

A NOTE ON THE FOURIER COEFFICIENTS OF A COHEN-EISENSTEIN SERIES

SRILAKSHMI KRISHNAMOORTHY

ABSTRACT. We prove a formula for the coefficients of a weight $3/2$ Cohen-Eisenstein series of square-free level N . This formula generalizes a result of Gross and in particular, it proves a conjecture of Quattrini. Let l be an odd prime number. For any elliptic curve E defined over \mathbb{Q} of rank zero and square-free conductor N , if $l \mid |E(\mathbb{Q})|$, under certain conditions on the Shafarevich-Tate group III_D , we show that l divides $|\text{III}_D|$ if and only if l divides the class number $h(-D)$ of $\mathbb{Q}(\sqrt{-D})$.

Keywords: Half-integral weight modular forms; Fourier coefficients, Shafarevich-Tate group.

Mathematics Subject Classification: Primary 11F37; Secondary: 11F67, 11R52.

1. INTRODUCTION

Let E be an elliptic curve of prime conductor N and analytic rank 0. Let f be the new form of weight 2 of level N on $\Gamma_0(N)$ associated to E . Gross (Section 12, [Gr87]) constructed

$$\mathcal{G} = \sum_D m_D q^D,$$

a weight $3/2$ modular form in terms of certain modular forms g_i , associated with f . A special case of Waldspurger's formula (Proposition 13.5, [Gr87]) relates the product of the L -functions

$$L(f, 1)L(f \times \epsilon_{-D}, 1)$$

to m_D^2 , where $(\frac{-D}{N})\text{sgn}(W_N) \neq -1$ and $f \times \epsilon_{-D}$ is the cusp form corresponding to the twist by $-D$ of E , and W_N is the Atkin-Lehner involution. Bocherer and Schulze-Pillot generalized Gross's construction (Section 3, [BS90]) for square-free level N . Quattrini collected many numerical examples (Section 3.7, [Qu11]) of certain definite quaternion algebras ramified at exactly one prime and presented a conjecture (Conjecture 2.3) on the coefficients of the Cohen-Eisenstein series

$$\mathcal{H} = \sum_{i=1}^n \frac{1}{w_i} g_i,$$

where g_i and w_i are certain orders defined in Section 2. We work with certain definite quaternion algebras ramified at finitely many primes p_1, p_2, \dots, p_k , and we compute the coefficients of \mathcal{H} for square-free level in theorem 5.1. As a consequence, we deduce the conjecture 2.3 (Corollary 5.3).

Date: March 28, 2016.

The estimation of the number of imaginary quadratic fields whose ideal class group has an element of order $l \geq 2$ and the analogous questions for quadratic twists of elliptic curves has been the center of interest in many results. For elliptic curves E of prime conductors, using the theory of p -adic L -functions and Eisenstein quotients, Mazur [Ma79] showed that under certain conditions, the quadratic twist of E by a primitive, odd quadratic Dirichlet character χ has finite Mordell-Weil group of order not divisible by a prime l if and only if the quadratic field associated to χ has class number prime to l . In [Fr88], Frey obtained the information about the elements of order l in the Selmer group of E_D , the quadratic twist of E by $-D$, by assuming the elliptic curve E over \mathbb{Q} contains a \mathbb{Q} -rational torsion point of prime order l . In [Ja99], James proved that 3 divides the order of the Selmer group of $X_0(11)_D$ if and only if 3 divides the class number $h(-D)$ under the similar assumption that the elliptic curve E contains a rational torsion point of order 3. In [Wo99], Wong showed that there are infinitely many negative fundamental discriminants $-D$ such that the twist $X_0(11)_D$ of the modular curve $X_0(11)$ has rank 0 over \mathbb{Q} and an element of order 5 in its Shafarevich-Tate group. Using the circle method and results of Frey, Kolyvagin, Ono [Ono01] proved a result for the nontriviality of class groups of imaginary quadratic fields and results on the nontriviality of the Shafarevich-Tate groups of certain elliptic curves. It is also known that for almost all primes l , there exist infinitely many square-free integers D such that $l \nmid |\text{III}_D|$ ([Ko99]).

We prove that (Theorem 2.6) if E is an elliptic curve with square-free conductor N and l is an odd prime dividing $|E(\mathbb{Q})|$, under certain conditions on the Shafarevich-Tate group III_D , the proportion of III_D in the family, divisible by l , is the same as the proportion of class numbers $h(-D)$ divisible by l in the family of negative quadratic fields $\mathbb{Q}(\sqrt{-D})$ with the same Kronecker conditions.

To prove theorem 5.1, we follow the strategy of Gross and we use Eichler's formula. The contents of this paper are as follows. In section 2, we discuss some preliminaries. In section 3, we compute the Fourier coefficients of the modular forms g_i in terms of $h(\mathcal{O}_{-D}, R_i)$, the number of all optimal embeddings of the order of discriminant D into certain maximal orders R_i . In section 4, we show that a certain odd prime divides the order of Shafarevich-Tate group of quadratic twists of elliptic curves if and only if it divides the class number of the corresponding imaginary quadratic field. In section 5, we compute the coefficients of the Cohen-Eisenstein series and we deduce Conjecture 2.3.

2. PRELIMINARIES AND STATEMENT OF RESULTS

Bocherer and Schulze-Pillot generalized Gross's construction (Section 3, [BS90]) for square-free level N as follows. Let B be a definite quaternion algebra ramified at primes p_1, p_2, \dots, p_k and at ∞ . Let $N = p_1 p_2 \dots p_k M$ ($p_i \nmid M$) be a square-free integer. Let \mathcal{O} be an order of level N . Let I_1, I_2, \dots, I_n be a set of left ideals representing the distinct ideal classes of \mathcal{O} , with $I_1 = \mathcal{O}$. Let R_1, R_2, \dots, R_n be the respective right orders (of level N) of each ideal I_i . For each R_i , let L_i be the rank 3 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 . Let w_i be the order of the finite group $R_i^*/\pm 1$ for $i = 1$ to n . Define

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

The forms g_i are in the Kohnen plus-space which is the space of modular forms $\sum a_n q^n$ of weight $3/2$ on $\Gamma_0(4N)$ whose Fourier coefficients a_n are 0 if $-n \equiv 2, 3 \pmod{4}$.

2.1. Brandt matrices and Theta series. Let m be a positive integer. The Brandt matrix B_m is defined by $B_m = (b_{ij}(m))_{n \times n}$, where $b_{ij}(m) = \frac{1}{e_j} |\{\alpha \in I_j^{-1} I_i : N(\alpha) \frac{N(I_j)}{N(I_i)} = m\}|$, where $e_j = |R_j^*|$. The sum of any row in the matrix B_m is given by

$$b_m = \sum_{j=1}^n b_{ij}(m) = \sum_{d|m, (d, \frac{N}{M})=1} d.$$

It is also the m -th coefficient of the zeta function

$$\zeta_{\mathcal{O}} = \sum_I \frac{1}{\mathbb{N}(I)^{2s}} = \sum_{n=1}^{\infty} \frac{b_n}{n^{2s}},$$

where the sum runs over all integral \mathcal{O} -left ideals I . The vector $u = (1, 1, \dots, 1)$ is an eigenvector of the Brandt matrices, we have $B_m u^t = b_m u^t$, for all positive integers m . Fix $1 \leq i, j \leq n$.

These Brandt matrices define a collection of theta series

$$\theta_{ij}(\tau) = \frac{1}{e_j} \sum_{x \in I_j^{-1} I_i} q^{\frac{\mathbb{N}(x)\mathbb{N}(I_j)}{\mathbb{N}(I_i)}} = \sum_{m=0}^{\infty} b_{ij}(m) q^m$$

which are modular forms of weight 2 and level N .

The series $e_2(z) = \sum_{i=1}^n \frac{1}{2w_i} + \sum_{m=1}^{\infty} b_m q^m$ is an Eisenstein series of weight 2 and level N .

Let f be a new form of square-free level $N = PM$ with $P = p_1 p_2 \dots p_k$ on $\Gamma_0(N)$ such that

$$k \text{ is odd, } \text{sgn}(W_p) = -1, \text{ if } p \mid P, \text{sgn}(W_q) = +1, \text{ if } q \mid M. \quad (1)$$

Suppose the elliptic curve E corresponding to f has analytic rank 0 and l is an odd prime dividing the order of the torsion group of E , then it can be shown that (Proposition 3.2, [Qu11])

$$f \equiv e_2 \pmod{l}. \quad (2)$$

2.2. Waldspurger's formula. The Shimura correspondence [Sh73] relates the modular forms of half integral weight $k + 1/2$ with classical modular forms of even weight $2k$. We will define the modular form \mathcal{G} of weight $3/2$ which corresponds to the new form f satisfying (1). Consider the quaternion algebra B ramified exactly at ∞ and at the primes $p_i \mid N$, where $\text{sgn}(W_{p_i}) = -1$. The Brandt matrices B_m act on the the vector space V of formal linear combinations $\sum_{i=1}^n c_i I_i$, $c_i \in \mathbb{C}$. By Eichler's trace formula there is a one to one correspondence between Hecke eigenforms of weight 2 and level N and eigenvectors in V of all Brandt matrices (up to a constant multiple) (Section 2, [Po09]). Hence the

normalized new form $f \in S_2(N)$ corresponds to a one-dimensional eigenspace $\langle v = (v_1, v_2, \dots, v_n) \rangle$, of the Brandt matrices $\{B_p\}$ (of level N and prime degree p) in B , such that $B_p v^t = a_p v^t$, where a_p is the eigenvalue satisfying $T_p f = a_p f$, for all p . We can assume that $(\frac{v_1}{w_1}, \frac{v_2}{w_2}, \dots, \frac{v_n}{w_n})$ is primitive and has integer coordinates. Then

$$\mathcal{G} = \sum_{i=1}^n \frac{v_i}{w_i} g_i = \sum_D m_D q^D$$

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

Let $P = p_1 p_2 \dots p_k$. The modular form \mathcal{G} is zero unless $\text{sgn}(W_p) = \begin{cases} -1, & \text{for } p \mid P \\ +1, & \text{for } p \mid M \end{cases}$

If $-D$ is a fundamental discriminant such that $(\frac{-D}{p}) \text{sgn}(W_p) \neq -1$ for every prime $p \mid \frac{N}{\gcd(N, D)}$, then the following special case of Waldspurger's formula [Wa81] holds (Section 3, [BS90]).

$$\prod_{p \mid \frac{N}{\gcd(N, D)}} (1 + (\frac{-D}{p}) \text{sgn}(W_p)) L(f, 1) L(f \otimes \epsilon_{-D}, 1) = \frac{2^{\omega(N)}(f, f) m_D^2}{\sqrt{D} \sum \frac{v_i^2}{w_i^2}}. \quad (3)$$

Definition 2.1. *The Cohen-Eisenstein series is the Eisenstein series of weight $3/2$ corresponding to the eigenvector $u = (1, 1, \dots, 1)$, $\mathcal{H} := \sum_{i=1}^n \frac{1}{w_i} g_i$.*

Remark 2.2. (Multiplicity one modulo l). *When N is prime, using the results of Mazur and Emerton [Ma77], [Em02], one can show that the Brandt matrices $\{B_p\}$ reduced modulo l have a dimension one eigenspace for the eigenvalues $\sigma(p)_N$ (Theorem 3.6, [Qu11]). Since u and v are both eigenvectors for the Brandt matrices $\{B_p\}$, we have $\lambda u \equiv v \pmod{l}$ for some $\lambda \in \mathbb{F}_l^\times$. If N is square-free, then it is not clear whether the eigenspace corresponding to $u = (1, 1, \dots, 1)$ is one dimensional modulo l .*

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 $\text{Pic}(\mathcal{O}_{-D})$, and let $2u(-D)$ be the cardinality of the unit group \mathcal{O}_{-D}^* . When N is a square-free number, Quattinni made the following conjecture by observations on known congruences among weight two modular forms and known congruences among eigenvectors of Brandt matrices. The details can be found in Section 3.1 – 3.5 of [Qu11].

Conjecture 2.3. (Conjecture 3.7, [Qu11]) *Let B be a definite quaternion algebra ramified at exactly one finite prime p and let $N = pM$ ($p \nmid M$) be a square-free integer. Let $\mathcal{H} = \sum_{i=1}^n \frac{1}{w_i} g_i = \sum_{i=1}^n \frac{1}{2w_i} + \sum_{D>0} \mathcal{H}(D) q^D$. Let $D \in \mathbb{N}$ be such that $-D$ is a fundamental discriminant and $(\frac{-D}{p}) \neq 1$, and $(\frac{-D}{q}) \neq -1$ for every prime $q \mid M$. Then*

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

where $\omega(N)$ is the number of distinct primes that divide N and $s(D)$ is the number of primes that divide N and ramify in $\mathbb{Q}(\sqrt{-D})$. If $M = 1$, then the above conjecture is the following result of Gross (Section 1, [Gr87]).

Proposition 2.4. *If B is a definite quaternion algebra ramified only at a prime N and $-D$ is a fundamental discriminant such that $(\frac{-D}{N}) \neq 1$, then the coefficients $\mathcal{H}(D)$ of the weight $3/2$ Eisenstein series are given by*

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

In Conjecture 2.3 and in Proposition 2.4, Gross and Quattrini considered definite quaternion algebras ramified at exactly one prime p and at ∞ . We consider the generalized case, square-free level and definite quaternion algebras ramified at finitely many primes p_1, p_2, \dots, p_k and at ∞ (See Theorem 5.1). 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 , $|\text{III}_D|$ is m_D^2 , up to a power of 2 and we also have $\lambda u \equiv v \pmod{l}$, for some $\lambda \in \mathbb{F}_l^\times$ (remark 2.2). We state the following result of Quattrini (Proposition 3.8, [Qu11]).

Proposition 2.5. *Let E be the strong Weil curve of rank 0 and prime conductor N . Consider the family $\{E_D\}$ of negative quadratic twists of E , for $-D$ a fundamental discriminant and satisfying $(\frac{-D}{N}) = 1$. Suppose E has a torsion point defined over \mathbb{Q} , of odd prime order l . Then, $|\text{III}_D|$ is divisible by l , if and only if the class number $h(-D)$ of $\mathbb{Q}(\sqrt{-D})$ is divisible by l .*

We generalize the above proposition to square-free level N as follows.

Let E be an elliptic curve of analytic rank zero and square-free conductor $N = PM$ with $P = p_1 p_2 \dots p_k$. Let f be the new form of level N on $\Gamma_0(N)$ corresponding to E satisfying

$$\text{Assume } k \text{ is odd, } \text{sgn}(W_p) = -1, \text{ if } p \mid P, \text{sgn}(W_q) = +1, \text{ if } q \mid M. \quad (4)$$

Consider the family $\{E_D\}$ of negative quadratic twists of E satisfying the Kronecker condition

$$\left(\frac{-D}{p}\right) \neq 1 \text{ for } p \mid P, \left(\frac{-D}{q}\right) \neq -1, \text{ for } q \mid M. \quad (5)$$

We consider the definite quaternion algebra B ramified exactly at all $p \mid P$ and at ∞ . We assume the following.

$$\text{If } P \text{ is composite, then } w_i \in \mathbb{F}_l^\times \text{ for } l = 3, 5 \text{ or } 7. \quad (6)$$

The new form f and the Eisenstein series e_2 of weight 2 correspond to the $3/2$ weight forms \mathcal{G} and the Cohen-Eisenstein series \mathcal{H} respectively, under the Shimura correspondence. Let v and u be the eigenvectors of the Brandt matrices associated with the forms f and e_2 respectively. Suppose $\lambda u \equiv v \pmod{l}$ for some $\lambda \in \mathbb{F}_l^\times$, then the congruence (2) in weight 2 can be lifted to a congruence in weight $3/2$,

$$\lambda \mathcal{G} \equiv \mathcal{H} \pmod{l}. \quad (7)$$

Thus we have the following result

Theorem 2.6. *Let E be an elliptic curve of analytic rank zero and square-free conductor $N = PM$. Let f be the new form of level N corresponding to E satisfying (4). Consider the family $\{E_D\}$ of negative quadratic twists of E satisfying the Kronecker condition (5). Suppose E has a torsion point defined over \mathbb{Q} , of odd prime order l and that $|\text{III}_D| = m_D^2$ (upto a power of 2). Assume that $\lambda u \equiv v \pmod{l}$, for some $\lambda \in \mathbb{F}_l^\times$ and (6) holds. Then, $|\text{III}_D|$ is divisible by l , if and only if the class number $h(-D)$ of $\mathbb{Q}(\sqrt{-D})$ is divisible by l .*

3. OPTIMAL EMBEDDINGS

We continue with the notation set out in the previous sections. Let K be a quadratic field over \mathbb{Q} . 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 3.1. *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 $i_1(y) = xi_2(y)x^{-1}$ for all $y \in K$.

$$\begin{aligned} \text{The Legendre symbol } \left(\frac{-D}{p}\right) \text{ is defined by } \left(\frac{-D}{p}\right) &:= \begin{cases} 1, & \text{if } p \text{ splits in } K \\ 0, & \text{if } p \text{ ramifies in } K \\ -1, & \text{if } p \text{ is inert in } K. \end{cases} \\ \text{The Eichler symbol } \left\{\frac{-D}{p}\right\} \text{ is defined by } \left\{\frac{-D}{p}\right\} &:= \begin{cases} 1, & \text{if } p^2 \mid D \\ 0, & \text{if } p \mid D, p^2 \nmid D \\ \left(\frac{-D}{p}\right), & \text{if } p \nmid D. \end{cases} \end{aligned}$$

We prove a lemma and a proposition. We will use them in the proof of Theorem 5.1.

Lemma 3.2. *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 . Then*

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

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

(1) The norm of \mathfrak{M} is square-free 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 $\left\{\frac{-D}{p_i}\right\} = -1$ or q is a prime divisor of M with $\left\{\frac{-D}{q}\right\} = 1$ and

(2) \mathfrak{B} is an integral ideal coprime to the conductor of \mathcal{O}_{-D} .

It is easy to observe that the number of $(\mathfrak{M}, \mathfrak{B})$ satisfying (1) and (2) is equal to

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

There is a one-to-one correspondence between the set of all $(\mathfrak{M}, \mathfrak{B})$ satisfying (1) and (2) and equivalence classes of optimal embeddings of the order of discriminant $-D$ into R_i . For the proof of this correspondence, we refer to Section 3.2 of [Sh65] (or) Satz 6,7 of [Ei55]. \square

We compute the Fourier coefficients of the modular forms g_i , for $i = 1$ to k in the following proposition.

Proposition 3.3. *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 $\text{Tr}(b) = 0$, $b \in \mathbb{Z} + 2R_i$, $\mathbb{N}(b) = D$. 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 $u(d) = 1$ unless $d = -3, -4$ when $u(d) = 3, 2$ respectively.

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

For a negative integer d , if $f : \mathbb{Q}(\sqrt{d}) \hookrightarrow B$ is an embedding of an order \mathcal{O}_d into R_i , then

$b = f(\sqrt{d})$ is an element with trace 0 and norm $-d$. Since $\mathcal{O}_d = \mathbb{Z} + \mathbb{Z}\frac{(-d+\sqrt{d})}{2}$, we have $b \in (\mathbb{Z} + 2R_i)$.

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

Conversely, if b is an element in S_i^0 with norm $-d$, then $f(\sqrt{d}) = b$ 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 $f(\sqrt{d}) = b$ is optimal if and only if $b \notin f(\mathbb{Z} + 2R_i)$

for some $f > 1$. Let $h^*(\mathcal{O}_{-D}, R_i)$ be the the number of optimal embeddings of \mathcal{O}_{-D} into R_i . Using the above connection we proved that

$$a_i(D) = |S| = \sum_{-D=df^2} \{b \in S, \frac{b}{f} \in S_i^0, \frac{b}{f} \notin n(\mathbb{Z} + 2R_i) \text{ for } n > 1\} = \sum_{-D=df^2} h^*(\mathcal{O}_d, R_i).$$

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

$$|S/\Gamma_i| = \sum_{-D=df^2} h(\mathcal{O}_d, R_i).$$

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 have shown that

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

where $w_i = |\Gamma_i|$. \square

Gross computed the traces of the Brandt matrices for prime level case (cf. Proposition 1.9, [Gr87]). It holds for square-free level, as we state in the following.

Proposition 3.4. *For all $m \geq 0$,*

$$\mathrm{Tr}(B(m)) = \sum_{s \in \mathbb{Z}, s^2 - 4m \leq 0} \mathcal{H}(4m - s^2).$$

Proof. The diagonal entry of the brandt matrix $B(m)$ is $b_{ii}(m) = \frac{1}{e_i} |\{b, b \in R_i, \mathbb{N}(b) = m\}|$.

If $m = 0$, then

$$\mathrm{Tr}(B(0)) = \frac{1}{24} \prod_{i=1}^k (p_i - 1) \prod_{q|M} (q + 1) = \sum_{i=1}^n \frac{1}{2w_i} = \mathcal{H}(0).$$

Let $A_i(s, m)$ be the set of elements $b \in R_i$ with $\mathrm{Tr}(b) = s$ and $\mathbb{N}(b) = m$.

This is a finite set. If $s^2 - 4m > 0$, then it is an empty set. Hence

$$\mathrm{Tr}(B(m)) = \sum_{i=1}^n b_{ii}(m) = \sum_{i=1}^n \sum_{s^2 \leq 4m} \frac{|A_i(s, m)|}{|R_i^*|} = \sum_{s^2 \leq 4m} \left(\sum_{i=1}^n \frac{|A_i(s, m)|}{|R_i^*|} \right).$$

If $s^2 = 4m$, then the inner sum

$$\sum_{i=1}^n \frac{|A_i(s, m)|}{|R_i^*|} = \sum_{i=1}^n \frac{1}{2w_i} = \mathcal{H}(0).$$

Assume that $D = 4m - s^2 > 0$. As in the proof of Proposition 3.3, we can show that

$$\frac{|A_i(s, m)|}{|R_i^*|} = \sum_{-D=df^2} \frac{1}{2} \frac{h(\mathcal{O}_d, R_i)}{u(d)}.$$

By Lemma 3.2 and Theorem 5.1,

$$\sum_{i=1}^n \frac{|A_i(s, m)|}{|R_i^*|} = \sum_{i=1}^n \sum_{-D=df^2} \frac{1}{2} \frac{h(\mathcal{O}_d, R_i)}{u(d)} = \mathcal{H}(4m - s^2).$$

□

4. THE ORDER OF THE SHAFAREVICH-TATE GROUP

Recall that we have equation (3) which relates the L-function of f with the coefficients m_D^2 ,

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

If E is the elliptic curve with conductor N associated with $f \in S_2(\Gamma_0(N))$, then we have $L(E, 1) = L(f, 1)$. Then 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 $f \otimes \epsilon_{-D} \in S_2(\Gamma_0(ND^2))$. Assume that the rank of E is 0. The rank 0 case of Birch and Swinnerton-Dyer Conjecture gives

$$\frac{L(f \otimes \epsilon_{-D}, 1)}{\Omega_D} = \frac{L(E_D, 1)}{\Omega_D} = \frac{|\mathrm{III}_D| \prod c_{p,D}}{|\mathrm{Tor}(E_D)|^2},$$

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

$$C(D) = \frac{\prod_{p|\frac{N}{\gcd(N,D)}} (1 + (\frac{-D}{p}) \text{sgn}(W_p)) \Omega_D \prod c_{p,D} \sqrt{D} \frac{v_i^2}{w_i^2} L(f, 1)}{2^{\omega(N)} (f, f) |\text{Tor}(E_D)|^2}.$$

Then $|\text{III}_D| = \frac{m_D^2}{C(D)}$. Math softwares can be used to compute the term $C(D)$.

4.1. Proof of Theorem 2.6.

Proof. We prove the theorem when P is prime. One can conclude the theorem similarly when P is composite. If l is an odd prime 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 . From $\lambda\mathcal{H} - \mathcal{G} = \sum_{i=1}^n \frac{(\lambda - v_i)}{w_i} g_i$, it follows that the congruence $\lambda u \equiv v \pmod{l}$, for some $\lambda \in \mathbb{F}_l^\times$ gives a congruence $\lambda\mathcal{H} \equiv \mathcal{G} \pmod{l}$. This yields a congruence on the coefficients $\lambda\mathcal{H}(D) \equiv m_D^2 \pmod{l}$. From Corollary 5.2, we see that l divides $\mathcal{H}(D)$ if and only if l divides $h(-D)$. We also have $|\text{III}_D| = m_D^2$ (up to a power of 2). Hence $|\text{III}_D|$ is divisible by l , if and only if the class number $h(-D)$ of $\mathbb{Q}(\sqrt{-D})$ is divisible by l . \square

By letting $k = 1$ in the above Theorem, we deduce the following corollary.

Corollary 4.1 (Proposition 3.9, [Qu11]). *Let E, E_D, l and III_D be as in Theorem 2.6. Assume that there is exactly one prime $p \mid N$ such that the sign of $W_p = -1$. Then, $|\text{III}_D|$ is divisible by l , if and only if the class number $h(-D)$ of $\mathbb{Q}(\sqrt{-D})$ is divisible by l .*

5. COHEN-EISENSTEIN SERIES

5.1. Examples. We calculate the Fourier coefficients of the weight $3/2$ Eisenstein series $\mathcal{H} = \sum_{i=1}^n \frac{1}{w_i} g_i$ and the class numbers of imaginary quadratic fields $K = \mathbb{Q}(\sqrt{-D})$ for $d \leq 2000$ by using MAGMA. Let $D > 0$ 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 $\text{Pic}(\mathcal{O}_{-D})$, and let $2u(-D)$ be the cardinality of the unit group \mathcal{O}_{-D}^* . A prime l is inert, splits or ramifies in \mathcal{O}_{-D}^* if the Kronecker symbol $(\frac{-D}{l})$ is $-1, 1, 0$ respectively.

We consider the strong Weil curves of rank zero with an odd torsion point from Cremona's table [Cr97].

• $N = 66 = 2.3.11$

We have elliptic curve $E = 66C(I) = [1, 0, 0, -45, 81]$ of level 66 with analytic rank zero and $|\text{Tor}(E)| = 10$. We have $\text{sgn}(W_2) = \text{sgn}(W_3) = \text{sgn}(W_{11}) = -1$. We work in the quaternion algebra ramified at 2, 3, 11 and at ∞ . We calculate the Brandt matrices for an order of level 66. We have, for $D \leq 2000$ such that $-D$ is a fundamental discriminant and $(\frac{-D}{2}), (\frac{-D}{3})$ and $(\frac{-D}{11}) \neq 1$:

$$\mathcal{H}(D) := \begin{cases} \frac{2^2 h(-D)}{u(-D)}, & \text{if none of the primes } 2, 3, 11 \text{ ramifies in } K \\ \frac{2^1 h(-D)}{u(-D)}, & \text{if exactly one prime } p \mid 66 \text{ ramifies in } K \\ \frac{h(-D)}{u(-D)}, & \text{if exactly two primes } p \mid 66 \text{ ramify in } K \\ \frac{h(-D)}{2u(-D)}, & \text{if } 2, 3 \text{ and } 11 \text{ ramify in } K. \end{cases}$$

• $N = 210 = 2 \cdot 3 \cdot 5 \cdot 7$

We have elliptic curve $E = 210A(A) = [1, 0, 0, -41, -39]$ of level 210 with analytic rank zero and $|\text{Tor}(E)| = 6$. We have $\text{sgn}(W_2) = \text{sgn}(W_3) = \text{sgn}(W_7) = -1$ and $\text{sgn}(W_5) = +1$. We work in the quaternion algebra ramified at 2, 3, 7 and at ∞ . We calculate the Brandt matrices for an order of level 210. We have, for $D \leq 2000$ such that $-D$ is a fundamental discriminant and $(\frac{-D}{2}), (\frac{-D}{3}), (\frac{-D}{7}) \neq 1$ and $(\frac{-D}{5}) \neq -1$:

$$\mathcal{H}(D) := \begin{cases} \frac{2^3 h(-D)}{u(-D)}, & \text{if none of the primes } 2, 3, 5, 7 \text{ ramifies in } K \\ \frac{2^2 h(-D)}{u(-D)}, & \text{if exactly one of the primes } p \mid 210 \text{ ramifies in } K \\ \frac{2^1 h(-D)}{u(-D)}, & \text{if exactly two of the primes } p \mid 210 \text{ ramify in } K \\ \frac{h(-D)}{u(-D)}, & \text{if exactly three primes } p \mid 210 \text{ ramify in } K \\ \frac{h(-D)}{2u(-D)}, & \text{if } 2, 3, 5 \text{ and } 7 \text{ ramify in } K. \end{cases}$$

We have also computed the Fourier coefficients $\mathcal{H}(D)$ for the rank 0 elliptic curves $E = 110A1(C) = [1, 1, 1, 10, -45]$ with $\text{Tor}(E) = 5$, $E = 114A(A) = [1, 0, 0, -8, 0]$ with $\text{Tor}(E) = 6$, $E = 130B(A) = [1, -1, 1, -7, -1]$ with $\text{Tor}(E) = 4$, $E = 210B(A) = [1, 0, 1, -498, 4228]$ with $\text{Tor}(E) = 6$ and several other examples. Based on our numerical examples, we observed a generalization of the conjecture 2.3 which we prove in Corollary 5.2.

Theorem 5.1. *Let B be a definite quaternion algebra ramified at p_1, p_2, \dots, p_k . Let $N = p_1 p_2 \dots p_k M$ ($p_i \nmid M$) be a square-free integer. Denote by $\mathcal{H} = \sum_{i=1}^n \frac{1}{w_i} g_i = \sum_{i=1}^n \frac{1}{2w_i} + \sum_{D>0} \mathcal{H}(D) q^D$. Then we have*

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

Proof. Consider the weight 3/2 Cohen-Eisenstein Series \mathcal{H} ,

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

By Proposition 3.3, we see that

$$\sum_{i=1}^n \sum_{D>0} \frac{a_i(D)}{w_i} q^D = \frac{1}{2} \sum_{D>0} \sum_{-D=df^2} \left(\sum_{i=1}^n \frac{h(\mathcal{O}_d, R_i)}{u(d)} \right). \quad (8)$$

By Lemma 3.2, we have

$$\sum_{i=1}^n h(\mathcal{O}_d, R_i) = h(d) \prod_{i=1}^k \left(1 - \left\{\frac{d}{p_i}\right\}\right) \prod_{q|M} \left(1 + \left\{\frac{d}{q}\right\}\right). \quad (9)$$

Substituting equations (8) and (9) in the Fourier expansion of \mathcal{H} , we get

$$\mathcal{H} = \sum_{i=1}^n \frac{1}{w_i} g_i = \frac{1}{2} \sum_{i=1}^n \frac{1}{w_i} + \frac{1}{2} \sum_{D>0} \sum_{-D=df^2} \left[\frac{h(d)}{u(d)} \prod_{i=1}^k \left(1 - \left\{\frac{d}{p_i}\right\}\right) \prod_{q|M} \left(1 + \left\{\frac{d}{q}\right\}\right) \right] q^D.$$

Hence

$$\mathcal{H}(D) = \frac{1}{2} \sum_{-D=df^2} \left[\frac{h(d)}{u(d)} \prod_{i=1}^k \left(1 - \left\{\frac{d}{p_i}\right\}\right) \prod_{q|M} \left(1 + \left\{\frac{d}{q}\right\}\right) \right]. \quad (10)$$

This completes the proof. \square

We deduce the following corollary which generalizes the result of Gross (Proposition 2.4) for square-free level N .

Corollary 5.2. *Let B and \mathcal{H} be as in Theorem 5.1. If $-D$ is the fundamental discriminant, $\omega(N)$ is the number of distinct primes that divide N , $s(D)$ is the number of primes that divide N and ramify in $\mathbb{Q}(\sqrt{-D})$, and $\left(\frac{-D}{p_i}\right) \neq 1$, for every $i = 1$ to k , and $\left(\frac{-D}{q}\right) \neq -1$ for every prime $q \mid M$, then*

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

Proof. If $-D$ is the fundamental discriminant satisfying the Kronecker conditions, then from the equation (10), we have

$$\mathcal{H}(D) = \prod_{i=1}^k \left(1 - \left\{\frac{-D}{p_i}\right\}\right) \prod_{q|M} \left(1 + \left\{\frac{-D}{q}\right\}\right) \frac{1}{2} \frac{h(-D)}{u(-D)} = \frac{2^{\omega(N)-1-s(D)} h(-D)}{u(-D)}.$$

\square

Corollary 5.3. *Conjecture 2.3 holds.*

Proof. Conjecture 2.3 follows immediately from Corollary 5.2 by letting $k = 1$. \square

ACKNOWLEDGEMENTS

This work was done when the author was a Visiting Postdoctoral Fellow at the Max Planck Institute for Mathematics, Bonn. She would like to thank the institute for providing excellent working conditions. She would like to thank Neil Dummigan, Tomoyoshi Ibukiyama and Narasimha Kumar and for helpful discussions. She would also like to thank Chitrabhanu Chaudhuri, Rafael von Känel, Rachel Newton and Sarang Sane for helpful comments on earlier drafts of this paper. The research of the author was supported by a DST-INSPIRE Grant.

REFERENCES

- [BS90] S. Bocherer, R. Schulze-Pillot, On a theorem of Waldspurger and on Eisenstein series of Klingen type, *Math. Ann.*, 288, (1990), 361–388.
- [Ei55] M. Eichler, Zur Zahlentheorie der Quaternion-Algebren. *J. Reine Angew. Math.*, **195** (1955), 127–151.
- [Cr97] J.E. Cremona, Algorithms for Modular Elliptic Curves, Cambridge University Press, 1997.
- [Em02] M. Emerton, Supersingular elliptic curves, theta series and weight two modular forms. *J. Amer. Math. Soc.* Vol **15**, (2002), no. 3, 671–714.
- [Fr88] G. Frey, On the Selmer group of twists of elliptic curves with \mathbb{Q} -rational torsion points, *Canad. J. Math.*, Vol **40**, no. 3, (1988) 649–665.
- [Gr87] B. Gross, Heights and the special values of L -series, *CMS conference Proceedings*, Vol **7**, (1987), 115–187.
- [Ko99] W. Kohlen, K. Ono, Indivisibility of class numbers of imaginary quadratic fields and orders of Tate-Shafarevich groups of elliptic curves with complex multiplication. *Invent. Math.* Vol **135** (1999), no. 2, 387–398.
- [Ma77] B. Mazur, Modular curves and the Eisenstein ideal. *Inst. Hautes Etudes Sci. Publ. Math.*, (1977), no. 47, 33–186.
- [Ma79] B. Mazur, On the arithmetic of special values of L functions. *Invent. Math.*, Vol **55** (1979), no. 3, 207–240.
- [Po09] P. Ponomarev, New forms of squarefree level and theta series. *Math. Ann.* Vol **345** (2009), no. 1, 185–193.
- [Qu11] P.L. Quattrini, The effect of torsion on the distribution of III among quadratic twists of an elliptic curve, *Journal of Number Theory*, no. 2, (2011), 195–211.
- [Sh65] H. Shimizu, On Zeta Functions of Quaternion Algebras *Ann. Math.* Vol **81** no. 1, (1965), 166–193.
- [Sh73] G. Shimura, *On modular forms of half-integral weight*, Ann. of Math. **97** (1973), 440–481.
- [Ono01] K. Ono, Nonvanishing of quadratic twists of modular l -functions and applications to elliptic curves *J. Reine Angew. Math.* Vol **553** (2001), 81–97.
- [Ja99] K. James, Elliptic curves satisfying the Birch and Swinnerton Dyer conjecture and mod 3 *J. Number Theory*. Vol **128** (2008) 2823–2835.
- [Wa81] J.L. Waldspurger, Sur les coefficients de Fourier des formes modulaires de poids demi-entier. *J. Math. Pures Appl.* (9) Vol **60** (1981), no. 4, 375–484.
- [Wo99] S. Wong, Elliptic curves and class number divisibility *Int. Math. Res. Not.*, **12** (1999), 661–672.

INDIAN INSTITUTE OF TECHNOLOGY MADRAS, TAMIL NADU, INDIA.

E-mail address: `srilakshmi@iitm.ac.in`, `lakshmi@pim-bonn.mpg.de`