operator* T_p *with eigenvalue* $a_p \in k_f$ *if*

$$T_p f \equiv a_p f \quad mod\ m_\lambda.$$

Theorem 39. *Let* $0 \neq f \in M_k(\Gamma_0(N), \chi)$ *with* $k \geqslant 1$ *with Fourier coefficients in* K*. Suppose that* f *is* λ*-integral but* $f \not\equiv 0$ *mod* m_λ *and that* f *is an eigenform of* T_p *modulo* m_λ *for* $p \nmid N$*:*

$$T_p(f) \equiv a_p f \quad mod\ m_\lambda \quad for\ all\ p \nmid Nl.$$

Let k_f *be the subextension of* k_λ *generated by the* a_p *and the* $\chi(p)$ *mod* m_λ*. Then there is a semi-simple representation*

$$\rho : G_{\mathbb{Q}} \to GL_2(k_f)$$

unramified outside Nl *such that for all primes* $p \nmid Nl$ *one has:*

$$\begin{aligned} &Tr(Frob_p) = a_p \\ &det(Frob_p) \equiv \chi(p)p^{k-1} \quad mod\ \lambda; \end{aligned} \tag{43}$$

Proof: First, we do three preliminary reductions:

1. Suppose that $(K', \lambda', f', k', \chi', (a'_p))$ is as in the hypothesis of the theorem with $K \subseteq$

K' and $\lambda'|\lambda$. We can reduce to the case where $f \equiv f' \bmod \lambda'$, $\chi = \chi'$ and $k \equiv k' \bmod (l-1)$: In fact, if $a_p \equiv a'_p \bmod m_{\lambda'}$ and $\chi(p)p^{k-1} \equiv \chi'(p)p^{k'-1} \bmod m_{\lambda'}$ for all $p \nmid Nl$, then the theorem holds for f if and only if it holds for f'.

2. Reduction to the case $k \geqslant 2$:
Fix a prime $\lambda \lhd \mathcal{O}_K$ and let ℓ be the prime dividing $\mathrm{Norm}_{\mathbb{Q}}^{K}(\lambda)$ (in fact, $\mathrm{Norm}_{\mathbb{Q}}^{K}(\lambda) = \ell^{f(K|\mathbb{Q})}$). Consider the Eisenstein series $E_{\ell-1}$ of weight $\ell - 1$ where $\ell \geqslant 5$. Its Fourier expansion is given by

$$E_{\ell-1} = 1 - \frac{2(\ell-1)}{B_{\ell-1}} \sum_{n=1}^{\infty} \sigma_{\ell-2}(n) q^n$$

where B_n is the nth Bernoulli number, is given by

$$\frac{x}{e^x - 1} = \sum_{n \geqslant 1} B_n \frac{x^n}{n!}.$$

Proposition 40. ***(CLAUSEN-VON STAUDT)*** *The denominator of* $\frac{B_n}{2^n}$ *is* $\prod_{p-1|n} p^{1+v_p(n)}$.
In particular, if ℓ *is a prime, then* $\frac{B_k}{2k}$ *is integral at* ℓ *if and only if* $(\ell-1) \nmid k$.

Proof: See [1] .■

The result above implies that the Eisenstein series $E_{\ell-1}(q)$ has Fourier coefficients in $\mathbb{Z}_{(\ell)}$(the localization of $\mathbb{Z}$ at ℓ) and

$$E_{\ell-1}(q) \equiv 1 \pmod{\ell} .$$

Since λ is a prime ideal of $\mathcal{O}_K$ above ℓ, we see that:

$$E_{\ell-1} \equiv 1 \mod \ell \Rightarrow E_{\ell-1} \equiv 1 \mod \lambda .$$

Hence $F_\lambda := f E_{\ell-1} \equiv f \bmod \lambda$. The modular form $F_\lambda = f E_{\ell-1}$ lies in $\mathcal{M}_{k+\ell-1}(\Gamma_0(N), \chi)$. Thus the theorem for f is equivalent to the theorem for F_λ which has weight $\geqslant 2$.

3. Reduction to the case where f is an eigenvector of T_p: It is enough to verify the theorem for f' eigenform of T_p's with $p \nmid Nl$ such that $(K', \lambda', f', k, \chi, (a'_p))$ is as in the theorem and $K \subseteq K'$, $\lambda'|\lambda$ and $a_p \equiv a'_p \bmod \lambda'$. We give a preliminary lemma.

Lemma 41. *Let* M *be a free module of finite rank over a discrete valuation ring* $\mathcal{O}$. *Let* $m \subseteq \mathcal{O}$ *be the maximal ideal,* k *the residue field and* K *the field of fractions of* $\mathcal{O}$. *Let* $\mathcal{T} \subseteq End_{\mathcal{O}}(K)$ *be a set of endomorphisms which commute two by two. Let* $f \in M/mM$ *be a nonzero common eigenvector for all the* $T \in \mathcal{T}$, *with eigenvalues* a_T. *Then there exists:*
1) a discrete valuation ring $\mathcal{O}' \supseteq \mathcal{O}$ *with maximal ideal* m' *such that* $m' \cap \mathcal{O} = m$ *and with field of fractions* K' *such that* $[K' : K] < \infty$;
2) an element $0 \neq f' \in M' = \mathcal{O}' \otimes_{\mathcal{O}} M$ *which is an eigenvector for all the* $T \in \mathcal{T}$ *with eigenvalues* a'_T *with* $a'_T \equiv a_T \bmod m'$.

Proof: See [7]. ■

We apply the above lemma to $M = \{f \in \mathcal{M}_k(\Gamma_0(N), \chi) |$ f has coefficients in $\mathcal{O}_\lambda\}$ and $\mathcal{T} = \{T_p\}_{p \nmid Nl}$.

Let
$$\rho_\lambda : G_{\mathbb{Q}} \to \mathrm{GL}_2(K_\lambda)$$
be the representation associated to f by the theorem 35. We can assume that $\mathrm{im}(\rho_\lambda) \subseteq \mathrm{GL}_2(\widehat{\mathcal{O}}_\lambda)$ where $\widehat{\mathcal{O}}_\lambda$ is the ring of integers of K_λ or equivalently, the completion of $\mathcal{O}_\lambda$. By reduction mod λ, we get a representation
$$\widetilde{\rho}_\lambda : G_{\mathbb{Q}} \to \mathrm{GL}_2(k_\lambda).$$
Let φ be the semi-simplification of $\widetilde{\rho}_\lambda$; it is a semi-simple representation, unramified outside Nl which satisfies (43). The group $\varphi(G_{\mathbb{Q}})$ is finite. By Chebotarev density theorem, we deduce that every element in $\varphi(G_{\mathbb{Q}})$ is of the form $\varphi(\mathrm{Frob}_{\mathfrak{p}})$ with $\mathfrak{p} \cap \mathbb{Q} = p$ and $p \nmid Nl$. By the definition of k_f, we have:
- For all $g \in \varphi(G_{\mathbb{Q}})$, the coefficients of $\det(1 - gX)$ lie in k_f.

We can now apply the lemma below and conclude the result; *The end of the proof of the theorem 39* . ■

Lemma 42. *Let $\varphi : G \to GL_2(k')$ be a semi-simple representation of the group G over a finite field k'. Let k be a subfield of k' containing all the coefficients of polynomials* $\det(1 - \varphi(g)X)$ *for all $g \in G$. Then φ is realisable over k, i.e. it is isomorphic to a representation $\rho : G \to GL_2(k)$.*

Proof: The proof is essentially the same as the lemma 33. ■

3.2.2 Step 2: A uniform bound on the image of $\overline{\rho}_\lambda$'s

Let
$$\begin{aligned} \sum &= \{\lambda \lhd \mathcal{O}_K : \ \lambda | \ell \text{ and } \ell \text{ splits completely in } K/\mathbb{Q}\} \\ &= \{\lambda \lhd \mathcal{O}_K : \ \mathcal{O}_K/\lambda \cong \mathbb{F}_\ell\}. \end{aligned}$$
By Chebotarev density theorem, $\sum$ is infinite. Now ,for each $\lambda \in \sum$, let ℓ be the rational prime lying below it. Furthermore let
$$G_\lambda := \overline{\rho}_\lambda(G_{\mathbb{Q}}) \subseteq \mathrm{GL}_2(\mathbb{F}_\ell).$$
We wish to bound $|G_\lambda|$ independently of ℓ.

Definition 43. *Fix an integer $X > 0$. A subgroup $G \subseteq GL_2(\mathbb{F}_\ell)$ is X-sparse if there is a subset $H \subseteq G$ such that:*

1. $|H| \geqslant \frac{3}{4}|G|$,

2. *the elements of H have at most X distinct characteristic polynomials.*

Lemma 44. *There exists an $X > 0$ such that all the groups G_λ ($\lambda \in \sum$) are X-sparse.*

Proof: By the proposition 30, for all $\eta > 0$, there exists finite set $X_\eta \subseteq \mathbb{C}$ such that $a_p \in X_\eta$ for all p outside a set Y_η of density η. Take $\eta < \frac{1}{4}$ and set $X = |X_\eta|\mathrm{ord}(\varepsilon)$. We show that G_λ is X-sparse. Let

$$H = \bigcup_{p \notin Y_\eta} \rho(\mathrm{Frob}_p).$$

By Chebotarev density theorem, the inequality $\mathrm{dens}(Y_\eta) > \frac{3}{4}$ implies $|H| \geqslant \frac{3}{4}|G|$. Moreover, the number of distinct characteristic polynomials of elements of H is less that $X = |X_\eta|\mathrm{ord}(\varepsilon)$. ■

Definition 45. *A subgroup G of $GL_2(\mathbb{F}_\ell)$ is semi-simple if the underlying 2 dimensional representation of G is semi-simple, i.e. either irreducible or a direct sum of 1 dimensional representations.*

Example 46. *The groups $SL_2(\mathbb{F}_\ell)$ and $GL_2(\mathbb{F}_\ell)$ are irreducible, hence semi-simple.*

Example 47. *Let $G = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \mid a, b \in \mathbb{F}_\ell^\times \right\}$ the "split Cartan subgroup", then G is semi-simple and reducible.*

Example 48. *Let $\mathbb{F}_{\ell^2}^\times$ act by left multiplication on $\mathbb{F}_{\ell^2}$ viewed as a $\mathbb{F}_\ell$-vector space with any choice of basis. Let G be the image of $\mathbb{F}_{\ell^2}^\times$ in $Aut_{\mathbb{F}_\ell}(\mathbb{F}_{\ell^2}) \cong GL_2(\mathbb{F}_\ell)$ (a "non-split Cartaan subgroup"). Then G is semi-simple.*

Example 49. *If T is a Cartan subgroup, it has index 2 in its normalizer G. Then G is semi-simple.*

Example 50. *The group $G = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid a, d \in \mathbb{F}_\ell^\times,\ b \in \mathbb{F}_\ell \right\}$ is reducible but not decomposable (the subspace $\mathbb{F}_\ell \times O$ is invariant under the action of G but its complement $0 \times \mathbb{F}_\ell$ is not invariant.) Hence G is not semi-simple.*

Theorem 51. *Fix X, there exists a constant A_X (depending on X but not ℓ) such that $|G| < A_X$ for all semi-simple X-sparse subgroups of $GL_2(\mathbb{F}_\ell)$.*

Remark 52. *The semi-simplicity assumption is crucial, for example if we consider*

$$G = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} :\ a \in \mathbb{F}_\ell \right\},$$

then G is 1-sparse but $|G| = \ell$ therefore one cannot bound $|G|$ independently of ℓ.

We give a preliminary proposition before proving the theorem.

Proposition 53. *If G is a semi-simple subgroup of $GL_2(\mathbb{F}_\ell)$ then only the following four cases can arise:*
1. $G \supseteq SL_2(\mathbb{F}_\ell)$
2. G is contained in a Cartan subgroup T, either split or non-split, which means that

$T \simeq \mathbb{F}_\ell^\times \times \mathbb{F}_\ell^\times$ or $T \simeq \mathbb{F}_{\ell^2}^\times$.
3. $G \subset N_{GL_2(\mathbb{F}_\ell)}(T)$ where $N_{GL_2(\mathbb{F}_\ell)}(T)$ is the normaliser of a Cartan subgroup T.
(therefore $[N_{GL_2(\mathbb{F}_\ell)}(T) : T] = 2$ and there exists a split exact sequence:
$1 \to T \to N(T) \to \pm 1 \to 1$.)
4. G is an "exceptional subgroup", namely its image in $PGL_2(\mathbb{F}_\ell)$ is A_4, S_4 or A_5.

Proof: See [14] section 2.5 or [21]. ■

Theorem 54. *If G is a semi-simple X-sparse subgroup of $GL_2(\mathbb{F}_\ell)$, then there exists A independent of ℓ such that $|G| \leqslant A$.*

Proof: By the above proposition, we have to bound $|H|$ by bounding the number of elements in $\mathrm{GL}_2(\mathbb{F}_\ell)$ which have the same characteristic polynomial, i.e. by bounding the number of elements in a given conjugacy class.

We do this in the four cases of the proposition 53.

1. We have $|\mathrm{GL}_2(\mathbb{F}_\ell)| = (\ell^2-1)(\ell^2-\ell) = \ell(\ell+1)(\ell-1)^2$. Let $\sigma \in \mathrm{GL}_2(\mathbb{F}_\ell)$, then the cardinality of the set $C(\sigma) := \left\{\tau\sigma\tau^{-1} :\ \tau \in \mathrm{GL}_2(\mathbb{F}_\ell)\right\}$ is given by $|C(\sigma)| = \frac{|\mathrm{GL}_2(\mathbb{F}_\ell)|}{\mathrm{Z}(\sigma)}$ where $\mathrm{Z}(\sigma) = \{\tau :\ \tau\sigma = \sigma\tau\}$. There are 3 cases to consider for the characteristic polynomial of an element of $\sigma \in H$:

Case 1: $\mathrm{char}(\sigma)$ has two roots in $\mathbb{F}_\ell$, i.e. $\mathrm{char}(\sigma) = (T-a)(T-b)$ where $a \neq b$: We have:

$$\left|\left\{\sigma :\ \mathrm{char}(\sigma) = (T-a)(T-b),\ a, b \in \mathbb{F}_\ell^\times,\ a \neq b\right\}\right| = \left|C(\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix})\right| = \ell^2 + \ell.$$

Case 2: $\mathrm{char}(\sigma)$ has one root in $\mathbb{F}_\ell$, i.e. $\mathrm{char}(\sigma) = (T-a)^2$: This means that

$$\sigma \in C(\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}) \cup C(\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}).$$

Since

$$\left|Z(\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix})\right| = \left|\left\{\begin{pmatrix} u & v \\ 0 & u \end{pmatrix} :\ u \in \mathbb{F}_\ell^\times, v \in \mathbb{F}_\ell\right\}\right| = (\ell-1)\ell,$$

we have that $\sigma \in C(\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}) = \dfrac{\ell(\ell+1)(\ell-1)^2}{\ell^2-\ell} = \ell^2 - 1$. On the other hand, we have $C(\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}) = 1$. So

$$\left|\left\{\sigma :\ \mathrm{char}(\sigma) = (T-a)^2,\ a \in \mathbb{F}_\ell^\times\right\}\right| = \ell^2.$$

Case 3: $\mathrm{char}(\sigma)$ has no root in $\mathbb{F}_\ell$, i.e. $\mathrm{char}(\sigma)$ is irreducible over $\mathbb{F}_\ell$: We have $|Z(\sigma)| = \ell^2 - 1$, so that:

$$|C(\sigma)| = (\ell-1)\ell.$$

Therefore we can deduce:

$$\frac{3}{4}|\mathrm{SL}_2(\mathbb{F}_\ell)| = \frac{3}{4}\ell(\ell+1)(\ell-1) \leqslant |H| \leqslant X.\mathrm{Max}\left\{\ell^2+\ell, \ell^2, \ell^2-\ell\right\} = X(\ell^2+\ell).$$

For the inequalities to hold, we must have $\ell - 1 \leqslant \frac{4}{3}X$. So:

$$|H| \leqslant X(\frac{4}{3}X+1)(\frac{4}{3}X+2).$$

Therefore, we found a bound on H independent of ℓ.

2. In T, there are at most two elements with a given characteristic polynomial, in fact σ and $\overline{\sigma}$ have the same characteristic polynomial. Hence $|H| \leqslant 2X$ and so

$$|G| \leqslant \frac{8}{3}X.$$

3. Let $G_0 = G \cap T$ which has index two in G, so $|G_0| = \frac{1}{2}|G|$ and let $H_0 = H \cap T$ so that $|H_0| \geqslant \frac{1}{2}|G_0|$. We can apply the case 2 and get $|H_0| \leqslant 2X$ so that $|G_0| \leqslant 4X$ which implies

$$|G| \leqslant 8X.$$

4. Consider the following homomorphism of groups:

$$\begin{array}{rll} \eta: & G & \to \mathrm{PGL}_2(\mathbb{F}_\ell) \times \mathbb{F}_\ell^\times \\ & \sigma & \mapsto (\bar{\sigma}, \det(\sigma)). \end{array}$$

We know that the image of G in $\mathrm{PGL}_2(\mathbb{F}_\ell)$ is A_4, S_4 or A_5 and X is the number of different characteristic polynomials in H, therefore $|\eta(H)| \leqslant |A_5|X = 60X$. Since $\ker(\eta) = \left\{ \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix} \right\} \simeq \mathbb{Z}/2\mathbb{Z}$. This implies that $|H| \leqslant 120X$ and then

$$|G| \leqslant 160X.$$

We have concluded the proof of the theorem. ■

3.2.3 Step 3: Gluing the ℓ-adic representations ρ_λ

Fix a constant A such that $|G_\ell| \leqslant A$. Let $K \subset \mathbb{C}$ be a Galois number field containing the a_p and the $\chi(p)$ for all primes p. As before, let

$$\sum = \{\lambda \lhd \mathcal{O}_K : \ \mathcal{O}_K/\lambda \cong \mathbb{F}_\ell\}.$$

For all $\ell \in \sum$, fix a place λ_ℓ of K extending ℓ. By theorem 39, there exists a semi-simple continuous representation

$$\rho_\ell : G_\mathbb{Q} \to \mathrm{GL}_2(\mathbb{F}_\ell)$$

unramified outside of Nl and such that

$$\begin{aligned} \mathrm{char}(\rho_\ell(\mathrm{Frob}_p)) &= \det(\mathrm{Id}_2 - \rho_\ell(\mathrm{Frob}_p)T) \\ &\equiv 1 - a_pT + \chi(p)T^2 \mod \lambda_\ell . \end{aligned}$$

for all primes $p \nmid Nl$.

Up to replacing K with a bigger number field (reducing $\sum$ consequently), we may well suppose that K contains all n-th roots of unity for all $n \leqslant A$. Set

$$Y = \{(1-\alpha T)(1-\beta T) : \ \alpha \text{ and } \beta \text{ are roots of unity of order } \leqslant A\}.$$

The eigenvalues of $\rho_\ell(\mathrm{Frob}_p)$ are root of unity of order $\leqslant A$. Therefore there exist $R(T) \in Y$ such that

$$1 - a_p T + \chi(p) T^2 \equiv R(T) \bmod \lambda_\ell.$$

Since Y is finite and L is infinite, there must exist some $R(T) \in Y$ such that the above congruence is satisfied for an infinite number of ℓ's. This implies that such a congruence is in fact an equality. Thus the polynomials $1 - a_p T + \chi(p)T^2$ all lie in Y. Now let

$$\sum\nolimits' = \{\ell \in L : \ell > A, \ (R, S \in Y, \ R \neq S) \Rightarrow R \not\equiv S \bmod \lambda_\ell\}.$$

Since $\sum \setminus \sum'$ is infinite, $\sum'$ is finite. Choose $\ell \in L'$. It follows that $\gcd(|G_\ell|, \ell) = 1$ and therefore the identical representation $G_\ell \to \mathrm{GL}_2(\mathbb{F}_\ell)$ is the reduction modulo λ_ℓ of a representation $G_\ell \to \mathrm{GL}_2(\mathcal{O}_{\lambda_\ell})$ where $\mathcal{O}_{\lambda_\ell}$ is the valuation ring of λ_ℓ in K, namely we have a commutative diagram

$$\begin{tikzcd} G_\ell \arrow[r] \arrow[dr] & GL_2(\mathcal{O}_{\lambda_\ell}) \arrow[d] \\ & GL_2(\mathbf{F}_\ell) \end{tikzcd}$$

We then compose the representation $G_\ell \to \mathrm{GL}_2(\mathcal{O}_{\lambda_\ell})$ with the projection $G_\mathbb{Q} \to G_\ell$, we get a representation $\rho : G_\mathbb{Q} \to \mathrm{GL}_2(\mathcal{O}_{\lambda_\ell})$ which by construction is unramified outside Nl.

If $p \nmid Nl$, the eigenvalues of $\rho(\mathrm{Frob}_p)$ are roots of unity of order $\leqslant A$, because $\rho(G_\mathbb{Q}) \cong G_\ell$ and $|G_\ell| \leqslant A$. Therefore $\det(Id_2 - \rho(\mathrm{Frob}_p)T) \in Y$. On the other hand, by construction:

$$\det(Id_2 - \rho(\mathrm{Frob}_p)T) \equiv 1 - a_p T + \chi(p)T^2 \bmod \lambda_\ell.$$

Since $1 - a_p T + \chi(p)T^2 \in Y$ and $\ell \in L'$, the last congruence is an equality. Now repeat the same construction by choosing another $\ell' \in L'$. We obtain a second representation $\rho' : G_\mathbb{Q} \to \mathrm{GL}_2(\mathcal{O}_{\lambda_\ell})$ which has the same properties as ρ but for $p \nmid Nl'$. This implies that

$$\det(Id_2 - \rho(\mathrm{Frob}_p)T) = \det(Id_2 - \rho'(\mathrm{Frob}_p)T) \quad \text{for all } p \nmid N\ell\ell'.$$

By theorem 36, it easily follows that ρ and ρ' are isomorphic as representation over $\mathrm{GL}_2(K)$ and so they are isomorphic also as complex representations. Moreover, since ρ is unramified at ℓ' and symmetrically ρ' is unramified at ℓ', then both ρ and ρ' are unramified outside N and

$$\det(Id_2 - \rho(\mathrm{Frob}_p)T) = 1 - a_p T + \chi(p)T^2 \quad ,\forall p \nmid N.$$

The last thing to prove is that ρ is irreducible. Suppose that it is not, then there exists two 1-dimensional representations $\chi_1, \chi_2 : G_\mathbb{Q} \to \mathbb{C}^*$ such that $\rho \cong \chi_1 + \chi_2$. It follows that $\chi = \chi_1\chi_2$ and $a_p = \chi_1(p) + \chi_2(p)$ for $p \nmid N$ and both χ_1 and χ_2 are unramified outside N. Then we have:

$$\sum_{p\in\mathcal{P}} |a_p|^2 p^{-s} = 2\sum_{p\in\mathcal{P}} p^{-s} + \sum \chi_1(p)\overline{\chi_2(p)}p^{-s} + \sum_{p\in\mathcal{P}} \overline{\chi_1(p)}\chi_2(p)p^{-s}.$$

We should have $\chi_1\overline{\chi_2} \neq \mathbf{1}$, because otherwise we would have $\chi = \chi_1\chi_2 = \chi_1^2$ and so $\chi(-1) = 1$ but the character χ is supposed to be odd. Therefore, since the character $\chi_1\overline{\chi_2}$ is not trivial, we have:

$$\sum_{p\in\mathcal{P}} \overline{\chi_1}(p)\chi_2(p)p^{-s} = O(1),$$
$$\sum_{p\in\mathcal{P}} \chi_1(p)\overline{\chi_2}(p)p^{-s} = O(1).$$

On the other hand, it is well-known that:

$$\sum_{p\in\mathcal{P}} p^{-s} = \log\left(\frac{1}{s-1}\right) + O(1).$$

We then obtain that

$$\sum_{p\in\mathcal{P}} |a_p|^2 p^{-s} = 2\log\left(\frac{1}{s-1}\right) + O(1)$$

which is in contradiction with the theorem 24 so we get the conclusion. ■

Corollary 3. *Let f be a modular form of weight 1 and character χ. Then for all primes p, the coefficient $a_p(f)$ is a sum of two roots of unity. In particular:*

$$|a_p(f)| \leqslant 2.$$

Proof: By the Deligne-Serre's theorem, $a_p(f)$ is equal to $tr(\mathrm{Frob}_p)$, hence the sum of its two eigenvalues. We saw that the eigenvalues of $\sigma(\mathrm{Frob}_p)$ are roots of unity. The result follows immediately. ■

4 The Birch and Swinnerton-Dyer conjecture and the Rankin-Selberg method

Let K be a number field and let E be an elliptic curve over K. We state the theorem of Mordell-Weil and discuss about the structure of the group of points of E and give the definition of $r_K(E)$, i.e. the rank of E over K. Then we state the Birch and Swinnerton-Dyer conjecture (henceforth abbreviated BSD conjecture). If we assume the BSD conjecture, we can prove a more general form of it, i.e. the twisted BSD conjecture. In the last part of this chapter, we gather some numerical evidence for the twisted BSD.

4.1 The Mordell-Weil theorem and the Birch and Swinnerton-Dyer conjecture

Let K be a number field and let E be an elliptic curve over K. The points of E over K has an abelian group structure denoted $E(K)$. Mordell and Weil proved the important theorem below:

Theorem 55. *The group $E(K)$ is finitely generated.*

Proof: See for example [17]. ■

The Mordell-Weil theorem tells us that the *Mordell-Weil* group $E(K)$ has the form

$$E(K) \cong E(K)_{\text{tors}} \oplus \mathbb{Z}^r$$

where the torsion subgroup $E(K)_{\text{tors}}$ is finite and the *rank* r of $E(K)$ (denoted also by $r_K(E)$) is a nonnegative integer. It is relatively easy to compute the torsion subgroup but there is no known procedure that is guaranteed to yield the rank $r_K(E)$.

The L-series of an elliptic curve is a generating function that records information about the reduction of the curve modulo every prime. Consider an elliptic curve E over $\mathbb{Q}$ with a general Weierstrass equation E defined over $\mathbb{Q}$:

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_1, ...a_6 \in \mathbb{Q}$$

View two integral Weierstrass equations as equivalent if they are related by a *general admissible change of variable* over $\mathbb{Q}$:

$$x = u^2x^{'} + r, \quad y = u^3y' + su^2x^{'} + t \quad u, r, s, r \in \mathbb{Q}, \; u \neq 0.$$

After an admissible change of variable of the form $(x, y) = (u^2x^{'}, u^3y^{'})$ we can assume that the coefficients a_i's are integer. For each prime p, let $v_p(E)$ denote the smallest power of p appearing in the discriminant of any integral Weierstrass equation equivalent to E, i.e. the minimum of a set of nonnegative integers

$$v_p(E) = \min\{v_p(\Delta(E')) : \quad E^{'} \text{ integral, equivalent to } E\}.$$

Define the *global minimal discriminant* of E to be

$$\Delta_{\min}(E) = \prod_p p^{v_p(E)}.$$

This is a finite product since $v_p = 0$ for all $p \nmid \Delta(E)$. One can show that the p-adic valuation of the discriminant can be minimized to $v_p(E)$ simultaneously for all p under an admissible change of variable. That is, E is isomorphic over $\mathbb{Q}$ to an integral model $E^{'}$ with discriminant $\Delta(E^{'}) = \Delta_{\min}(E)$. This is the *global minimal Weierstrass equation* $E^{'}$, the model of E to reduce modulo primes.

Consider the reduction map modulo $p\mathbb{Z}$:

$$\widetilde{\ } : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} = \mathbf{F}_p.$$

This map reduces a global minimal Weierstrass equation E to a Weierstrass equation $\widetilde{E}$ over $\mathbf{F}_p$ and this defines an elliptic curve over $\mathbf{F}_p$ if and only if $p \nmid \Delta_{\min}(E)$. The reduction modulo p is called
1) *good [nonsingular, stable]* if $\widetilde{E}$ is again an elliptic curve,

a) *ordinary* if $\widetilde{E}[p] = \mathbb{Z}/p\mathbb{Z}$,

b) *supersingular* if $\widetilde{E}[p] = \{0\}$,

2) *bad [singular]* if $\widetilde{E}$ is not an elliptic curve, in which case it has only one singular point,

a) *multiplicative [semistable]* if $\widetilde{E}$ has a node,

b) *additive [unstable]* if $\widetilde{E}$ has a cusp.

Define the *algebraic conductor* of E:

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

where

$$f_p = \begin{cases} 0 & \text{if} \quad \text{E has good reduction at p,} \\ 1 & \text{if} \quad \text{E has multiplicative reduction at p} \quad , \\ 2 & \text{if} \quad \text{E has additive reduction at p and} \quad p \nmid \{2,3\}, \\ 2+\delta_p & \text{if} \quad \text{E has additive reduction at p and} \quad p \in \{2,3\}. \end{cases}$$

Here $\delta_2 \leqslant 6$ and $\delta_3 \leqslant 3$. There is also a closed-form formula for f_p. (see [17])

Denote $\widetilde{E}(\mathbf{F}_p)$ the elliptic curve $\widetilde{E}$ over $\mathbf{F}_p$.

Definition 56. *Let E be an elliptic curve over $\mathbb{Q}$. Assume E is in reduced form. Let p be a prime and let $\widetilde{E}$ be the reduction of E modulo p. Then define*

$$\begin{aligned} a_1(E) &= 1 \\ a_p(E) &= p+1-|\widetilde{E}(\boldsymbol{F}_p)|. \end{aligned} \tag{44}$$

The coefficients $a_{p^e}(E)$ *satisfy the same recurrence as the coefficients* $a_{p^e}(f)$ *of a normalised eigenform in* $\mathcal{S}_2(\Gamma_0(N))$ *(see [6] section 8.3):*

$$a_{p^e}(E) = a_p(E)a_{p^{e-1}}(E) - \mathbf{1}_E(p)pa_{p^{e-2}}(E) \quad \text{for all } e \geqslant 2$$

Here $\mathbf{1}_E$ *is the trivial character modulo the algebraic conductor* N_E *of* E*. We extend the definition for all positive integers* m *by setting*

$$a_{mn}(E) = a_m(E)a_n(E) \quad \text{if } (m,n) = 1. \tag{45}$$

Theorem 57. ***(Modularity Theorem, Version*** a_p***)*** *Let* E *be an elliptic curve over* $\mathbb{Q}$ *with conductor* N_E*. Then for some newform* $f \in \mathcal{S}_2(\Gamma_0(N_E))$*,*

$$a_p(f) = a_p(E) \quad \text{for all primes } p.$$

This version of the Modularity theorem rephrases in terms of L-function. Recall that if $f \in \mathcal{S}(\Gamma_0(N))$ is a newform then its L-function is

$$L(f,s) = \sum_{n=1}^{\infty} \frac{a_n(f)}{n^s} = \prod_p \frac{1}{1 - a_p(f)p^{-s} + \mathbf{1}_N(p)p^{1-2s}},$$

with convergence in a right half plane. Define the *Hasse-Weil L-function of E* as:

$$\begin{aligned} L(E,s) &= \sum_{n=1}^{\infty} \frac{a_n(E)}{n^s} \\ &= \prod_p \frac{1}{1 - a_p(E)p^{-s} + \mathbf{1}_E(p)p^{1-2s}} \end{aligned} \tag{46}$$

where $\mathbf{1}_E$ is the trivial character modulo the conductor N_E. This L-function encodes all the solution-counts $a_p(E)$.

Then one can state another version for Modularity theorem:

Theorem 58. ***(Modularity Theorem, Version L)*** *Let* E *be an elliptic curve over* $\mathbb{Q}$ *with conductor* N_E*. Then for some newform* $f \in \mathcal{S}_2(\Gamma_0(N_E))$*,*

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

By Mordell-Weil theorem, we have

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

For a modular form f, one has the half plane convergence, analytic continuation, and functional equation of $L(f,s)$. Using the Modularity Theorem version L, we can also get the half plane convergence of $L(E,s)$ (which is $\mathcal{R}(s) > 2$) and the functional equation that determines $L(E,s)$ for $\mathcal{R}(s) < 0$, but the behaviour of $L(E,s)$ at the center of the remaining strip $\{0 \leqslant \mathcal{R}(s) \leqslant 2\}$ is what conjecturally determines the rank of $E(\mathbb{Q})$. The Weak Birch and Swinnerton-Dyer conjecture says that the rank r is equal to the order of vanishing of $L(E,s)$ at $s = 1$:

Conjecture 59. ***(Weak Birch and Swinnerton-Dyer):*** *Let E be an elliptic curve defined over $\mathbb{Q}$. Then the order of vanishing of $L(E,s)$ at $s=1$ is the rank of $E(\mathbb{Q})$. That is, if $E(\mathbb{Q})$ has rank r then*

$$L(E,s) = (s-1)^r g(s) \quad ; \; g(1) \neq 0, \infty.$$

Now let E/K be an elliptic curve and let $v \in M_K$ be a finite place at which E has good reduction. We denote the residue field of K at v by k_v, the reduction of E at v by $\widetilde{E}_v$ and we let $q_v = ||k_v||$ be the norm of the prime ideal corresponding to v. Put

$$a_v = q_v + 1 - ||\widetilde{E}_v(k_v)|| \tag{47}$$

and

$$L_v(T) = 1 - a_v T + q_v T^2 \;\in \mathbb{Z}[T]. \tag{48}$$

Definition 60. *The L-series of E/K is defined by the Euler product*

$$L(E/K,s) = \prod_{v \in M_K^0} L_v(q_v^{-s})^{-1} \tag{49}$$

where M_K^0 is the nonarchimedean absolute values in K.

The product defining $L(E/K,s)$ converges and gives an analytic function for all $\mathcal{R}(s) > \frac{3}{2}$. Its analytic continuation is conjectured as follows:

Conjecture 61. *The L-series $L(E/K,s)$ has an analytic continuation to the entire complex plane and satisfies a functional equation relating its values at s and $2-s$.*

Deuring and Weil proved this conjecture for elliptic curves having complex multiplication. Eichler and Shimura showed that this conjecture is true for all elliptic curves $E/\mathbb{Q}$ which are modular. Later, Wiles proved that all elliptic curves $E/\mathbb{Q}$ are modular. As a consequence, this conjecture is true for all elliptic curves $E/\mathbb{Q}$.

The *conductor* of E/K is the integral ideal of K defined by

$$N_{E/K} = \prod_{v \in M_K^0} \mathfrak{p}_v^{f_v}$$

where the exponent of the conductor f_v is defined by

$$f_v = \begin{cases} 0 & \text{if} \quad \text{E has good reduction at v} \\ 1 & \text{if} \quad \text{E has multiplicative reduction at v} \\ 2+\delta_v & \text{if} \quad \text{E has additive reduction at v} \end{cases} ,$$

where δ_v is an integer; see [12].

Now we state the BSD conjecture generalised for elliptic curves over any number field K.

Conjecture 62. ***(Birch and Swinnerton-Dyer)*** *Let E be an elliptic curve defined over a number field K. Then the order of vanishing of $L(E/K,s)$ at $s=1$ is the rank of $E(K)$. That is, if $E(K)$ has rank r then*

$$L(E/K,s) = (s-1)^r g(s) \quad ; \; g(1) \neq 0, \infty.$$

4.2 L-functions attached to representations

Assume that K is a number field such that the extension K/Q is Galois and denote $\mathcal{O}_K$ the ring of integers of K. Let p be a a rational prime. The ideal of $\mathcal{O}_K$ generated by p can be factorised as a product of maximal ideals of $\mathcal{O}_K$. In fact, we have:

$$\begin{aligned} p\mathcal{O}_K &= (\mathfrak{p}_1...\mathfrak{p}_g)^e \\ \mathcal{O}_K/\mathfrak{p}_i &\cong \mathbf{K}_{p^f} \quad \text{for } i = 1, ..., g \\ efg &= [\mathbf{K} : \mathbb{Q}]. \end{aligned}$$

e is called the *ramification degree* which says how many times each maximal ideal $\mathfrak{p}$ of $\mathcal{O}_K$ that lies over p repeats as a factor of $p\mathcal{O}_K$. We say that a prime p ramify in K if its ramification degree e is > 1.
The *residue degree* f is the dimension of the *residue field* $k_p = \mathcal{O}_K/\mathfrak{p}$ as a vector space over $\mathbf{F}_p = \mathbb{Z}/p\mathbb{Z}$ for any $\mathfrak{p}$ over p.
The *decomposition index* g is the number of distinct $\mathfrak{p}$ over p.

Example 63. *Let N be a positive integer and let $K = \mathbb{Q}(\mu_N)$ where $\mu_N = e^{2\pi i/N}$. Then $[K : \mathbb{Q}] = \phi(N)$ and the extension $K/\mathbb{Q}$ is Galois with Galois group isomorphic to $(\mathbb{Z}/N\mathbb{Z})^*$. The isomorphism is given by*

$$\begin{gathered} Gal(K/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/N\mathbb{Z})^* \\ (\mu_N \mapsto \mu_N^a) \mapsto a(\ mod\ N). \end{gathered}$$

On can show that cyclotomic integers are $\mathcal{O}_K = \mathbb{Z}[\mu_N]$. A prime p ramifies in K if and only if $p|N$. For a prime $p \nmid N$ one can write $p\mathcal{O}_K = \mathfrak{p}_1...\mathfrak{p}_g$ and its residue degree f is equal to the order of p (mod N) in $(\mathbb{Z}/N\mathbb{Z})^*$.

For each maximal ideal $\mathfrak{p}$ of $\mathcal{O}_F$ lying over p, the **decomposition group** of $\mathfrak{p}$ is the subgroup of the Galois group that fixes $\mathfrak{p}$ as a set

$$\mathcal{D}_\mathfrak{p} = \{\sigma \in \mathrm{Gal}(K/\mathbb{Q}) : \sigma(\mathfrak{p}) = \mathfrak{p}\}.$$

The decomposition group $\mathcal{D}_\mathfrak{p}$ has order ef so $[\mathrm{Gal}(K/\mathbb{Q}) : \mathcal{D}_\mathfrak{p}] = g$. One can define a well-defined action of $\mathcal{D}_\mathfrak{p}$ on $k_\mathfrak{p} = \mathcal{O}_K/\mathfrak{p}$:

$$\begin{aligned} \mathcal{D}_\mathfrak{p} \times k_\mathfrak{p} &\to k_\mathfrak{p} \\ (\sigma, x + \mathfrak{p}) &\mapsto \sigma(x) + \mathfrak{p}, \end{aligned}$$

where $x \in \mathcal{O}_K$. The **inertia group** of $\mathfrak{p}$ is the kernel of the above action:

$$I_\mathfrak{p} = \{\sigma \in \mathrm{Gal}(K/\mathbb{Q}) : \ \sigma(x) \equiv x \text{ for all } x \in \mathcal{O}_K\}.$$

Obviously, $I_\mathfrak{p} \subseteq \mathcal{D}_\mathfrak{p}$. The inertia group $I_\mathfrak{p}$ has order e, so it is trivial for all $\mathfrak{p}$ lying over any unramified p. The kernel of composition map $\mathbb{Z} \to \mathcal{O}_K \to \mathcal{O}_K/\mathfrak{p}$ is $p\mathbb{Z}$. So we can view $\mathbf{F}_p = \mathbb{Z}/p\mathbb{Z}$ as a subfield of $k_\mathfrak{p} = \mathcal{O}_K/\mathfrak{p}$ then there is an injection

$$\mathcal{D}_\mathfrak{p}/I_\mathfrak{p} \to \mathrm{Gal}(k_\mathfrak{p}/\mathbf{F}_p).$$

Since both groups have order f, this map is in fact an isomorphism. Any Galois group of an finite field is cyclic, so the is an element σ_p that generates $\mathrm{Gal}(k_{\mathfrak{p}}/\mathbf{F}_p)$:

$$\mathrm{Gal}(k_{\mathfrak{p}}/\mathbf{F}_p) = \langle \sigma_p \rangle .$$

By isomorphism, the quotient $\mathcal{D}_{\mathfrak{p}}/I_{\mathfrak{p}}$ has a generator that maps to σ_p. Any representative of this generator in $\mathcal{D}_p$ is called a **Frobenius element** of $\mathrm{Gal}(K/\mathbb{Q})$ and denoted $\mathrm{Frob}_{\mathfrak{p}}$. It satisfies:

$$x^{\mathrm{Frob}_{\mathfrak{p}}} \equiv x^p \mod \mathfrak{p} \quad \text{for all } x \in \mathcal{O}_K.$$

When the number field K is Galois over $\mathbb{Q}$, the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ acts transitively on the maximal ideals lying over p, i.e. for any two maximal ideal $\mathfrak{p}$ and $\mathfrak{p}^{'}$, there is an automorphism $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ such that $\sigma(\mathfrak{p}) = \mathfrak{p}^{'}$. Therefore

$$\mathcal{D}_{\sigma(\mathfrak{p})} = \sigma^{-1}\mathcal{D}_{\mathfrak{p}}\sigma, \quad \mathcal{I}_{\sigma(\mathfrak{p})} = \sigma^{-1}\mathcal{I}_{\mathfrak{p}}\sigma.$$

It follows that

$$\mathrm{Frob}_{\sigma(\mathfrak{p})} = \sigma^{-1}\mathrm{Frob}_{\mathfrak{p}}\sigma.$$

In particular, if the Galois group is abelian, then $\mathrm{Frob}_{\mathfrak{p}} = \mathrm{Frob}_{\mathfrak{p}'}$ for any $\mathfrak{p}$ and $\mathfrak{p}^{'}$ primes above p. Hence $\mathrm{Frob}_{\mathfrak{p}}$ ($\mathcal{D}_{\mathfrak{p}}$ and $\mathcal{I}_{\mathfrak{p}}$) for any $\mathfrak{p}$ lying over p can be denoted Frob_p (respectively $\mathcal{D}_p$ and $\mathcal{I}_p$).

Now, consider an artin representation:

$$\rho : G_{\mathbb{Q}} \to \mathrm{GL}(V)$$

where V is a complex vector space of dimension n. Define V^{I_p} to be the subspace of V on which $\rho(I_p)$ acts as the identity. One can see that the characteristic polynomial of $\rho(\mathrm{Frob}_p)|_{V^{I_p}}$ only depends on its conjugacy class. Therefore we can define the *Artin L-function of* (V, ρ) as follows:

$$L(\rho, s) := \prod_p \frac{1}{\det(\mathrm{Id}_n - \rho(\mathrm{Frob}_p)|_{V^{I_p}}.p^{-s})}.$$

Whenever $\rho(I_p) = Id_n$, we say that ρ is *unramified* at p. In this case, $\rho(\mathrm{Frob}_p)|_{V^{I_p}}$ acts on all of V.

For example, if we take $\rho_{\mathrm{triv}} : G_{\mathbb{Q}} \to \mathrm{Aut}(\mathbb{C})$ the trivial representation, then $L(\rho_{\mathrm{triv}}) = \zeta(s)$.
Analogously, we can define an L-function attached to a Galois representation with ℓ-adic coefficients. Assume

$$\rho : G_{\mathbb{Q}} \to \mathrm{GL}(V)$$

where V is a $\mathbb{Q}_\ell$-vector space of dimension n. We need to restrict our attention to ℓ-adic representations where the characteristic polynomial of $\rho(\mathrm{Frob}_p)|_{V^{I_p}}$ has rational coefficients. Then we can define similarly:

$$L(\rho, s) := \prod_p \frac{1}{\det(\mathrm{Id}_n - \rho(\mathrm{Frob}_p)|_{V^{I_p}}.p^{-s})}.$$

4.3 The twisted Birch and Swinnerton-Dyer conjecture

Let E be an elliptic curve over $\mathbb{Q}$ and let τ be a continuous and irreducible complex representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Assume $\ker(\tau) = (\overline{\mathbb{Q}}/K)$ where K is a number field. Let ρ_E denote the 2-dimensional Galois representation of the elliptic curve E, namely, the p-adic Tate module of E.

We shall be interested in the twisted L-function

$$L(E, \tau, s) := L(\rho_E \otimes \tau, s).$$

We give a version of the Birch Swinnerton-Dyer conjecture saying that the order of vanishing of $L(E, \tau, s)$ at $s = 1$ is equal to the multiplicity of τ in the representation of $G_{\mathbb{Q}}$ on $\mathbb{C} \otimes_{\mathbb{Z}} E(K)$. By Mordell-Weil theorem, we have $E(K) \cong E(K)_{\text{tors}} \oplus \mathbb{Z}^r$, therefore:

$$\begin{aligned} \mathbb{C} \otimes_{\mathbb{Z}} E(K) &\cong \mathbb{C} \otimes_{\mathbb{Z}} (E(K)_{\text{tors}} \oplus \mathbb{Z}^r) \\ &\cong (\mathbb{C} \otimes_{\mathbb{Z}} E(K)_{\text{tors}}) \oplus (\mathbb{C} \otimes_{\mathbb{Z}} \mathbb{Z}^r) \\ &\cong \mathbb{C}^r. \end{aligned}$$

For, $E(K)_{\text{tors}}$ is a finite abelian group of the form $\mathbb{Z}/m_1\mathbb{Z} \oplus \mathbb{Z}/m_2\mathbb{Z} \oplus ... \oplus \mathbb{Z}/m_v\mathbb{Z}$ where $m_v|... \; |m_2 \; |m_1$ and for any integer m, we have

$$\mathbb{C} \otimes_{\mathbb{Z}} (\mathbb{Z}/m\mathbb{Z}) \cong (\mathbb{C}/m\mathbb{C}) \otimes_{\mathbb{Z}} \mathbb{Z} \cong \mathbb{C}/m\mathbb{C} \cong 0.$$

There is a natural strengthening of the Birch and Swinnerton-Dyer conjecture as follows:

Conjecture 64. *Assume the Birch Swinnerton-Dyer conjecture. Then*

$$ord_{s=1} L(E, \tau, s) = \langle \tau, \mathbb{C} \otimes_{\mathbb{Z}} E(K) \rangle = \text{multiplicity of } \tau \text{ in } \mathbb{C} \otimes_{\mathbb{Z}} E(K)$$

where K is the finite extension of $\mathbb{Q}$ which is fixed by the kernel of τ.

Proof: See [13] page 127. ■

Remark 65. *If we replace τ by trivial representation, we recover the BSD conjecture:*

$$ord_{s=1} L(E, \mathbf{1}, s) = ord_{s=1} L(E, s) = r_{\mathbb{Q}}(E) \ .$$

In fact, any rational point P is fixed by all elements of $G_{\mathbb{Q}}$. But if $P \notin \mathbb{Q}^2$, then there is an element $\sigma \in G_{\mathbb{Q}}$ such that $\sigma(P) \neq P$. Therefore the multiplicity of trivial representation in $\mathbb{C} \otimes_{\mathbb{Z}} E(K)$ is equal to $r_{\mathbb{Q}}(E)$.

In the next section, using the Deligne-Serre theorem 32, we shall compute and present some numerical evidence for this theorem .

4.4 Some numerical evidence for the generalized BSD conjecture

We saw that the vanishing order of $L(E,\tau,s)$ at $s=1$ is equal to the multiplicity of τ in $\mathbb{C}\otimes_{\mathbb{Z}} E(K)$. In this section, we take for τ the representation arising from a modular form of weight 1. In fact, by the Deligne-Serre theorem 32, for any cusp form $g=\sum_{n=1}^{\infty} b_n q^n \in \mathcal{S}_1(\Gamma_0(N),\chi)$ of weight 1 and character χ, one can associate an odd, continuous and irreducible Galois representation $\rho_g : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{C})$ such that

$$\mathrm{char}(\rho_g(\mathrm{Frob}_p)) = X^2 - b_p X + \chi(p) \quad \text{for any } p \nmid N.$$

Assume $\ker(\rho_g) = \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ where K is a number field. We abuse the notation and denote ρ_g also for the induced representation $\mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{C})$. The conjecture 64 implies:

$$\mathrm{ord}_{s=1} L(E,\rho_g,s) \stackrel{?}{=} \langle \rho_g, \mathbb{C}\otimes E(K)\rangle = \text{ multiplicity of } \rho_g \text{ in } \mathbb{C}\otimes E(K)$$

We aim to compute the constant term of $L(E,\rho_g,s)$ at $s=1$. Thus, if we assume the BSD, we deduce:

$$L(E,\rho_g,1)=0 \quad \stackrel{?}{\Longrightarrow} \quad \mathrm{Hom}_{G_{\mathbb{Q}}}(\rho_g, \mathbb{C}\otimes E(K)) \neq 0.$$

Let f be a modular form of weight 2 (of trivial character) attached to an elliptic curve $E/\mathbb{Q}$:

$$f=\sum_{n=1}^{\infty} a_n q^n \in \mathcal{S}_2(\Gamma_0(N))$$

where a_n's are integers, hence $f=f^*$. Let g be a modular form of weight 1 attached to an Artin representation $\rho : Gal(K/\mathbb{Q}) \to GL_2(\mathbb{C})$ by the Deligne-Serre theorem:

$$g=\sum_{n=1}^{\infty} b_n q^n \in \mathcal{S}_1(\Gamma_0(N'),\chi)$$

where $N'|N$. We wish to compute the special value of $L(E,\rho_g,s) = L(f\otimes g,s)$ at $s=1$. Writing the formula (32) for these choices of f and g, we have for $\mathcal{R}(s) > \frac{3}{2}$:

$$\left\langle \widetilde{E}_1'(z,s-1;\chi^{-1};N)g(z), f(z)\right\rangle_{2,N} = \frac{2\Gamma(s)}{(4\pi)^s}\mathcal{D}(f,g,s). \tag{50}$$

The series of $\mathcal{D}(f,g,s) = \sum_{n=0}^{\infty} \frac{a_n b_n}{n^s}$ is convergent for $\mathcal{R}(s) > \frac{3}{2}$, but we have seen that

$$L(f\otimes g,s) = L(\chi,2s-1)\mathcal{D}(f,g,s).$$

Dirichlet showed that $L(\chi,s)$ can be extended to a meromorphic function on the whole complex plane and $L(\chi,1)\neq 0$ if χ is not trivial. We also saw that $L(f\otimes g,s)$ can be extended to an entire function. So $\mathcal{D}(f,g,s)$ is a meromorphic function witch has the same vanishing property as $L(f\otimes g,s)$ at $s=1$. Therefore, we need only to to compute the value of $\mathcal{D}(f,g,s)$ at $s=1$ by the formula (50):

$$\left\langle \widetilde{E}_1'(z;\chi^{-1};N)g(z), f(z)\right\rangle_{2,N} = \frac{1}{2\pi}\mathcal{D}(f,g,1)\ . \tag{51}$$

Hence

$$\begin{aligned} L(f \otimes g, 1) &= L(\chi, 1)\mathcal{D}(f, g, 1) \\ &= 2\pi L(\chi, 1)\left\langle \widetilde{E}_1'(z; \chi^{-1}; N)g(z), f(z)\right\rangle_{2,N} . \end{aligned} \tag{52}$$

Notice that $\widetilde{E}_1'(z;\chi^{-1};N)g(z)$ is a cusp form of weight 2 and character trivial, i.e. $\widetilde{E}_1'(z;\chi^{-1};N)g(z)$ belongs to $\mathcal{S}_2(\Gamma_0(N))$. We wish to find a suitable basis for the vector space $\mathcal{S}_2(\Gamma_0(N))$ in order to compute $\left\langle \widetilde{E}_1'(z;\chi^{-1};N)g(z), f(z)\right\rangle_{2,N}$.

By definition, the space of newforms at level N is the orthogonal complement of the space of oldforms with respect to the Petersson inner product:

$$\mathcal{S}_2(\Gamma_1(N))^{\text{new}} = (\mathcal{S}_2(\Gamma_1(N))^{old})^{\perp}.$$

On the other hand:

$$\mathcal{S}_2(\Gamma_1(N)) = \bigoplus \mathcal{S}_2(\Gamma_0(N), \chi)$$

where the sum is over all Dirichlet characters modulo N. Recall that $\mathcal{S}_2(\Gamma_1(N), \mathbf{1}) = \mathcal{S}_2(\Gamma_0(N))$. Then

$$\mathcal{S}_2(\Gamma_1(N))^{\text{new}} \cap \mathcal{S}_2(\Gamma_0(N)) = (\mathcal{S}_2(\Gamma_1(N))^{old})^{\perp} \cap \mathcal{S}_2(\Gamma_0(N))$$

or:

$$\mathcal{S}_2(\Gamma_0(N))^{\text{new}} = (\mathcal{S}_2(\Gamma_0(N))^{old})^{\perp}.$$

Assume

$$\begin{aligned} \dim\ (\mathcal{S}_2(\Gamma_0(N))^{\text{old}}) &= w\ , \\ \dim\ (\mathcal{S}_2(\Gamma_0(N))^{\text{new}}) &= v\ . \end{aligned}$$

Then

$$\dim\ (\mathcal{S}_2(\Gamma_0(N))) = d = w + v.$$

From the Spectral Theorem of linear algebra, given a commuting family of normal operators on a finite-dimensional inner product space, the space has an orthogonal basis of simultaneous eigenvectors for the operators. In our case, the vector space $\mathcal{S}_2(\Gamma_0(N))$ is finite-dimensional and Hecke operators T_n and $\langle n\rangle$ commutate and are normal relative to the Petersson inner product on $\mathcal{S}_2(\Gamma_0(N))$ for all n coprime to N:

Theorem 66. *The space $\mathcal{S}_2(\Gamma_0(N))$ has an orthogonal basis of simultaneous eigenforms for all the Hecke operators $\{\langle n\rangle, T_n :\ (n, N) = 1\}$.*

Now consider $B_1 = \{f = f_1,\ f_2,\ ...,\ f_v\}$ the basis of eigenforms for the space of newforms $\mathcal{S}_2(\Gamma_0(N))^{\text{new}}$ where we can assume $f = f_1$ (since f is a newform by modularity theorem.) Take any basis $B_2 = \{f = f_{v+1},\ f_{v+2},\ ...,\ f_d\}$ for the space of oldforms $\mathcal{S}_2(\Gamma_0(N))^{\text{old}}$. Then $B = B_1 \cup B_2$ is a basis for $\mathcal{S}_2(\Gamma_0(N))$. By definition of the space of newforms:

$$\langle f_i(z), f_j(z)\rangle_{2,N} = 0$$

for any $f_i \in B_1$ and $f_j \in B_2$. Now write the modular form $\widetilde{E}_1'(z;\chi^{-1};N)g(z)$ as a linear combination of the elements of the basis B:

$$\widetilde{E}_1'(z;\chi^{-1};N)g(z) = \alpha_1 f + \alpha_2 f_2 + ... + \alpha_d f_d.$$

(Recall that we set $f = f_1$) It follows:

$$\begin{aligned} \left\langle \widetilde{E}_1'(z;\chi^{-1};N)g(z), f(z) \right\rangle_{2,N} &= \sum \alpha_i \left\langle f_i(z), f(z) \right\rangle_{2,N} \\ &= \alpha_1 \left\langle f(z), f(z) \right\rangle_{2,N}. \end{aligned} \tag{53}$$

Combining this with (52), we get

$$L(f \otimes g, 1) = 2\pi\alpha_1 L(\chi, 1) \left\langle f(z), f(z) \right\rangle_{2,N} . \tag{54}$$

Notice that $\left\langle f(z), f(z) \right\rangle_{2,N}$ is nonzero. In summary,

$$\begin{aligned} \mathrm{Hom}_{G_{\mathbb{Q}}}(\rho_g, \mathbb{C} \otimes E(K)) \neq 0 &\overset{?}{\Leftrightarrow} \mathrm{ord}_{s=1} L(E, \rho_g, s) > 0 \\ &\Leftrightarrow L(f \otimes g, 1) = 0 \\ &\Leftrightarrow \mathcal{D}(f, g, 1) = 0 \\ &\Leftrightarrow \left\langle \widetilde{E}_1'(z;\chi^{-1};N)g(z), f(z) \right\rangle_{2,N} = 0 \\ &\Leftrightarrow \alpha_1 = 0. \end{aligned}$$

Take any $g \in \mathcal{S}_1(\Gamma_0(N_g), \chi)$. Then consider all elliptic curves of conductor N with $N_g | N$. Using the Sage database, we can compute the value α_1 relating to each $L(f \otimes g, 1)$ and as a consequence, we can observe if $L(f \otimes g, 1) = 0$.

For any $d | \frac{N}{N_g}$, one can also compute $L(f(z) \otimes g(dz), 1)$, since $g(dz) \in \mathcal{S}_1(\Gamma_0(dN_g), \chi) \subset \mathcal{S}_1(\Gamma_0(N), \chi)$. However the representation associated to $g(dz)$ using the Deligne-Serre theorem is the same as one associated to $g(z)$. Hence the vanishing order of $L(f(z) \otimes g(dz), s)$ at $s = 1$ doesn't give any new information about $\langle \rho_g, \mathbb{C} \otimes_{\mathbb{Z}} E(K) \rangle$.

Proposition 67. *For $\mathcal{R}(s) > \frac{1}{2}$, we have:*

$$\left\langle \widetilde{E}_1'(z, s-1;\chi^{-1};N)g(dz), f(z) \right\rangle_{2,N} = 2\frac{a_d}{d^s}\frac{\Gamma(s)}{(4\pi)^s}\mathcal{D}(f, g, s) . \tag{55}$$

In particular at $s = 1$, we obtain:

$$\left\langle \widetilde{E}_1'(z;\chi^{-1};N)g(dz), f(z) \right\rangle_{2,N} = \frac{a_d}{d}\frac{1}{2\pi}\mathcal{D}(f, g, 1) .$$

Proof: Using again Rankin's unfolding trick, one can show:

$$\begin{aligned}
\left\langle \widetilde{E}_1'(z;\chi^{-1};N)g(dz), f^*(z)\right\rangle_{2,N} &= \int_{y=0}^{\infty}\int_{x=0}^{1} y^{1+s} g(dz) f(-\bar{z})\frac{dxdy}{y^2} \\
&= \int_{y=0}^{\infty}\int_{x=0}^{1} y^{1+s}\left(\sum_{n\geqslant 1} b_n e^{2\pi i dnz}\right)\left(\sum_{m\geqslant 1} a_m e^{-2\pi i m\bar{z}}\right)\frac{dxdy}{y^2} \\
&= \int_{y=0}^{\infty}\int_{x=0}^{1} y^{1+s}\sum_{n,m\geqslant 1} b_n a_m e^{2\pi i n(dx+iy)} e^{-2\pi i m(dx-iy)}\frac{dxdy}{y^2} \\
&= \int_{y=0}^{\infty} y^{1+s}\sum_{n,m\geqslant 1} b_n a_m e^{-2\pi(dn+m)y}\left(\int_{x=0}^{1} e^{2\pi i(dn-m)x}dx\right)\frac{dy}{y^2}
\end{aligned}$$

The integral in the parenthesis is equal to the Kronecker delta $\delta_{(dn,m)}$. So the last line is equal to:

$$\begin{aligned}
&= \int_{y=0}^{\infty} y^{1+s}\sum_{n\geqslant 1} a_{dn} b_n e^{-2\pi(dn+dn)y}\frac{dy}{y^2} \\
&= \sum_{n\geqslant 1} a_{dn} b_n \int_{y=0}^{\infty} y^s e^{-4\pi dny}\frac{dy}{y} \\
&= \left(\sum_{n\geqslant 1}\frac{a_{dn}b_n}{(4\pi dn)^s}\right)\int_0^{\infty} u^s e^{-u}\frac{du}{u}\ . \qquad (56)
\end{aligned}$$

If $d = p_1^{\alpha_1} p_2^{\alpha_2} ... p_v^{\alpha_v}$, since $d|N$ where N is the conductor of the elliptic curve corresponding to f, we have $a_{p_j n} = a_{p_j} a_n$ for any $j = 1, ..., v$, thus $a_{dn} = a_d a_n$ and

$$(56) = \frac{a_d}{d^s}\left(\sum_{n\geqslant 1}\frac{a_n b_n}{(4\pi n)^s}\right)\int_0^{\infty} u^s e^{-u}\frac{du}{u}.$$

Putting $s = 1$ gives the required result. ■

We conclude that

$$\left\langle \widetilde{E}_1'(z;\chi^{-1};N)g(dz), f(z)\right\rangle_{2,N} = \frac{a_d}{d}\left\langle \widetilde{E}_1'(z;\chi^{-1};N)g(z), f(z)\right\rangle_{2,N}. \qquad (57)$$

Thus $\left\langle \widetilde{E}_1'(z;\chi^{-1};N)g(dz), f(z)\right\rangle_{2,N}$ and $\left\langle \widetilde{E}_1'(z;\chi^{-1};N)g(z), f(z)\right\rangle_{2,N}$ vanish together unless $a_d \neq 0$ which can happen for some elliptic curves. The computations done in Sage confirm this formula.

Let $g \in \mathcal{S}_1(\Gamma_0(N_g), \chi)$ where χ is an odd character. Using the Deligne-Serre theorem, we get a 2-dimensional representation $\rho_g : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{C})$ associated to g. Let $\tilde{\rho}_g : G_{\mathbb{Q}} \to \mathrm{PGL}_2(\mathbb{C})$ be the projective representation obtained from ρ_g. We say ρ_g is a *dihedral* representation if its image $\mathrm{im}(\tilde{\rho}_g) \subset \mathrm{PGL}_2(\mathbb{C})$ is isomorphic to the dihedral group D_n of order $2n$ for some $n \geqslant 2$. A dihedral representation is irreducible. (see [16])

Let C_n be a cyclic subgroup of D_n of order n. If $n \geqslant 3$, C_n is uniquely determined. The composition:

$$w : G_{\mathbb{Q}} \xrightarrow{\tilde{\rho}_g} D_n \longrightarrow D_n/C_n = \{\pm 1\}$$

can be viewed as a 1-dimensional complex representation of $G_{\mathbb{Q}}$ of order 2. Let $\ker(w) = \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ where K is a number field. Since the order of w is 2, the index $[G_{\mathbb{Q}} : \mathrm{Gal}(\overline{\mathbb{Q}}/K)]$ is equal to 2. Hence K is a quadratic extension of $\mathbb{Q}$. Put $G_K := \mathrm{Gal}(\overline{\mathbb{Q}}/K) \subset G_{\mathbb{Q}}$, then $\tilde{\rho}_g(G_K) \subset C_n$. Since $[D_n : C_n] = [\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) : \mathrm{Gal}(\overline{\mathbb{Q}}/K)] = 2$, we have $\tilde{\rho}_g(G_K) = C_n$ a cyclic group. Therefore $\rho_g(G_K)$ is an abelian group. Consider

$$G_K \longrightarrow G_K/\mathrm{ker}\rho_g \xrightarrow{\rho_g} \mathrm{GL}_2(\mathbb{C})$$

where ρ_g is denoted also for the induced representation $\rho_g : G_K/\mathrm{ker}\rho_g \to \mathrm{GL}_2(\mathbb{C})$. Since $G_K/\mathrm{ker}\rho_g \cong \rho_g(G_K)$ is abelian, the representation $\rho_g|_{G_K} : G_K/\mathrm{ker}\rho_g \to \mathrm{GL}_2(\mathbb{C})$ is reducible. From this, one can easily see that the representation $\rho_g|_{G_K} : G_K \to \mathrm{GL}_2(\mathbb{C})$ is also reducible. One can write

$$\begin{aligned} \rho_g|_{G_K} : \quad G_K &\to \mathrm{GL}_2(\mathbb{C}) \\ \gamma &\mapsto \begin{pmatrix} \chi(\gamma) & 0 \\ 0 & \chi'(\gamma) \end{pmatrix} \end{aligned}$$

for some 1-dimensional representations χ and χ' of G_K. If σ lies in the non-identity coset of $G_{\mathbb{Q}}/G_K$, then $\chi' = \chi_\sigma$ where:

$$\chi_\sigma(\gamma) = \chi(\sigma\gamma\sigma^{-1}), \quad \gamma \in G_K.$$

Moreover, $\rho_g = \mathrm{Ind}_{K/\mathbb{Q}}(\chi)$.

Suppose, conversely, that we start with a quadratic number field $K/\mathbb{Q}$ corresponding to a character w of $G_{\mathbb{Q}}$ and a 1-dimensional linear representation χ of G_K. Let $\rho = \mathrm{Ind}_{K/\mathbb{Q}}(\chi)$, and let $\tilde{\rho}$ be the associated projective representation of $G_{\mathbb{Q}}$. If σ generates $\mathrm{Gal}(K/\mathbb{Q})$, let χ_σ be as above. Finally, let $\mathfrak{m}$ be the conductor of χ and d_K be the discriminant of K.

Proposition 68. *With the above notation:*
a) The following are equivalent:
i) ρ is irreducible;
ii) ρ is dihedral;
iii) $\chi \neq \chi_\sigma$.
b) The conductor of ρ is $|d_K|.N_{K/\mathbb{Q}}(\mathfrak{m})$.
c) ρ is odd if and only if one of the following holds:
i) K is imaginary.
ii) K is real and χ has signature +,- at infinity, that is, if c and c' are Frobenius elements at the two real places of K then $\chi(c) \neq \chi(c')$.
d) If $\tilde{G_{\mathbb{Q}}} = D_n$, then n is the order of $\chi^{-1}\chi_\sigma$.

Proof: see [16]. ■

Let $\rho = \mathrm{Ind}_{K/\mathbb{Q}}(\chi)$ be a dihedral representation of $G_{\mathbb{Q}}$ where K is imaginary and χ is unramified. Hence, we can view χ as a character of the ideal class group of $\mathcal{O}_K$. For any ideal $\mathfrak{a}$ of $\mathcal{O}_K$, the ideal $\mathfrak{a}.\sigma(\mathfrak{a})$ is principal, so $\chi \neq \chi_\sigma$ if and only if $\chi^2 \neq 1$. Therefore an imaginary quadratic field K gives rise to a dihedral representation of $G_{\mathbb{Q}}$ if its ideal class group is not an elementary abelian 2-group, i.e. $(\mathbb{Z}/2\mathbb{Z})^r$. The smallest value of $|d_K|$ for which this happens is 23. Let CL_K be the ideal class group of K and H be the Hilbert class field of K. There is an isomorphism $\mathrm{Gal}(H/K) \cong \mathrm{CL}_K$. For any character of $\mathrm{Gal}(H/K)$, the induced representation of $\mathrm{Gal}(H/\mathbb{Q})$ is dihedral and irreducible.

We present the results shown in tables 1 to 14 via some examples.

Example 69. *Consider the modular form g of level $p = 23$ discussed in the example 5 of section 1.2. For any elliptic curve of level N with $23|N$, we can compute $L(f \otimes g, 1)$ where f is the modular form arising from an elliptic curve of conductor N.*

There is no elliptic curve of conductor $N = 23$. However for level $N = 2 * 23$, there is one elliptic curve $E = [1, -1, 0, -10, -12]$ (up to isogeny) for which $L(f \otimes g, 1) \neq 0$. One can also consider $L(f(z) \otimes g(2z), 1) \neq 0$ since $g(2z) \in \mathcal{S}_1(\Gamma_0(2 * 23))$. In the table (1), we see that $L(f(z) \otimes g(2z), 1) \neq 0$ (in the column $g(d_1 z)$). This supports the formula (55), since the second fourier coefficient of the modular form attached to E is nonzero ($a_2 = -1$). Then the twisted BSD conjecture implies:

$$\textit{multiplicity of } \rho_g \textit{ in } \mathbb{C} \otimes E(H) \stackrel{?}{=} 0$$

where H is the Hilbert class field of $\mathbb{Q}(\sqrt{-23})$; The class number of $\mathbb{Q}(\sqrt{-23})$ is 3 so $[H : \mathbb{Q}(\sqrt{-23})] = 3$ hence $im(\tilde{\rho}_g) = D_3$.

For $N = 16 * 23$, there are 7 elliptic curves of level N up to isogeny. For two of them, $L(f \otimes g, 1) \neq 0$. For any $d|\frac{N}{23} = 16$, we can also consider $g(dz) \in \mathcal{S}_1(\Gamma_0(16 * 23))$ (in the table 1, the ordered divisors 2,4,8 and 16 are denoted by $d_1 = 2$, $d_2 = 4$, $d_3 = 8$ and $d_4 = 16$ respectively.) Since $a_2 = 0$ for all these 7 elliptic curves, we then have $L(f \otimes g(dz), 1) = 0$. It follows that for these 2 elliptic curves E of conductor $N = 16 * 23 = 368$:

$$\textit{multiplicity of } \rho_g \textit{ in } \mathbb{C} \otimes E(H) \stackrel{?}{=} 0.$$

For the other 5 elliptic curves we have $L(f \otimes g, 1) = 0$, therefore

$$\textit{multiplicity of } \rho_g \textit{ in } \mathbb{C} \otimes E(H) \stackrel{?}{\geqslant} 1.$$

Assuming the BSD conjecture, one has for these 5 elliptic curves:

$$\textit{rank of } E \textit{ over } H \quad = \quad r_H(E) \stackrel{?}{\geqslant} 2.$$

Example 70. *There is only one elliptic curve of conductor* $N = 23 * 31 = 693$ *up to isogeny. We shall consider two cusp forms arising from theta series:*

$$\begin{aligned} g_1 &\in \mathcal{S}_1(\Gamma_0(23), (\tfrac{-23}{\cdot})) \\ g_2 &\in \mathcal{S}_1(\Gamma_0(31), (\tfrac{-31}{\cdot})). \end{aligned}$$

For both g_1 *and* g_2 *we have:*

$$L(f \otimes g_1, 1) = 0$$
$$L(f \otimes g_2, 1) = 0 \ .$$

Therefore assuming the twisted BSD conjecture, one can say:

$$ord_{s=1} L(E, \rho_{g_1}, s) \stackrel{?}{=} \text{ multiplicity of } \rho_{g_1} \text{ in } \mathbb{C} \otimes E(H_1) \geqslant 1$$
$$ord_{s=1} L(E, \rho_{g_2}, s) \stackrel{?}{=} \text{ multiplicity of } \rho_{g_2} \text{ in } \mathbb{C} \otimes E(H_2) \geqslant 1$$

where H_1 *(*H_2*) is the Hilbert class field of* $\mathbb{Q}(\sqrt{-23})$ *(*$\mathbb{Q}(\sqrt{-31})$ *respectively). The class number of* $\mathbb{Q}(\sqrt{-31})$ *is 3 so* $[H_2 : \mathbb{Q}(\sqrt{-31})] = 3$ *hence* $im(\tilde{\rho}_{g_2}) = D_3$*.*
As an immediate consequence, assuming the BSD conjecture, one has:

$$\begin{aligned} \text{rank of } E \text{ over } H_1 &= r_{H_1}(E) \stackrel{?}{\geqslant} 2 + r_{\mathbb{Q}}(E) = 3 \\ \text{rank of } E \text{ over } H_2 &= r_{H_2}(E) \stackrel{?}{\geqslant} 2 + r_{\mathbb{Q}}(E) = 3. \end{aligned}$$

Example 71. ***(Octahedral type)*** *The space* $\mathcal{S}_1(\Gamma_0(283), (\frac{-283}{\cdot}))$ *has two cuspforms* g_1, g_2 *of type* S_4 *(octahedral) and one cuspform* g_3 *of type* D_3 *(dihedral):*

$$\begin{aligned} g_1 &= q + \sqrt{-2}q^2 - \sqrt{-2}q^3 - q^4 - \sqrt{-2}q^5 + 2q^6 - q^7 - q^9 + ... \\ g_2 &= q - \sqrt{-2}q^2 + \sqrt{-2}q^3 - q^4 + \sqrt{-2}q^5 + 2q^6 - q^7 - q^9 + ... \\ g_3 &= q - q^4 - q^7 - q^9 - q^{11} + ... \quad . \end{aligned}$$

Let $\rho_i : G_{\mathbb{Q}} \to GL_2(\mathbb{C})$ *be the Galois representation attached to* g_i *for* $i = 1, 2, 3$*. Let* K *be the field corresponding to the kernel of* ρ_1 *(or equivalently* ρ_2*) and* K' *be the field corresponding to the kernel of* $\widetilde{\rho}_1$*. As before, the field corresponding to the kernel of* ρ_3 *is* $H(\mathbb{Q}(\sqrt{-283}))$*, i.e. the Hilbert class field of* $\mathbb{Q}(\sqrt{-283})$*. Then*

$$\mathbb{Q}(\sqrt{-283}) \subset H(\mathbb{Q}(\sqrt{-283})) \subset K' \subset K.$$

We have $Gal(H(\mathbb{Q}(\sqrt{-283})) : \mathbb{Q}) = S_3 = D_3$ *and* $Gal(E : \mathbb{Q}) = S_4$*. These fields are constructed explicitly as follows. Let* $x^3 + 4x - 1 = (x - \alpha)(x - \beta_1)(x - \beta_2)$ *where* $\alpha \in \mathbb{R}$ *and* $\beta_2 = \overline{\beta_1}$*. Then we have* $H = \mathbb{Q}(\alpha, \beta_1, \beta_2)$ *and* $L = \mathbb{Q}(\sqrt{\alpha}, \sqrt{\beta_1}, \sqrt{\beta_2})$*. (see [18]) There is only one elliptic curve* E*, up to isogeny, of conductor 2*283. Concerning the tables 12 to 14, one can say (again, assuming the BSD conjecture):*

$$ord_{s=1} L(E, \rho_{g_1}, s) \stackrel{?}{=} \text{ multiplicity of } \rho_{g_1} \text{ in } \mathbb{C} \otimes E(K) \geqslant 1$$
$$ord_{s=1} L(E, \rho_{g_2}, s) \stackrel{?}{=} \text{ multiplicity of } \rho_{g_2} \text{ in } \mathbb{C} \otimes E(K) \geqslant 1.$$

Therefore:

$$\text{rank of } E \text{ over } K = r_K(E) \stackrel{?}{\geqslant} 4 + r_{\mathbb{Q}}(E) = 5. \quad \blacksquare$$

Example 72. ***(Octahedral type)*** *There are four newforms on $\Gamma_0(229)$ of weight 1. If g_1, g_2, g_3 and g_4 are these newforms, their first coefficients are:*

$$\begin{aligned}
g_1 &= q + q^3 - iq^4 + iq^5 + (i-1)q^7 - iq^{11} - iq^{12} - (1+i)q^{13} + iq^{15} - q^{16} + q^{17} - q^{19} + \ldots \\
g_2 &= q + (1+i)q^2 - q^3 + iq^4 + iq^5 - (1+i)q^6 + (-1+i)q^{10} - iq^{11} - iq^{12} - iq^{15} + q^{16} \\
&\quad -q^{17} + q^{19} + \ldots \\
g_3 &= \overline{g_1} \\
g_4 &= \overline{g_2} \quad .
\end{aligned}$$

Let χ be the character of order 4 of $(\mathbb{Z}/229\mathbb{Z})^\times$ such that $\chi(2) = i$. Then $g_1, g_2 \in \mathcal{S}_1(\Gamma_0(229), \chi)$ and $g_3, g_4 \in \mathcal{S}_1(\Gamma_0(229), \overline{\chi})$. Let $\rho_i : G_{\mathbb{Q}} \to GL_2(\mathbb{C})$ be the Galois representation attached to g_i for $i = 1, 2, 3, 4$. They are representations of type S_4 (Octahedral). Let K_i be the field corresponding to the kernel of ρ_i for $i = 1, 2, 3, 4$. If x_1, x_2 and x_3 are the roots of $x^3 - 4x + 1 = 0$, then K_1 is the field generated by the $\sqrt{-3 + 8x_i}$ and K_2 is the field generated by the $\sqrt{4 - 3x_i^2}$ (see [16]). Clearly, $K_3 = K_1$ and $K_4 = K_2$. There are two elliptic curves of conductor $2 * 229$ up to isogeny. Concerning the tables 8 to 11, one can say (again, assuming the BSD conjecture):

$$\begin{aligned}
\textit{multiplicity of } \rho_{g_i} \textit{ in } \mathbb{C} \otimes E(K_i) &\stackrel{?}{=} 0 \\
\textit{multiplicity of } \rho_{\overline{g_i}} \textit{ in } \mathbb{C} \otimes E(K_i) &\stackrel{?}{=} 0
\end{aligned}$$

for $i = 1, 2$. ■

If the BSD conjecture is true, one can deduce a more general form of it, namely the twisted BSD conjecture. Using the Deligne-Serre theorem and the Rankin method, we could compute the constant term of $L(E, \rho_g, s)$ at $s = 1$. It is also interesting to find a method in order to compute the coefficients of higher degree and compute the order of $L(E, \rho_g, s)$ at $s = 1$. Then one can compute the rank of E over certain number field K, i.e. $r_K(E)$. The numerical examples in this thesis are done for dihedral representations arising from theta series. It is interesting to find more cusp forms of weight 1 such that the image of its associated projective representation is one of the exceptional groups A_4, S_4 or A_5 and provide more numerical examples. Unfortunately, there seems to be relatively little published regarding explicit computations of weight 1 cusp forms. However, there are some examples in [2], [3], [5], [9], [16] and [18].

Tables

Notation:

$E = [a_1, a_2, a_3, a_4, a_6]$: Elliptic curve E with Weierstrass equation

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

N: The conductor of E.

d_1, d_2,...are divisors of $\frac{N}{N_g}$ in increasing order where N_g =the level of g.

The column under $g(d_iz)$, $i = 1, 2, ...$, shows the coefficient α_1 in the equation $\widetilde{E}_1'(z; \chi^{-1}; N)g(d_iz) = \alpha_1 f + \alpha_2 f_2 + ... + \alpha_d f_d$ where the modular forms $\widetilde{E}_1'(z; \chi^{-1}; N)$, $f, f_2, ..., f_d$ are as in the text.

For each level N, all elliptic curves, up to isogeny, are listed.

$g(z)=\eta(z)\eta(23z)\in\mathcal{S}_1(\Gamma_0(23),\left(\frac{-23}{\cdot}\right))$, $\mathrm{Im}(\widetilde{\rho}_g)=D_3$, $K=H(\mathbb{Q}(\sqrt{-23}))$								
N	$E=[a_1,a_2,a_3,a_4,a_6]$	$r_{\mathbb{Q}}(E)$	$g(z)$	$g(d_1z)$	$g(d_2z)$	$g(d_3z)$	$g(d_4z)$	$g(d_5z)$
2*23	[1, -1, 0, -10, -12]	0	4/5	$-2/5$				
3*23	[1, 0, 1, -16, -25]	0	0	0				
4*23	[0, 0, 0, -1, 1]	1	1	0	0			
	[0, 1, 0, -18, -43]	0	0	0	0			
5*23	[0, 0, 1, 7, -11]	0	0	0				
6*23	[1, 1, 0, -31, 55]	1	0	0	0	0		
	[1, 0, 1, -771, 1342]	0	0	0	0	0		
	[1, 0, 1, -36, 82]	0	0	0	0	0		
7*23	[1, -1, 1, -124, 560]	0	14/5	2/5				
8*23	[0, -1, 0, 0, 1]	1	3/2	0	0	0		
	[0, -1, 0, -4, 5]	1	0	0	0	0		
	[0, 0, 0, -35, 62]	0	4/3	0	0	0		
	[0, 0, 0, -55, -157]	0	1/6	0	0	0		
9*23	[1, -1, 1, -140, 668]	1	27/8	0	0			
14*23	[1, -1, 0, -238, 1470]	1	0	0	0	0		
	[1, 1, 0, -605, 5117]	0	1/4	-1/8	1/28	-1/56		
	[1, 0, 0, -174, 868]	1	0	0	0	0		
	[1, 1, 1, -14, -23]	0	0	0	0	0		
15*23	[0, 1, 1, -100, 406]	1	45/32	15/32	9/32	3/32		
	[1, 0, 0, -411, -3234]	0	3/2	1/2	-3/10	-1/10		
	[0, -1, 1, -731, -7369]	0	0	0	0	0		
	[0, 1, 1, -1, 1]	1	0	0	0	0		
	[1, 0, 1, -30134, 2010071]	0	3/10	1/10	-3/50	-1/50		
	[0, -1, 1, 30, -97]	0	5/16	-5/48	1/16	-1/48		
16*23	[0, 0, 0, -55, 157]	1	0	0	0	0	0	
	[0, -1, 0, -18, 43]	1	3	0	0	0	0	
	[0, 0, 0, -35, -62]	1	0	0	0	0	0	
	[0, 0, 0, -2723, 54690]	0	0	0	0	0	0	
	[0, 1, 0, 0, -1]	1	0	0	0	0	0	
	[0, 1, 0, -4, -5]	0	1/2	0	0	0	0	
	[0, 0, 0, -1, -1]	0	0	0	0	0	0	
18*23	[1, -1, 0, -2223, -39785]	1	0	0	0	0	0	
	[1, -1, 1, -1532, 23455]	1	0	0	0	0	0	
	[1, -1, 1, -6935, -36241]	0	0	0	0	0	0	
	[1, -1, 1, -284, -1767]	0	0	0	0	0	0	
19*23	[0, -1, 1, 19, 100]	1	0	0				
	[0, -1, 1, 0, -5]	0	0	0				
20*23	[0, -1, 0, -10, 17]	1	5/2	0	0	1/2	0	0
	[0, 0, 0, -8, -12]	0	10/9	0	0	-2/9	0	0
	[0, 1, 0, -46, 529]	1	0	0	0	0	0	0
	[0, 0, 0, -73, 2453]	0	1/20	0	0	-1/100	0	0

Table 1: $g\in\mathcal{S}_1(\Gamma_0(23),\left(\frac{-23}{\cdot}\right))$

$g(z) = \eta(z)\eta(23z) \in \mathcal{S}_1(\Gamma_0(23), \left(\frac{-23}{\cdot}\right))$, $\mathrm{Im}(\widetilde{\rho}_g) = D_3$, $K = H(\mathbb{Q}(\sqrt{-23}))$										
N	$E = [a_1, a_2, a_3, a_4, a_6]$	$r_{\mathbb{Q}}(E)$	$g(z)$	$g(d_1z)$	$g(d_2z)$	$g(d_3z)$	$g(d_4z)$	$g(d_5z)$	$g(d_6z)$	$g(d_7z)$
21*23	[0, 1, 1, 2, 1]	0	0	0	0	0				
	[0, 1, 1, -96, -457]	0	7/50	7/150	-1/50	-1/150				
22*23	[1, 0, 1, -48, -130]	1	33/14	-33/28	-3/14	3/28				
	[1, 0, 1, -397, -3072]	0	3/2	-3/4	3/22	-3/44				
	[1, -1, 0, -290561, 60356981]	0	0	0	0	0				
	[1, -1, 0, -935, 11229]	1	0	0	0	0				
	[1, 0, 0, -86, 292]	1	33/26	33/52	3/26	3/52				
	[1, -1, 1, -4, -1]	1	0	0	0	0				
24*23	[0, -1, 0, -1144, -14516]	1	0	0	0	0	0	0	0	0
	[0, -1, 0, -46648, 3893500]	0	27/28	0	-9/28	0	0	0	0	0
	[0, -1, 0, -752, 6972]	1	3/2	0	-1/3	0	0	0	0	0
	[0, -1, 0, -56, -132]	0	3/4	0	-1/4	0	0	0	0	0
	[0, 1, 0, -2944, 60512]	0	0	0	0	0	0	0	0	0
25*23	[0, 1, 1, -18, 24]	1	75/14	0	0					
	[0, 0, 1, 175, -1344]	1	0	0	0					
	[1, -1, 1, -55, 72]	1	15/2	0	0					
	[1, -1, 0, -2, 1]	1	0	0	0					
	[0, -1, 1, -458, 3943]	1	0	0	0					
26*23	[1, -1, 0, 44, 496]	1	13/10	-13/20	1/10	-1/20				
	[1, -1, 0, -1802, 29898]	1	13/8	-13/16	1/8	-1/16				
	[1, 1, 1, 4, -1443]	1	39/34	39/68	-3/34	-3/68				
	[1, 1, 1, -14, -27]	0	0	0	0	0				
27*23	[1, -1, 1, -14, -16]	1	27/8	0	0	0				
	[1, -1, 0, -123, 548]	0	0	0	0	0				
28*23	[0, -1, 0, 2, -7]	1	7/2	0	0	1/2	0	0		
	[0, 1, 0, 6, -43]	1	0	0	0	0	0	0		
31*23	[1, 0, 1, -1, 1]	1	0	0						
33*23	[1, 1, 1, -1238, -17152]	1	0	0	0	0				
	[1, 0, 0, -93104, -10942305]	1	99/32	33/32	-9/16	-3/16				

Table 2: $g \in \mathcal{S}_1(\Gamma_0(23), \left(\frac{-23}{\cdot}\right))$

$g(z) \in \mathcal{S}_1(\Gamma_0(31), \left(\frac{-31}{\cdot}\right))$, $\mathrm{Im}(\widetilde{\rho}_g) = D_3$, $K = H(\mathbb{Q}(\sqrt{-31}))$								
N	$E = [a_1, a_2, a_3, a_4, a_6]$	$r_{\mathbb{Q}}(E)$	$g(z)$	$g(d_1 z)$	$g(d_2 z)$	$g(d_3 z)$	$g(d_4 z)$	$g(d_5 z)$
2*31	[1, -1, 1, -331, 2397]	0	0	0				
4*31	[0, 1, 0, -2, 1]	1	1	0	0			
	[0, 0, 0, -17, -27]	0	0	0	0			
5*31	[0, -1, 1, -840, -9114]	1	3/2	3/10				
	[1, 1, 1, -26, -62]	0	5/4	-1/4				
	[0, -1, 1, -1, 1]	1	0	0				
6*31	[1, 1, 0, -83, -369]	0	0	0	0	0		
	[1, 0, 1, -17, -28]	0	3/7	-3/14	1/7	-1/14		
	[1, 0, 0, -1395, -20181]	0	0	0	0	0		
8*31	[0, 1, 0, 0, 1]	1	0	0	0	0		
	[0, 1, 0, -32, -32]	0	0	0	0	0		
	[0, 0, 0, 1, -1]	1	1/5	0	0	0		
10*31	[1, 0, 0, -2046, 15376]	1	5/8	5/16	-1/8	-1/16		
	[1, 1, 1, -1066, -13841]	0	0	0	0	0		
12*31	[0, -1, 0, -6, 9]	1	0	0	0	0	0	0
	[0, 1, 0, -2, 9]	1	3/2	0	1/2	0	0	0
	[0, 1, 0, -164, 756]	0	0	0	0	0	0	0
	[0, 1, 0, -250914, -48460347]	0	0	0	0	0	0	0
14*31	[1, -1, 0, -47, 133]	1	0	0	0	0		
	[1, -1, 1, -2364, -43641]	0	0	0	0	0		
	[1, 0, 0, -139, 465]	1	0	0	0	0		
	[1, 0, 0, -3374, -75754]	0	0	0	0	0		
	[1, 1, 1, -522, 4373]	0	0	0	0	0		
15*31	[1, 0, 0, -170, 837]	1	45/16	15/16	9/16	3/16		
	[1, 1, 0, -162, 729]	1	0	0	0	0		
16*31	[0, 0, 0, 1, 1]	1	0	0	0	0	0	
	[0, 0, 0, -5291, -148134]	1	2	0	0	0	0	
	[0, 0, 0, -17, 27]	1	1	0	0	0	0	
	[0, -1, 0, -2, -1]	0	0	0	0	0	0	
	[0, -1, 0, 0, -1]	0	1/2	0	0	0	0	
	[0, -1, 0, -32, 32]	0	1	0	0	0	0	
18*31	[1, -1, 0, -12555, 544887]	1	27/10	-27/20	0	0	0	0
	[1, -1, 0, 0, 2]	1	0	0	0	0	0	0
	[1, -1, 0, -2976, -61750]	0	0	0	0	0	0	0
	[1, -1, 0, -48, 288]	0	9/10	-9/20	0	0	0	0
	[1, -1, 1, -434, -7343]	1	9/10	9/20	0	0	0	0
	[1, -1, 1, -149, 749]	1	0	0	0	0	0	0
	[1, -1, 1, -2, -53]	0	0	0	0	0	0	0
	[1, -1, 1, -752, 9213]	0	9/22	9/44	0	0	0	0
20*31	[0, 0, 0, 8, 4]	1	0	0	0	0	0	0
	[0, 0, 0, -1207, 9006]	1	0	0	0	0	0	0
	[0, 1, 0, -101, 359]	1	5/3	0	0	-1/3	0	0
23*31	[1, 0, 1, -1, 1]	1	0					

Table 3: $g \in \mathcal{S}_1(\Gamma_0(31), \left(\frac{-31}{\cdot}\right))$

$g(z)=\eta(z)\eta(47z)\in\mathcal{S}_1(\Gamma_0(47),\left(\frac{-47}{\cdot}\right))$, $\mathrm{Im}(\widetilde{\rho}_g)=D_5$, $K=H(\mathbb{Q}(\sqrt{-47}))$								
N	$E=[a_1,a_2,a_3,a_4,a_6]$	$r_{\mathbb{Q}}(E)$	$g(z)$	$g(d_1z)$	$g(d_2z)$	$g(d_3z)$	$g(d_4z)$	$g(d_5z)$
2*47	[1, -1, 1, -10, -9]	0	0	0				
3*47	[0, 1, 1, -12, 2]	1	-6/7	-2/7				
	[1, 1, 1, -143, -718]	0	1/2	-1/6				
	[1, 0, 0, -752, 7875]	0	0	0				
	[0, -1, 1, -1, 0]	1	0	0				
	[0, 1, 1, -26, -61]	0	0	0				
5*47	[1, 1, 1, -3551, -82926]	0	0	0				
	[1, 1, 1, -5, 0]	1	0	0				
	[0, -1, 1, 4, 1]	0	0	0				
6*47	[1, 1, 1, -255, 1461]	1	3/16	3/32	-1/16	-1/32		
	[1, 1, 1, -3502, -81181]	0	0	0	0	0		
7*47	[1, 1, 1, 246, -1376]	0	-49/90	7/90				
9*47	[0, 0, 1, -9, 10]	1	0	0	0			
	[0, 0, 1, -237, 1404]	1	-33/16	0	0			
	[0, 0, 1, -12, 4]	1	9/16	0	0			
	[1, -1, 0, -6768, -212625]	1	3/2	0	0			
	[1, -1, 0, -1287, 18094]	0	0	0	0			
	[0, 0, 1, -111, -171]	0	0	0	0			
	[0, 0, 1, -81, -277]	0	9/16	0	0			
10*47	[1, 1, 0, -97, 281]	1	0	0	0	0		
	[1, 0, 1, -44, 106]	1	-5/4	5/8	1/4	-1/8		
	[1, 0, 1, -6348, 132618]	0	-3/2	3/4	-3/10	3/20		
	[1, -1, 1, -117, 141]	1	5/7	5/14	1/7	1/14		
	[1, 1, 1, -11, 9]	1	0	0	0	0		
	[1, 0, 0, -176, -844]	0	0	0	0	0		
11*47	[0, 0, 1, -16, -26]	0	-11/36	-1/36				
	[0, -1, 1, -52, -3863]	1	0	0				
	[0, -1, 1, 36, -3]	0	0	0				
12*47	[0, -1, 0, -221, -1191]	1	4/5	0	-4/15	0	0	0
	[0, 1, 0, -517, -4681]	1	0	0	0	0	0	0
13*47	[0, 0, 1, -1, 1]	0	0	0				

Table 4: $g\in\mathcal{S}_1(\Gamma_0(47),\left(\frac{-47}{\cdot}\right))$

$g(z)=\eta(z)\eta(71z)\in\mathcal{S}_1(\Gamma_0(71),\left(\frac{-71}{\cdot}\right))$, $\mathrm{Im}(\widetilde{\rho}_g)=D_7$, $K=H(\mathbb{Q}(\sqrt{-71}))$						
$\boldsymbol{N}$	$E=[a_1,a_2,a_3,a_4,a_6]$	$r_{\mathbb{Q}}(E)$	$g(z)$	$g(d_1z)$	$g(d_2z)$	$g(d_3z)$
2*71	[1, 1, 0, -1, -1]	1	0	0		
	[1, -1, 0, -41, -91]	0	-4/9	2/9		
	[1, -1, 0, -2626, 52244]	0	2/81	-1/81		
	[1, -1, 1, -12, 15]	1	-2/9	-1/9		
	[1, 0, 0, -58, -170]	0	0	0		
3*71	[1, 0, 1, -15, 19]	0	0	0		
5*71	[0, 1, 1, -95, -396]	0	0	0		
6*71	[1, 1, 0, -286, 1780]	1	0	0	0	0
	[1, 0, 1, -23007, 1341682]	0	0	0	0	0
	[1, 0, 0, -230, -5202]	0	0	0	0	0
7*71	[1, 1, 0, 25, -14]	1	0	0		
8*71	[0, -1, 0, -72, -212]	0	-2/5	0	0	0
9*71	[1, -1, 1, -131, -520]	0	15/8	0	0	0
11*71	[0, 0, 1, -1378, 347]	0	0	0		
	[0, 0, 1, -808, 8840]	1	0	0		

Table 5: $g\in\mathcal{S}_1(\Gamma_0(71),\left(\frac{-71}{\cdot}\right))$

$g(z)=\eta(z)\eta(167z)\in\mathcal{S}_1(\Gamma_0(167),\left(\frac{-167}{\cdot}\right))$, $\mathrm{Im}(\widetilde{\rho}_g)=D_{11}$, $K=H(\mathbb{Q}(\sqrt{-167}))$				
$\boldsymbol{N}$	$E=[a_1,a_2,a_3,a_4,a_6]$	$r_{\mathbb{Q}}(E)$	$g(z)$	$g(d_1z)$
2*167	[1, -1, 1, -1, -1]	0	0	0
3*167	[1, 1, 0, -12, -15]	0	6/23	-2/23
7*167	[1, -1, 0, -1, 2]	0	2/7	2/49

Table 6: $g\in\mathcal{S}_1(\Gamma_0(167),\left(\frac{-167}{\cdot}\right))$

$g(z)=\eta(z)\eta(191z)\in\mathcal{S}_1(\Gamma_0(191),\left(\frac{-191}{\cdot}\right))$, $\mathrm{Im}(\widetilde{\rho}_g)=D_{13}$, $K=H(\mathbb{Q}(\sqrt{-191}))$				
$\boldsymbol{N}$	$E=[a_1,a_2,a_3,a_4,a_6]$	$r_{\mathbb{Q}}(E)$	$g(z)$	$g(d_1z)$
3*191	[0, 1, 1, -4, -2]	0	1/5	1/15
5*191	[1, -1, 1, -16663, 832042]	0	23/44	-23/220

Table 7: $g\in\mathcal{S}_1(\Gamma_0(191),\left(\frac{-191}{\cdot}\right))$

$g_1 \in \mathcal{S}_1(\Gamma_0(229), \chi)$ where $\chi(2) = i$, $\operatorname{Im}(\widetilde{\rho}_{g_1}) = S_4$				
$\boldsymbol{N}$	$E = [a_1, a_2, a_3, a_4, a_6]$	$r_{\mathbb{Q}}(E)$	$g_1(z)$	$g_1(d_1 z)$
2*229	[1, -1, 0, -19, 37]	1	-(1/12)i	(1/24)i
	[1, 1, 1, -16, -15]	1	-3/10	-3/20
5*229	[1, 0, 0, -596, 5551]	1	-40/87	8/87

Table 8: $g_1 \in \mathcal{S}_1(\Gamma_0(229), \chi)$

$g_2 \in \mathcal{S}_1(\Gamma_0(229), \chi)$ where $\chi(2) = i$, $\operatorname{Im}(\widetilde{\rho}_{g_2}) = S_4$				
$\boldsymbol{N}$	$E = [a_1, a_2, a_3, a_4, a_6]$	$r_{\mathbb{Q}}(E)$	$g_2(z)$	$g_2(d_1 z)$
2*229	[1, -1, 0, -19, 37]	1	(1/12)(1-i)	(-1/24)(1-i)
	[1, 1, 1, -16, -15]	1	(-1/2)(1+i)	(-1/4)(1+i)
5*229	[1, 0, 0, -596, 5551]	1	(10/87)(1-i)	(-2/87)(1-i)

Table 9: $g_2 \in \mathcal{S}_1(\Gamma_0(229), \chi)$

$g_3 = \overline{g_1} \in \mathcal{S}_1(\Gamma_0(229), \overline{\chi})$ where $\chi(2) = i$, $\operatorname{Im}(\widetilde{\rho}_{g_3}) = S_4$				
$\boldsymbol{N}$	$E = [a_1, a_2, a_3, a_4, a_6]$	$r_{\mathbb{Q}}(E)$	$g_3(z)$	$g_3(d_1 z)$
2*229	[1, -1, 0, -19, 37]	1	(1/12)i	-(1/24)i
	[1, 1, 1, -16, -15]	1	-3/10	-3/20
5*229	[1, 0, 0, -596, 5551]	1	-40/87	8/87

Table 10: $g_3 \in \mathcal{S}_1(\Gamma_0(229), \overline{\chi})$

$g_4 = \overline{g_2} \in \mathcal{S}_1(\Gamma_0(229), \overline{\chi})$ where $\chi(2) = i$, $\operatorname{Im}(\widetilde{\rho}_{g_4}) = S_4$				
$\boldsymbol{N}$	$E = [a_1, a_2, a_3, a_4, a_6]$	$r_{\mathbb{Q}}(E)$	$g_4(z)$	$g_4(d_1 z)$
2*229	[1, -1, 0, -19, 37]	1	(1/12)(1+i)	(-1/24)(1+i)
	[1, 1, 1, -16, -15]	1	(-1/2)(1-i)	(-1/4)(1-i)
5*229	[1, 0, 0, -596, 5551]	1	(10/87)(1+i)	(-2/87)(1+i)

Table 11: $g_4 \in \mathcal{S}_1(\Gamma_0(229), \overline{\chi})$

$g_1 \in \mathcal{S}_1(\Gamma_0(283), \left(\frac{-283}{\cdot}\right))$, $\mathrm{Im}(\widetilde{\rho}_{g_1}) = S_4$				
$\boldsymbol{N}$	$E = [a_1, a_2, a_3, a_4, a_6]$	$r_{\mathbb{Q}}(E)$	$g_1(z)$	$g_1(d_1 z)$
2*283	[1, -1, 0, -2, 4]	1	0	0
3*283	[1, 0, 0, 1, -1]	0	1/13	1/39

Table 12: $g_1 \in \mathcal{S}_1(\Gamma_0(283), \left(\frac{-283}{\cdot}\right))$

$g_2 \in \mathcal{S}_1(\Gamma_0(283), \left(\frac{-283}{\cdot}\right))$, $\mathrm{Im}(\widetilde{\rho}_{g_2}) = S_4$				
$\boldsymbol{N}$	$E = [a_1, a_2, a_3, a_4, a_6]$	$r_{\mathbb{Q}}(E)$	$g_2(z)$	$g_2(d_1 z)$
2*283	[1, -1, 0, -2, 4]	1	0	0
3*283	[1, 0, 0, 1, -1]	0	1/13	1/39

Table 13: $g_2 \in \mathcal{S}_1(\Gamma_0(283), \left(\frac{-283}{\cdot}\right))$

$g_3 \in \mathcal{S}_1(\Gamma_0(283), \left(\frac{-283}{\cdot}\right))$, $\mathrm{Im}(\widetilde{\rho}_{g_3}) = S_3$, $K = H(\mathbb{Q}(\sqrt{-283}))$				
$\boldsymbol{N}$	$E = [a_1, a_2, a_3, a_4, a_6]$	$r_{\mathbb{Q}}(E)$	$g_3(z)$	$g_3(d_1 z)$
2*283	[1, -1, 0, -2, 4]	1	1/2	-1/4
3*283	[1, 0, 0, 1, -1]	0	1/13	1/39

Table 14: $g_3 \in \mathcal{S}_1(\Gamma_0(283), \left(\frac{-283}{\cdot}\right))$

Codes

```
sage: Nf=3*144   # the level of the modular form f arising from the elliptic curve EC
sage: Ng=144     # the level of the modular form g of weight 1
sage: etiquette=0    # index for the elements of the basis S_1(Gamma_1(Ng))

sage: BoP=53  ## bits of precision

sage: S = CuspForms(Gamma0(Nf),2,base_ring =ComplexField());
sage: bound=S.sturm_bound()
sage: M = ModularForms(Gamma0(Nf),2,base_ring =ComplexField());
sage: m= ModularForms(Gamma0(Nf),2).dimension()
sage: d= CuspForms(Gamma0(Nf),2).dimension()
sage: S.set_precision(bound)
sage: BS= S.basis()
sage: M.set_precision(bound)
sage: BM= M.basis()

sage: EC = EllipticCurve([1, 1, 0, -12, -15]);   # elliptic curve of conductor Nf
sage: Erank= EC.rank();
sage: EConductor= EC.conductor();
sage: f = EC.modular_form();

# computing the coefficients of the Eisenstein series E for dihedral representation
# the character is not supposed to be primitive
sage: def EisensteinCoeffP(n,Level,Mod):
...       l=Level/Mod
...       if n==0:
...          sum = (l)*quadratic_L_function__exact(0, -Mod)/2
...          Div = prime_divisors(Level/Mod)
...          for i in range (0, len(Div)):
...                sum= sum * (1-kronecker(Div[i],Ng)/Div[i] )
...          return sum
...       sum=0
...       for c in range(1,n+1):
...           if (n % c == 0):
...              for d in range(1,GCD(l,c)+1):
...                  if GCD(l,c) % d  == 0:
...                     sum = sum+d*moebius(l/d)*kronecker(l/d,Ng)*kronecker(c/d,Ng)
...       return sum

sage: def EisensteinP(Level, Mod, prec):
...       if Level % Mod <> 0:
...          return false
...       R.<q> = PowerSeriesRing(ComplexField(BoP))
...       E=0
...       for h in range(0,prec+1):
...           E = E + EisensteinCoeffP(h,Level,Mod)*q^(h)
...       return E + O(q^prec)

sage: def EisensteinCoeff(n,Level,Mod, char):
```

```
...       const=0
...       if n==0:
...          for a in range (0,Mod):
...              const= const + a * char(a)
...          return -const/(2*Mod)
...       sum=0
...       for d in range(1,n+1):
...           if n % d == 0:
...              sum = sum + char(d)
...       return sum

sage: def Eisenstein(Level,Mod , char, prec):
...       R.<q> = PowerSeriesRing(ComplexField(BoP))
...       E=0
...       for h in range(0,prec):
...           E = E + EisensteinCoeff(h,Level,Mod,char) * q^( (Level/Mod) * h)
...       return E + O(q^prec)

# computing the coefficients of g of level 283
sage: def CoeffIter283(n, etiquette):
...      L.<z> = NumberField(x^2+1)
...      RootI=L.complex_embeddings()[1](z)
...      K.<w> = NumberField(x^2-2)
...      Sq2=K.complex_embeddings()[1](w)
...      C= Matrix([[2 , 3 , 5 , 7 , 11 , 13 , 17 , 19 , 23 , 29 , 31 , 37 , 41 , 43 , 47 ,
53 , 59 , 61 , 67 , 71 , 73 , 79 , 83 , 89 , 97 , 101 , 103 , 107 , 109 , 113 ,
127 , 131 , 137 , 139 , 149 , 151 , 157 , 163 , 167 , 173 , 179 , 181 , 191 ,  193 , 197 ,
283 , 293 , 307 , 311 , 313 , 317, 331, 337, 347, 349 ,353 ,359, 367, 373, 379, 383,
389, 397, 401, 409 ],
[-Sq2*RootI, Sq2*RootI, Sq2*RootI, -1, 1, 1, 0, -Sq2*RootI, -1, -1,
-Sq2*RootI, 0, 1, -Sq2*RootI, Sq2*RootI, 0,1, 1, 0, 0, 0, 0 , -2, -1, 1 ,
0 , -1 , 0  , Sq2*RootI , 0, 0 , 0 , 1 , Sq2*RootI , -Sq2*RootI ,
-1 , -1 , -1 , Sq2*RootI , -Sq2*RootI , 1 , 0 , 0 , 0 , 0, 1 , -1 , Sq2*RootI , 0 , 0 ,
-1 , 0 , 0 , 1 , -1,  -1 , -1 , 1 , -Sq2*RootI , 0, 1 , 1, 1, 0 , -Sq2*RootI, 1, 0 , 1 , 0, -1,
1, 0, 0, -1, 1,0, -1, Sq2*RootI  , 0, 0]] )
...      D = Matrix([[2 , 3 , 5 , 7 , 11 , 13 , 17 , 19 , 23 , 29 , 31 , 37 , 41 , 43 , 47 ,
53 , 59 , 61 , 67 , 71 ,73 , 79 , 83 , 89 , 97 ,101 , 103 , 107 , 109 , 113 ,
127 , 131 , 137 , 139 , 149 , 151 , 157 , 163 , 167 , 173 , 179 , 181 , 191 ,  193 , 197 ,
199 , 211 , 223 , 227 , 229 , 233 , 239 , 241 , 251 , 257, 263 , 269 , 271 , 277 , 281 ,
283 , 293 , 307 , 311 , 313 ],
[0,0,0,-1,-1, -1, 0, 0, -1, -1,0,0,-1 ,0 ,0,0,-1,-1,0,2,2,0,2,-1,-1,2,-1,0,0,2, 2,0,-1,0,0,
-1,-1,-1,0,0, -1,2,0,0,0,-1,-1,0,2,-0 ,-1,0,0,-1,-1 , -1,-1,-1,0,2 ,2,-1,-1,2,0 ]] )
...      if n==1:
...         return 1
...      if n in Primes():
...         for k in range (0,65):
...             if etiquette<2:
...                if C[0][k]==n:
...                   return C[1][k]
...             else:
...                if D[0][k]==n:
...                   return D[1][k]
```

```
...       else:
...          F=factor(n)
...          l=len(F)
...          r=1
...          if l==1:
...             if F[0][1]==1:
...                return CoeffIter283(F[0][0], etiquette) *
 CoeffIter283(F[0][0]^(F[0][1]-1), etiquette) - kronecker(-283,F[0][0])
...             if F[0][1]>1:
...                return CoeffIter283(F[0][0], etiquette) *
CoeffIter283(F[0][0]^(F[0][1]-1), etiquette) -
kronecker(-283,F[0][0])*CoeffIter283(F[0][0]^(F[0][1]-2), etiquette)
...          else:
...             for i in range (0,len(F)):
...                r = r * CoeffIter283(F[i][0]^F[i][1], etiquette)
...             return r


# computing the coefficients of g
sage: def g(Level, Mod):
...       R.<q> = PowerSeriesRing(ComplexField(BoP))
...       l = bound
...       a=Level/ Mod
...       Ng=Mod
...       g=0
...       if Ng % 24 == 23:
...           if etiquette==0:
...              for m in range (-l,l):
...                 for n in range (-l,l):
...                    if 0<(Ng+1)/24*m^2+m*n+6*n^2 < l:
...                        g = g + (1/2)* q^(a*((Ng+1)/24*m^2+m*n+6*n^2));
...                    if 0<(Ng+25)/24*m^2+5*m*n+6*n^2 < l:
...                        g = g - (1/2)* q^(a*((Ng+25)/24*m^2+5*m*n+6*n^2));
...       if etiquette==1:
...           if Ng==47:
...              g= q - q^3 - q^6 - q^8 + q^9 + O(q^12)
...              e = DirichletGroup(47)
...              psi=e.list()
...              g= ComputeCoeff( g, Eisenstein(Ng,Ng, psi[23], bound) ,bound)
...              if Level>Mod:
...                 gP=0
...                 for r in range (1,(bound/a)+1):
...                     gP = gP + g[r] * q^(a*r);
...                 g=gP
...       if etiquette==0:
...           if Ng==229:
...              e = DirichletGroup(229)
...              psi=e.list()
...              L.<z> = NumberField(x^2+1)
...              RootI=L.complex_embeddings()[0](z)
...              g= q + q^3 - RootI*q^4 + RootI*q^5 + (RootI - 1)*q^7 - RootI*q^11
 - RootI*q^12 +(-RootI - 1)*q^13 +RootI*q^15 - q^16 + q^17 - q^19 + q^20
```

```
  + (RootI - 1)*q^21 + (RootI + 1)*q^23 - q^27 + (RootI + 1)*q^28 -RootI*q^33
  + (-RootI - 1)*q^35 + (-RootI - 1)*q^39 + q^43 - q^44 + (RootI - 1)*q^47 - q^48
  - RootI*q^49 + q^51 + (RootI - 1)*q^52 + 2*q^53 + q^55 +
 (0)*(RootI + 1)*(q^2 + (RootI - 1)*q^3 + (RootI + 1)*q^4 - q^6 - RootI*q^7
 + RootI*q^10 + q^13 + (-RootI - 1)*q^15 + (-RootI + 1)*q^16 + (RootI - 1)*q^17
 + (-RootI + 1)*q^19 + (RootI - 1)*q^20 - RootI*q^21 - RootI*q^22 - 2*q^23 +
 (-RootI + 1)*q^27 - q^28 - RootI*q^30 - q^31 + q^32 + (RootI + 1)*q^33 - q^34
 + q^35 + q^38 + q^39 + RootI*q^41 + (RootI - 1)*q^43 + (-RootI + 1)*q^44+
(-RootI - 1)*q^46 + (RootI + 1)*q^49 - RootI*q^52 + (RootI - 1)*q^53 + q^54) +O(q^57)
...              g= ComputeCoeff( g, Eisenstein(Ng,Ng, psi[57], bound) ,bound)
...              if Level>Mod:
...                 gP=0
...                 for r in range (1,(bound/a)+1):
...                     gP = gP + g[r] * q^(a*r);
...                 g=gP
...       if Ng==144:
...           for m in range (-20,1+20):
...              for n in range (-20,1+20):
...                  if m%3==1:
...                     if n%3==0:
...                        if (m+n)%2==1:
...                           g = g + ((-1)^n)*q^(a*(m^2+n^2))
...       if Ng==31:
...           for m in range (-l,l):
...              for n in range (-l,l):
...                 if 0<(m^2+m*n+8*n^2) < l:
...                     g = g + (1/2)* q^(a*(m^2+m*n+8*n^2));
...                 if 0<2*m^2+m*n+4*n^2 < l:
...                     g = g - (1/2)* q^(a*(2*m^2+m*n+4*n^2));
...       if etiquette==0:
...          if Ng==124:
...             e = DirichletGroup(124)
...             psi=e.list()
...             L.<z> = NumberField(x^2-x+1)
...             zeta = L.complex_embeddings()[1](z)
...             g= q - q^4 + (zeta - 1)*q^5 - zeta*q^6 + (-zeta + 1)*q^13
+ zeta*q^14 + q^16 -zeta*q^17 + (-zeta + 1)*q^20 + (zeta - 1)*q^21 + (zeta - 1)*q^22
 + zeta*q^24 + q^30 - q^33 - zeta*q^37 - zeta*q^38 + (zeta - 1)*q^41
+ i* (q^2 + zeta^5*q^3 - zeta^5*q^7 - q^8 + (zeta^5 - 1)*q^10 + (-zeta^5 + 1)*q^11 -
zeta^5*q^12 - q^15 + zeta^5*q^19 + (-zeta^5 + 1)*q^26 - q^27 + zeta^5*q^28 -
q^31 + q^32 - zeta^5*q^34 + q^35 + q^39 + (-zeta^5 + 1)*q^40 + (zeta^5 - 1)*q^42
+ zeta^5*q^43 + (zeta^5 - 1)*q^44) + O(q^45)
...             g= ComputeCoeff( g, Eisenstein(p,p, psi[41], bound) ,bound)
...             if Level>Mod:
...                gP=0
...                for r in range (1,(bound/a)+1):
...                    gP = gP + g[r] * q^(a*r);
...                g=gP
...       if Ng==283:
...          for r in range (1,l):
...              g = g + CoeffIter283(r,etiquette) * q^(a*r);
...       return g + O(q^l)
```

```
# computing all coefficients of g smaller than "bound"
sage: def ComputeCoeff(g,E,bound):
...       R.<q> = PowerSeriesRing(ComplexField(BoP),bound)
...       Sp = CuspForms(Gamma0(p),2,base_ring =ComplexField());
...       Basisp= Sp.basis()
...       dp= CuspForms(Gamma0(p),2).dimension()
...       boundp=2*Sp.sturm_bound()
...       gE1=g*E
...       gE=0
...       for i in range(1,boundp+1):
...           for j in range (0,dp):
...               if Order(Basisp[j],boundp)== i:
...                  gE = gE + gE1[i] * Basisp[j]
...       f1=0
...       f2=E[0]
...       for r in range (1,bound):
...          f1 = f1 + gE[r] * q^(r);
...          f2 = f2 + E[r] * q^(r);
...       v=f1/f2
...       return v

sage: def Order (f,s):
...      Ord=1
...      for i in range (1,s):
...          if f[i]==1:
...             return Ord
...          else:
...             Ord=Ord+1

sage: def MulBy(f, a):
...        R.<q> = PowerSeriesRing(ComplexField(BoP))
...        h=0
...        for i in range(1,(bound/a)+1):
...            for j in range (0,d):
...                if Order(BS[j],bound)== a * i:
...                   h = h + f[i] * BS[j]
...        return h

#test: gE is a modular form?
sage: def Test(Series, Modularform):
...        Cr=0
...        for i in range (0, bound):
...            if abs( Modularform[i] - Series[i]) > 1.1e-6:
...               Cr=1
...        if Cr==1:
...           print "gE is not a modular form"

sage: MatSpa = MatrixSpace(ComplexField(BoP),d)
sage: BasisMS = MatSpa.basis()
sage: VecSpa = VectorSpace(QQbar,bound)
```

```
sage: W = matrix(ComplexField(BoP),d,d)
sage: B = matrix(ComplexField(BoP),d,bound)
sage: OrtA=B.new_matrix()
sage: BB = matrix(ComplexField(BoP),3*d,bound)
sage: Alak=BB.new_matrix()

sage: NewF=Newforms(Gamma0(Nf),2, names='alpha')
sage: l=len(NewF)
sage: redundant=0
sage: counter=0
sage: cs=0

#Computing a basis of newforms for S_{2}(Gamma_{Nf})
sage: D= divisors(Nf)
...   for z in range (0,len(D)):
...       Nd= Nf/D[z]
...       NewF=Newforms(Gamma0(Nd),2, names='alpha')
...       l=len(NewF)
...       Mult= divisors (D[z])
...       MultLen=len(Mult)
...       for i in range (0,l):
...          K=NewF[i].base_ring()
...          redundant=0
...          if K.degree() > 1:
...             u=len (K.complex_embeddings());
...             for j in range (0,u):
...                h=0
...                for s in range (0,d):
...                    Ord=Order(BS[s],bound )
...                    t=K.complex_embeddings()[j](NewF[i][Ord])
...                    h= h + t*BS[s]
...                for v in range(cs,counter):
...                    if OrtA.row(v)==h.coefficients(bound):
...                       redundant=1
...                if redundant==0:
...                   OrtA.set_row(counter, h.coefficients(bound))
...                   counter = counter+1
...                if MultLen>1:
...                   for r in range (1,MultLen):
...                      if redundant==0:
...                          OrtA.set_row(counter, MulBy(h , Mult[r]).coefficients(bound))
...                          counter = counter+1
...                cs=counter
...          else:
...             OrtA.set_row(counter, NewF[i].coefficients(bound) )
...             counter = counter+1
...             if MultLen>1:
...                for r in range (1,MultLen):
...                   OrtA.set_row(counter, MulBy(NewF[i] , Mult[r]).coefficients(bound) )
...                   counter = counter+1
...             cs=counter
```

```
sage: Columns = vector([ Order(BS[i], bound) for i in range (0,d)])
sage: G=W.new_matrix()
sage: for j in range (0,d):
...      G.set_column(j, OrtA.column(Columns[j]-1))

sage: fVector = vector ([ f[Columns[i]] for i in range (0,d)])
sage: Y=vector(ComplexField(BoP), d)
sage: for j in range (0,d):
...      Y.set(j, fVector[j])

# Set the Eisenstein series E in order to compute \alpha_{1} in the formula
#  <Eg,f>=\alhpa_{1}f+\alpha_{2}f_{2}+...+\alpha_{d}f_{d}
sage: if Ng==144:
...      e = DirichletGroup(144)
...      psi=e.list()
# Eisenstein series for Nf=3*144
...      E= 1*Eisenstein(Nf,Ng, psi[1], bound)
            -(psi[1](3))*Eisenstein(Nf,Ng, psi[1], bound)

sage: if Ng==283:
...      e = DirichletGroup(283)
...      psi=e.list()
# Eisenstein series for Nf=2*283
...      E= Eisenstein(Nf,Ng, psi[141], bound)
            - (psi[141](2)/2)*Eisenstein(Ng,Ng, psi[141], bound)

sage: if Ng==229:
...      e = DirichletGroup(229)
...      psi=e.list()
# Eisenstein series for Nf=2*229
...      E= 2*Eisenstein(Nf,Ng, psi[57], bound)
            - (psi[57](2)/1)* Eisenstein(Nf,Ng, psi[57], bound)

sage: if Ng==124:
...      e = DirichletGroup(124)
...      psi=e.list()
...      E= 1*Eisenstein(Nf,Ng, psi[41], bound)

sage: if Ng==47:
...      if etiquette==1:
...         e = DirichletGroup(47)
...         psi=e.list()
...         E= EisensteinP(Nf, Ng, bound)

#sage: E= EisensteinP(Nf, Ng, bound)
sage: print "E=",E

# computing the inverse of G by a numerical method
sage: Id=identity_matrix(d)
sage: GInv=transpose(G)/(G.norm(1)*G.norm(Infinity));
sage: for i in range(0,40):
...      GInv=GInv*(2*Id-G*GInv)
```

```
# Computing the coefficient \alpha_{1}
sage: Div= divisors(Nf/Ng)
sage: Output = Matrix(ComplexField(BoP),4*len(Div),d);
sage: for i in range (0, len(Div)):
...       print "Div[i]*Ng=", Div[i]*Ng
...       Z=vector(ComplexField(BoP), d)
...       print "g=", g(Div[i]*Ng , Ng)
...       gE1= E * g(Div[i]*Ng , Ng)
...       gE = MulBy(gE1,1)
...       Test(gE1, gE)
...       gEVector = vector([ gE[Columns[i]] for i in range (0,d)])
...       for j in range (0,d):
...           Z.set(j, gEVector[j])
...       X=Z*GInv
...       print (X[0].real()).nearby_rational(max_error=0.00001)
# X[0],X[1],... correspond to \alpha_{1} related to elliptic curves of conductor Nf
```

References

[1] T. M. Apostol; Introduction to Analytic Number Theory; Springer-Verlag, 1976.

[2] J. P. Buhler; Icosahedral Galois representations, Springer-Verlag, Berlin, 1978, Lecture Notes in Mathematics, Vol. 654.

[3] K. Buzzard; Computing weight one modular forms over $\mathbb{C}$ and $\overline{\mathbf{F}}_p$.

[4] H. Cohen; Haberland's formula and numerical computation of petersson scalar products, 2012.

[5] T. Crespo; Galois representations, embedding problems and modular forms. Collect. Math. 48 (1997), 63-83.

[6] F. Diamond, Jerry Shurman; A first Course in Modular Forms. Springer, 2005.

[7] P. Deligne and J.-P. Serre; Formes modulaires de poids 1. Annales scientifiques de l'E.N.S. 4^e serie, 7:507-530, 1974.

[8] P. Deligne; Valeurs de fonctions L et periodes d'integrales, in Automorphic Forms, Representations, and L-functions, Proc. Symp. Pure Math., Vol. 33, part 2, Amer. Math. Soc, Providence, Rhode Island, 1979, pp. 313-346.

[9] G. Frey (ed.); On Artin's conjecture for odd 2-dimensional representations, Springer-Verlag, Berlin, 1994.

[10] H. Hida; Elementary theory of L-functions and Eisenstein series, London Math. Soc. Student Texts 26. Cambridge University Press, second edition, 1993.

[11] T. Miyake; Modular forms. Springer-Verlag, 1989.

[12] A. P. Ogg; Elliptic curves and wild ramification; Amer. J. Math., 89:1-21, 1967.

[13] R. E. Rohrlich; The vanishing of certain Rankin-Selberg convolutions, Automorphic Forms and Analytic Number Theory, Les publications CRM, Montreal, 1990, pp 123-133.

[14] J.-P. Serre; Proprietes galoisiennes des points d'ordre fini des courbes elliptiques. Invent. Math, vol. 15:259-331, 1972.

[15] J.-P. Serre; A course in arithmetic. Springer-Verlag, New York, Graduate Texts in Mathematics, 1973.

[16] J.-P. Serre; Modular forms of weight one and galois representations. Algebraic Number Fields, ed A. Frohlich, Proc. Symp. Durham 1975, 193-268, Academic Press (London), 1977.

[17] J. H. Silverman; The arithmetic of elliptic curves; Springer, second edition, 2008.

[18] Y. TANIGAWA; On Cusp Forms of Octahedral Type; Proc. Japan Acad., 62, Ser. A ,1986.

[19] D. Zagier; Introduction to modular forms, in From Number Theory to Physics, eds. M. Waldschmidt et al, Springer-Verlag, Heidelberg (1992) 238-291.

[20] L. Washington; Introduction to Cyclotomic Fields, 2nd edition, Springer-Verlag, New York, 1997.

[21] H. Weber; Lehrbuch der Algebra, Bd. II (zw. Auf.) Braunschweig 1899.