Canadian Mathematical Society
Conference Proceedings
Volume 7 (1987)

Heights and the Special Values of L-series

Benedict H. Gross

In this paper I will present a geometric approach to Eichler's arithmetic theory of definite quaternion algebras and to Waldspurger's results on the central critical values of L-series. The method uses the heights of special points on algebraic curves, and the arguments are similar to those that Zagier and I used to study central critical derivatives. Fortunately, the calculations are much less intimidating in this case; I have also restricted to forms of weight 2 and prime level N to simplify the exposition.

Table of contents:

1. Brandt matrices and Eichler's trace formula.

In this section, we will review the arithmetic theory of maximal orders and ideals in definite quaternion algebras of prime discriminant. Almost all of these results are due to Eichler [2].

Let N be a rational prime, and let B be "the" quaternion algebra over $\mathbb{Q}$ which is ramified at the two places N and ∞. Let R be a fixed maximal order in B. A left ideal I of R is a lattice in B which is stable under left multiplication by R. The right order $\{b \in B : Ib \subset I\}$ of I is another maximal order in B. Furthermore, the set $I^{-1} = \{b \in B : IbI \subset I\}$ is a right ideal for R whose left order is the right order of I.

Two left ideals I and J are in the same class if $J = Ib$ with $b \in B^*$. The set of left ideal classes is finite, and its order n is independent of the choice of R. Let $\{I_1, I_2, \ldots, I_n\}$ be a set of left ideals representing the distinct ideal classes, with $I_1 = R$.

For $1 \leq i \leq n$ we let R_i be the right order of the ideal I_i. Then each conjugacy class of maximal orders in B is represented (once or twice) in the set $\{R_1, R_2, \ldots, R_n\}$. We let $t \leq n$ be the number of distinct conjugacy classes of maximal orders in B. In the classical literature, n is the class number and t is the type number of B.

The groups $\Gamma_i = R_i^*/\mathbb{Z}^* = R_i^*/\langle\pm 1\rangle$ are all finite, as they embed as discrete subgroups of the compact Lie group $(B \otimes \mathbb{R})^*/\mathbb{R}^* \simeq SO_3(\mathbb{R})$. Let $w_i = [\Gamma_i]$, where for any finite set S we let $[S]$ denote its cardinality.

The integer

$$W = \prod_{i=1}^{n} w_i \qquad (1.1)$$

is independent of the choice of R , and is equal to the exact denominator of the rational number $(\frac{N-1}{12})$. Eichler's mass formula states that

$$\sum_{i=1}^{n} \frac{1}{w_i} = \frac{N-1}{12} . \qquad (1.2)$$

We therefore have the following values of n .

Table 1.3

N	W	$w_i > 1$	n
2	12	12	1
3	6	6	1
$\equiv 5\ (12)$	3	3	$\frac{N+7}{12}$
$\equiv 7\ (12)$	2	2	$\frac{N+5}{12}$
$\equiv 11(12)$	6	3,2	$\frac{N+13}{12}$
$\equiv 13(12)$	1		$\frac{N-1}{12}$

Now fix $1 \le i,j \le n$. The product $M_{ij} = I_j^{-1} I_i = \{\Sigma a_k b_k : a_k \in I_j^{-1}, b_k \in I_i\}$ is a left ideal of R_j with right order R_i. For any element $b \in M_{ij}$ we let $\mathbb{N}b$ be its reduced norm, and define $\mathbb{N}M_{ij}$ as the unique positive rational number such that the quotients $\mathbb{N}b/\mathbb{N}M_{ij}$ are all integers with no common factor. Define the theta series f_{ij} by

$$f_{ij} = \frac{1}{2w_j} \sum_{b \in M_{ij}} e^{2\pi i(\mathbb{N}b/\mathbb{N}M_{ij})\tau} \tag{1.4}$$

$$= \sum_{m \ge 0} B_{ij}(m) q^m \qquad q = e^{2\pi i \tau} .$$

These functions on the upper half plane are all modular forms of weight 2 for the group $\Gamma_0(N)$. Their Fourier coefficients $B_{ij}(m)$ give the entries of the Brandt matrix of degree m :

$$B(m) = ((B_{ij}(m)))_{1 \le i,j \le n} . \tag{1.5}$$

The matrix $B(0)$ has the form

$$B(0) = \frac{1}{2}\left(\left(\begin{matrix} \frac{1}{w_1} & \frac{1}{w_2} & & \frac{1}{w_n} \\ \vdots & \vdots & \cdots\cdots & \vdots \\ \frac{1}{w_1} & \frac{1}{w_2} & & \frac{1}{w_n} \end{matrix}\right)\right) \tag{1.6}$$

and $B(1)$ is the identity matrix. For $m \ge 1$ the matrix $B(m)$ has non-negative integral entries. An efficient algorithm for computing these matrices is given in Pizer [9].

We will now give a formula for the trace of $B(m)$ in terms of Hurwitz's class numbers $H(D)$. If d is a negative discriminant we let $h(d)$ be class number of primitive binary quadratic forms of discriminant d, and let $u(d) = 1$ unless $d = -3,-4$ when $u(d) = 3,2$ respectively. If $\mathcal{O}$ is the order of discriminant d and rank 2 over $\mathbb{Z}$, then $h(d)$ is the order of the finite group $\mathrm{Pic}(\mathcal{O})$ and $u(d)$ is the order of the finite group $\mathcal{O}^*/\mathbb{Z}^* = \mathcal{O}^*/\langle\pm 1\rangle$. For $D > 0$ we define

$$(1.7) \qquad H(D) = \sum_{df^2=-D} h(d)/u(d) ;$$

a short table is given below.

D	H(D)
3	1/3
4	1/2
7	1
8	1
11	1
12	4/3
15	2
16	3/2
19	1
20	2
23	3
24	2
27	4/3
28	2
31	3
32	3
35	2
36	5/2
39	4
40	2
43	1
44	4
47	5
48	10/3
51	2
52	2
55	4
56	4

We use the prime N to define the modified invariant $H_N(D)$ as follows.

$\frac{1}{2} L_{(N)}(0,\varepsilon_D)$
// for fund D

Zagier's [illegible]
L-function for [illegible]
fund D

$$(1.8) \qquad H_N(D) = \begin{cases} 0 & \text{if } N \text{ splits in } \mathcal{O} = \mathcal{O}_{-D}\,, \\ H(D) & \text{if } N \text{ is inert in } \mathcal{O}, \\ \frac{1}{2}H(D) & \text{if } N \text{ is ramified in } \mathcal{O}, \text{ but does not divide the conductor of } \mathcal{O}\,, \\ H_N(D/N^2) & \text{if } N \text{ divides the conductor of } \mathcal{O}. \end{cases}$$

$\frac{1}{2} \zeta_{(N)}(-1)$
//

We also define $H_N(0) = \frac{N-1}{24}$. Then $H_N(D) = 0$ unless $D \geq 0$, $-D \equiv 0,1 \pmod 4$ (mod 4), and $\left(\frac{-D}{N}\right) \neq 1$. Using Table 1.3 one can show that $W \cdot H_N(D)$ is integral for $D > 0$, and $2WH_N(0)$ is an integer.

Eichler's trace formula is the following identity

Proposition 1.9. For all $m \geq 0$, $\text{Trace } B(m) = \sum\limits_{\substack{s \in \mathbb{Z} \\ s^2 \leq 4m}} H_N(4m - s^2)$.

Before sketching the proof, we will give two examples. Taking $m = 1$ in Proposition 1.9 we find

$$n = \text{Trace } B(1) = H_N(4) + 2H_N(3) + 2H_N(0)$$

$$= \frac{1}{4}\left(1 - \left(\frac{-4}{N}\right)\right) + \frac{1}{3}\left(1 - \left(\frac{-3}{N}\right)\right) + \frac{N-1}{12}$$

which agrees with the entries in Table 1.3. Taking $m = N$ in Proposition 1.9 we find

$$(1.10) \qquad \text{Trace } B(N) = \begin{cases} 1 & \text{if } N = 2,3 \\ H_N(4N) & \text{if } N > 3\,, \end{cases}$$

as in the latter case $H_N(4n-s^2) = 0$ for all $s \neq 0$. Using (1.8) we find

$$(1.11) \qquad H_N(4N) = \begin{cases} \frac{1}{2}h(-4N) & N \equiv 1\ (4) \\ h(-N) & N \equiv 7\ (8) \\ 2h(-N) & N \equiv 3\ (8)\ ,\ N \geq 11\ . \end{cases}$$

We now turn to the proof of Proposition 1.9. The result for $m = 0$ is equivalent to the mass formula, which is best proved using zeta functions, so we shall assume $m \geq 1$. The diagonal entry $B_{ii}(m)$ is equal to the number of elements $b \in R_i = M_{ii}$ of reduced norm m, modulo left multiplication by the $2w_i$ units in R_i^*. For every integer s, we define

$$A_i(s,m) = \{b \in R_i : \mathrm{Tr}(b) = s\ ,\ \mathbf{N}(b) = m\}\ .$$

Then $A_i(s,m)$ is a finite set, which is empty once $s^2 > 4m$ (as every element $b \in R_i$ has discriminant $s^2-4m \leq 0$). We therefore have

$$\begin{aligned} \mathrm{Trace}\ B(m) &= \sum_{i=1}^{n} \sum_{s^2 \leq 4m} \frac{[A_i(s,m)]}{[R_i^*]} \\ &= \sum_{s^2 \leq 4m} \left(\sum_{i=1}^{n} \frac{[A_i(s,m)]}{[R_i^*]} \right)\ . \end{aligned}$$

We will show that the inner sum is equal to $H_N(4m-s^2)$. This follows from the mass formula when $4m-s^2 = 0$, so $b = s/2$ is an integer. Hence we will assume that $D = 4m-s^2$ is positive.

In this case, every $b \in A_i(s,m)$ gives rise to an embedding of the order $\mathcal{O} = \mathcal{O}_{-D}$ into R_i. The group $\Gamma_i = R_i^*/\pm 1$ acts on $A_i(s,m)$ and the set of these embeddings by conjugation, and the Γ_i orbits of A_i correspond to embeddings of $\mathcal{O}$ up to conjugation by R_i^*. For each negative discriminant d, we let $h_i(d)$ be the number of optimal embeddings of the order of discriminant d into R_i, modulo conjugation by R_i^*; an embedding is optimal if it does not extend to any larger order in the quotient field. Then we have shown that

$$[A_i(s,m)/\Gamma_i] = \sum_{df^2=-D} h_i(d).$$

The order of the stabilizer of an element $b \in A_i(s,m)$ under the action of Γ_i is equal to 1 unless the corresponding embedding of $\mathcal{O}$ extends to $\mathbb{Z}[\mu_6]$ or $\mathbb{Z}[\mu_4]$, when it is equal to 3 or 2 respectively. Hence

$$[A_i(s,m)] = w_i \sum_{df^2=-D} h_i(d)/u(d) .$$

On the other hand, Eichler calculated the sum $\sum_{i=1}^{n} h_i(d)$ of all optimal embeddings of the order of discriminant d into the n maximal orders R_i. His result is given by the formula:

$$(1.12) \qquad \sum_{i=1}^{n} h_i(d) = \begin{cases} (1-(\frac{d}{N}))h(d) & \text{if} \quad d \neq N^2d' \\ 0 & \text{if} \quad d = N^2d' \end{cases} .$$

Combining this with our previous formula shows that

$$\sum_{i=1}^{n} \frac{[A_i(s,m)]}{2w_i} = H_N(D) = H_N(4m-s^2)$$

as desired.

2. Supersingular elliptic curves

It is known that the Brandt matrices for prime level N are related to isogenies between supersingular elliptic curves in characteristic N. We will review this connection, then use the theory of elliptic curves to establish some of the basic properties of these matrices. In this section, we shall assume that $m \geq 1$, so $B(m)$ lies in $M(n,\mathbb{Z})$.

Let $\mathbb{F}$ be an algebraically closed field of characteristic N. There are n distinct isomorphism classes of supersingular elliptic curves over $\mathbb{F}$, which may be ordered $E_1, E_2, \dots, E_n$ so that $\mathrm{End}(E_i) \simeq R_i$. One then has an isomorphism

$$(2.1) \qquad M_{ij} \simeq \mathrm{Hom}(E_i,E_j)$$

as a left R_j and right R_i module. The degree of an isogeny $\phi_b : E_i \to E_j$ corresponding to a non-zero element $b \in M_{ij}$ is given by the formula

$$(2.2) \qquad \deg \phi_b = \mathbb{N}b/\mathbb{N}M_{ij} .$$

Proposition 2.3. *The entry $B_{ij}(m)$ is equal to the number of subgroup schemes C of order m in E_i such that $E_i/C \simeq E_j$.*

Proof. By (2.2) and the definition of $B_{ij}(m)$ in (1.4), $B_{ij}(m)$ is the number of equivalence classes of isogenies $\phi : E_i \to E_j$ of order m, we identify ϕ' with ϕ if $\phi' = \alpha\phi$ and $\alpha \in \mathrm{Aut}(E_j) = R_j^*$. This has the effect of identifying two isogenies with the same kernel C, which is a subgroup scheme of order m in E_i.

It is also known that the orders R_i and R_j are conjugate in B if and only if the elliptic curves E_i and E_j are conjugate by an automorphism of the field $\mathbb{F}$. Since the modular invariants of all of the curves E_i lie in the field of N^2 elements, the curves are conjugate by an automorphism of $\mathbb{F}$ if and only if $i = j$ or $E_i^N \simeq E_j$. Since the kernel of the Frobenius morphism $E_i \to E_i^N$ is the only subgroup scheme of order N in E_i, we find by Proposition 2.3 that

<u>Proposition 2.4</u>. <u>The curves</u> E_i <u>and</u> E_j <u>are conjugate by an automorphism of</u> $\mathbb{F}$ <u>if and only if</u> $i = j$ <u>or</u> $B_{ij}(N) = 1$. <u>The number of supersingular moduli which lie in the prime field is equal to the trace of</u> $B(N)$.

As a corollary of Proposition 2.4, we find that the type number of our quaternion algebra is given by the formula

$$\begin{aligned} t &= \mathrm{Trace}\ B(N) + \frac{n - \mathrm{Trace}\ B(N)}{2} \\ &= \mathrm{Trace}\left(\frac{B(1)+B(N)}{2}\right). \end{aligned} \tag{2.5}$$

This is equal to the number of distinct irreducible factors of the supersingular polynomial over the prime field $\mathbb{Z}/N$. By our formula for Trace $B(1)$ and Trace $B(N)$, given in (1.9-1.11), we see that

$t = \frac{N}{24} + \mathcal{O}(N^{1/2+\varepsilon})$. Here is a table of the relevant invariants for small N .

Table 2.6

N	n	t	supersingular polynomial [1, pg. 143]
2	1	1	j
3	1	1	$j-1728$
5	1	1	j
7	1	1	$j-1728$
11	2	2	$j(j-1728)$
13	1	1	$j-5$
17	2	2	$j(j-8)$
19	2	2	$(j-1728)(j-7)$
23	3	3	$j(j-1728)(j+4)$
29	3	3	$j(j-2)(j+4)$
31	3	3	$(j-1728)(j-2)(j-4)$
37	3	2	$(j-8)(j^2-6j-6)$
41	4	4	$j(j-3)(j+9)(j+13)$
43	4	3	$(j-1728)(j+2)(j^2+19j+16)$
47	5	5	$j(j-1728)(j-9)(j-10)(j+3)$
53	5	4	⋮
59	6	6	
61	5	4	
67	6	4	
71	7	7	
73	6	4	
79	7	6	
83	8	7	
89	8	7	
97	8	5	

Proposition 2.7. 1) *The row sums* $\sum_j B_{ij}(m)$ *are independent of* i *and equal to* $\sigma(m)_N \underset{\text{defn.}}{=} \sum_{\substack{d|m \\ (d,N)=1}} d$.

2) *If* $(m,m') = 1$ *then* $B(m)B(m') = B(mm')$.

3) $B(N)$ *is a permutation matrix of order dividing 2 and for* $k \geq 1$ $B(N^k) = B(N)^k$.

4) *If* $p \neq N$ *is prime and* $k \geq 2$, $B(p^k) = B(p^{k-1})B(p) - pB(p^{k-2})$.

5) *The matrices* $B(m)$ *for* $m \geq 1$ *generate a commutative subring* $\mathbb{B}$ *of* $M(n,\mathbb{Z})$.

6) *We have the symmetry relation* $w_j B_{ij}(m) = w_i B_{ji}(m)$.

7) *The commutative algebra* $\mathbb{B} \otimes \mathbb{Q}$ *is semi-simple, and isomorphic to the product of totally real number fields.*

Proof. 1) The sum $\sum_j B_{ij}(m)$ is, by Proposition 2.3, the number of subgroup schemes C of order m in E_i . This is multiplicative in m , equal to 1 if $m = N^k$, and equal to $1+p+p^2+\ldots+p^k$ if $m = p^k$ with $p \neq N$. Hence $\sum_j B_{ij}(m) = \sigma(m)_N$.

2) By Proposition 2.3, $B_{ij}(mm')$ is the number of subgroup schemes $C_{mm'}$ of order m in E_i with $E_i/C_{mm'} \simeq E_j$. Let C_m be the unique subgroup scheme of order m in $C_{mm'}$, and let $E_k = E_i/C_m$. Let $C_{m'}$ be the image of $C_{mm'}$ on E_k ; this has order m' and $E_k/C_{m'} \simeq E_j$. Since any isogeny of degree mm' may be uniquely factored in this fashion: $B_{ij}(mm') = \sum_k B_{ik}(m)B_{kj}(m')$. This proves the matrix identity.

3) Each E_i has a unique subgroup scheme C_N of order N , which is the kernel of the Frobenius mapping $E_i \to E_i^N$. Hence $B_{ij}(N) = 1$ if

$E_i^N \simeq E_j$ and $B_{ij}(N) = 0$ otherwise. This shows $B(N)$ is a permutation matrix of order dividing 2. Since the unique subgroup scheme of order N^k is the kernel of $Fr^k : E_i \to E_i^{N^k}$, this shows $B(N^k) = B(N)^k$.

4) Any isogeny $\phi : E_i \to E_j$ of order p^k can be factored as an isogeny $E_i \to E_k$ of degree p followed by an isogeny $E_k \to E_j$ of degree p^{k-1}. This factorization is unique if the kernel C of ϕ is cyclic. If the kernel is not cyclic, so $\phi = p \cdot \phi'$ with ϕ' of degree p^{k-2}, there are $p+1$ possible factorizations. Hence $B(p^k)_{ij} = \sum_{\ell} B_{i\ell}(p)B_{\ell j}(p^{k-1}) - pB(p^{k-2})_{ij}$, which proves the matrix identity.

5) By 3) and 4) the algebra $\mathbb{B}$ is generated over $\mathbb{Z}$ by the matrices $B(N)$ and $B(p)$ for $p \neq N$. These commute with each other by 2).

6) The duality $\phi \longleftrightarrow \phi^{\vee}$ identifies $\mathrm{Hom}(E_i,E_j)$ with $\mathrm{Hom}(E_j,E_i)$ and preserves the degree. Since $w_jB_{ij}(m)$ is ½ the number of elements in $\mathrm{Hom}(E_i,E_j)$ of degree m, the symmetry follows.

7) Define an inner product on the group $\mathbb{Z}^n = \bigoplus_{i=1}^{n} \mathbb{Z}e_i$ by the formula $\langle e_i,e_j \rangle = w_i\delta_{ij}$. This is positive definite on $\mathbb{R}^n$, and by 6) the matrices $B(m)$ give self-adjoint endomorphisms of $\mathbb{Z}^n$. The result now follows from the spectral theorem.

We may interpret optimal embeddings of $\mathcal{O}$ into R_i as singular liftings of the supersingular elliptic curve E_i. Assume that $\mathcal{O} \otimes \mathbb{Z}_N$ is a discrete valuation ring, so local optimal embeddings exist at all finite primes, and let W be a complete discrete valuation ring containing $\mathcal{O} \otimes \mathbb{Z}_N$

with residue field $\mathbb{F}$. Then the $h_i(d)$ optimal embedding $\mathcal{O} \to R_i$, modulo conjugation by R_i^*, correspond to the elliptic curves E with complex multiplication by $\mathcal{O}$ over W which are isomorphic to E_i over $\mathbb{F}$, together with a fixed isomorphism $g : \mathcal{O} \xrightarrow{\sim} \mathrm{End}_W(E)$. We identify (E,g) with (E',g') if there is an isomorphism $i : E \xrightarrow{\sim} E'$ over $\mathbb{F}$ such that $g'(\alpha)\circ i = i\circ g(\alpha)$ for all $\alpha \in \mathcal{O}$.

3. Curves of genus zero and their special points.

We begin with an adèlic reinterpretation of Eichler's results. Let $\hat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z} = \prod_p \mathbb{Z}_p$ be the profinite completion of $\mathbb{Z}$ and $\hat{\mathbb{Q}} = \hat{\mathbb{Z}} \otimes \mathbb{Q}$ the ring of finite adèles of $\mathbb{Q}$. For any prime p we let $R_p = R \otimes \mathbb{Z}_p$ be the local component of R in $B_p = B \otimes \mathbb{Q}_p$, and put $\hat{R} = R \otimes \hat{\mathbb{Z}} = \prod_p R_p$ and $\hat{B} = B \otimes \hat{\mathbb{Q}}$. Since every left ideal I for R is locally principal, we have $I_p = R_p g_p$ with $g_p \in R_p^* \backslash B_p^*$. The element $g_I = (\ldots g_p \ldots)$ then lies in $\hat{R}^* \backslash \hat{B}^*$; conversely any such coset determines a left ideal $I = \hat{R}g \cap B$ of R.

The left ideal classes correspond to the orbits of B^* acting on the right of $\hat{R}^* \backslash \hat{B}^*$, so the class number is the number of double cosets:

$$n = [\hat{R}^* \backslash \hat{B}^* / B^*] . \tag{3.1}$$

The choice of representative ideals $I_1, I_2, \ldots, I_n$ corresponds to a choice of cosets $g_1, g_2, \ldots, g_n$ in $\hat{R}^* \backslash \hat{B}^*$ such that

$$\hat{B}^* = \bigcup_{i=1}^{n} \hat{R}^* g_i B^* . \tag{3.2}$$

The right order R_i of the ideal I_i is given by the formula $R_i = B \cap g_i^{-1} \hat{R} g_i$. Since the maximal orders in B are all locally conjugate in $\hat{B}$, and the subgroup fixing $\hat{R}$ is the normalizer $N\hat{R}^*$ of $\hat{R}$, we have

$$t = [N\hat{R}^*\backslash\hat{B}^*/B^*] . \tag{3.3}$$

We remark that $\hat{R}^*\hat{\mathbb{Q}}^*$ is a normal subgroup of index 2 in $N\hat{R}^*$, and the quotient is generated by the non-trivial class in $R_N^*\mathbb{Q}_N^*\backslash B_N^*$.

The optimal embeddings $f : \mathcal{O} \to R_i$ also admit an adèlic description. To give f is equivalent to giving a field homomorphism $f : K \to B$ such that $f(K) \cap g_i^{-1}\hat{R}g_i = f(\mathcal{O})$ in $\hat{B}$. The group B^* acts on the right of the set $\hat{R}^*\backslash\hat{B}^* \times \mathrm{Hom}(K,B)$ by the formula. $(g,f) \longmapsto (gb,b^{-1}fb)$. Since $\hat{B}^* = \bigcup \hat{R}^* g_i B^*$, the set of all optimal embeddings of $\mathcal{O}$ into the n orders R_i, modulo conjugation by R_i^*, is then identified with the classes (g,f) in the quotient space $(\hat{R}^*\backslash\hat{B}^* \times \mathrm{Hom}(K,B))/B^*$ which satisfy $f(K) \cap g^{-1}\hat{R}g = f(\mathcal{O})$. This quotient space admits a geometric interpretation, as the K-valued points of a curve X over $\mathbb{Q}$.

Indeed, let Y be the curve of genus zero over $\mathbb{Q}$ which is associated to the quaternion algebra B. The points of Y in any $\mathbb{Q}$-algebra E are given by $\{\alpha \in B \otimes E : \alpha \neq 0, \mathrm{Tr}\alpha = 0, \mathbb{N}\alpha = 0\}/E^*$. The group B^* acts on Y on the right by conjugation: $\alpha \to b^{-1}\alpha b$ and $\mathbb{Q}^*$ acts trivially; in fact, the automorphism group of Y is the $\mathbb{Q}$-form of PGL_2 associated to the quaternion algebra B. In particular, $\mathrm{Aut}_{\mathbb{Q}}(Y) \simeq B^*/\mathbb{Q}^*$. If K is a quadratic field we have a canonical identification $Y(K) = \mathrm{Hom}(K,B)$: to each embedding $f : K \to B$ we let $y = y_f$ be the image of the unique K-line on the quadric $\{\alpha \in B \otimes K : \mathrm{Tr}\alpha = \mathbb{N}\alpha = 0\}$ on which conjugation by $f(K^*)$ acts by multiplication by the character $k \longmapsto k/\bar{k}$. Then y_f is one of 2 fixed points of $f(K^*)$ acting on $Y(K)$; the other is the image of the line where conjugation acts by the character $k \longmapsto \bar{k}/k$.

The curve X is defined as the double coset space

$$X = \hat{R}^* \backslash \hat{B}^* \times Y/B^* , \tag{3.4}$$

which is the disjoint union of n curves of genus zero over $\mathbb{Q}$. Indeed the decomposition $\hat{B}^* = \bigcup \hat{R}^* g_i B^*$ gives an isomorphism

$$X \simeq \coprod_{i=1}^{n} Y/\Gamma_i \tag{3.5}$$

which takes the double coset $\hat{R}^* g_i \times y \pmod{B^*}$ to the coset $y \pmod{\Gamma_i}$ on the i^{th} component $X_i = Y/\Gamma_i$ of X .

The special points on X over K are the image of $\hat{R}^* \backslash \hat{B}^* \times Y(K)$ in $X(K)$. We say the point $x = g \times y$ has discriminant d iff $f(K) \cap g^{-1} \hat{R} g = f(\mathcal{O})$ is the image of the order of discriminant d , where $f : K \to B$ is the embedding corresponding to y . If the component g of x is congruent to g_i in $\hat{R}^* \backslash \hat{B}^* / B^*$, then the special point x lies on the component $X_i(K)$. There are exactly $h_i(d)$ special points of discriminant d on this component, as they correspond to the number of optimal embeddings of $\mathcal{O}$ into R_i , modulo conjugation by R_i^* .

We can now prove Eichler's formula (1.12) for the total number $\sum_{i=1}^{n} h_i(d)$ of special points of discriminant d on X . We will show this number is divisible by $h(d) = [\mathrm{Pic}(\mathcal{O})]$ by exhibiting a free action of the group $\hat{\mathcal{O}}^*\backslash\hat{K}^*/K^* \simeq \mathrm{Pic}(\mathcal{O})$ on the set of special points of this discriminant; we will then count the number of orbits using the theory of local embeddings. Let $a \in \hat{K}^*$ be a finite idèle of K and $x = g \times y$ a special point of discriminant d. Let $f : K \to B$ be the embedding corresponding to y; this induces a homomorphism $\hat{f} : \hat{K}^* \to \hat{B}^*$ and we define

$$(3.6) \qquad x_a = g\hat{f}(a) \times y \quad .$$

If $x \equiv g' \times y'$ then $g' = gb$ and $f' = b^{-1}fb$; hence $g'\hat{f}'(a) \times y' = gb(b^{-1}\hat{f}(a)b) \times y' = g\hat{f}(a)b \times y' \equiv x_a$ so the action is well-defined independent of our choice of representative for x.

Let us first verify that x_a has discriminant d. Since $\hat{f}(\hat{K}^*)$ is commutative, $f(K) \cap g\hat{f}(a)^{-1}\hat{R}\, g\hat{f}(a) = \hat{f}(a)^{-1}(f(K) \cap g^{-1}\hat{R}\, g)\hat{f}(a) = \hat{f}(a)^{-1}\, f(\mathcal{O})\, \hat{f}(a) = f(\mathcal{O})$. The subgroups K^* and $\hat{\mathcal{O}}^*$ of $\hat{K}^*$ act trivially; conversely if $x = x_a$ then a lies in the subgroup $K^*\hat{\mathcal{O}}^*$. Hence $\hat{\mathcal{O}}^*\backslash\hat{K}^*/K^* \simeq \mathrm{Pic}(\mathcal{O})$ acts freely. The orbit space is identified with the double cosets

$$(3.7) \qquad \hat{R}^*\backslash\hat{N}^*/f(\hat{K}^*) \; ,$$

where $f : K \to B$ is a fixed embedding (if any exist) and $\hat{N}^* = \{g \in \hat{B}^* : f(K) \cap g^{-1}\hat{R}\, g = f(\mathcal{O})\}$. But the space in (3.7) is a product of local terms $R_p^*\backslash N_p^*/f(K_p^*)$, which classify the number of optimal embeddings of $\mathcal{O}_p$ into the maximal order R_p modulo conjugation by R_p^*. This number is 1 for all $p \neq N$, for $p = N$ it is 0,1, or 2 depending on the behavior of N in $\mathcal{O}$. This gives a geometric proof of (1.12)

Another description of the points of discriminant d on the component $X_i = Y/\Gamma_i$ as corresponding to optimal embeddings $f : \mathcal{O} \to R_i$ is useful in many computational contexts. Here we describe the action of $\mathrm{Pic}(\mathcal{O})$ on these points in terms of ideals. Let $\mathfrak{a}$ be the ideal (= projective module of rank 1 in K) which is determined by the idèle a (mod $\hat{\mathcal{O}}^*$) ; specifically $\mathfrak{a} = K \cap a\hat{\mathcal{O}}$. Let R' be the right order of the left R_i module $R_i\mathfrak{a}$; since $\mathcal{O}$ also acts on the right of $\mathfrak{a}$, the map f induces an optimal embedding $\mathcal{O} \to R'$ which corresponds to the point x_a .

We may refine our modified Hurwitz class numbers by defining the rational divisor c_D on X for $D > 0$ by

$$c_D = \frac{1}{2} \sum_{-D=df^2} \frac{1}{u(d)} \sum_{\substack{x \text{ of} \\ \text{discriminant } d \\ \text{on } X}} (x) \qquad (3.8)$$

Then $\deg(c_D) = H_N(D)$ by formula (1.12). The element c_D lies in $\frac{1}{2W}\mathrm{Div}(x)$; we will analyze its class in $\mathrm{Pic}(X)$ in the next section.

The action of $\mathrm{Gal}(K/\mathbb{Q})$ on the special points in $Y(K)$ preserves the points of discriminant d and may be described as follows.
If x corresponds to the embedding $\mathcal{O} \to R_i$ then $\bar{x}$ corresponds to the embedding $\alpha \to f(\bar{\alpha})$; in particular, $\bar{x}$ lies on the same component as x . When N is inert in $\mathcal{O}$ the group $\mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Pic}(\mathcal{O})$ acts simply transitively on the points of discriminant d . When N is ramified in $\mathcal{O}$,

the group $\mathrm{Pic}(\mathcal{O})$ acts simply transitively; we have $x = \bar{x}$ if and only if x corresponds to an embedding $f : \mathcal{O} \to R_i$ where $f(\bar{\alpha}) = j\alpha j^{-1}$ for a 4th root of unity j in R_i^*. In this case, $w_i \equiv 0 \pmod 2$. Hence $w_i h_i(d)$ is always an <u>even</u> integer.

4. Correspondences and the height pairing.

The curve X has a large ring of correspondences over $\mathbb{Q}$, which come from the geometry of the coset space $\hat{R}^*\backslash\hat{B}^*$. Since the class number of $\mathbb{Q}$ is 1, we have $\hat{\mathbb{Q}}^* = \mathbb{Q}^*\hat{\mathbb{Z}}^*$ and

$$(4.1) \qquad X \simeq (\hat{R}^*\backslash\hat{B}^*/\hat{\mathbb{Q}}^*) \times Y / (B^*/\mathbb{Q}^*) .$$

The elements $g = (\dots g_p \dots)$ lie in the product of local spaces $R_p^*\backslash B_p^*/\mathbb{Q}_p^*$.

When $p \neq N$ the space $R_p^*\backslash B_p^*/\mathbb{Q}_p^* \simeq PGL_2(\mathbb{Z}_p)\backslash PGL_2(\mathbb{Q}_p)$ has the structure of the set of vertices in a homogeneous tree of degree $p+1$ [10, pg. 70]. When $p = N$ the space $R_p^*\backslash B_p^*/\mathbb{Q}_p^*$ has 2 elements, so may be viewed as the vertices in a homogeneous tree of degree 1. Let δ_p denote the distance function on the tree at the place p; for $m \geq 1$ we define a correspondence t_m on the product of these trees by the formula

$$(4.2) \qquad t_m(g) = \sum_{\substack{\delta_p(g_p,h_p) \leq \mathrm{ord}_p(m) \\ \delta_p(g_p,h_p) \equiv \mathrm{ord}_p(m) \pmod 2}} (h)$$

This is self-dual of degree $\sigma(m)_N$. It preserves $\hat{R}^*\backslash\hat{B}^*/\hat{\mathbb{Q}}^*$, as m is divisible by only a finite number of primes. Since the right action of $B^*/\mathbb{Q}^*$ in (4.1) preserves distance, t_m induces a correspondence on X

$$(4.3) \qquad t_m(g \times y) = \sum_{h \in t_m(g)} (h \times y) .$$

The correspondences t_m on X commute, and satisfy the same relations as the Brandt matrices in Proposition 2.7 [10, pg. 73].

The group Pic(X) of line bundles on X is isomorphic to $\mathbb{Z}^n$, and is generated by the classes e_i of degree 1 on each component X_i. The correspondences t_m on X induce endomorphisms of the group Pic(X), and we have the following

Proposition 4.4. For all $m \geq 1$ and $i = 1,2,\ldots,n$

$$t_m\, e_i = \sum_{j=1}^{n} B_{ij}(m) e_j \ .$$

In other words, on the basis $\langle e_i \rangle_{i=1}^{n}$ of Pic(X), the action of t_m is given by the transpose $B(m)^{tr}$ of the m^{th} Brandt matrix. This gives a geometric interpretation of Brandt matrices.

Proof. The components of X are indexed by the supersingular elliptic curves E_i. The number of points in the divisor class $t_m e_i$ which lie on the component X_j is equal to the number of isogenies $E_i \to E_j$ of degree m, which two isogenies identified if they have the same kernel. This follows from the definition of t_m in (4.2)-(4.3) and Tate's theorem that an isogeny is determined by its action on the Tate modules $T_p E_i$ and Dieudonné module $T_N E_i$. But the number of such isogenies is equal to $B_{ij}(m)$ by Proposition 2.3.

We define a height pairing $\langle , \rangle$ on Pic(X) with values in $\mathbb{Z}$ by setting

$$(4.5)\qquad \begin{aligned} \langle e_i, e_j \rangle &= 0 \quad \text{if} \quad i \neq j \\ \langle e_i, e_i \rangle &= w_i \end{aligned}$$

and extending bi-additively. If $e = \Sigma\, a_i e_i$ and $e' = \Sigma\, a_i' e_i$ are two divisor classes, then

$$\langle e, e' \rangle = \sum_{i=1}^{n} w_i a_i a_i' \, .$$

This pairing is clearly positive definite. It gives an isomorphism of $\mathrm{Pic}(X)^\vee = \mathrm{Hom}(\mathrm{Pic}(X), \mathbb{Z})$ with the subgroup of $\mathrm{Pic}(X) \otimes \mathbb{Q}$ with basis $\langle e_i^\vee = e_i/w_i \rangle_{i=1}^{n}$.

Proposition 4.6. *For all classes* e *and* e' *in* $\mathrm{Pic}(X)$

$$\langle t_m e, e' \rangle = \langle e, t_m e' \rangle \, .$$

Proof. It suffices to verify the equality when $e = e_i$ and $e' = e_j$. The left hand side is then $w_j B_{ij}(m)$ by Proposition 4.4, and the right hand side is $w_i B_{ji}(m)$. These are equal by Proposition 2.7.

We let e_D denote the class of the divisor c_D defined in (3.8). This lies in $\mathrm{Pic}(X) \otimes \mathbb{Q}$, but in fact we have

Proposition 4.7. *The class* e_D *lies in the subgroup* $\mathrm{Pic}(X)^\vee$ *of* $\mathrm{Pic}(X) \otimes \mathbb{Q}$.

Proof. By its definition, we have $e_D = \sum_{i=1}^{n}\left(\sum_{-D=df^2} \frac{h_i(d)}{2u(d)}\right) e_i = \sum_{i=1}\left(\sum_{-D=df^2} \frac{w_i h_i(d)}{2u(d)}\right) e_i^{\vee}$ in $\mathrm{Pic}(X)$. We must show that

$$\frac{w_i h_i(d)}{2u(d)} \in \mathbb{Z} .$$

This is clear if w_i is odd, as then $u(d)$ divides w_i and 2 divides $h_i(d)$. If $w_i \equiv 2 \pmod 4$, the only possible problem is when $u(d) = 2$; but in this case $d = -4$, N is odd, and $h_i(d)$ is even. If $N = 2$ and $w_i = 12$, then $w_i/2u(d)$ is always integral.

We define e_0 in $\mathrm{Pic}(X)^{\vee}$ as the class

(4.8) $$e_0 = \sum_{i=1} \frac{1}{w_i} e_i = \sum_{i=1}^{n} e_i^{\vee} .$$

The $\deg(e_0) = \frac{N-1}{12}$ by the mass formula. By proposition 4.4 we have

(4.9) $$t_m e_0 = \sigma(m)_N \cdot e_0 \qquad \text{for } m \geq 1 .$$

For any class e in $\mathrm{Pic}(X)$ we have the height formula:

(4.10) $$\langle e, e_0 \rangle = \deg e .$$

5. Modular forms of weight 2.

We recall the slash notation for functions on the upper half plane $\mathfrak{h}$. Let $f : \mathfrak{h} \to \mathbb{C}$ be a function, $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ a matrix in $GL_2(\mathbb{R})$ with positive determinant, and $k \geq 0$ an integer. Then

$$(5.1) \qquad f|_k A = f\left(\frac{az+b}{cz+b}\right)(cz+d)^{-k} \; (\det A)^{k/2}$$

defines a right action of the matrices: $f|_k AB = (f|_k A)\,|_k B$. We say f is a modular form of weight k for $\Gamma_0(M)$ with character ε if f is holomorphic on $\mathfrak{h}$, regular at the cusps, and satisfies

$$(5.2) \qquad f|_k A = \varepsilon(d) f$$

for all $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $SL_2(\mathbb{Z})$ with $c \equiv 0 \pmod{M}$. In this section, we shall only consider modular forms of weight 2 and trivial character for $\Gamma_0(N)$.

The set of these modular forms forms a complex vector space $M_{\mathbb{C}}$, and it is well-known that $\dim M_{\mathbb{C}} = n$. Every function f in $M_{\mathbb{C}}$ has a Fourier expansion

$$f(\tau) = \sum_{m \geq 0}^{\infty} a_m q^m \quad \text{with} \quad q = e^{2\pi i \tau} .$$

We define M as the subgroup of those modular forms which satisfy

$$(5.3) \qquad \begin{cases} a_m \in \mathbb{Z} \quad \text{for all} \quad m \geq , \\ \\ Wa_0 \in \frac{1}{2}\mathbb{Z} . \end{cases}$$

Then M is a free $\mathbb{Z}$-module of rank n and $M \otimes \mathbb{C} = M_{\mathbb{C}}$. Some examples of elements in M are the theta-series f_{ij} defined in (1.4). We remark that the condition on a_0 is forced by the condition on the higher coefficients.

The Hecke algebra $\mathbb{T} = \mathbb{Z}[\ldots T_m \ldots]$ acts on the lattice M by the well-known formulae. This algebra is generated over $\mathbb{Z}$ by the operators of prime index, and the operators satisfy the same relations as the Brandt matrices in Proposition 2.7. If $p \neq N$ is prime we have

$$\sum a_m q^m \mid T_p = \sum \{a_{mp} + pa_{m/p}\} q^m .$$

If $p = N$ we have

$$\sum a_m q^m \mid T_N = \sum a_{mN}\, q^m .$$

We remark that as endomorphisms of M , $T_N + W_N = 0$ where W_N is the canonical involution $f \longmapsto f \mid \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}$. Also, the subgroup M^+ on which $T_N = +1$ (or $W_N = -1$) has rank t . It is also know that $M \otimes \mathbb{Q}$ is a free $\mathbb{T} \otimes \mathbb{Q}$ module of rank 1 , this is a restatement of the multiplicity one theorem, as every eigenform in $M \otimes \mathbb{R}$ is a new form of level N .

By computing the trace of T_m on the homology of the Riemann surface $\mathfrak{H}^*/\Gamma_0(N)$ using Lefschetz's fixed point formula, and comparing with Proposition 1.9, Eichler established the identity

$$(5.4) \qquad \text{Trace } T_m = \text{Trace } B(m) \quad \text{for all} \quad m \geq 1 .$$

The left hand side is the trace of T_m as an endomorphism of M, or equivalently, of $M_{\mathbb{C}}$. The semi-simplicity of the algebras $\mathbb{T} \otimes \mathbb{Q}$ and $\mathbb{B} \otimes \mathbb{Q}$ then shows that they are conjugate inside $M(n,\mathbb{Q})$. Hence the map $T_m \to B(m)$ induces a ring isomorphism $\mathbb{T} \simeq \mathbb{B}$. Since we have seen that $\mathbb{B}$ is isomorphic to the ring of correspondences $\mathbb{Z}[\cdots t_m \cdots]$ acting on Pic(X) (Proposition 4.4), we may also identify this ring with the Hecke algebra $\mathbb{T}$.

We will now compute the action of the Hecke operators on our theta series f_{ij}.

<u>Proposition 5.5</u>. <u>For all</u> $m \geq 1$ <u>we have</u>

$$f_{ij} \mid T_m = \sum_k B_{ik}(m) f_{kj} = \sum_k B_{kj}(m) f_{ik} .$$

<u>Proof</u>. The second identity will follow from the first, as $w_j f_{ij} = w_i f_{ji}$ and $w_k B_{ik}(m) = w_i B_{ki}(m)$. It also suffices to calculate $f_{ij} \mid T_m$ for prime indices, as these operators generate $\mathbb{T}$ and satisfy the same relations as the matrices $B(m)$ in $\mathbb{B}$. Since $f_{ij} = \frac{1}{2w_j} + \sum B_{ij}(m) q^n$ we must show

$$B_{ij}(mp) + p\ B_{ij}(m/p) = \sum_k B_{ik}(p)B_{kj}(m)$$

$$B_{ij}(mN) = \sum_k B_{ik}(N)B_{kj}(m)\ .$$

These follow from Proposition 2.7.

In simple terms, Proposition 5.5 states that the subgroups

$$\begin{cases} N_j = \langle f_{1j}, f_{2j}, \ldots, f_{nj} \rangle \\ N_j' = \langle f_{j1}, f_{j2}, \ldots, f_{jn} \rangle \end{cases}$$

are stable under the action of $\mathbb{T}$, and that T_m acts on the spanning sets by $B(m)^{tr}$ and $B(m)$ respecticely. Since $w_j f_{ij} = w_i f_{ji}$, these two $\mathbb{Z}$-modules have the same rank n_j, which depends on the order R_j. The determination of n_j is Hecke's basis problem, which is still open and appears rather difficult. From (5.4) it follows that the n^2 theta-series $\{f_{ij}\}$ span $M \otimes Q$.

We will now use the curve X to construct elements of M.

<u>Proposition 5.6</u>. <u>The map</u> $\phi(e,e^\vee) = \frac{\deg e \cdot \deg e^\vee}{2} + \sum_{m\geq 1} \langle t_m, e, e^\vee \rangle q^m$ <u>defines a</u> $\mathbb{T}$-<u>module homomorphism</u> $\phi : \mathrm{Pic}(X) \otimes_{\mathbb{T}} \mathrm{Pic}(X)^\vee \to M$ <u>which is an isomorphism over</u> $\mathbb{T} \otimes Q$.

<u>Proof</u>. We first verify that $\phi(e,e^\vee)$ is an element of M. The definition is bi-additive in each variable, so it suffices to check this when $e = e_i$ and $e^\vee = e_j^\vee$. Then $\langle t_m, e, e^\vee \rangle = B_{ij}(m)$, so $\phi(e,e^\vee) = f_{ij}$.

The $\mathbb{T}$-linearity follows from Proposition 5.5 and Proposition 4.4. The fact that ϕ gives an isomorphism over $\mathbb{Q}$ results from the fact that $\mathrm{Pic}(X)\otimes\mathbb{Q} \simeq \mathrm{Pic}(X)^{\vee}\otimes\mathbb{Q}$ and $M\otimes\mathbb{Q}$ are free $\mathbb{T}\otimes\mathbb{Q}$ modules of rank 1 , and the map ϕ is surjective (the n^2 theta series f_{ij} generate $M\otimes\mathbb{Q}$)

We now discuss the normalized Eisenstein series F of weight 2 for $\Gamma_0(N)$ and the cuspidal eigenforms. The Eisenstein series is given by

$$(5.7)\qquad \begin{aligned} F &= \phi(e_i,e_0) \quad \text{for any } i = 1,2,\dots,n \\ &= \sum_{j=1}^{n} f_{ij} \quad \text{for any } i = 1,2,\dots,n \\ &= \frac{N-1}{24} + \sum_{m\ge1} \sigma(m)_N q^m . \end{aligned}$$

It satisfies $F|T_m = \sigma(m)_N F$ for any $m \geq 1$. The other characters in the spectral decomposition of $\mathbb{T}\otimes\mathbb{R}$ correspond to normalized cusp forms f in M with $a_0 = 0$, $a_1 = 1$, and $a_m = O(m^{1/2+\varepsilon})$. The rank of the subgroup of cusp forms is equal to $n-1$, which is the genus of the modular curve $X_0(N)$.

6. Some examples

Consider first the case when $N = 2$, so $n = t = 1$. The algebra B was found by Hamilton: $B = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k$, $i^2 = j^2 = k^2 = -1$. $ij = -ji = k$. A maximal order, which is unique up to conjugacy, was found by Hurwitz:

$$R = \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}k + \mathbb{Z}\left(\frac{1+i+j+k}{2}\right). \tag{6.1}$$

The supersingular elliptic curve E in characteristic 2 with $\mathrm{End}(E) = R$ has the equation $y^2+y = x^3$ and invariant $j = 0$. The group $\mathrm{Aut}(E) = R^*$ has order 24, and is given by

$$R^* = <\pm 1, \pm i, \pm j, \pm k, \frac{\pm 1 \pm i \pm j \pm k}{2}>. \tag{6.2}$$

By considering the action on the 3-division points of E, one obtains an isomorphism $R^* \simeq SL_2(\mathbb{Z}/3)$. Hence $\Gamma = R^*/\pm 1$ is isomorphic to $PSL_2(\mathbb{Z}/3)$, or to the alternating group on 4 letters. We have $W = w_1 = 12$. The theta series $f = f_{11}$ is given by

$$\begin{aligned} f &= \frac{1}{24} \sum_{b \in R} q^{\mathbb{N}b} \\ &= \frac{1}{24} \sum_{x \equiv y \equiv z \equiv w \pmod 2} q^{(x^2+y^2+z^2+w^2)/4} \\ &= \frac{1}{24} + q + q^2 + 4q^3 + q^4 + 6q^5 + \cdots \end{aligned} \tag{6.3}$$

By (5.7), the m^{th} Fourier coefficient of f is equal to $\sigma(m)_2$; in particular, this shows that every integer $\equiv 0\ (4)$ is the sum of 4 squares.

The first case where $n > 1$ and there are cusp forms is when $N = 11$. There $n = t = 2$, $w_1 = 2$ and $w_2 = 3$. The first few Brandt matrices are:

$$B(0) = \begin{pmatrix} 1/4 & 1/6 \\ 1/4 & 1/6 \end{pmatrix} \qquad B(3) = \begin{pmatrix} 2 & 2 \\ 3 & 1 \end{pmatrix}$$

$$B(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad B(4) = \begin{pmatrix} 5 & 2 \\ 3 & 4 \end{pmatrix}$$

$$B(2) = \begin{pmatrix} 1 & 2 \\ 3 & 0 \end{pmatrix} \qquad B(5) = \begin{pmatrix} 4 & 2 \\ 3 & 3 \end{pmatrix}.$$

The unique normalized cusp form is

$$(6.4) \qquad \begin{aligned} f &= f_{11} - f_{21} = f_{22} - f_{12} = 3f_{22} - 2f_{11} \\ &= q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 + \dots \\ &= q \prod_{m\geq 1} (1-q^m)^2 (1-q^{11m})^2 . \end{aligned}$$

Its Mellin transform is the zeta function of the elliptic curve $X_0(11)$ with equation $y^2+y = x^3-x^2-10x-20$ over Q. We have the congruence

$$(6.5) \qquad f \equiv F \pmod{5M}$$

where F is the Eisenstein series:

$$F = f_{11} + f_{12} = f_{21} + f_{22} = 3f_{11} - 2f_{22} \tag{6.6}$$

$$= \frac{5}{12} + q + 3q^2 + 4q^3 + 7q^4 + 6q^5 + \ldots$$

Indeed, $F - f = 5(f_{11} - f_{22})$, and $M = \mathbb{Z} f_{11} + \mathbb{Z} f_{22}$

7. The main identity

For the next five sections $f = \sum_{m\geq 1} a_m q^m$ will be a cusp form in $M_{\mathbb{C}}$, K will denote an imaginary quadratic field of discriminant $-D$ where the prime N is inert, and $\mathcal{O}$ will denote the ring of integers in K. We let A denote a fixed ideal class of $\mathcal{O}$ and ε the quadratic character of $(\mathbb{Z}/D\mathbb{Z})^*$ determined by $\varepsilon(p) = \left(\frac{-D}{p}\right)$ for primes p not dividing D. Also, $u = u(-D)$ and $h = h(-D)$.

Let $\omega_f = 2\pi i f(\tau)d\tau = \sum_{m\geq 1} a_m q^m \frac{dq}{q}$ be the holomorphic differential associated to f on the Riemann surface $X_0(N)$. If g is any element in $M_{\mathbb{C}}$, we define the Petersson product of f and g by the formula

$$(7.1) \qquad (f,g) = \iint_{X_0(N)} \omega_f \wedge \overline{i\omega_g}$$

$$= 8\pi^2 \iint_{\Gamma_0(N)\backslash \mathfrak{H}} f(z)\, \overline{g(z)}\, dxdy \qquad z = x+iy .$$

Let E_A be the theta series of weight 1 which is determined by the ideal class A:

$$(7.2) \qquad E_A(z) = \frac{1}{2u} \sum_{\lambda\in\mathfrak{a}} q^{\mathbf{N}\lambda/\mathbf{N}\mathfrak{a}}$$

$$= \frac{1}{2u} + \sum_{m\geq 1} r_A(m) q^m .$$

In this formula, $\mathfrak{a}$ is any ideal in the class A. Hecke showed that E_A is a modular form of weight 1 for $\Gamma_0(D)$ with character ε. The sum over all classes

$$(7.3) \qquad E = \sum_A E_A = \frac{h}{2u} + \sum_{m\geq 1} R(m)q^m$$

is the weight 1 Eisenstein series, whose Fourier coefficients $R(m)$ are the number of ideals of $\mathcal{O}$ of norm m. We put $R(0) = \frac{h}{2u} = \frac{h}{w}$ for consistency.

Define the L-function $L(f,A,s)$ as the product of the two Dirichlet series:

$$(7.4) \qquad L(f,A,s) = \sum_{\substack{m=1\\(m,N)=1}}^{\infty} \frac{\varepsilon(m)}{m^{2s-1}} \sum_{m=1}^{\infty} \frac{a_m r_A(m)}{m^s} .$$

The first is a modification of the Dirichlet L-function $L(\varepsilon,2s-1)$ and the second converges for $\mathrm{Re}(s) > 3/2$. In the next section, we will show that $L(f,A,s)$ admits an analytic continuation to the entire plane. It also satisfies the functional equation

$$(7.5) \quad L^*(f,A,s) \underset{\text{defn.}}{=} \left[(2\pi)^{-s}\Gamma(s)\right]^2 (ND)^s L(f,A,s) = L^*(f,A,2-s) .$$

Our main result gives the value of $L(f,A,s)$ at $s = 1$ in terms of the heights of special points of discriminant $-D$ on the curve X. Let x be a fixed point of this discriminant, and define the element g_A of M by taking the sum over all classes B in $\mathrm{Pic}(\mathcal{O})$

$$g_A = \sum_B \phi(x_B, x_{BA}) \tag{7.6}$$

and using Proposition 5.6. The main identity to be proved is then

<u>Proposition 7.7</u>. $L(f,A,1) = \dfrac{(f,g_A)}{u^2\sqrt{D}}$.

We will prove (7.7) by a method similar to Gross-Zagier [3]. First we will use Rankin's method to obtain the analytic identity

$$L(f,A,1) = \frac{(f,G_A)}{\sqrt{D}} \cdot \text{ with } G_A(z) = \mathrm{Trace}\begin{Bmatrix}\Gamma_0(ND) \\ \Gamma_0(N)\end{Bmatrix} E_A(z)E(Nz) .$$

We will then explicitly compute the trace and obtain the Fourier coefficients a_m of G_A . (These computations are performed in greater detail in Chapter IV of [3]). Finally, we well explicitly compute the height pairing $<x_B, t_m x_{AB}>$ and compare with our previous results to obtain the identity

$$u^2 a_m = \sum_B < x_B, t_m x_{AB} >$$

for all $m \geq 1$. This shows that $u^2 G_A = g_A$ and completes the proof.

8. Rankin's method

We now discuss Rankin's integral representation for $L^*(f,A,s)$; more details can be found in [3, Ch. IV]. Let $\Gamma_\infty = \left\{\pm\begin{pmatrix}1 & n\\ 0 & 1\end{pmatrix} : n \in \mathbb{Z}\right\}$; a fundamental domain for Γ_∞ on $\mathfrak{H}$ is the region $0 \leq x < 1$, $0 < y < \infty$. For $\mathrm{Re}(s)$ large, we therefore have

$$(4\pi)^{-s}\Gamma(s) \sum_{m=1}^{\infty} \frac{a_m r_A(m)}{m^s} = \int_0^\infty \left(\sum_{m=1}^{\infty} a_m r_A(m) e^{-4\pi my}\right) y^s \frac{dy}{y}$$

$$= \int_0^\infty \left(\int_0^1 f(x+iy)\overline{E_A(x+iy)}dx\right) y^s \frac{dy}{y}$$

$$= \iint_{\Gamma_\infty\backslash\mathfrak{H}} f(z)\overline{E_A(z)}\ y^{s+1} \frac{dxdy}{y^2}$$

$$= \sum_{\gamma\in\Gamma_\infty\backslash\Gamma_0(ND)} \iint_{\gamma F_{ND}} f(z)\overline{E_A(z)}\ y^{s+1} \frac{dxdy}{y^2} .$$

where F_{ND} is any fundamental domain for the action of $\Gamma_0(ND)$ on $\mathfrak{H}$. Using the modular behavior of f and E_A under this subgroup:

$$\begin{cases} f(\gamma z) = f(z)(cz+d)^2 \\ E_A(\gamma z) = \overline{E_A(z)}\ (c\bar{z}+d)\ \varepsilon(d) \\ \mathrm{Im}(\gamma z) = \dfrac{y}{|c\bar{z}+d|^2} , \end{cases}$$

and the invariance of the measure $\frac{dxdy}{y^2}$ under $SL_2(\mathbb{R})$, we find that the last expression is equal to

$$\sum_{\gamma\in\Gamma_\infty\backslash\Gamma_0(ND)} \iint_{F_{ND}} f(\gamma z)\overline{E_A(\gamma z)}\ \mathrm{Im}(\gamma z)^{s+1}\,\frac{dxdy}{y^2} =$$

(8.1)
$$\sum_{\gamma=\pm\begin{pmatrix}\cdot & \cdot\\ c & d\end{pmatrix}\Gamma_\infty\backslash\Gamma_0(ND)} \iint_{F_{ND}} f(z)\overline{E_A(z)}\,\frac{\varepsilon(d)}{(c\bar{z}+d)}\,\frac{y^{s-1}}{|cz+d|^{2s-2}}\,dxdy\ .$$

We now introduce the Eisenstein series $E_{ND}(s,z)$ of weight 1, level ND, and character ε, defined by

(8.2)
$$E_{ND}(s,z) = \sum_{\substack{m=1\\(m,N)=1}} \frac{\varepsilon(m)}{m^{2s+1}} \sum_{\pm\begin{pmatrix}\cdot & \cdot\\ c & d\end{pmatrix}\in\Gamma_\infty\backslash\Gamma_0(ND)} \frac{\varepsilon(d)}{cz+d}\,\frac{y^s}{|cz+d|^{2s}}$$

$$= \frac{1}{2}\sum_{\substack{c,d\in\mathbb{Z}\\ c\equiv 0\,(ND)\\ (d,ND)=1}} \frac{\varepsilon(d)}{(cz+d)}\,\frac{y^s}{|cz+d|^{2s}}\ .$$

Then switching the order of integration and summation in (8.1) and multiplying by the Dirichlet L-function $\sum_m \frac{\varepsilon(m)}{m^{2s+1}}$ gives the identity

(8.3)
$$(4\pi)^{-s}\Gamma(s)L(f,A,s) = \iint_{F_{ND}} f(z)\ \overline{E_A(z)E_{ND}(\bar{s}-1,z)}\ dxdy\ .$$

Since the function $\pi^{-s}\Gamma(s)\,E_{ND}(s,z)$ can be continued to an entire function on the s-plane [3], this gives the analytic continuation of $L^*(f,A,s)$; the functional equation (7.5) also follows from a functional equation for the Eisenstein series. Setting $s = 1$ in (8.3) gives the formula

$$(8.4) \qquad L(f,A,1) = 4\pi \iint_{F_{ND}} f(z)\, \overline{E_A(z)E_{ND}(0,z)}\, dxdy .$$

We wish to express this as a Petersson product on $X_0(N)$; for any form g of wieght 2 on $\Gamma_0(ND)$ we define the trace to $\Gamma_0(N)$ by

$$(8.5) \qquad \mathrm{Tr}_N^{ND}\, g = \sum_{\gamma\in\Gamma_0(ND)\backslash\Gamma_0(N)} g|_2\, \gamma .$$

Then with our normalization of the Petersson product (7.1), formula (8.4) becomes

$$(8.6) \qquad L(f,A,1) = \frac{1}{2\pi}\left(f, \mathrm{Tr}_N^{ND}\left\{E_A(z)E_{ND}(0,z)\right\}\right) .$$

Finally, we remark that the imprimitive Eisenstein series $E_{ND}(s,z)$ can be expressed in terms of the Eisenstein series $E(s,z)$ of weight 1 and level D, defined by

$$(8.7) \qquad E(s,z) = \frac{1}{2} \sum_{\substack{c,d\in\mathbb{Z} \\ c\equiv 0(D)}} \frac{\varepsilon(d)}{(cz+d)} \frac{y^s}{|cz+d|^{2s}} .$$

At $s = 0$ this gives the identity:

$$E_{ND}(0,z) = E(0,Nz) + N^{-1}E(0,z) .$$

The second term contributes 0 to the trace, as $N^{-1}E_A(z)E(0,z)$ has weight 2 and level D, so $\mathrm{Tr}_N^{ND}(N^{-1}E_A(z)E(0,z) = \mathrm{Tr}_1^D(N^{-1}E_A(z)E(0,z)) = 0$ (there are no holomorphic forms of weight 2 and level 1). Hence

$$L(f,A,1) = \frac{1}{2\pi}\left(f,\mathrm{Tr}_D^{ND}\left\{E_A(z)E(0,Nz)\right\}\right).$$

On the other hand, Hecke proved that $E(0,z)$ was related to the holomorphic Eisenstein series $E = \sum\limits_A E_A$ by the formula

$$E(0,z) = \frac{2\pi}{\sqrt{D}} E(z) . \tag{8.8}$$

Combining this with the previous formula, we see we have proved:

<u>Proposition 8.9</u>. <u>Let</u> $G_A(z) = \mathrm{Tr}_D^{ND}\left\{E_A(z)E(Nz)\right\}$. <u>Then</u>

$$L(f,A,1) = \frac{(f,G_A)}{\sqrt{D}}$$

<u>for any cusp form of</u> f <u>weight 2 on</u> $\Gamma_0(N)$.

9. The trace computation.

We put $g = E_A(z)E(Nz)$ and $G_A = \mathrm{Tr}_N^{ND}\, g$. Our aim in this section is to compute the Fourier coefficients of the modular form G_A of weight 2 on $\Gamma_0(N)$. To simplify the exposition, we shall treat the case when D is prime in detail, and refer the reader to [3] for the proof in the general case.

Proposition 9.1. Assume that D is prime. Then

1) $G_A(z) = g(z) + \frac{1}{D} \sum_{j\,(\mathrm{mod}\ D)} g\left(\frac{z+j}{D}\right)$.

2) The Fourier coefficients of $G_A = \sum_{m\geq 0} a_m q^m$ are given by the formula:

$$a_m = \sum_{n=0}^{Dm/N} r_A(Dm-nN)\ \delta(n)R(n) = \frac{r_A(m)h}{u} + \sum_{n=1}^{Dm/N} r_A(Dm-nN)\ \delta(n)R(n)$$

where $\delta(n) = \begin{cases} 1 & \text{if } (n,D) = 1 \\ 2 & \text{if } n \equiv 0 \pmod{D} \end{cases}$.

Proof. We will show how 2) follows from 1). Then we will derive 1) after a transformation lemma. If $g = \sum_{m\geq 0} b_m q^m$ then 1) gives the formula $a_m = b_m + b_{nD}$. By the definition of g , we have.

$$b_m = \sum_{\ell\geq 0} r_A(m-\ell N)\ R(\ell)$$

$$= \sum_{\substack{n\geq 0 \\ n\equiv 0\,(D)}} r_A(mD-nN)\ R(n)$$

where $n = D\ell$, as $r_A(k) = r_A(Dk)$ for all $k \geq 1$. Using the second formula for b_m and the first for b_{mD}, we get 2).

Lemma 9.2. 1) If $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is in $SL_2(\mathbb{Z})$ and $c \not\equiv 0 \pmod{D}$ then $E_A\big|_1 \gamma = \frac{\varepsilon(c)}{i\sqrt{D}} E_A\left(\frac{z+c^* d}{D}\right)$ where c^* is an inverse for $c \pmod{D}$

2) If γ is in $\Gamma_0(N)$ and $c \not\equiv 0 \pmod{D}$ then $E(Nz)\big|_1\gamma = \frac{-\varepsilon(c)}{i\sqrt{D}} E\left(N\left(\frac{z+c^* d}{D}\right)\right)$.

Proof. 1) We will use the well-known formula $E_A\big|_1 \begin{pmatrix} 0 & -1 \\ D & 0 \end{pmatrix} = \frac{1}{i} E_A$, which follows from Poisson summation. First consider the special case when $\gamma = \begin{pmatrix} 0 & -1 \\ 1 & j \end{pmatrix} = \frac{1}{D}\begin{pmatrix} 0 & -1 \\ D & 0 \end{pmatrix}\begin{pmatrix} 1 & j \\ 0 & D \end{pmatrix}$. Then

$$E_A\big|_1 \gamma = \frac{1}{i} E_A\big|_1 \begin{pmatrix} 1 & j \\ 0 & D \end{pmatrix} = \frac{1}{i\sqrt{D}} E_A\left(\frac{z+j}{D}\right).$$

This gives 1) in this case, as $c = 1$ and $c^* d = j$. The general case follows from this, as the matrices $\begin{pmatrix} 0 & -1 \\ 1 & j \end{pmatrix}$ represent the non-trivial cosets of $\Gamma_0(D)\backslash\Gamma_0(1)$. Hence any γ has the form $\gamma = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & j \end{pmatrix}$ with $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ in $\Gamma_0(D)$. Then

$$\begin{aligned} E_A\big|_1 \gamma &= \varepsilon(\delta) E_A\big|_1 \begin{pmatrix} 0 & -1 \\ 1 & j \end{pmatrix} \\ &= \frac{\varepsilon(c)}{i\sqrt{D}} E_A\left(\frac{z+c^* d}{D}\right) \end{aligned}$$

as $c = \delta$ and $c^* d \equiv j \pmod{D}$.

2) Clearly $E|\gamma = \frac{\varepsilon(c)}{i\sqrt{D}} E\left(\frac{z+c^*d}{D}\right)$ as $E = \sum_A E_A$. Now use the matrix identity

$$\begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & bN \\ c/N & d \end{pmatrix}\begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}$$

to obtain:

$$E(Nz)\Big|_1\gamma = E\Big|_1\begin{pmatrix} a & bN \\ c/N & d \end{pmatrix}\ (Nz)$$

$$= \frac{\varepsilon(c/N)}{i\sqrt{D}} E\left(\frac{Nz+Nc^*d}{D}\right)$$

$$= \frac{-\varepsilon(c)}{i\sqrt{D}} E\left(N\left(\frac{z+c^*d}{D}\right)\right).$$

The last identity follows from the fact that $\varepsilon(N) = -1$.

We are now ready to prove part 1) of Proposition 9.1. The $D+1$ cosets of $\Gamma_0(ND)\backslash\Gamma_0(N)$ are represented by $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and matrices $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $\Gamma_0(N)$ with $c \not\equiv 0 \pmod{D}$ and $j = c^*d$ running through the D residue classes (mod D) . We have

$$g|_2\gamma = E_A\Big|_1\gamma\cdot E(Nz)|_1\gamma$$

$$= \frac{\varepsilon(c)}{i\sqrt{D}} E_A\left(\frac{z+j}{D}\right)\cdot\frac{-\varepsilon(c)}{i\sqrt{D}} E\left(N\left(\frac{z+j}{D}\right)\right.$$

$$= \frac{1}{D}\, g\left(\frac{z+j}{D}\right)$$

by Lemma 9.2. Summing over the $D+1$ cosets gives 1).

The analog of part 2) of Proposition 9.1 in the general case when D is composite requires some genus theory. Let q be a prime with $q \equiv -N \pmod{D}$. Then $q = \mathfrak{q} \cdot \bar{\mathfrak{q}}$ is split in $\mathcal{O}$. Let $\mathfrak{a}$ be an ideal in the class of A ; we say an ideal $\mathfrak{b}$ is in the genus $\{-NA\}$ if $\mathfrak{b}\mathfrak{a}\mathfrak{q}$ has square class in $\mathrm{Pic}(\mathcal{O})$. We let $R_{\{-NA\}}(n)$ be the number of integral ideals in the genus $\{-NA\}$ of norm n ; this is equal to $R(n)$ or zero, as two ideals with the same norm lie in the same genus. Let $\delta(n)$ be equal to 2^k, where k is the number of primes which divide both n and D.

<u>Proposition 9.3</u>. <u>The Fourier coefficients of</u> $G_A = \sum_{m\geq 0} a_m q^m$ <u>are given by the formula</u>

$$a_m = \frac{r_A(m)h}{u} + \sum_{n=1}^{Dm/N} r_A(mD-nN)\ \delta(n) R_{\{-NA\}}(n) \ .$$

For example, we have $a_0 = \frac{1}{2}\frac{h}{u^2}$, so G_A is not a cusp form.

10. The heights of special points.

Let x be a special point of discriminant $-D$ on X. For A and B in $\mathrm{Pic}(\mathcal{O})$ we wish to compute $\langle x_B, t_m x_{AB}\rangle$. To do this, we must determine how many points in the divisor $t_m x_{AB}$ lie on the same component as x_B. The components of X are indexed by the supersingular elliptic curves in characteristic N, and we have

$$(10.1) \qquad \langle x_B, t_m x_{AB}\rangle = \tfrac{1}{2}[\phi \in \mathrm{Hom}(E,E') : \deg \phi = m]$$

where E is the component of x_B and E' the component of x_{AB}. We will denote the group $\mathrm{Hom}(E,E')$ by $\mathrm{Hom}(x_B, x_{AB})$ in this section.

First we will consider the case when D is prime. Let $\mathcal{D} = (\sqrt{-D})$ be the different ideal of $\mathcal{O}$. The quaternion algebra has the form $B = K+Kj$, where $j^2 = -N$, $j\alpha = \bar{\alpha}j$ for all $\alpha \in K$. Let ε be a solution of the congruence $\varepsilon^2 \equiv -N \pmod{D}$. The point $x = x_1$ may be chosen so that

$$(10.2) \qquad \mathrm{End}(x_1) = \{\alpha+\beta j : \alpha \in \mathcal{D}^{-1}, \beta \in \mathcal{D}^{-1}, \quad \alpha \equiv \varepsilon\beta \ (\mathrm{mod}\ \mathcal{O}_{\mathcal{D}})\}.$$

Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals in the classes of A and B which are relatively prime to $\mathcal{D}$.

<u>Proposition 10.3</u>. <u>We have a bijection</u>

$$\mathrm{Hom}(x_{AB}, x_B) \overset{\rightarrow}{\sim} \{\alpha+\beta j : \alpha \in \mathcal{D}^{-1}\mathfrak{a}, \beta \in \mathcal{D}^{-1}\mathfrak{b}^{-1}\bar{\mathfrak{b}}\bar{\mathfrak{a}}, \quad \alpha \equiv \varepsilon\beta \quad (\mathrm{mod}\ \mathcal{O}_{\mathcal{D}})\}.$$

If ϕ *corresponds to* $\alpha+\beta j$ *then* $\deg \phi = (\mathbf{N}\alpha + N\,\mathbf{N}\beta)/\mathbf{N}\mathfrak{a}$.

Proof. The ring $\mathrm{End}(x_B)$ is the right order of the left $\mathrm{End}(x)$ module $\mathrm{End}(x)\cdot\mathfrak{b}$, and $\mathrm{Hom}(x_{AB},x_B)$ can be identified with the left $\mathrm{End}(x_B)$ module $\mathrm{End}(x_B)\cdot\mathfrak{a}$. The proposition now follows from a calculation in $K+Kj = B$.

By (10.1) and Proposition 10.3, we wish to count half the number of solutions to the identity

$$\mathbf{N}\alpha + N\,\mathbf{N}\beta = m\,\mathbf{N}\mathfrak{a}\ ,$$

(10.4)

$$\text{with}\quad \alpha \in \mathcal{D}^{-1}\mathfrak{a}\ ,\beta \in \mathcal{D}^{-1}\mathfrak{b}^{-1}\bar{\mathfrak{b}}\,\bar{\mathfrak{a}}\,,\quad \alpha \equiv \epsilon\beta \pmod{\mathcal{O}_{\mathcal{D}}}.$$

This is most easily done by introducing the integral ideals

$$\mathfrak{c} = (\alpha)\mathcal{D}\mathfrak{a}^{-1}$$

(10.5)

$$\mathfrak{c}' = (\beta)\mathcal{D}\mathfrak{b}\,\bar{\mathfrak{b}}^{-1}\bar{\mathfrak{a}}^{-1}\ ,$$

which satisfy the identity

$$\mathbf{N}\mathfrak{c} + N\,\mathbf{N}\mathfrak{c}' = mD\ . \qquad (10.6)$$

The ideals $\mathfrak{c}$ and $\mathfrak{c}'$ lie in the classes of A^{-1} and AB^2 respectively, and the number of solutions to (10.6) with ideals in these classes is equal to

$$r_{A^{-1}}(mD) + \sum_{n>0} r_{A^{-1}}(mD-nN) r_{AB^2}(n) \ ,$$

where $n = \mathbf{N}\mathfrak{c}'$ and $mD-nN = \mathbf{N}\mathfrak{c}$.

But a solution to (10.6) in ideals gives a solution to (10.4) in elements (α,β) by inverting formula (10.5). There are a priori w^2 possible choices for (α,β) , except when $n = 0$ when there are w choices. These all satisfy the condition $\alpha \equiv \varepsilon\beta \pmod{\mathcal{O}_{\mathcal{D}}}$ in (10.4) when $n \equiv 0 \pmod{D}$, but when $n \not\equiv 0 \pmod{D}$ only half of them satisfy this final condition.
Hence we find

$$\langle x_B, t_m x_{AB} \rangle = u^2 \sum_{n=0}^{mD/N} r_{A^{-1}}(mD-nN)\ \delta(n)\ r_{AB^2}(n) \ .$$

We sum this result over the classes B and use the fact that $\Sigma r_{AB^2}(n) = R(n)$, as D is prime and there are no elements of order 2 in $\mathrm{Pic}(\mathcal{O})$. Since $r_{A^{-1}}(k) = r_A(k)$, we have the final result

Proposition 10.7. *If* D *is prime, then for all* $m \geq 1$

$$\sum_B \langle x_B, t_m x_{AB} \rangle = u^2 \sum_{n=0}^{mD/N} r_A(mD-nN)\ \delta(n) R(n) \ .$$

In the case when D is composite, we let q be a rational prime with $q \equiv -N \pmod{D}$. Then $q = \mathfrak{q}\cdot\bar{\mathfrak{q}}$ is split in K and $B = K+Kj$ with $j^2 = -Nq$. We then find

$$\mathrm{Hom}(x_{AB},x_B) \xrightarrow{\sim} \{\alpha+\beta j \ : \ \alpha \in \mathcal{D}^{-1}\mathfrak{a} \ , \ \beta \in \mathcal{D}^{-1}\mathfrak{q}^{-1}\mathfrak{b}^{-1}\bar{\mathfrak{b}}\bar{\mathfrak{a}}, \ \ \alpha \equiv q\beta \pmod{\mathcal{O}_{\mathcal{D}}}.$$

and

$$<x_B, t_m x_{AB}> = u^2 \sum_{n=0}^{mD/N} r_{A^{-1}}(mD-nN)\ \delta(n) r_{A\mathfrak{q}B^2}(n) .$$

The sum over all classes B now only gives the ideals in the genus $\{A\mathfrak{q}\} = \{-NA\}$, so we find

<u>Proposition 10.8</u>. <u>For all</u> $m \geq 1$, <u>we have</u>

$$\sum_B <x_B, t_m x_{AB}> = u^2 \sum_{n\ 0}^{mD/N} r_A(mD-nN)\ \delta(n)\ R_{\{-NA\}}(n) .$$

$$= ur_A(m)h + \sum_{n=1}^{mD/N} r_A(mD-nN)\ \delta(n)\ R_{\{-NA\}}(n) .$$

If we compare Proposition 10.8 with proposition 9.3, we see that we have established the identity

$$\sum_B <x_B, t_m x_{AB}> = u^2 a_m \quad \text{for} \quad m \geq 1 .$$

Since the constant coefficient of $\sum_B \phi(x_B, x_{AB})$ is equal to $h/2 = u^2 a_0$, we have established the important:

<u>Corollary 10.9</u>. $u^2 G_A = \sum_B \phi(x_B, x_{AB})$ in M.

On the other hand, we have

$$L(f,A,1) = \frac{(f,G_A)}{\sqrt{D}}$$

by Proposition 8.9. Hence we have completed the proof of the main identity in Proposition 7.7. The rest of this paper will be devoted to a discussion of its corollaries.

11. Special values of L-series.

We now consider L-series with Euler products. Let χ be a complex character of the group $\mathrm{Pic}(\mathcal{O})$, and assume that f is a normalized eigenform for the Hecke algebra $\mathbb{T}$. Define

$$L(f,\chi,s) = \sum_A \chi(A)\, L(f,A,s)\ . \tag{11.1}$$

This has an Euler product, where the general local term is of degree 4. If we write

$$L(f,s) = \prod_p (1-\alpha_p p^{-s})(1-\alpha_p' p^{-s})^{-1}$$

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

then we have

$$L(f,\chi,s) = \prod_p (1-\alpha_p\beta_p p^{-s})(1-\alpha_p\beta_p' p^{-s})(1-\alpha_p'\beta_p p^{-s})(1-\alpha_p'\beta_p' p^{-s})^{-1}.$$

The product $\alpha_p\alpha_p'\beta_p\beta_p'$ is equal to $p\varepsilon(p)$ if p does not divide ND; otherwise this product is equal to zero.

To describe the value of $L(f,\chi,s)$ at $s = 1$, we let $c_{f,\chi}$ be the projection of the divisor $c_\chi = \sum_A \chi^{-1}(A) x_A$ to the f-isotypical component of $\mathrm{Pic}(X)\otimes\mathbb{C}$. Note that $\deg c_{f,\chi} = 0$, as f is a cusp form.

Proposition 11.2. $L(f,\chi,1) = \dfrac{(f,f)}{u^2\sqrt{D}} \langle c_{f,\chi}, c_{f,\chi}\rangle$.

Proof. We will adopt the convention that we extend $\mathbb{R}$-bilinear pairings, like $<,>$ and $\phi(\, , \,)$ to complex pairings which are linear in the first argument and anti-linear in the second. Thus

$$<c_\chi, c_\chi> = <\sum_A \chi^{-1}(A)x_A, \sum_B \chi^{-1}(B)x_B>$$

$$= \sum_{A,B} \chi(A^{-1}B)<x_A, x_B> .$$

Combining the definition (11.1) with the main identity in Proposition 7.7, we find

$$L(f,\chi,1) = \frac{(f, \sum_A \chi(A)g_A)}{u^2\sqrt{D}} ,$$

so we are reduced to showing that the coefficient of f in the eigenvector expansion of $\Sigma\chi(A)g_A$ is equal to the (real) number $<c_{f,\chi}, c_{f,\chi}>$. But by definition

$$\Sigma\chi(A)g_A = \sum_A \chi(A) \sum_B \phi\,(x_B, x_{AB})$$

$$= \sum_{A,B} \chi(A)\;\phi(x_B, x_{AB})$$

$$= \sum_{A',B'} \chi(A'^{-1}B')\;\phi(x_{A'}, {}_{B'}) \qquad \begin{array}{l} A' = B \\ B' = AB \end{array}$$

$$= \phi(c_\chi, c_\chi) \quad .$$

Since ϕ is $\mathbb{T}$-bilinear, the f-eigencomponent of the modular form $\phi(c_\chi, c_\chi)$ is equal to

$$\begin{aligned}\phi(c_{\chi,f}, c_\chi) = \phi(c_{\chi,f}, c_{\chi,f}) &= \sum_{m\geq 1} \langle c_{\chi,f}, t_m c_{\chi,f}\rangle q^m \\ &= \sum_{m\geq 1} \langle c_{\chi,f}, c_{\chi,f}\rangle \cdot a_m(f) q^m \\ &= \langle c_{\chi,f}, c_{\chi,f}\rangle \cdot f .\end{aligned}$$

This completes the proof.

Corollary 11.3. 1) $L(f,\chi,1) \geq 0$, *with equality if and only if* $c_{f,\chi} = 0$. 2) *For any automorphism* α *of* $\mathbb{C}$

$$(L(f,\chi,1)\sqrt{D}/(f,f))^\alpha = L(f^\alpha,\chi^\alpha,1)\sqrt{D}/(f^\alpha,f^\alpha) .$$

In particular, the ratio lies in the numberfield generated by the values of χ *and the Fourier coefficients of the eigenform* f .

3) $L(f,\chi,1) = 0$ *if and only if* $L(f^\alpha,\chi^\alpha,1) = 0$.

Proof. 1) follows from the fact that $\langle,\rangle$ induces a positive definite Hermitian pairing on $\mathrm{Pic}(X) \otimes \mathbb{C}$ and Proposition 11.2. Since this pairing is rational on $\mathrm{Pic}(X) \otimes \mathbb{Q}$, we have

$$\langle c_{f,\chi}, c_{f,\chi}\rangle^{\alpha} = \langle c_{f^{\alpha},\chi^{\alpha}}, c_{f^{\alpha},\chi^{\alpha}}\rangle$$

which gives 2). Part 3) is an immediate corollary of 2).

In the case where $\chi = 1$ we have a decomposition:

$$(11.4) \qquad L(f,\chi,1) = L(f,1)L(f\otimes\varepsilon,1) \ ,$$

where $f \otimes \varepsilon = \sum_{m\geq 1} a_m \varepsilon(m)q^m$ is the twist of f, which has level ND^2. Also, we have

$$(11.5) \qquad c_{\chi} = \sum_{A} x_A \equiv u \cdot e_D \qquad \text{in } \operatorname{Pic}(X) \ ,$$

where e_D is the class of the rational divisor $c_D = \frac{1}{2u} \sum_{\operatorname{disc}(x)=-D} (x)$ dein (3.8). This follows from the fact that $\operatorname{Pic}(\mathcal{O}) \times \operatorname{Gal}(K/\mathbb{Q})$ acts simply transitively on the special points, and the points x_A and $\bar{x}_A$ lie on the same component of X. Hence Proposition 11.2 becomes

<u>Corollary 11.6</u>. $L(f,1)L(f\otimes\varepsilon_D,1) = \frac{(f,f)}{\sqrt{D}}\langle e_{f,D}, e_{f,D}\rangle$.

We shall reinterpret this identity, using forms of weight 3/2, in section §13. Here we simply note that $e_{f,D}$ lies in the 1-dimensional space $(\operatorname{Pic}(X) \otimes \mathbb{R})^f$ for each value D, so the different values $\langle e_{f,D}, e_{f,D}\rangle$ have square ratios in the field generated by the fourier coefficients of f. This is a result due to Waldspurger.

Finally, we note that Proposition 11.2 can be extended to include the case where $f = F$ is the normalized Eisenstein series of weight 2. We have

$$L(F,s) = \sum_{m\geq 1} \sigma(m)_N m^{-s} = \zeta(s)\zeta(s-1) \cdot (1-N^{1-s}) .$$

and we define

$$(F,F) = \frac{-\pi \log N}{12} (N-1) .$$

This definition of the inner product is obtained by taking the residue of a Rankin L-function at $s = 2$, and was motivated by the considerations in Zagier [13]. Then the formula in Proposition 11.2 continues to hold, although for $\chi \neq 1$ both sides are equal to zero. When $\chi = 1$ we have

$$(11.7) \qquad \langle c_{F,\chi}, c_{F,\chi} \rangle = \frac{12h^2}{N-1} = \langle c_F, c_F \rangle$$

and both sides are equal to $\frac{-\pi \log N}{u^2\sqrt{D}} h^2$.

Formula (11.7) has some implications for cusp forms. Since $\langle c_\chi, c_\chi \rangle = \langle c_{F,\chi}, c_{F,\chi} \rangle + \sum_f \langle c_{f,\chi}, c_{f,\chi} \rangle$ is an integer, if p is a prime which divides the denominator of $\frac{12h^2}{N-1}$ it must also divide the denominator of some

$<c_{f,\chi},c_{f,\chi}>$ for $\chi = 1$. One then shows easily that $f \equiv F \pmod{pM}$, so we have obtained a result of Mazur.

Corollary 11.8. *Assume* p *divides* $\frac{N-1}{12}$ *but does not divide* h . *Then there is a cusp form* f *which is congruent to the Eisenstein series* $F \pmod p$ *and satisfies* $L(f,1)L(f\otimes\varepsilon,1) \neq 0$.

12. Modular forms of weight 3/2.

We begin by defining a subspace $M_{\mathbb{C}}^{*}$ of the space of modular forms of weight 3/2 on $\Gamma_0(4N)$ with trivial character, which is due to Kohnen [4]. (In his paper, Kohnen denotes the cusp forms in this subspace by $S_{3/2}(N)^{-}$.) Recall that a modular form of weight 3/2 and level $4N$ is a function $g(\tau)$ on the upper half-plane which is regular at the cusps and satisfies

$$(12.1)\qquad g(\tau)/\theta(\tau)^3 \quad \text{is invariant under} \quad \Gamma_0(4N) .$$

where $\theta(\tau) = \sum q^{n^2}$ is the standard theta-series of weight 1/2. Then g has a Fourier explansion

$$(12.2)\qquad g(\tau) = \sum_{D\geq 0} a_D q^D ,$$

and Kohnen's subspace $M_{\mathbb{C}}^{*}$ consists of those forms with

$$(12.3)\qquad a_D = 0 \quad \text{unless } -D \equiv 0,1 \pmod 4 \quad \text{and} \quad \left(\frac{-D}{N}\right) \neq 1 .$$

The space $M_{\mathbb{C}}^{*}$ has dimension t and is stable under Shimura's Hecke operators $T_{m^2}^{*}$ of degree m^2 for all m prime to $4N$. Kohnen defined operators $T_{m^2}^{*}$ on $M_{\mathbb{C}}^{*}$ for all m, and used the trace formula to prove that [4, pg. 47].

(12.4) $$\mathrm{Trace}\ T^*_{m^2} = \mathrm{Trace}\ T_m | M^+_{\mathbb{C}}$$

where T_m is the Hecke operator on forms of weight 2 for $\Gamma_0(N)$ and $M^+_{\mathbb{C}}$ is the subspace of $M_{\mathbb{C}}$ where $T_N = 1$ (or $W_N = -1$). The action of the operators with prime-squared index on Fourier coefficients is given by

(12.5) $$\begin{cases} \Sigma a_D q^D | T^*_{p^2} = \Sigma\{a_{Dp^2} + (\frac{-D}{N}) a_D + p\ a_{D/p^2}\} q^D \ , \ p \neq N \\ \Sigma a_D q^D | T^*_{N^2} = \Sigma a_{DN^2} q^D \ . \end{cases}$$

On the subspace $M^*_{\mathbb{C}}$ the operator $T^*_{N^2}$ acts as the identity, so $a_D = a_{DN^2}$. There is a lattice M^* of rank t in $M^*_{\mathbb{C}}$ which is stable under the Hecke algebra $\mathbb{T}^*$; this consists of the forms g whose Fourier coefficients satisfy (12.3) as well as the integrality conditions

(12.6) $$\begin{aligned} &a_D \text{ is integral for all } D > 0 \\ &a_0 \in \tfrac{1}{2}\mathbb{Z} \ . \end{aligned}$$

We now use our maximal orders to construct elements in the lattice M^*. For each i with $1 \leq i \leq n$ we let S_i be the suborder of index 8 in R_i which is defined by

$$(12.7) \qquad S_i = \mathbb{Z} + 2R_i \quad .$$

Let S_i^o be the subgroup of elements of trace zero in S_i ; this has rank 3 over $\mathbb{Z}$. Let g_i be the theta-series of the lattice S_i^o with its norm form (which is positive definite):

$$(12.8) \qquad g_i(\tau) = \frac{1}{2} \sum_{b \in S_i^o} q^{\mathbf{N}b} = \frac{1}{2} + \sum_{D>0} a_i(D) q^D \quad .$$

Then $a_i(D)$ is one half the number of elements $b \in R_i$ with

$$\begin{cases} b \equiv 0,1 \mod 2R_i \\ \mathrm{Tr} b = 0 \\ \mathbf{N}b = D = -b^2 \end{cases} \quad .$$

This is an integer (as $b \neq -b$), which is zero unless $-D \equiv 0,1 \pmod 4$ and $(\frac{-D}{N}) \neq 1$. Since $g_i(\tau)$ is well-known to have weight 3/2 and level $4N$, the forms g_i all lie in Kohnen's subgroup M^* . Since the orders associated to the curves E_i and E_i^N are conjugate in B and give the same theta-series, only t of the modular forms $g_1, g_2, \cdots, g_n$ are distinct.

Proposition 12.9. *For* $1 \le i \le n$ *and* $D > 0$ *we have*

$$a_i(D) = \frac{w_i}{2} \sum_{-D=df^2} \frac{h_i(d)}{u(d)}$$

where $h_i(d)$ *is the number of optimal embeddings of the order of discriminant* d *into* R_i , *modulo conjugation by* R_i^* .

Proof. Let $\mathcal{O}$ be the order of discriminant $-D$. Any embedding $f : \mathcal{O} \to R_i$ gives rise to an element $b = f(\sqrt{-D})$ in R_i with $\mathrm{Tr}b = 0$ and $\mathrm{N}b = D$. Since $\mathcal{O} = \mathbb{Z} + \mathbb{Z}(\frac{D + \sqrt{-D}}{2})$ we have the congruence $b \equiv -D \pmod{2R_i}$, so b lies in S_i^0 and contributes to $c_i(D)$.

Conversely, if $b \in S_i^0$ then $b^2 = -D$, so $b \equiv -D \pmod{2R_i}$. Hence $\frac{b + D}{2}$ lies in R_i and we obtain an embedding $f : \mathcal{O} \to R_i$ by taking $\frac{\sqrt{-D} + D}{2}$ to $\frac{b + D}{2}$. This bijection completes the proof when $w_i = 1$. When $w_i > 1$ we take Γ_i orbits and analyse the stabilizers, as in the proof of Proposition 1.9.

Proposition 12.10. *For all* $m \geq 1$ *we have*

$$g_i | T^*_{m^2} = \sum_k B_{ik}(m) g_k = w_i \sum_k B_{ki}(m)(g_k/w_k) \quad .$$

In particular, the subgroups spanned by $\langle g_1, \dots, g_n \rangle$ *and* $\langle g_1/w_1, \dots, g_n/w_n \rangle$ *are stable under the Hecke algebra* $\mathbb{T}^*$, *and* $T^*_{m^2}$ *acts on the spanning sets by* $B(m)^{tr}$ *and* $B(m)$ *respectively*.

Proof. It suffices to check this when m is prime, as these operators generate $\mathbb{T}^*$ over $\mathbb{Z}$ and satisfy the same relations as the Brandt matrices in Proposition 2.7. Also, the second identity follows from the first, as $w_k B_{ik}(m) = w_i B_{ki}(m)$.

When $m = N$ we have $g_i | T^*_{N^2} = \frac{1}{2} + \sum_i a_i(DN^2) q^D$ by (12.5). But $a_i(DN^2) = a_i(D)$ using (12.9), as $h_i(DN^2) = 0$. Therefore $g_i | T^*_{N^2} = g_i$. On the other-hand, $\sum_k B_{ik}(m) g_k = g_j$ where $E_j \simeq E_i^N$ is the conjugate elliptic curve. Then $R_j \simeq R_i$ and $g_j = g_i$. This proves the identity in this case, as both sides are equal to g_i .

Now assume that $m = p$ is a prime not equal to N . According to (12.5), we must verify the identity:

$$c_i(Dp^2) + \left(\frac{-D}{p}\right) c_i(D) + p\ c_i(D/p^2) = \sum_k B_{ik}(p) c_k(D) \ .$$

First assume that $D \not\equiv 0 \pmod p$, so the third term on the left hand side is zero. Let a be an element of trace 0 and norm D in the order S_k and let $\phi : E_i \to E_k$ be an isogeny of degree p . Then the element $b = \phi^\vee \circ a \circ \phi$ lies in S_i , has trace zero and norm Dp^2 , and depends only on the kernel of ϕ .

In fact, all elements b of this trace and norm which are not divisible by p in S_i are obtained uiquely as $\phi^\vee \circ a \circ \phi$. Indeed, let $\phi : E_i \to E_k$

be the unique isogeny of degree p with $\ker\phi \subset \ker b$. Then the isogeny b factors through $E_k : E_i \xrightarrow[\phi]{} E_k \xrightarrow[\psi]{} E_i$. Since $b + b^\vee = 0$, $\ker\phi$ is the unique subgroup of order p in $\ker b^\vee$. Hence $\ker\phi \subset \ker\psi^\vee$ and the dual diagram factors

$$\begin{tikzcd}
E_i & E_i \arrow[l, "b^\vee"'] \arrow[d, "\phi"] \\
E_k \arrow[u, "\psi^\vee"] & E_k \arrow[l, "a^\vee"]
\end{tikzcd}$$

to define $a^\vee$ (and hence $a \in S_k$).

The element b is divisible by p in S_i if a stabilizes the subgroup $\phi(E_i[p]) = \ker\phi^\vee$. There are $(1 + (\frac{-D}{p}))$ subgroups of this type, and each gives a way to write $b = \phi^\vee \circ a \circ \phi$. Hence

$$\sum_k B_{ik}(p)c_k(D) = \{c_i(Dp^2)-c_i(D)\} + (1 + (\tfrac{-D}{p}))c_i(D)$$

$$= c_i(Dp^2) + (\tfrac{-D}{p})c_i(D) \ .$$

We leave the case when p divides D to the reader.

As a corollary of Proposition 12.9 and Eichler's formula (1.12) the element G has Fourier expansion

$$(12.11)\qquad \begin{aligned} G &= \sum_{i=1}^{n} \frac{1}{w_i} g_i \\ &= \frac{N-1}{24} + \sum_{D>0} H_N(D) q^D \quad . \end{aligned}$$

As a corollary of Proposition 12.10, G is an eigenvector for the algebra $\mathbb{T}^*$ acting on $M^* \otimes Q$ with eigenvalues $\sigma(m)_N$:

$$(12.12)\qquad G|T^*_{m^2} = \sigma(m)_N \cdot G \qquad \text{for all } m \geq 1 .$$

This is the normalized Eisenstein series of weight 3/2 and level $4N$; the multiple WG lies in the lattice M^*. Also, Eichler's trace formula in Proposition 1.9 is simply the identity

$$(12.13)\qquad G\cdot\theta|T_4 = \sum_{i=1}^{n} f_{ii}$$

among forms of weight 2 on $\Gamma_0(4N)$. We note that T_4 takes the product $G\cdot\theta$ to a form of level N , which generates $M \otimes Q$ over $\mathbb{T} \otimes Q$.

We conclude with a famous example, when $N = 2$. From (6.1) we find

$$S_1 = \mathbb{Z} + 2\mathbb{Z}i + 2\mathbb{Z}j + 2\mathbb{Z}k + \mathbb{Z}(1+i+j+k) .$$

Hence

$$S_1^o = \{b = xi+yj+zk : x,y,z \in \mathbb{Z} , x \equiv y \equiv z \pmod 2\}$$

$$g_1 = \frac{1}{2} \sum_{x \equiv y \equiv z (2)} q^{x^2+y^2+z^2}$$

$$= \frac{1}{2} + 4q^3 + 3q^4 + 6q^8 + 12q^{11} + \dots \quad .$$

Since $g_1 = 12G = \frac{1}{2} + \sum_{D>0} 12H_2(D)q^D$, this gives the classical results on the number of representations of integers $D \equiv 3,4 \pmod 4$ as the sum of 3 squares.

13. Waldspurger's formula

Recall the classes e_D defined in $\mathrm{Pic}(X)^\vee$ by (3.8) and (4.7), and the class $e_0 = \sum_{i=1}^{n} e_i^\vee$. Define the formal series

$$(13.1) \qquad g = \frac{1}{2} e_0 + \sum_{D>1} e_D q^D .$$

Then g may be viewed as a modular form of weight 3/2 with coefficients in $\mathrm{Pic}(X)^\vee$, or more precisely as an element of $\mathrm{Pic}(X)^\vee \otimes M^*$. Indeed, Proposition 12.9 gives the identity

$$(13.2) \qquad g = \sum_{i=1}^{n} e_i^\vee \otimes g_i ,$$

where g_i are the theta-series defined in (12.8) and $e_i^\vee = e_i/w_i$ is the basis of $\mathrm{Pic}(X)^\vee$.

Actually, a little more is true. We have the following.

Proposition 13.3. *g is an element of* $\mathrm{Pic}(X)^\vee \otimes_{\mathbb{T}} M^* = \mathrm{Hom}_{\mathbb{T}}(\mathrm{Pic}(X), M^*)$. *More precisely, for any class* $e \in \mathrm{Pic}(X)$ *the series*

$$g(e) = \frac{\deg e}{2} + \sum_{D>1} \langle e, e_D \rangle q^D$$

is an element of M^* , *and* $g(t_m e) = g(e)|T^*_{m^2}$ *for all* $m \geq 1$.

Proof. It suffices to check this when $e = e_i$. But $g(e_i) = g_i$ and $g(t_m e_i) = \sum_{j=1}^{n} B_{ij}(m)\ g_i$ by Proposition 4.4. This agrees with $g_i|T^*_m$ by Proposition 12.10.

Now let e_f be a non-zero element in the f-isotypical component of $\mathrm{Pic}(X) \otimes \mathbb{R}$, where f is an eigenform for $\mathbb{T}$. This component has dimension 1 , so e_f is determined up to a real scalar multiple. The modular form

$$g(e_f) = \sum m_D q^D \tag{13.4}$$

then lies in the f-isotypical component of $M^* \otimes \mathbb{R}$. It is clearly zero unless $f|T_N = f$, so the sign in the functional equation for $L(f,s)$ is $+1$.

Proposition 13.5. *Let* $-D$ *be a fundamental discriminant with* $(\frac{-D}{N}) = -1$. *Then*

$$L(f,1)L(f\otimes\varepsilon_D,1) = \frac{(f,f)}{\sqrt{D}}\ \frac{m_D^2}{\langle e_f,e_f\rangle} \quad .$$

Proof. We will use Corollary 11.6 and show that

$$\langle e_{f,D},e_{f,D}\rangle = \frac{m_D^2}{\langle e_f,e_f\rangle}$$

By definition: $m_D = \langle e_f, e_D\rangle = \langle e_f, e_{f,D}\rangle$. Hence

$$e_{f,D} = \frac{m_D^2}{\langle e_f, e_f\rangle} e_f \qquad \text{in} \quad (\mathrm{Pic}(X) \otimes \mathbb{R})^f \ .$$

The formula in Proposition 13.5 is due to Waldspurger [11], and gives the variation of the special values with the discriminant $-D$. If $-D$ is fundamental and $D \equiv 0(N)$ the correct formula is:

$$L(f,1)L(f\otimes\varepsilon_D,1) = \frac{(f,f)}{\sqrt{D}} \frac{2 \cdot m_D^2}{\langle e_f, e_f\rangle} \ .$$

We will not prove this here; it follows from methods similar to those in §8-10.

<u>Corollary 13.6</u>. <u>The rank of the subgroup spanned by the</u> t <u>distinct theta series</u> g_i <u>in</u> M^* <u>is equal to the number of eigenforms</u> f <u>(including the weight 2 Eisenstein series) with</u> $L(f,1) \neq 0$.

<u>Proof</u>. Since the subgroup spanned is stable under $\mathbb{T}^*$, it suffices to determine which eigenforms f satisfy $g(e_f) \neq 0$. By Proposition 13.5 this will be true if $L(f,1)L(f\otimes\varepsilon_D,1) \neq 0$ for a fundamental discriminant $-D$ with $(\frac{-D}{N}) = -1$. But Waldspurger has shown [12] that it is always possible to choose D so that $(\frac{-D}{N}) = -1$ and $L(f\otimes\varepsilon_D,1) \neq 0$, the condition reduces to $L(f,1) \neq 0$.

One case where the rank is less than t is when $N = 389$. Here $t = 22$ and the rank is 21; there is an eigenform with rational Fourier coefficients with $\mathrm{ord}_{s=1} L(f,s) = 2$. It would be interesting to determine the linear relation on the theta-series explicitly in this case.

We end this section by explicitly computing an example, in level $N = 11$. The unique normalized cusp form f was given in (6.4) and corresponds to the elliptic curve $X_0(11)$. We have $e_f = e_2 - e_1$ and $\langle e_f, e_f \rangle = 5$. If $K = \mathbf{Q}(\sqrt{-D})$, and 11 is inert in K, we obtain

$$L(X_0(11)/K) = \frac{(f,f)}{5\sqrt{D}}\, m_D^2 \tag{13.7}$$

where m_D is the D^{th} coefficient of $g(e_f) = g_2 - g_1$. If 11 is ramified in K, the above formula holds with m_D^2 replaced by $2m_D^2$.

We recall that the maximal orders in B are distinguished by $w_1 = 2$ and $w_2 = 3$; we find after an explicit description of R_1 and R_2 that

$$g_1 = \frac{1}{2} \sum_{x \equiv y \,(\mathrm{mod}\, 2)} q^{x^2+11y^2+11z^2} = \frac{1}{2} + q^4 + q^{11} + 2q^{12} + 2q^{15} + q^{16} + \ldots$$

$$g_2 = \frac{1}{2} \sum_{\substack{x \equiv y \,(\mathrm{mod}\, 3) \\ y \equiv z \,(\mathrm{mod}\, 2)}} q^{(x^2+11y^2+33z^2)/3} = \frac{1}{2} + q^3 + q^{12} + 3q^{15} + 3q^{16} + \ldots$$

Here is a table of the first few coefficients of the eigenform $g(e_f)$:

D	m_D
3	1
4	-1
11	-1
12	-1
15	1
16	2
20	1
23	-1
27	-1
31	-1
36	0
44	1
47	0
48	0
55	1
56	2
59	-1
60	-3
64	-2
67	3
71	1

Since $2g(e_f) \equiv 6G \pmod{5M^*}$, where G is the normalized Eisenstein series defined in (12.11), we obtain the congruences

$$m_D \equiv 3H_{11}(D) \pmod{5} \tag{13.8}$$

for all $D > 0$. Using (13.7) this gives congruences for the special values, which are due to Mazur [6].

In the next section, we shall see that if $-D$ is the discriminant of an imaginary quadratic field K and $m_D \neq 0$, then the conjecture of Birch and Swinnerton-Dyer predicts that

$$m_D^2 = [\text{Ш}(X_0(11)/K)] . \tag{13.9}$$

In particular, the integer m_D should always annihilate $\text{Ш}(X_0(11)/K))$.

14. Elliptic curves with prime conductor

We now consider the special case where the normalized eigenform f has integral Fourier coefficients. Then f corresponds to an isogeny class of elliptic curves $\{E\}$ over $\mathbb{Q}$ with conductor N which appear as quotients of the modular curve $X_0(N)$. The L-series of E over $\mathbb{Q}$ is equal to $L(f,s)$.

In the isogeny class $\{E\}$ there is a distinguished curve E_0, called the strong Weil curve, where the covering

$$(14.1) \qquad \pi : X_0(N) \to E$$

has minimal degree. In this case, the induced map on homology $\pi_* : H_1(X_0(N)(\mathbb{C}),\mathbb{Z}) \to H_1(E_0(\mathbb{C}),\mathbb{Z})$ is surjective, so the induced map of Jacobians has a connected kernel (which is an abelian variety).

$$(14.2) \qquad 0 \to A \to J_0(N) \to E_0 \to 0 .$$

For any curve in the isogeny class, we let ω be a Néron differential on E, $\Delta = \Delta(\omega)$ the minimal discriminant, and t be the order of the finite group $E(\mathbb{Q})_{tor}$. We assume that the parametrization given by (14.1) has minimal degree for E, and adjust its sign so that $\pi^*(\omega) = c \cdot f(q)\frac{dq}{q}$ with $c > 0$. We will assume Manin's conjecture that $c_0 = 1$ for the strong Weil curve E_0 in each isogeny class. (Raynaud has recently proved that $c_0 = 1$ or 2).

The strong Weil curve E_0 is the unique curve in its $\mathbb{Q}$-isogeny class and $t_0 = 1$, except in the following cases [7].

N	curves(see [1,pg.82-84])	c	t	Δ	deg π
11	$E_0 = J_0(11)$	1	5	-11^5	1
	E_0/μ_5	5	5	-11	5
	$E_0/(\mathbb{Z}/5)$	1	1	-11	5
17	$E_0 = J_0(17)$	1	4	-17^4	1
	E_0/μ_2	2	4	17^2	2
	E_0/μ_4	4	4	17	4
	$E_0/(\mathbb{Z}/4)$	2	2	17	4
19	$E_0 = J_0(19)$	1	3	-19^3	1
	E_0/μ_3	3	3	-19	3
	$E_0/(\mathbb{Z}/3)$	1	1	-19	3
37	$E_0 = J_0(37)^{W=-1}$	1	3	37^3	2
	E_0/μ_3	3	3	37	6
	$E_0/(\mathbb{Z}/3)$	1	1	37	6
$64+u^2$	$E_0:y^2 = x^3-2ux^2+Nx$	1	2	$-N^2$	?
(if π exists)	$E_0/\mu_2:y^2 = x^3+ux^2-16x$	2	2	N	2?

In particular, we have $c \le t \le 5$.

When E_0 is the unique curve in its Q-isogeny class, it is reasonable to conjecture that $\Delta = \pm N$; some evidence for this conjecture is given in [5,§9]. When combined with the information in the previous table, this leads to the slightly more general conjecture that

$$(14.3) \qquad t \overset{?}{=} c \cdot \mathrm{ord}_N(\Delta) \ .$$

Now let e_f be an element in the f-isotypical component of Pic(X) which is not divisible by any integer $n > 1$; then e_f is well-determined up to sign and Proposition 13.5 gives the identity

$$(14.4) \qquad L(f,1)L(f\otimes\varepsilon_D,1) = \frac{(f,f)}{\sqrt{D}} \frac{m_D^2}{\langle e_f,e_f\rangle} \ ,$$

where m_D is the D^{th} coefficient of the form $g(e_f)$ in M^* . The left hand side of this identity is equal to the L-function of E over the field K = $Q(\sqrt{-D})$ where N is inert. If $L(E/K,1) \neq 0$, then the conjecture of Birch and Swinnerton-Dyer predicts that the rank of E(K) is equal to zero and that

$$(14.5) \qquad L(E/K,1) \overset{?}{=} \frac{\int_{E(\mathbb{C})} \omega\wedge\bar{\omega}}{\sqrt{D}} \ \frac{\mathrm{ord}_N(\Delta)}{t^2} \ [Ш_D] \ ,$$

where $Ш_D$ is the (conjecturally finite) Tate-Shafarevitch group of E over K .

Since $c^2(f,f) = \deg \pi \cdot \int_{E(\mathbb{C})} \omega\wedge\bar{\omega}$, and Mestre and Oesterlé have recently shown that the identity

$$(14.6) \qquad \langle e_f, e_f \rangle \overset{?}{=} \deg \pi \cdot \mathrm{ord}_N(\Delta)$$

follows from conjecture (14.3), we are led to the following.

Conjecture 14.7. *If* $m_D \neq 0$ *then* $E(K)$ *is finite of order* t *and* Ш$_D$ *is finite of order* m_D^2.

15. Bibliography

1. Birch, B. J. and Kuyk, W., Modular functions of One Variable IV. Springer Lecture Notes 476 (1975).

2. Eichler, M., Zur Zahlentheorie der Quaternion-Algebren. Crelle J. 195 (1955), 127-151.

3. Gross, B. and Zagier, D., Heegner points and derivatives of L-series. Inv. Math. (1986).

4. Kohnen, W., Newforms of half-integral weight. Crelle J. 333 (1982), 32-72.

5. Kramer, K. and Brumer, A., The rank of elliptic curves. Duke Math J. 44 (1977), 715-743.

6. Mazur, B., On the arithmetic of special values of L-functions. Inv. math. 55 (1979), 207-240.

7. Miyakawa, I., Elliptic curves of prime conductor with Q-rational points of finite order. Osaka J. math. 10 (1973), 309-323.

8. Ohta, M., Theta series mod p . J. Fac. Sci. Tokyo 28 (1981), 679-686.

9. Pizer, A., An algorithm for computing modular forms on $\Gamma_0(N)$. J. Algebra 64 (1980), 340-390.

10. Serre, J-P., Trees, Springer-Verlag (1980).

11. Waldspurger, J-L., Sur les coefficients de Fourier des formes modulaires de poids demi-entier. J. Math. pures et appl. 60 (1981), 375-484.

12. Waldspurger, J-L., Correspondance de Shimura et Quaternions.

13. Zagier, D., The Rankin-Selberg method for automorphic functions which are not of rapid decay. J. Fac. Sci. Tokyo 28 (1982), 415-438.

BENEDICT H. GROSS
DEPARTMENT OF MATHEMATICS
HARVARD UNIVERSITY
CAMBRIDGE, MA 02138, USA.