On the Fourier coefficients of a Cohen-Eisenstein series

Srilakshmi Krishnamoorthy
Inspire Faculty, I.I.T. Madras

Theoretical and Computational Aspects of the BSD Conjecture
ICTS, Bangalore

Dec 22nd, 2016

Cohen-Eisenstein series

Let $N = p_1 p_2 \ldots p_k M$ be a squarefree integer.
Let B be a definite quaternion algebra ramified at primes $p_1, p_2, \ldots, p_k$ and at ∞.
Let $\mathcal{O}$ be an order of level N.
Let $I_1, I_2, \ldots, I_n$ be a set of left ideals representing the distinct ideal classes of $\mathcal{O}$, with $I_1 = \mathcal{O}$ and $R_1, R_2, \ldots, R_n$ be the respective right orders of each ideal I_i.
For each R_i, let L_i be the lattice $\mathbb{Z} + 2R_i$.
Denote the trace zero elements of L_i by S_i^0.
For $b \in S_i^0$, let $\mathbb{N}(b)$ be the norm of b. For each $i = 1$ to n, Define

$$g_i = \frac{1}{2} \sum_{b \in S_i^0} q^{\mathbb{N}(b)}, \ q = e^{2\pi i z}.$$

Cohen-Eisenstein series

- The modular forms g_i are in the Kohnen's plus-space [the space of modular forms of weight $3/2$ on $\Gamma_0(4N)$ whose Fourier coefficients a_m are 0 if $-m \equiv 2, 3 \pmod 4$.]
- The Cohen-Eisenstein series $\mathcal{G}$ is defined by $\mathcal{G} = \sum_{i=1}^{n} \frac{1}{w_i} g_i$.

Shimura Lift

- Let $f \in S_2(N)$ be a normalized newform. It corresponds to a one-dimensional eigenspace $\langle v = (v_1, v_2, ..., v_n) \rangle$, of the Brandt matrices $\{B_p\}$ in B, such that $B_p v = a_p v$, where a_p is the eigenvalue satisfying $T_p f = a_p f$, for all p.

  Let w_i be the order of the finite group $R_i^* / \pm 1$ for $i = 1$ to n.Then

$$\mathcal{H} = \sum_{i=1}^{n} \frac{v_i}{w_i} g_i = \sum_{d} m_d q^d$$

  is the weight $3/2$ modular form which corresponds to f via the Shimura correspondence.

Shimura Lift

The modular form $\mathcal{H} = \sum_{i=1}^{n} \frac{v_i}{w_i} g_i = \sum_d m_d q^d$ is zero unless

$$\mathrm{sgn}(W_p) = \begin{cases} -1, & \text{for } p = p_i, i = 1 \textit{ to } k \\ +1, & \text{for } \; p \mid M. \end{cases}$$

Let d be a natural number and let $\mathcal{O}_d$ be the ring of integers in $\mathbb{Q}(\sqrt{-d})$. let $h(d)$ be the cardinality of the group $\mathrm{Pic}(\mathcal{O}_d)$, and let $2u(d)$ be the cardinality of the unit group $\mathcal{O}_d^*$.

Let d be a natural number and let $\mathcal{O}_d$ be the ring of integers in $\mathbb{Q}(\sqrt{-d})$. let $h(d)$ be the cardinality of the group $\mathrm{Pic}(\mathcal{O}_d)$, and let $2u(d)$ be the cardinality of the unit group $\mathcal{O}_d^*$.

- The Legendre symbol $(\frac{-d}{p})$ is defined by

$$(\frac{-d}{p}) := \begin{cases} 1, & \text{if } p \text{ splits in } K \\ 0, & \text{if } p \text{ ramifies in } K \\ -1, & \text{if } p \text{ inert in } K. \end{cases}$$

Let d be a natural number and let $\mathcal{O}_d$ be the ring of integers in $\mathbb{Q}(\sqrt{-d})$. let $h(d)$ be the cardinality of the group $\mathrm{Pic}(\mathcal{O}_d)$, and let $2u(d)$ be the cardinality of the unit group $\mathcal{O}_d^*$.

- The Legendre symbol $(\frac{-d}{p})$ is defined by

$$(\frac{-d}{p}) := \begin{cases} 1, & \text{if } p \text{ splits in } K \\ 0, & \text{if } p \text{ ramifies in } K \\ -1, & \text{if } p \text{ inert in } K. \end{cases}$$

Let c be the conductor of $\mathcal{O}_d$.

Let d be a natural number and let $\mathcal{O}_d$ be the ring of integers in $\mathbb{Q}(\sqrt{-d})$. let $h(d)$ be the cardinality of the group $\mathrm{Pic}(\mathcal{O}_d)$, and let $2u(d)$ be the cardinality of the unit group $\mathcal{O}_d^*$.

- The Legendre symbol $(\frac{-d}{p})$ is defined by

$$(\frac{-d}{p}) := \begin{cases} 1, & \text{if } p \text{ splits in } K \\ 0, & \text{if } p \text{ ramifies in } K \\ -1, & \text{if } p \text{ inert in } K. \end{cases}$$

  Let c be the conductor of $\mathcal{O}_d$.

- The Eichler symbol $\{\frac{-d}{p}\}$ is defined by

$$\{\frac{-d}{p}\} := \begin{cases} 1, & \text{if } p^2 \mid c \\ (\frac{-d}{p}), & \text{if } p^2 \nmid c. \end{cases}$$

Waldspurger's formula

- Let D be a natural number and $-D$ be a fundamental discriminant. If $(\frac{-D}{p})\mathrm{sgn}(W_p) \neq -1$ for every prime $p \mid N$, then the following Waldspurger's formula holds.

Waldspurger's formula

- Let D be a natural number and $-D$ be a fundamental discriminant. If $(\frac{-D}{p})\mathrm{sgn}(W_p) \neq -1$ for every prime $p \mid N$, then the following Waldspurger's formula holds.

$$\prod_{p \mid \frac{N}{\mathrm{gcd}(N,D)}} (1+(\frac{-D}{p})sgn(W_p))L(f,1)L(f\otimes\epsilon_D,1) = \frac{2^{\omega(N)}(f,f)m_D^2}{\sqrt{D}\sum_{i=1}^{n}\frac{v_i^2}{w_i^2}},$$

where $\omega(N)$ is the number of distinct primes that divide N.

Gross's formula

- Theorem (Gross)

  If N is prime and $-D$ is a fundamental discriminant such that $(\frac{-D}{N}) \neq 1$, then the coefficients $\mathcal{G}(D)$ of the weight $3/2$ Eisenstein series,

$$\mathcal{G} = \sum_{i=1}^{n} \frac{1}{w_i} g_i = \sum_{i=1}^{n} \frac{1}{2w_i} + \sum_{d>0} \mathcal{G}(d) q^d,$$

  are given by

$$\mathcal{G}(D) = \frac{(1 - (\frac{-D}{N}))}{2} \frac{h(D)}{u(D)}.$$

A Conjecture

- What can we say about the coefficients when the level N is squarefree?

A Conjecture

- What can we say about the coefficients when the level N is squarefree?

Quattrini presented the following conjecture on the coefficients of $\mathcal{G}$.

A Conjecture

- What can we say about the coefficients when the level N is squarefree?

Quattrini presented the following conjecture on the coefficients of $\mathcal{G}$.

- Conjecture (Quattrini)

Let B be a quaternion algebra ramified at exactly one finite prime p and let $N = pM$ be a square free integer. Let $\mathcal{G} = \sum_{i=1}^{n} \frac{1}{w_i} g_i = \sum_{i=1}^{n} \frac{1}{2w_i} + \sum_{d>0} \mathcal{G}(d) q^d$. Let $D \in \mathbb{N}$ be such that $-D$ is a fundamental discriminant and $\left(\frac{-D}{p}\right) \neq 1$, and $\left(\frac{-D}{q}\right) \neq -1$ for every prime $q \mid M$. If $s(D)$ is the number of primes that divide N and ramify in $\mathbb{Q}(\sqrt{-D})$, then

$$\mathcal{G}(D) = \frac{2^{\omega(N)-s(D)-1} h(D)}{u(D)}.$$

Some Numerical Examples

$E = 14A1 = [1, 0, 1, 4, -6]$ has conductor $N = 14$ and a 3-torsion point.

$\mathrm{sgn}(W_7) = -1$ and $\mathrm{sgn}(W_2) = +1$.

We consider the quaternion algebra ramified at the prime 7 and ∞.

For $D \leq 1000$ such that $-D$ is a fundamental discriminant and $(\frac{-D}{7}) \neq 1$ and $(\frac{-D}{2}) \neq -1$, the coefficients of $\mathcal{G}$ are given by

$$\mathcal{G}(D) = \begin{cases} 2\frac{h(D)}{u(\mathcal{O}_D)}, & \text{if } 7 \text{ is inert and } 2 \text{ splits in } \mathcal{O}_D \\ \frac{h(D)}{u(\mathcal{O}_D)}, & \text{if } 7 \text{ is inert and } 2 \text{ ramified in } \mathcal{O}_D \\ \frac{h(D)}{u(\mathcal{O}_D)}, & \text{if } 7 \text{ is ramified and } 2 \text{ splits in } \mathcal{O}_D \\ \frac{1}{2}h(D), & \text{if } 7 \text{ and } 2 \text{ ramify in } \mathcal{O}_D. \end{cases}$$

Some Numerical Examples

$E = 26A1 = [1, 0, 1, -5, -8]$ has conductor $N = 26$ and a 3-torsion point.

$\mathrm{sgn}(W_{13}) = -1$ and $\mathrm{sgn}(W_2) = +1$.

We consider the quaternion algebra ramified at the prime 13 and ∞.

For $D \leq 1000$ such that $-D$ is a fundamental discriminant and $(\frac{-D}{13}) \neq 1$ and $(\frac{-D}{2}) \neq -1$, we get

$$\mathcal{G}(D) = \begin{cases} 2\frac{h(D)}{u(\mathcal{O}_D)}, & \text{if } 13 \text{ is inert and } 2 \text{ splits in } \mathcal{O}_D \\ \frac{h(D)}{u(\mathcal{O}_D)}, & \text{if } 13 \text{ is inert and } 2 \text{ ramified in } \mathcal{O}_D \\ \frac{h(D)}{u(\mathcal{O}_D)}, & \text{if } 13 \text{ is ramified and } 2 \text{ splits in } \mathcal{O}_D \\ \frac{1}{2}\frac{h(D)}{u(\mathcal{O}_D)}, & \text{if } 13 \text{ and } 2 \text{ ramify in } \mathcal{O}_D. \end{cases}$$

Some Numerical Examples

$E = 30A11 = [1, 0, 1, 1, 2]$ has a 2 and 3-torsion point.

$\mathrm{sgn}(W_3) = -1$ and $\mathrm{sgn}(W_2) = \mathrm{sgn}(W_5) = +1$.

We consider the quaternion algebra ramified at the prime 3 and ∞.

For $D \leq 1000$ such that $-D$ is a fundamental discriminant and $(\frac{-D}{3}) \neq 1$, $(\frac{-D}{2}) \neq -1$, $(\frac{-D}{5}) \neq -1$, we get

$$\mathcal{G}(D) = \begin{cases} 2^2 \frac{h(D)}{u(\mathcal{O}_D)}, & \text{if } 3 \text{ is inert and 2,5 split in } \mathcal{O}_D \\ 2\frac{h(D)}{u(\mathcal{O}_D)}, & \text{if exactly one of the primes 2,3,5 ramifies in } \mathcal{O}_D \\ \frac{h(D)}{u(\mathcal{O}_D)}, & \text{if exactly two of the primes ramify in } \mathcal{O}_D \\ \frac{1}{2}\frac{h(D)}{u(\mathcal{O}_D)}, & \text{if 2,3,5 all ramify in } \mathcal{O}_D. \end{cases}$$

Main Theorem

Let B be a definite quaternion algebra ramified at $p_1, p_2, ..., p_k$ and at ∞. Let $N = p_1 p_2 ... p_k M$ be a square free integer. Denote by $\mathcal{G} = \sum_{i=1}^{n} \frac{1}{w_i} g_i = \sum_{i=1}^{n} \frac{1}{2w_i} + \sum_{d>0} \mathcal{G}(d) q^d$. Let $D \in \mathbb{N}$ such that $-D$ is a fundamental discriminant and $(\frac{-D}{p_i}) \neq 1$ for $i = 1$ to k and $(\frac{-D}{q}) \neq -1$ for every prime $q \mid M$, then

$$\mathcal{G}(D) = \frac{2^{\omega(N)-s(D)-1} h(D)}{u(D)}.$$

Main Theorem

Let B be a definite quaternion algebra ramified at $p_1, p_2, ..., p_k$ and at ∞. Let $N = p_1 p_2 ... p_k M$ be a square free integer. Denote by $\mathcal{G} = \sum_{i=1}^{n} \frac{1}{w_i} g_i = \sum_{i=1}^{n} \frac{1}{2w_i} + \sum_{d>0} \mathcal{G}(d) q^d$. Let $D \in \mathbb{N}$ such that $-D$ is a fundamental discriminant and $(\frac{-D}{p_i}) \neq 1$ for $i = 1$ to k and $(\frac{-D}{q}) \neq -1$ for every prime $q \mid M$, then

$$\mathcal{G}(D) = \frac{2^{\omega(N)-s(D)-1} h(D)}{u(D)}.$$

Corollary

Quattrini's Conjecture holds by letting $k = 1$ in the above theorem.

Optimal embeddings

Let K be a quadratic field over $\mathbb{Q}$ such that the primes $p_1, p_2, \ldots, p_k$ are either ramified or inert in K. Let ϕ be an embedding of K into B. The field K is totally imaginary as B is a definite quaternion algebra. Let $\mathcal{O}_d$ be an order of K of discriminant d.

Optimal embeddings

Let K be a quadratic field over $\mathbb{Q}$ such that the primes $p_1, p_2, \ldots, p_k$ are either ramified or inert in K. Let ϕ be an embedding of K into B. The field K is totally imaginary as B is a definite quaternion algebra. Let $\mathcal{O}_d$ be an order of K of discriminant d.

Definition

We say that ϕ is an optimal embedding of the order $\mathcal{O}_d$ into R_i if ϕ is an embedding of K into B such that $\phi(\mathcal{O}_d) = \phi(K) \cap R_i$.

Optimal embeddings

Let K be a quadratic field over $\mathbb{Q}$ such that the primes $p_1, p_2, ..., p_k$ are either ramified or inert in K. Let ϕ be an embedding of K into B. The field K is totally imaginary as B is a definite quaternion algebra. Let $\mathcal{O}_d$ be an order of K of discriminant d.

Definition

We say that ϕ is an optimal embedding of the order $\mathcal{O}_d$ into R_i if ϕ is an embedding of K into B such that $\phi(\mathcal{O}_d) = \phi(K) \cap R_i$.

- Two optimal embeddings i_1, i_2 are equivalent if they are conjugate to each other by an element in R_i^*. In other words, if there exists $x \in R_i^*$ such that $i_1(y) = x i_2(y) x^{-1}$ for all $y \in K$.

Optimal embeddings

Proposition

Let $h(\mathcal{O}_d, R_i)$ be the number of equivalence classes of optimal embeddings of the order of discriminant d into R_i. Let $h(d)$ be the cardinality of the group $\mathrm{Pic}(\mathcal{O}_d)$. Then

$$\sum_{i=1}^{n} h(\mathcal{O}_d, R_i) = h(d) \prod_{i=1}^{k} (1 - \{\frac{-d}{p_i}\}) \prod_{q|M} (1 + \{\frac{-d}{q}\}).$$

Optimal embeddings

Proposition

Let $h(\mathcal{O}_d, R_i)$ be the number of equivalence classes of optimal embeddings of the order of discriminant d into R_i. Let $h(d)$ be the cardinality of the group $\mathrm{Pic}(\mathcal{O}_d)$. Then

$$\sum_{i=1}^{n} h(\mathcal{O}_d, R_i) = h(d) \prod_{i=1}^{k} (1 - \{\frac{-d}{p_i}\}) \prod_{q|M} (1 + \{\frac{-d}{q}\}).$$

Sketch of the proof. Let $\{\mathfrak{M}\}$ be a system of representatives of two-sided R_i ideals modulo two-sided R_i ideals of the form $R_i\xi$ where ξ is an $\mathcal{O}_d$ ideal. Let $\{\mathfrak{B}\}$ be a system of representatives of the ideal classes in $\mathcal{O}_d$.

Optimal embeddings

Consider the set of all $(\mathfrak{M}, \mathfrak{B})$ such that

- (1) The norm of $\mathfrak{M}$ is squarefree and if q is a prime divisor of the norm of $\mathfrak{M}$, then either $q = p_i$ (for some $i = 1$ to k) with $\{\frac{-d}{p_i}\} = -1$ or q is a prime divisor of M with $\{\frac{-d}{q}\} = 1$,

Optimal embeddings

Consider the set of all $(\mathfrak{M}, \mathfrak{B})$ such that

- (1) The norm of $\mathfrak{M}$ is squarefree and if q is a prime divisor of the norm of $\mathfrak{M}$, then either $q = p_i$ (for some $i = 1$ to k) with $\{\frac{-d}{p_i}\} = -1$ or q is a prime divisor of M with $\{\frac{-d}{q}\} = 1$,
- (2) $\mathfrak{B}$ is an integral ideal coprime to the conductor of $\mathcal{O}_d$.

Optimal embeddings

Consider the set of all $(\mathfrak{M}, \mathfrak{B})$ such that

- (1) The norm of $\mathfrak{M}$ is squarefree and if q is a prime divisor of the norm of $\mathfrak{M}$, then either $q = p_i$ (for some $i = 1$ to k) with $\{\frac{-d}{p_i}\} = -1$ or q is a prime divisor of M with $\{\frac{-d}{q}\} = 1$,
- (2) $\mathfrak{B}$ is an integral ideal coprime to the conductor of $\mathcal{O}_d$.

The number of pairs $(\mathfrak{M}, \mathfrak{B})$ satisfying the conditions (1) and (2) is equal to

$$h(d) \prod_{i=1}^{k} (1 - \{\frac{-d}{p_i}\}) \prod_{q|M} (1 + \{\frac{-d}{q}\}).$$

Optimal embeddings

There is a one-to-one correspondence between the set of all pairs $(\mathfrak{M}, \mathfrak{B})$ satisfying (1) and (2) and equivalence classes of optimal embeddings of the order of discriminant d into R_i. Hence

$$\sum_{i=1}^{n} h(\mathcal{O}_d, R_i) = h(d) \prod_{i=1}^{k} (1 - \{\frac{-d}{p_i}\}) \prod_{q|M} (1 + \{\frac{-d}{q}\}).$$

Fourier coefficients of the modular forms g_i

Proposition

Let $g_i = \frac{1}{2} + \frac{1}{2}\sum_{d>0} a_i(d) q^d$. *Then* $a_i(d)$ *is the number of elements* $b \in R_i$ *with* $\mathrm{Tr}(b) = 0$, $b \in \mathbb{Z} + 2R_i$, $\mathbb{N}(b) = d$. *For* $i = 1$ *to* n, *we have*

$$a_i(d) = w_i \sum_{-d=-Df^2} \frac{h(\mathcal{O}_D, R_i)}{u(D)},$$

where $u(D) = \begin{cases} 3, & \text{if } -D = -3 \\ 2, & \text{if } -D = -4 \\ 1 & \text{otherwise.} \end{cases}$

Fourier coefficients of the modular forms g_i

Sketch of the proof.

Let S be the set of elements $b \in R_i$ with $\mathrm{Tr}(b) = 0$, $b \in \mathbb{Z} + 2R_i$ and $\mathbb{N}(b) = d$.

For a positive integer D, if $g : \mathbb{Q}(\sqrt{-D}) \hookrightarrow B$ is an embedding of an order $\mathcal{O}_D$ into R_i, then $b = g(\sqrt{-D})$ is an element in $\{x \in B | \mathrm{Tr}(x) = 0\}$ and the norm of b is D. Since $\mathcal{O}_D = \mathbb{Z} + \mathbb{Z}\frac{(D+\sqrt{-D}))}{2}$, we have $b \in (\mathbb{Z} + 2R_i)$.

$$\Rightarrow b \in S_i^0 = \{x \in B | \mathrm{Tr}(x) = 0\} \cap (\mathbb{Z} + 2R_i).$$

Fourier coefficients of the modular forms g_i

Conversely, if b is an element in S_i^0 such that the norm of b is D , then $g(\sqrt{-D}) = b$ gives rise to an embedding of the order $\mathcal{O}_D = \mathbb{Z} + \mathbb{Z}\frac{(D+\sqrt{-D})}{2}$ into R_i.

Fourier coefficients of the modular forms g_i

Conversely, if b is an element in S_i^0 such that the norm of b is D , then $g(\sqrt{-D}) = b$ gives rise to an embedding of the order $\mathcal{O}_D = \mathbb{Z} + \mathbb{Z}\frac{(D+\sqrt{-D})}{2}$ into R_i.

The embedding $g(\sqrt{-D}) = b$ is optimal if and only if $b \notin m(\mathbb{Z} + 2R_i)$ for some $m > 1$. Let $h^*(\mathcal{O}_D, R_i)$ be the number of optimal embeddings of $\mathcal{O}_D$ into R_i.

Fourier coefficients of the modular forms g_i

Conversely, if b is an element in S_i^0 such that the norm of b is D , then $g(\sqrt{-D}) = b$ gives rise to an embedding of the order $\mathcal{O}_D = \mathbb{Z} + \mathbb{Z}\frac{(D+\sqrt{-D})}{2}$ into R_i.

The embedding $g(\sqrt{-D}) = b$ is optimal if and only if $b \notin m(\mathbb{Z} + 2R_i)$ for some $m > 1$. Let $h^*(\mathcal{O}_D, R_i)$ be the number of optimal embeddings of $\mathcal{O}_D$ into R_i.

Using the above connection we get

$$a_i(d) = \sharp S = \sum_{-d=-Df^2} \{b \in S, \frac{b}{f} \in S_i^0, \frac{b}{f} \notin m(\mathbb{Z}+2R_i) \text{ for } m > 1\}.$$

$$= \sum_{-d=-Df^2} h^*(\mathcal{O}_D, R_i).$$

Fourier coefficients of the modular forms g_i

The group $\Gamma_i = R_i^* / \pm 1$ acts on S. The Γ_i orbits of S correspond to equivalence classes of optimal embeddings. Hence

$$\sharp\ S/\Gamma_i = \sum_{-d=-Df^2} h(\mathcal{O}_D, R_i).$$

The order of the stabilizer of an element $b \in S$ is 1 unless the corresponding embedding extends to $\mathbb{Z}[\mu_6]$ or $\mathbb{Z}[\mu_4]$, when it is 3 or 2 respectively.

Fourier coefficients of the modular forms g_i

The group $\Gamma_i = R_i^* / \pm 1$ acts on S. The Γ_i orbits of S correspond to equivalence classes of optimal embeddings. Hence

$$\sharp\, S/\Gamma_i = \sum_{-d=-Df^2} h(\mathcal{O}_D, R_i).$$

The order of the stabilizer of an element $b \in S$ is 1 unless the corresponding embedding extends to $\mathbb{Z}[\mu_6]$ or $\mathbb{Z}[\mu_4]$, when it is 3 or 2 respectively.

Thus we see that

$$a_i(d) = \#\Gamma_i \sum_{-d=-Df^2} \frac{h(\mathcal{O}_D, R_i)}{u(D)} = w_i \sum_{-d=-Df^2} \frac{h(\mathcal{O}_D, R_i)}{u(D)}.$$

Proof of the Main Theorem

Proof

- Consider the weight 3/2 Cohen-Eisenstein Series $\mathcal{G}$,

$$\mathcal{G} = \sum_{i=1}^{n} \frac{1}{w_i} g_i = \frac{1}{2} \sum_{i=1}^{n} \frac{1}{w_i} + \sum_{d>0} \sum_{i=1}^{n} \frac{a_i(d)}{w_i} q^d.$$

Proof of the Main Theorem

Proof

- Consider the weight 3/2 Cohen-Eisenstein Series $\mathcal{G}$,

$$\mathcal{G} = \sum_{i=1}^{n} \frac{1}{w_i} g_i = \frac{1}{2} \sum_{i=1}^{n} \frac{1}{w_i} + \sum_{d>0} \sum_{i=1}^{n} \frac{a_i(d)}{w_i} q^d.$$

We know that

- $$\sum_{i=1}^{n} \sum_{d>0} \frac{a_i(d)}{w_i} q^d = \frac{1}{2} \sum_{d>0} \sum_{-d=-Df^2} \left(\sum_{i=1}^{n} \frac{h(\mathcal{O}_D, R_i)}{u(D)} \right).$$

Proof of the Main Theorem

Proof

- Consider the weight 3/2 Cohen-Eisenstein Series $\mathcal{G}$,

$$\mathcal{G} = \sum_{i=1}^{n} \frac{1}{w_i} g_i = \frac{1}{2} \sum_{i=1}^{n} \frac{1}{w_i} + \sum_{d>0} \sum_{i=1}^{n} \frac{a_i(d)}{w_i} q^d.$$

We know that

- $$\sum_{i=1}^{n} \sum_{d>0} \frac{a_i(d)}{w_i} q^d = \frac{1}{2} \sum_{d>0} \sum_{-d=-Df^2} \left(\sum_{i=1}^{n} \frac{h(\mathcal{O}_D, R_i)}{u(D)} \right).$$

- $$\sum_{i=1}^{n} h(\mathcal{O}_D, R_i) = h(D) \prod_{i=1}^{k} \left(1 - \{\frac{-D}{p_i}\}\right) \prod_{q|M} \left(1 + \{\frac{-D}{q}\}\right).$$

Proof of the Main Theorem

Hence

$$\mathcal{G} = \sum_{i=1}^{n} \frac{1}{w_i} g_i = \frac{1}{2} \sum_{i=1}^{n} \frac{1}{w_i} + \sum_{d>0} \mathcal{G}(d) q^d,$$

where

$$\mathcal{G}(d) = \frac{1}{2} \sum_{-d=-Df^2} \left[\frac{h(D)}{u(D)} \prod_{i=1}^{k} \left(1 - \left\{ \frac{-D}{p_i} \right\} \right) \prod_{q|M} \left(1 + \left\{ \frac{-D}{q} \right\} \right) \right].$$

Proof of the Main Theorem

Hence

$$\mathcal{G} = \sum_{i=1}^{n} \frac{1}{w_i} g_i = \frac{1}{2} \sum_{i=1}^{n} \frac{1}{w_i} + \sum_{d>0} \mathcal{G}(d) q^d,$$

where

$$\mathcal{G}(d) = \frac{1}{2} \sum_{-d=-Df^2} \left[\frac{h(D)}{u(D)} \prod_{i=1}^{k} \left(1 - \{\frac{-D}{p_i}\}\right) \prod_{q|M} \left(1 + \{\frac{-D}{q}\}\right)\right].$$

- In particular, if $-D$ is the fundamental discriminant and $(\frac{-D}{p_i}) \neq 1$, for every $i = 1$ to k, and $(\frac{-D}{q}) \neq -1$ for every prime $q \mid M$, then

$$\mathcal{G}_N(D) = \frac{2^{\omega(N)-s(D)-1} h(D)}{u(D)}.$$

.

Application

We have an equation which relates L-function of f with the coefficients m_D^2,

$$\prod_{p|\frac{N}{\gcd(N,D)}}(1+(\frac{-D}{p})sgn(W_p))L(f,1)L(f\otimes\epsilon_D,1)=\frac{2^{\omega(N)}(f,f)m_D^2}{\sqrt{D}\sum\frac{v_i^2}{w_i^2}}.$$

Application

We have an equation which relates L-function of f with the coefficients m_D^2,

$$\prod_{p|\frac{N}{\gcd(N,D)}} (1+(\frac{-D}{p})sgn(W_p))L(f,1)L(f\otimes\epsilon_D,1) = \frac{2^{\omega(N)}(f,f)m_D^2}{\sqrt{D}\sum\frac{v_i^2}{w_i^2}}.$$

If E is the elliptic curve with conductor N associated with $f\in S_2(\Gamma_0(N))$, then we have $L(E,1)=L(f,1)$ and the L-function $L(f\otimes\epsilon_D,1)=L(E_D,1)$, where E_D is the $-D$ quadratic twist of E associated with $f\otimes\epsilon_D\in S_2(\Gamma_0(ND^2))$.

Order of the Tate-Shafarevich group

Assume that the rank of E is 0.

The rank 0 case of Birch-Swinnerton Conjecture gives

$$\frac{L(E_D, 1)}{\Omega_D} = \frac{\#\mathrm{Sh}_D \prod c_{p,D}}{|\mathrm{Tor}(E_D)|^2},$$

where $c_{p,D}$'s are the Tamagawa numbers and $\mathrm{Tor}(E_D)$ is the torsion subgroup of $E_D(\mathbb{Q})$, Ω_D is the real period of E_D.

Order of the Tate-Shafarevich group

Assume that the rank of E is 0.

The rank 0 case of Birch-Swinnerton Conjecture gives

$$\frac{L(E_D,1)}{\Omega_D} = \frac{\#\mathrm{Sh}_D \prod c_{p,D}}{|\mathrm{Tor}(E_D)|^2},$$

where $c_{p,D}$'s are the Tamagawa numbers and $\mathrm{Tor}(E_D)$ is the torsion subgroup of $E_D(\mathbb{Q})$, Ω_D is the real period of E_D.
Under the assumptions, $(\frac{-D}{p})sgn(W_p) = 1$ for all $p \mid \frac{N}{\gcd(N,D)}$, and $\#\mathrm{Sh}_D = \frac{m_D^2}{2^*}$ for some integer $*$, cardinality of Sh_D is related to the class number.

Order of the Tate-Shafarevich group

Proposition

Let E be an elliptic curve of analytic rank zero and square-free conductor N. Let $\{p_1, p_2, ..., p_k\}$ $=\{p \mid N$ and sign of W_p is $-1\}$. Suppose k is odd.
Consider the family $\{E_D\}$ of negative quadratic twists of E satisfying the condition $(\frac{-D}{p_i}) \neq 1$ for $i = 1$ to k and $(\frac{-D}{q}) \neq -1$ for every prime $q \mid M$, where $N = p_1 p_2 ... p_k . M$. Suppose E has a torsion point defined over $\mathbb{Q}$, of odd prime order l and that $\#\mathrm{Sh}_D = \frac{m_D^2}{2^*}$. Assume that $\lambda u \equiv v \pmod{l}$, for some $\lambda \in \mathbb{F}_l^\times$.
Then, $\#\mathrm{Sh}_D$ is divisible by l, if and only if the class number $h(D)$ of $\mathbb{Q}(\sqrt{-D})$ is divisible by l.

Order of the Tate-Shafarevich group

Some examples of elliptic curves satisfying the hypotheses of the Proposition.

- From Cremona's tables, the strong Weil curves of rank zero and prime conductor with an odd torsion point, are listed by $E = 11A1$, $E = 19A1$ and $E = 37B1$. The first one has a 5-torsion point. The other two curves have a 3-torsion point. For the (-D) quadratic twists of E, We also have $\#\mathrm{Sh}_D$ is m_D^2, upto a power of 2.

- For the elliptic curves $17A1$, $67A1$, $73A1$, $89B1$, $109A1$, $139A1$, $307A1$, $307B1$, $307C1$, $307D1$ with $D \leq 10^6$ and for the elliptic curves $14A1$, $26A1$, $26B1$ with $D \leq 2000$, we have $\#\mathrm{Sh}_D$ is m_D^2, upto a power of 2.

Order of the Tate-Shafarevich group

Proof.

- Consider $\lambda\mathcal{G} - \mathcal{H} = \sum_{i=1}^{n} \frac{(\lambda - v_i)}{w_i} g_i$.

Order of the Tate-Shafarevich group

Proof.

- Consider $\lambda\mathcal{G} - \mathcal{H} = \sum_{i=1}^{n} \frac{(\lambda - v_i)}{w_i} g_i$.
- If l is an odd prime number, dividing the order of the group of torsion points of the elliptic curve E, by Mazur's theorem, $l = 3, 5$ or 7. We know that $w_i \mid 12$, the product $\prod_{i=1}^{n} w_i$ equals the exact denominator of $\frac{N-1}{12}$ and 3 divides the exact numerator of $\frac{N-1}{12}$. Hence $w_i \in \mathbb{F}_l^{\times}$ for $l = 3, 5$ or 7.

Order of the Tate-Shafarevich group

Proof.

- Consider $\lambda\mathcal{G} - \mathcal{H} = \sum_{i=1}^{n} \frac{(\lambda - v_i)}{w_i} g_i$.
- If l is an odd prime number, dividing the order of the group of torsion points of the elliptic curve E, by Mazur's theorem, $l = 3, 5$ or 7. We know that $w_i \mid 12$, the product $\prod_{i=1}^{n} w_i$ equals the exact denominator of $\frac{N-1}{12}$ and 3 divides the exact numerator of $\frac{N-1}{12}$. Hence $w_i \in \mathbb{F}_l^{\times}$ for $l = 3, 5$ or 7.
- The congruence $\lambda u \equiv v \pmod{l}$, for some $\lambda \in \mathbb{F}_l^{\times}$ gives a congruence $\lambda\mathcal{G} \equiv \mathcal{H} \pmod{l}$.
- We get the congruence on the coefficients, $\lambda\mathcal{G}(D) \equiv m_D^2 \pmod{l}$. Hence l divides $h(D)$ if and only if $\#\mathrm{Sh}_D$.

□

Bibliography

S. Bocherer, R. Schulze-Pillot, On a theorem of Waldspurger and on Eisenstein series of Klingen type, *Math. Ann.*, 288, (1990), 361–388.

M. Eichler, Zur Zahlentheorie der Quaternion-Algebren. *J. Reine Angew. Math.*, **195** (1955), 127–151.

G. Frey, On the Selmer group of twists of elliptic curves with Q-rational torsion points, *Canad. J. Math.*, Vol **40**, no. 3, (1988) 649–665.

B. Gross, Heights and the special values of L-series, *CMS conference Proceedings*, Vol **7**, (1987), 115–187.

K. James, Elliptic curves satisfying the Birch and Swinnerton Dyer conjecture and mod 3 *J. Number Theory.* Vol **128** (2008) 2823–2835.

Bibliography

P.L. Quattrini, The effect of torsion on the distribution of Sh among quadratic twists of an elliptic curve, *Journal of Number Theory*, no. 2, (2011), 195–211.

K. Ono, Nonvanishing of quadratic twists of modular *l*-functions and applications to elliptic curves *J. Reine Angew. Math.* Vol **553** (2001), 81–97.

H. Shimizu, On Zeta Functions of Quaternion Algebras *Ann. Math.* Vol **81** no. 1, (1965), 166–193.

S. Wong, Elliptic curves and class number divisibility *Int. Math. Res. Not.*, **12** (1999), 661–672.

Thank you