Heegner points and derivatives of L-series

by

Benedict H. Gross

and

Don B. Zagier

followed by

On canonical and quasi-canonical liftings

by

Benedict H. Gross

Department of Mathematics
Brown University
Providence, RI 02912
U.S.A.

Department of Mathematics
University of Maryland
College Park, MD 20742
U.S.A.

and

Max-Planck-Institut für Mathematik
Gottfried-Claren-Straße 26
D-5300 Bonn 3
F.R.G.

MPI/SFB 85-30

Table of Contents

Chapter I. Introduction and statement of results

The main theorem of this paper gives a relation between the heights of Heegner divisor classes on the Jacobian of the modular curve $X_0(N)$ and the first derivatives at $s = 1$ of the Rankin L-series of certain modular forms. In the first six sections of this chapter, we will develop enough background material on modular curves, Heegner points, heights, and L-functions to be able to state one version of this identity precisely. In §7 we will discuss some applications to the conjecture of Birch and Swinnerton-Dyer for elliptic curves. For example,
we will show that any modular elliptic curve over $\mathbb{Q}$ whose L-function has a simple zero at $s = 1$ contains points of infinite order. Combining our work with that of Goldfeld [12], one obtains an effective lower bound for the class numbers of imaginary quadratic fields as a function of their discriminants (§8). In §9 we will describe the plan of proof and the contents of the remaining chapters.

Many of the results of this paper were announced in our Comptes Rendus note [17]. A more leisurely introduction to Heegner points and Rankin L-series may be found in our earlier paper [13].

§1. The Curve $X_0(N)$ over $\mathbb{Q}$

Let $N \geq 1$ be an integer. The curve $X = X_0(N)$ may be informally described over $\mathbb{Q}$ as the compactification of the space of moduli of elliptic curves with a cyclic subgroup of order N. It is known to be a complete, non-singular, geo-

metrically connected curve over $\mathbb{Q}$. Over a field k of characteristic zero, the points x of X correspond to diagrams:

$$(1.1) \qquad \phi : E \to E'$$

where E and E' are (generalized) elliptic curves over k and ϕ is an isogeny over k whose kernel A is isomorphic to $\mathbb{Z}/N$ over an algebraic closure $\bar{k}$. The function field of X over $\mathbb{Q}$ is generated by the modular invariants $j(x) = j(E)$ and $j'(x) = j(E')$; these satisfy the classical modular equation of level N : $\phi_N(j,j') = 0$ [2].

The cusps of X are the points where $j(x) = j'(x) = \infty$. They correspond to diagrams (1.1) between certain degenerate elliptic curves, where $A = \ker\phi$ meets each geometric component of E [7, 173ff]. There is a unique cusp where E has 1 component and a unique cusp where E has N components; these are denoted ∞ and 0 respectively and are rational over $\mathbb{Q}$.

§2. Automorphisms and correspondences

The canonical involution w_N of X takes the point $x = (\phi : E \to E')$ to the point

$$(2.1) \qquad w_N(x) = (\phi' : E' \to E)$$

where ϕ' is the dual isogeny. This involution interchanges the cusps ∞ and 0.

The other modular involutions w_d of X correspond to positive divisors d of N with $(d,N/d) = 1$. Let D and D' denote the unique subgroups of $\ker\phi$ and $\ker\phi'$ of order d, and define $w_d(x)$ by the composite isogeny

$$(2.2) \qquad w_d(x) : (E/D \to E/\ker\phi \simeq E' \to E'/D').$$

These involutions form a group $W \subseteq \mathrm{Aut}_{\mathbb{Q}}(X)$ isomorphic to $(\mathbb{Z}/2)^t$, where t is the number of distinct prime factors of N. The group law is given by $w_d w_{d'} = w_{d''}$, where $d'' = dd'/\gcd(d,d')^2$.

For an integer $m \geq 1$ the Hecke correspondence T_m is defined on X by

$$(2.3) \qquad T_m(x) = \sum_C (x_C),$$

where the sum is taken over all subgroups C of order m in E which are disjoint from $\ker\phi$, and x_C is the point of X corresponding to the induced isogeny $(E/C \to E'/\phi(C))$. This endomorphism of the group of divisors on X is induced by an algebraic correspondence on $X \times X$ which is rational over $\mathbb{Q}$. When $(m,N) = 1$ the correspondence T_m is self-dual, of bidegree $\sigma_1(m) = \sum_{d|m} d$.

Let J be the Jacobian of X: its points $J(k)$ over any field k of characteristic zero correspond to the divisor classes of degree zero on X which are rational over k. The correspondences T_m induce endomorphisms of J over $\mathbb{Q}$; we let $\mathbb{T} \subseteq \mathrm{End}_{\mathbb{Q}}(J)$ be the commutative sub-algebra they generate.

§3. Heegner points

Let K be an imaginary quadratic field whose discriminant D is relatively prime to N. Let $\mathcal{O}$ be the ring of integers in K, let h denote the class number of K-- the order of the finite group $\mathrm{Pic}(\mathcal{O})$, and let u denote the order of the finite group $\mathcal{O}^*/\pm 1$. We have $u = 1$ unless $D = -3,-4$, when $u = 3,2$ respectively.

We say $x : (E \to E')$ is a Heegner point of discriminant D on X if the elliptic curves E and E' both have complex multiplication by $\mathcal{O}$. Such points will exist if and only if D is congruent to a square (mod $4N$). In this case, there are $2^t \cdot h$ Heegner points on X, all rational over the Hilbert class field $H = K(j(E))$ of K. They are permuted simply-transitively by the abelian group $W \times \mathrm{Gal}(H/K)$. We remark that there are also Heegner points with non-fundamental discriminants and with discriminants not relatively prime to N on X [13], but we will not consider them in this paper. Also, we shall assume throughout that D is <u>odd</u>, hence square free and congruent to 1 (mod 4).

Fix a Heegner point x of discriminant D; then the class of the divisor $c = (x) - (\infty)$ defines an element in $J(H)$. A fundamental question, first posed by Birch [3], is to determine the cyclic module spanned by c over the ring $\mathbb{T}[\mathrm{Gal}(H/K)]$, which acts as endomorphisms of $J(H)$. Our approach to this problem uses the theory of canonical heights, as developed by Néron and Tate, as well as the L-series assciated by Rankin to the product of two modular forms. We will show (Theorem 6.3) that the eigencomponent $c_{f,\chi}$ of c is non-zero in $J(H) \otimes \mathbb{C}$ if and only if the first derivative of an associated Rankin L-series

$L(f,\chi,s)$ is non-zero at $s = 1$. (Here f is an eigenform of weight 2 for the Hecke algebra $\mathbb{T}$ and χ a complex character of $\mathrm{Gal}(H/K)$.)

§4. Local and global heights

For each place v of H, let H_v denote the completion and define the valuation homomorphism $|\,|_v : H_v^* \to \mathbb{R}_+^*$ by:

$$|\alpha|_v = \begin{cases} \alpha\bar{\alpha} = |\alpha|^2 & \text{if } H_v \simeq \mathbb{C} \\ q_v^{-v(\alpha)} & \text{if } H_v \text{ is non-archimedean, with prime } \pi \text{ satisfying } v(\pi) = 1 \text{ and finite residue field of order } q_v \end{cases}$$

For any $\alpha \in H^*$, almost all of the local terms $|\alpha|_v$ are equal to 1, and we have the product formula: $\prod_v |\alpha|_v = 1$.

Néron's theory gives a unique local symbol $\langle a,b\rangle_v$ with values in $\mathbb{R}$, defined on relatively prime divisors of degree zero on X over H_v [27]. This symbol is characterized by being bi-additive, symmetric, continuous, and equal to

$$(4.1) \qquad \langle a,b\rangle_v = \log|f(a)|_v = \Sigma m_x \log|f(x)|_v$$

whenever $a = \Sigma m_x(x)$ and $b = \mathrm{div}(f)$. One can obtain formulae for the local

symbol using potential theory when v is archimedean and intersection theory when v is non-archimedean [14].

If a and b are relatively prime and defined over H, the local symbols $\langle a,b\rangle_v$ are zero for almost all places v and the sum

$$(4.2) \qquad \langle a,b\rangle = \sum_v \langle a,b\rangle_v$$

depends only on the images of a and b in $J(H)$, by (4.1) and the product formula. The symbol $\langle\,,\rangle$ defines the global height pairing on $J \times J$ over the global field H and the quadratic form

$$(4.3) \qquad \hat{h}(a) = \langle a,a\rangle$$

is the canonical Tate height associated to the class of the divisor $2(\Theta)$, where Θ is a symmetric theta-divisor in J. Since this divisor is ample, $\hat{h}$ defines a positive definite quadratic form on the real vector space $J(H) \otimes \mathbb{R}$ [24]. This form may be extended to a Hermitian form on $J(H) \otimes \mathbb{C}$ in the usual manner.

§5. L-series

Let $f(\tau) = \sum_{n\geq 1} a_n e^{2\pi i n\tau}$ be an element in the vector space of new forms of weight 2 on $\Gamma_0(N)$ ([1], [34]). Thus f is a cusp form of weight 2 and level N which is orthogonal to any cusp form $g(\tau) = g_0(d\tau)$, where g_0 has level N_0 properly dividing N and d is a positive divisor of N/N_0.

We define the Petersson inner product on forms of weight 2 for $\Gamma_0(N)$ by

$$(5.1) \qquad (f,g) = \int_{\Gamma_0(N)\backslash\mathfrak{H}} f(\tau)\overline{g(\tau)}\,dxdy \qquad \tau = x + iy$$

where the integral is taken over any fundamental domain for the action of $\Gamma_0(N)$ on the upper half plane $\mathfrak{H}$.

Let σ be a fixed element in $\mathrm{Gal}(H/K)$. This group is canonically isomorphic to the class group Cl_K of K by the Artin map of global class field theory. Let A be the class corresponding to σ, and define the theta-series

$$(5.2) \qquad \theta_A(\tau) = \frac{1}{2u} + \sum_{\substack{\mathfrak{a}\in A \\ \mathfrak{a}\text{ integral}}} e^{2\pi i N\mathfrak{a}\tau} = \sum_{n\geq 0} r_A(n)e^{2\pi i n\tau}$$

where, for $n \geq 1$, $r_A(n)$ is the number of integral ideals $\mathfrak{a}$ in the class of A with norm n. This series defines a modular form of weight 1 on $\Gamma_1(D)$, with character $\varepsilon : (\mathbb{Z}/D)^* \to \pm 1$ associated to the quadratic extension $K/\mathbb{Q}$ (see, e.g., [19]).

Define the L-function associated to the newform f and the ideal class A by

$$(5.3) \qquad L_A(f,s) = \sum_{\substack{n\geq 1 \\ (n,DN)=1}} \varepsilon(n)n^{1-2s} \cdot \sum_{n\geq 1} a_n r_A(n)n^{-s} .$$

The first sum is the Dirichlet L-function of ε at the argument $2s - 1$, with the Euler factors at all primes dividing N removed. (These factors were not removed in our announcement [17], which is in error. Also, there we denoted this L-series by $L_\sigma(f,s)$, and $\theta_A(\tau)$ by $\theta_\sigma(\tau)$.)

If f is an eigenform under the action of the Hecke algebra $\mathbb{T}$, normalized by the condition that $a_1 = 1$, and χ is a complex character of the ideal class group of K, we define the L-function

$$(5.4) \qquad L(f,\chi,s) = \sum_A \chi(A)L_A(f,s) .$$

This has a formal Euler product, where the terms for $p \nmid ND$ have degree 4. The terms where $p|D$ or $p \| N$ have degree 2, and the terms where $p^2|N$ have degree 0 [13].

It is not difficult to show that the series defining $L_A(f,s)$ and the Euler product for $L(f,\chi,s)$ are absolutely convergent in the right half-plane $R(s) > 3/2$. Using "Rankin's method," we shall show

Proposition 5.5 *The functions $L_A(f,s)$ and $L(f,\chi,s)$ have analytic continuations to the entire plane, satisfy functional equations when s is replaced by $2 - s$, and vanish at the point $s = 1$.*

§6. The main result

We recall the notation we have established: x is a Heegner point of discriminant D, which we have assumed is square free and prime to N, and c is the class of the divisor $(x) - (\infty)$ in $J(H)$. The quadratic field $K = \mathbb{Q}(\sqrt{D})$ has class number h and contains $2u$ roots of unity; the element σ in the Galois group of H/K corresponds to the ideal class A under the Artin isomorphism. Finally, $\langle\, ,\rangle$ denotes the global height pairing on $J(H) \otimes \mathbb{C}$ and $(\ ,\ )$ the Peterson inner product on cusp forms of weight 2 for $\Gamma_0(N)$.

__Theorem 6.1__ __The series__ $g_A(\tau) = \sum_{m\geq 1} \langle c, T_m c^\sigma\rangle e^{2\pi i m\tau}$ __is a cusp form of weight__ 2 __on__ $\Gamma_0(N)$ __which satisfies__

$$(6.2) \qquad (f, g_A) = \frac{u^2|D|^{1/2}}{8\pi^2} L'_A(f,1)$$

__for all__ f __in the space of newforms of weight__ 2 __on__ $\Gamma_0(N)$.

By using the bilinearity of the global height pairing, we can derive a corresponding result for the first derivatives $L'(f,\chi,1)$, when f is a normalized eigenform and χ is a complex character of the class group of K. We identify χ with a character of $\mathrm{Gal}(H/K)$, and define $c_\chi = \sum_\sigma \chi^{-1}(\sigma)c^\sigma$ in the χ-eigenspace of $J(H) \otimes \mathbb{C}$. (This is h times the standard eigencomponent.) Finally, we let $c_{\chi,f}$ be the projection of c_χ to the f-isotypical component of $J(H) \otimes \mathbb{C}$ under the action of $\mathbb{T}$ [13]. Then we have

__Theorem 6.3__ $L'(f,\chi,1) = \dfrac{8\pi^2(f,f)}{hu^2|D|^{1/2}}\, \hat{h}(c_{\chi,f})$.

Here $\hat{h}$ is the canonical height on J over H, as in (4.3). The discrepancies in the constants of (6.2) and (6.3) from those in our announcement [17] come from the fact that there we were considering the global height on J over $\mathbb{Q}$. The heights over H, K and $\mathbb{Q}$ are related by the formula

$$(6.4) \qquad \langle a,b\rangle_H = h\langle a,b\rangle_K = 2h\langle a,b\rangle_{\mathbb{Q}}$$

We remark also that the quantity $8\pi^2(f,f)$ is equal to the period integral $\|\omega_f\|^2 = \iint_{X(\mathbb{C})} \omega_f \wedge \overline{i\omega_f}$, where $\omega_f = 2\pi i f(\tau)d\tau$ is the eigendifferential associated to f. Thus (6.3) may be re-written in the more attractive form

$$(6.5) \qquad L'(f,\chi,1) = \frac{\|\omega_f\|^2}{u^2|D|^{1/2}}\, \hat{h}_K(c_{\chi,f}).$$

We recall that when $|D| > 4$, $u = 1$.

§7. Applications to elliptic curves

Let E be an elliptic curve over $\mathbb{Q}$. The L-function $L(E,s)$ is a Dirichlet series $\sum_{n\geq 1} a_n n^{-s}$ defined by an Euler product which determines the number of points on E (mod p) for all primes p [35]. This product converges in the half plane $R(s) > 3/2$, but it is generally conjectured that the function $f(\tau) = \sum_{n\geq 1} a_n e^{2\pi i n\tau}$ is a newform of weight 2 and level equal to the conductor N of E [38,35]. In this case, the function

$L^*(E,s) = \int_0^\infty f(\frac{iy}{\sqrt{N}})y^s \frac{dy}{y} = N^{s/2}(2\pi)^{-s}\Gamma(s)L(E,s)$ is entire and satisfies a functional equation

$$(7.1) \qquad L^*(E,s) = \pm L^*(E,2-s) .$$

This conjecture may be verified for a given curve by a finite computation, and we will assume it is true for all of the elliptic curves considered below.

The conjecture of Birch and Swinnerton-Dyer predicts that the integer $r = \mathrm{ord}_{s=1}L(E,s)$ is equal to the rank of the finitely generated abelian group $E(Q)$ of rational points. This conjecture also gives an exact formula for the real number $L^{(r)}(E,1)$ of the form:

$$(7.2) \qquad L^{(r)}(E,1) = \alpha.\Omega.R ,$$

where Ω is the real period of a regular differential on E over Q, $R = \det(\langle P_i,P_j\rangle)$ is the regulator of the global height pairing on a basis $\langle P_1, \ldots ,P_r\rangle$ of $E(Q) \otimes Q$, and α is a non-zero rational number (for which there is also a conjectural description in terms of arithmetic invariants of the curve) [35]. We will combine Theorem 6.3 with a theorem of Waldspurger to obtain the following result, which may be viewed as an exotic contribution to the problem of finding rational solutions of cubic equations:

Theorem 7.3 Assume that $L(E,1) = 0$. Then there is a rational point P in $E(Q)$ such that $L'(E,1) = \alpha.\Omega.\langle P,P\rangle$ with $\alpha \in Q^*$. In particular:

1) If $L'(E,1) \neq 0$, then $E(Q)$ contains elements of infinite order.

2) If $L'(E,1) \neq 0$ and rank $E(Q) = 1$, then formula (7.2) is true for *some* non-zero rational number α.

If the sign in the functional equation (7.1) is -1 and the point P constructed in theorem (7.3) is trivial in $E(Q) \otimes Q$, then the order r of $L(E,s)$ at $s = 1$ must be at least 3. One example where this happens is the following (for a proof that P is trivial in this case, see [17] or [39]):

Proposition 7.4 The elliptic curve E defined by the equation $-139y^2 = x^3 + 10x^2 - 20x + 8$ has $\mathrm{ord}_{s=1}L(E,s) = \mathrm{rank}\ E(Q) = 3$.

§8. Application to the class number problem of Gauss

As well as providing some support for the conjecture of Birch and Swinnerton-Dyer, Proposition 7.4 furnishes a crucial hypothesis in Goldfeld's attack on Gauss's class number problem for imaginary quadratic fields [12]. Suppose K has discriminant D and class number $h = h(D)$, then one has the estimate:

Theorem 8.1. For any $\varepsilon > 0$ there is an effectively computable constant $\kappa(\varepsilon) > 0$ such that $h(D) > \kappa(\varepsilon)(\log|D|)^{1-\varepsilon}$.

For the analytic details of Goldfeld's method, see Oesterlé [28]. In fact, Oesterlé gives a sharper final result:

(8.2) $$h(D) > \frac{\kappa \log |D|}{\prod_{p|D}(1+2/\sqrt{p})}$$

for some effectively computable constant κ. In fact, it has recently been shown by Mestre [26], using some work of Serre, that Proposition 7.4 is also true for the elliptic curve defined by $y^2 - y = x^3 - 7x + 6$, a curve of much smaller conductor (5077 rather than 714877), and using this curve, one obtains quite good estimates. For example, Oesterlé and Mestre have shown that $h(D) > \frac{1}{55}\log|D|$ for $|D|$ prime, sufficient (in combination with previous results of Montgomery and Weinberger) to show that the smallest D with $h(D) = 3$ is -907.

§9. The plan of proof

We will now summarize the contents of the remaining chapters, and will indicate how these results fit together to yield a proof of theorem 6.1.

We begin with the question of calculating the global pairings $\langle c, T_m c^\sigma\rangle$ for those m which are prime to N. Set $d = (x) - (0)$; since the cuspidal divisor $(0) - (\infty)$ has finite order in $J(\mathbb{Q})$ we have $\langle c, T_m c^\sigma\rangle = \langle c, T_m d^\sigma\rangle$. On the other hand, it is easy to show that

Proposition 9.1 The divisors c and $T_m d^\sigma$ are relatively prime if and only if $N > 1$ and $r_A(m) = 0$.

In the cases where the hypotheses of (9.1) are met, we may calculate $\langle c, T_m d^\sigma\rangle$ as the sum of Néron's local symbols $\langle c, T_m d^\sigma\rangle_v$. The general case can be treated using (4.2) and a mild extension of Néron's local theory [14]. We will treat the case when $r_A(m) \neq 0$, but will assume for simplicity that $N > 1$ throughout. For a detailed consideration of the case $N = 1$, see [18].

In Chapter II the archimedean local symbols $\langle c, T_m d^\sigma\rangle_v$ are expressed in terms of a Green's function for the Riemann surface $X(\mathbb{C}) = \Gamma_0(N)\backslash\mathfrak{H}^*$ with the

two distinct points ∞ and 0 marked. In Chapter III the non-archimedean local symbols $\langle c, T_m d^\sigma\rangle_v$ are determined using intersection theory on a modular arithmetic surface with general fibre X. In both cases, there is considerable simplification when we consider the sum $\sum_{v|p}\langle c, T_m d^\sigma\rangle_v$ over all places of H dividing a fixed place p of $\mathbb{Q}$.

In Chapter IV we will use Rankin's method and the theory of holomorphic projection to find for each $k \geq 1$ a cusp form $\phi_A(\tau) = \sum_{m\geq 1} a_{m,A} e^{2\pi i m\tau}$ of weight $2k$ on $\Gamma_0(N)$ which satisfies

(9.2) $$(f, \phi_A) = \frac{(2k-2)!}{2^{4k-1}\pi^{2k}} |D|^{1/2} L_A'(f,k)$$

for all f in the space of newforms of weight $2k$ and level N. (The function $L_A(f,s)$ for $k > 1$ is defined as in (5.3) but with n^{1-2s} replaced by $n^{2k-1-2s}$; it satisfies a functional equation for $s \to 2k-s$ and vanishes at $s = k$.) The existence of some cusp form satisfying (9.2) follows from the non-degeneracy of the Petersson inner product on the space of new forms, which also shows that ϕ_A is well determined up to the addition of an old form. We shall give explicit formulas for the Fourier coefficients $a_{m,A}$ for those $m \geq 1$ which are prime to N. The computations are independent of those in Chapters II and III and are carried out in more generality: not only is k arbitrary, but the condition $D \equiv$ square (mod $4N$) is relaxed to $\varepsilon(N) = 1$. These more general results are also interesting as discussed in §§3-4 of Chapter V.

When $k=1$ and $D \equiv$ square (mod $4N$), the formula obtained for $a_{m,A}$ agrees (up to a factor u^2) with the sum of the local height contributions $\langle c, T_m d^\sigma\rangle_v$, so we have the identity

(9.3) $$\langle c, T_m c^\sigma\rangle = u^2 a_{m,A} \qquad (m \geq 1, \quad (m,N) = 1)$$

for the global height pairing. A formal argument (§1 of Chapter V) shows that the series $g_A(\tau) = \sum_{m\geq 1}\langle c, T_m c^\sigma\rangle e^{2\pi i m\tau}$ is a cusp form of weight 2 on $\Gamma_0(N)$, and (9.3) shows that g_A differs from $u^2\phi_A$ by an old form. Theorem 6.1 then follows from equation (9.2). The rest of Chapter V is devoted to the proofs of its various corollaries and generalizations.

§10. Acknowledgments

We would like to thank B. Birch, P. Deligne, W. Fulton, N. Katz, B. Mazur, J-P. Serre and J. Tate for their help and encouragement.

Chapter II. Archimedean local heights

In this chapter we compute the local symbols $\langle c, T_m d^\sigma\rangle_v$ as defined in §4 of the Introduction for archimedean places v of H. We recall the notation: $c=(x)-(\infty)$, $d=(x)-(0)$ where 0 and ∞ are cusps and x a Heegner point of discriminant $D=D_K$ on $X_0(N)$ and $\sigma\in \mathrm{Gal}(H/K)$, $\sigma=\sigma_A$ for some ideal class $A\in \mathrm{Cl}_K$.

§1. The curve $X_0(N)$ over $\mathbb{C}$

In Chapter I we gave the modular description over $\mathbb{Q}$ of the curve $X=X_0(N)$, its automorphisms and correspondences, and of Heegner points. We now describe this all over the complex numbers $\mathbb{C}$; this is of course the most classical and familiar description.

An elliptic curve E over $\mathbb{C}$ is determined up to isomorphism by the homothety type of its period lattice L: $E(\mathbb{C})\cong\mathbb{C}/L$. If $x=(E\xrightarrow{\varphi}E')$ is a non-cuspidal point of X, and we write $E(\mathbb{C})=\mathbb{C}/L$, $E'(\mathbb{C})=\mathbb{C}/L'$, then we can modify by a homothety to obtain $L'\supset L$, $\varphi=$ identity. Then $L'/L\simeq\mathbb{Z}/N\mathbb{Z}$, so we can choose an oriented basis $\langle\omega_1,\omega_2\rangle$ of L over $\mathbb{Z}$ ("oriented" means $\mathrm{Im}(\omega_1\bar\omega_2)>0$) such that $\langle\omega_1,\frac{1}{N}\omega_2\rangle$ is a basis for L'. The point $z=\omega_1/\omega_2$ then lies in $\underline{H}$, the complex upper half-plane, and the point $x\in X(\mathbb{C})$ uniquely determines z up to the action of

$$\Gamma=\Gamma_0(N)=\{\begin{pmatrix}a&b\\c&d\end{pmatrix}\in PSL_2(\mathbb{Z})\mid c\equiv 0 \pmod N\}.$$

Conversely, any $z\in\Gamma\backslash\underline{H}$ determines a point $x=(\mathbb{C}/\langle z,1\rangle\xrightarrow{\mathrm{id}}\mathbb{C}/\langle z,\frac{1}{N}\rangle)$ of $X(\mathbb{C})$. Thus

$$(X\smallsetminus\{\text{cusps}\})(\mathbb{C})\cong\Gamma_0(N)\backslash\underline{H}.$$

The compactification is given by $X(\mathbb{C})\cong\Gamma_0(N)\backslash\underline{H}^*$, where $\underline{H}^*=\underline{H}\cup\mathbb{P}^1(\mathbb{Q})$ with the usual topology. We have

$$(\{\text{cusps}\})(\mathbb{C})=\Gamma_0(N)\backslash\mathbb{P}^1(\mathbb{Q})\cong\coprod_{\substack{d|N\\d>0}}(\mathbb{Z}/f_d\mathbb{Z})^*$$

where $f_d=(d,N/d)$ and the map is given by

$$\frac{m}{n}\ (m,n\in\mathbb{Z},\ (m,n)=1)\longmapsto d=(n,N),\ (n/d)^{-1}m \pmod{f_d}$$

(one easily checks that n/d is prime to f_d and that the definition depends only on the class of $\frac{m}{n}$ modulo Γ). In particular, the number of cusps is

$$\sum_{d|N} \phi(f_d) \quad = \quad \prod_{\substack{p^\nu \| n \\ \nu>0}} \left(p^{[\nu/2]} + p^{[(\nu-1)/2]} \right) \quad .$$

The curve X over $\mathbb{C}$ has the following automorphisms and correspondences: The action of complex conjugation $c \in \mathrm{Gal}(\mathbb{C}/\mathbb{R})$ on $X(\mathbb{C})$ is induced by

$$c(z) \quad = \quad -\bar{z} \qquad (z \in \underline{H}^*) \quad ;$$

the minus sign arises because for a lattice $L \subset \mathbb{C}$ with oriented basis $\langle \omega_1, \omega_2 \rangle$ the conjugate lattice $c(L)$ has oriented basis $\langle -\bar{\omega}_1, \bar{\omega}_2 \rangle$, and the formula is compatible with the projection map $\underline{H} \to \Gamma \backslash \underline{H}$ because $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ normalizes Γ. The canonical involution w_N of X is induced by the Fricke involution

$$w_N(z) \quad = \quad -1/Nz \qquad (z \in \underline{H}^*) \, ;$$

more generally, for any positive divisor d of N with $(d, N/d)=1$ the involution $w_d \in W$ is induced by the action on $\underline{H}^*$ of any matrix

$$w_d \in \begin{pmatrix} d\mathbb{Z} & \mathbb{Z} \\ N\mathbb{Z} & d\mathbb{Z} \end{pmatrix}, \quad \det w_d = d \quad . \tag{1.1}$$

The Hecke correspondence T_m ($m \in \mathbb{N}$, $(m,N)=1$) acts by

$$T_m(z) \quad = \quad \sum_{\substack{\gamma \in \Gamma \backslash R_N \\ \det \gamma = m}} \gamma z \quad , \tag{1.2}$$

where $R_N = \begin{pmatrix} \mathbb{Z} & \mathbb{Z} \\ N\mathbb{Z} & \mathbb{Z} \end{pmatrix}$. It is easily checked that these descriptions over $\mathbb{C}$ agree with the modular interpretations of c, w_d and T_m given in Chapter I.

Finally, we give the description over $\mathbb{C}$ of the Heegner points. Let K be an imaginary quadratic field, D its discriminant, $\mathcal{O}$ its ring of integers; we suppose N is prime to D. Recall that a Heegner point on X was a non-cuspidal point $x = (E \xrightarrow{\varphi} E')$ such that both E and E' have complex multiplication by $\mathcal{O}$. Then $E(\mathbb{C}) = \mathbb{C}/L$, $E'(\mathbb{C}) = \mathbb{C}/L'$ where L and $L' \subset \mathbb{C}$ are rank 1 modules over $\mathcal{O}$; we can change by a homothety to ensure that L and L' are in K, and then both are (fractional) ideals of K. If we choose $L' \supset L$, $\varphi = \mathrm{id}$, $L/L' \simeq \mathbb{Z}/N\mathbb{Z}$ as before, then $\mathfrak{n} = LL'^{-1}$ is an integral ideal

of norm N and is primitive ("primitive" means $\mathcal{O}/\mathfrak{n} \simeq \mathbb{Z}/N\mathbb{Z}$ or equivalently that $\mathfrak{n}$ is not divisible as an ideal by any natural number >1). Thus $L = \mathfrak{a}$, $L' = \mathfrak{a}\mathfrak{n}^{-1}$ for some fractional ideal $\mathfrak{a}$ of K and some primitive ideal $\mathfrak{n} \subset \mathcal{O}$ of norm N. Conversely, given any such $\mathfrak{a}$ and $\mathfrak{n}$, the elliptic curves $\mathbb{C}/\mathfrak{a}$ and $\mathbb{C}/\mathfrak{a}\mathfrak{n}^{-1}$ over $\mathbb{C}$ have complex multiplication by $\mathcal{O}$ and the isogeny $\mathbb{C}/\mathfrak{a} \to \mathbb{C}/\mathfrak{a}\mathfrak{n}^{-1}$ induced by $\mathrm{id}_{\mathbb{C}}$ defines a Heegner point on X. Clearly two choices $\mathfrak{a}_1$, $\mathfrak{n}_1$ and $\mathfrak{a}_2$, $\mathfrak{n}_2$ define the same Heegner point iff $\mathfrak{a}_2 = \lambda \mathfrak{a}_1$ for some $\lambda \in K^\times$ and $\mathfrak{n}_1 = \mathfrak{n}_2$. Hence we have a 1:1 correspondence

$$\left\{ \begin{matrix} \text{Heegner points} \\ x \in X(\mathbb{C}) \end{matrix} \right\} \longleftrightarrow \left\{ \begin{matrix} \text{pairs } (A, \mathfrak{n}), \quad A \in \mathrm{Cl}_K, \ \mathfrak{n} \subset \mathcal{O} \text{ a} \\ \text{primitive ideal of norm } N \end{matrix} \right\}$$

$$(\mathbb{C}/\mathfrak{a} \xrightarrow{\mathrm{id}_{\mathbb{C}}} \mathbb{C}/\mathfrak{a}\mathfrak{n}^{-1}) \quad \longleftarrow\!\!\!\mid \quad ([\mathfrak{a}], \mathfrak{n}) \qquad ,$$

where Cl_K is the ideal class group of K. The action of c on x corresponds to

$$(A, \mathfrak{n}) \longrightarrow (\bar{A}, \bar{\mathfrak{n}}) = (A^{-1}, N\mathfrak{n}^{-1})$$

while $\mathrm{Gal}(H/K) \simeq \mathrm{Cl}_K$ acts by multiplication on A and trivially on $\mathfrak{n}$ (H = Hilbert class field of K). The Atkin-Lehner operators permute the possible choices of $\mathfrak{n}$. More specifically, let $N = p_1^{r_1} \ldots p_s^{r_s}$ ($r_i > 0$) be the prime factorization of N. The existence of Heegner points for K on X is equivalent to the requirement that all p_i split in K (if N were divisible by an inert prime, it could not be the norm of a primitive ideal, and we are supposing N prime to D), so there are precisely 2^s primitive ideals $\mathfrak{n}$ of norm N, namely the ideals $\mathfrak{p}_1^{r_1} \ldots \mathfrak{p}_s^{r_s}$ where $\mathfrak{p}_i$ is one of the two prime ideals of K dividing p_i. The effect of w_d ($d \| N$) on a Heegner point is to map it to another Heegner point with A replaced by $A[\mathfrak{d}]$, where $\mathfrak{d} = (d, \mathfrak{n})$, and an $\mathfrak{n}$ obtained by making the opposite choice of $\mathfrak{p}_i$ for all p_i dividing d. In particular,

i) w_N acts on Heegner points by $(A, \mathfrak{n}) \to (A[\mathfrak{n}], \bar{\mathfrak{n}})$;

ii) the group $\mathrm{Gal}(H/K) \times W$ ($W \simeq (\mathbb{Z}/2\mathbb{Z})^s$ the group of Atkin-Lehner operators) acts freely and transitively on the set of all Heegner points of discriminant D on X.

It will also be useful to have a description of Heegner points in terms of coordinates in $\underline{H}$. There is a 1:1 correspondence between primitive ideals $\mathfrak{n}\subset\mathcal{O}$ of norm N and solutions β of

(1.3) $$\beta\in\mathbb{Z}/2N\mathbb{Z}\,,\qquad \beta^2\equiv D\pmod{4N}$$

(notice that β^2 is well-defined modulo $4N$ if β is well-defined modulo $2N$) given by

$$\mathfrak{n}=\left(N,\frac{\beta+\sqrt{D}}{2}\right)=\mathbb{Z}N+\mathbb{Z}\frac{\beta+\sqrt{D}}{2}\,.$$

The point in H corresponding to a Heegner point $x=(\mathbb{C}/\mathfrak{a}\longrightarrow\mathbb{C}/\mathfrak{a}\mathfrak{n}^{-1})$ with $\mathfrak{a}\mathfrak{n}^{-1}$ integral is then the solution τ of a quadratic equation

(1.4) $$A\tau^2+B\tau+C=0\,,\quad A>0\,,\quad B^2-4AC=D\,,\quad A\equiv 0\pmod N\,,\quad B\equiv\beta\pmod{2N}\,,$$

with

(1.5) $$\mathfrak{a}=\mathbb{Z}\cdot A+\mathbb{Z}\frac{B+\sqrt{D}}{2}\,,\quad \mathfrak{a}\mathfrak{n}^{-1}=\mathbb{Z}\cdot AN^{-1}+\mathbb{Z}\frac{B+\sqrt{D}}{2}\,,\quad N_{K/\mathbb{Q}}(\mathfrak{a})=A\,.$$

Indeed, a point $\tau\in H$ gives rise to an elliptic curve $\mathbb{C}/\mathbb{Z}\tau+\mathbb{Z}$ with complex multiplication by $\mathcal{O}$ iff τ is the root of a quadratic equation $A\tau^2+B\tau+C=0$ with integral coefficients and discriminant D, and the requirement that $\frac{1}{N}\tau$ have the same property implies that $N|A$; then $B^2\equiv D\pmod{4N}$ and one checks easily that the class of $B\pmod{2N}$ is an invariant of τ under the action of $\Gamma_0(N)$ on H and that this invariant corresponds to the choice of $\mathfrak{n}$ as in (1.3).

For more details on the contents of this section we refer the reader to [13].

§2. Archimedean heights for $X_0(N)$

Let S be any compact Riemann surface. Recall from §4 of Chapter 1 that a height symbol on S is a real-valued function $\langle a,b\rangle_{\mathbb{C}}=\langle a,b\rangle$ defined on divisors of degree 0 with disjoint support, and satisfying

(2.1)
- a. $\langle a,b\rangle$ is additive with respect to a and b;
- b. $\langle a,\sum_j m_j(y_j)\rangle$ is continuous on $S\setminus|a|$ with respect to each variable y_j ($|a|$ denotes the support of a);
- c. $\langle\sum n_i(x_i),b\rangle=\sum_i n_i\log|f(x_i)|^2$ if $b=(f)$, a principal divisor.

Such a symbol is unique if it exists since for fixed a the difference of any two symbols $b\mapsto\langle a,b\rangle$ would define a continuous homomorphism $\mathrm{Jac}(S)\longrightarrow\mathbb{R}$ and hence vanish identically. Now fix two distinct points $x_0,\ y_0\in S$ and set

$$G(x,y)=\langle(x)-(x_0),(y)-(y_0)\rangle\qquad(x,y\in S,\ x\neq y_0,\ y\neq x_0,\ x\neq y)\,.$$

Then the biadditivity of $\langle\,,\rangle$ implies the formula

(2.2) $$\langle a,b\rangle=\sum_{i,j}n_im_j\,G(x_i,y_j)\qquad\text{for}\quad a=\sum n_i(x_i)\,,\quad b=\sum m_j(y_j)\,,$$

at least if $|a|\not\ni y_0$, $|b|\not\ni x_0$. Conversely, a function $G(x,y)$ will define via (2.2) a symbol satisfying (2.1) if for fixed $x\in S$ the function $y\mapsto G(x,y)$ is continuous and harmonic on $S\setminus\{x,x_0\}$ and has logarithmic singularities of residue $+1$ and -1 at $y=x$ and $y=x_0$, and similarly with the roles of x and y interchanged. (Here the terminology "g has a logarithmic singularity of residue C at x_0" means that $g(x)-C\log|\rho(x)|^2$ is continuous in a neighborhood of x_0, where $\rho(x)$ is a uniformizing parameter at x_0.) To prove this, we note that the symbol defined by (2.2) is obviously bi-additive and is continuous in all $y_j\notin|a|$ because the logarithmic singularities of $G(x_i,y)$ at $y=x_0$ cancel (since $\deg a=0$), so (2.1a), (2.1b) are satisfied; equation (2.1c) is also satisfied because the function $x\mapsto\log|f(x)|^2-\langle x,(f)\rangle$ is harmonic and has no singularities (the logarithmic singularities at $x=y_j\in|(f)|$ cancel) and hence is a constant, and this constant drops out in (2.1c) because $\sum n_i=0$. Notice, however, that the axioms we have imposed on G determine it only up to an additive constant (which of course has no effect in formula (2.2)); to make sure that $G(x,y)$ is exactly $\langle(x)-(x_0),(y)-(y_0)\rangle$ we must impose one extra condition, e.g. $G(x_0,y)=0$ for some $y\in S\setminus\{x_0\}$.

Now take $S=X_0(N)(\mathbb{C})=\Gamma_0(N)\setminus H\cup\{\text{cusps}\}$ and $x_0=\infty$, $y_0=0$ (we assume $N>1$, so $x_0\neq y_0$). We want to construct a function $G(x,y)$ satisfying the properties above, i.e. a function G on $H\times H$ satisfying

(2.3)
- a. $G(\gamma z,\gamma' z')=G(z,z')\qquad\forall\,z,z'\in H,\ \gamma,\gamma'\in\Gamma_0(N)$;
- b. $G(z,z')$ is continuous and harmonic for $z\notin\Gamma_0(N)z'$;
- c. $G(z,z')=e_z\log|z-z'|^2+O(1)$ as $z'\longrightarrow z$, where e_z is the order

of the stabilizer of z in $\Gamma_0(N)$;

d. For $z \in H$ fixed, $G(z,z') = 4\pi y' + O(1)$ as $z' = x' + iy' \longrightarrow \infty$ and $G(z,z') = O(1)$ as $z' \longrightarrow$ any cusp of $\Gamma_0(N)$ other than ∞ ; similarly, for z' fixed $G(z,z') = 4\pi \frac{y}{N|z|^2} + O(1)$ as $z = x + iy \longrightarrow 0$ and $G(z,z') = O(1)$ as $z \longrightarrow$ any cusp of $\Gamma_0(N)$ other than 0 .

The conditions in c. and d. come from noting that a uniformizing parameter for $X_0(N)$ at a point represented by $z \in H$ has the form $\rho(z') = (z'-z)^{e_z}(1 + O(z'-z))$, while uniformizing parameters at ∞ and 0 are $e^{2\pi iz}$ and $e^{-2\pi i/Nz}$, respectively. The most obvious way to obtain a function with the invariance property a. is to average a function $g(z,z')$ satisfying

a'. $g(\gamma z, \gamma z') = g(z,z') \qquad \forall \gamma \in PSL_2(\mathbb{R})$

over $\Gamma_0(N)$, i.e. to set $G(z,z') = \sum_{\gamma \in \Gamma_0(N)} g(z,\gamma z')$. To achieve the properties b. - c. we would also like

b'. $g(z,z')$ is continuous and harmonic in each variable on $H \times H \setminus$ diagonal;

c'. $g(z,z') = \log|z-z'|^2 + O(1)$ for $z' \longrightarrow z$.

A function satisfying a'. - c'. is given by

$$g(z,z') = \log \frac{|z-z'|^2}{|\bar{z}-z'|^2} \quad . \tag{2.4}$$

Unfortunately, the sum of $g(z,\gamma z')$ over $\Gamma_0(N)$ diverges (although only barely) for this choice of g . To resolve the difficulty, we modify the condition of harmonicity to $\Delta g = \varepsilon g$ with $\varepsilon > 0$, where $\Delta = y^2\left(\frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2}\right)$ denotes the Laplace operator on H , obtaining a function for which $\sum g(z,\gamma z')$ converges and which is an eigenfunction of the Laplacian with eigenvalue ε , and then take the limit as $\varepsilon \longrightarrow 0$, subtracting off any singularities. Condition a' requires that g be a function only of the hyperbolic distance between z and z' , or equivalently a function Q of the quantity $1 + \frac{|z-z'|^2}{2yy'}$ (which is the hyperbolic cosine of this distance). The equation $\Delta g = \varepsilon g$ then translates into the ordinary differential equation

$$\left((1-t^2)\frac{d^2}{dt^2} + 2t\frac{d}{dt} + \varepsilon\right)Q(t) = 0 \ .$$

This is the Legendre differential equation of index $s-1$, where $\varepsilon = s(s-1)$ with $s > 1$. The only solution (up to a scalar factor) which is small at infinity is the Legendre function of the second kind $Q_{s-1}(t)$, given by

$$Q_{s-1}(t) = \int_0^\infty (t + \sqrt{t^2-1}\cosh u)^{-s}\,du \qquad (t > 1,\ s > 0) \tag{2.5}$$

or

$$Q_{s-1}(t) = \frac{\Gamma(s)^2}{2\Gamma(2s)}\left(\frac{2}{1+t}\right)^s F\left(s,s;2s;\frac{2}{1+t}\right) \qquad (t > 1,\ s \in \mathbb{C}) \ , \tag{2.6}$$

where $F(a,b;c;z)$ is the hypergeometric function. From either of these closed formulas one easily deduces the asymptotic properties

$$Q_{s-1}(t) = -\frac{1}{2}\log(t-1) + O(1) \qquad (t \searrow 1) \ , \tag{2.7}$$

$$Q_{s-1}(t) = O(t^{-s}) \qquad (t \longrightarrow \infty) \ . \tag{2.8}$$

The first implies that the function

$$g_s(z,z') = -2\,Q_{s-1}\left(1 + \frac{|z-z'|^2}{2yy'}\right) \qquad (z,z' \in H,\ z \neq z') \tag{2.9}$$

satisfies axiom c' above and the second, that the sum

$$G_{N,s}(z,z') = \sum_{\gamma \in \Gamma_0(N)} g_s(z,\gamma z') \qquad (z,z' \in H,\ z' \notin \Gamma_0(N)z) \tag{2.10}$$

converges absolutely for $s > 1$. The differential equation of Q_{s-1} implies

$$\Delta_z G_{N,s}(z,z') = \Delta_{z'} G_{N,s}(z,z') = s(s-1)\,G_{N,s}(z,z') \qquad (z' \notin \Gamma_0(N)z) \ , \tag{2.11}$$

while the property

$$G_{N,s}(\gamma z, \gamma' z') = G_{N,s}(z,z') \qquad (\forall \gamma,\gamma' \in \Gamma_0(N)) \tag{2.12}$$

is obvious from the absolute convergence of (2.10) and the property a' of $g_s(z,z')$.

The function $G_{N,s}(z,z')$ on $(H/\Gamma_0(N))^2 \setminus$ (diagonal) is a well-known object called the resolvent kernel function for $\Gamma_0(N)$; its properties are discussed extensively in [20, Chapters 6-7] (note that Hejhal's normalization is $\frac{1}{4\pi}$ times ours). In particular, the series defining $G_{N,s}$ converges absolutely and locally uniformly for $\mathrm{Re}(s) > 1$ and defines a holomorphic function of s which can be extended meromorphically to a neighborhood of $s = 1$ with a simple pole of residue

$$(2.13) \qquad \kappa_N = \frac{-12}{[SL_2(\mathbb{Z}) : \Gamma_0(N)]} = -12\, N^{-1} \prod_{p|N} (1 + \tfrac{1}{p})^{-1}$$

(independent of z, z') at $s = 1$. We could thus "renormalize" at $s = 1$ by forming the limit $\lim_{s\to 1} [G_{N,s}(z,z') - \frac{\kappa_N}{s-1}]$. But this function would not be harmonic in z or z', since

$$\Delta\left(\lim_{s\to 1}[G_{N,s}(z,z') - \frac{\kappa_N}{s-1}]\right) = \lim_{s\to 1}[s(s-1)\,G_{N,s}(z,z')] = \kappa_N \neq 0 .$$

To get a harmonic function of z, we should instead subtract from $G_{N,s}(z,z')$ a $\Gamma_0(N)$-invariant function of z having the same pole $\frac{\kappa_N}{s-1}$ at $s=1$ and the same eigenvalue $s(s-1)$. Such a function is $-4\pi E_N(z,s)$, where

$$(2.14) \qquad E_N(z,s) = \sum_{\gamma\in\Gamma_0(N)} \mathrm{Im}(\gamma z)^s \qquad (z \in H,\ \mathrm{Re}(s) > 1)$$

is the Eisenstein series of weight 0 for the cusp ∞ of $\Gamma_0(N)$. Since we want our function $G(z,z')$ to have its singularities at $z=0$ and $z'=\infty$, we should in fact subtract $-4\pi\, E(w_N z,s)$ and $-4\pi\, E(z',s)$ from $G_{N,s}(z,z')$, where $w_N\colon z \mapsto -1/Nz$ is the involution of $X_0(N)$ interchanging 0 and ∞; we must then add back a term $\frac{\kappa_N}{s-1}$, since we have subtracted off the pole of $G_{N,s}$ twice. We therefore set

$$(2.15) \qquad G(z,z') = \lim_{s\to 1}[G_{N,s}(z,z') + 4\pi\, E_N(w_N z,s) + 4\pi\, E_N(z',s) + \frac{\kappa_N}{s-1}] + C ,$$

with a constant C still to be determined, and claim that it possesses all the properties (2.3). Indeed, (2.3a) and (2.3b) are obvious from the definition of $G_{N,s}(z,z')$ and the preceding discussion, and (2.3c) follows from (2.7). It remains only to check the behavior of the function (2.15) at the cusps, i.e. that it has the correct logarithmic singularities as z goes to 0 or z' to ∞ and is bounded at all other cusps; we would also like to choose the constant in (2.15) so that $G(z,z') \to 0$ as $z \to \infty$. We must therefore know the

expansions of $G_{N,s}$ and E_N at all cusps of $X_0(N)$. For E_N this is easily obtained from the elementary identity

$$(2.16) \qquad E_N(z,s) = N^{-s} \prod_{p|N} (1-p^{-2s})^{-1} \cdot \sum_{d|N} \frac{\mu(d)}{d^s}\, E(\tfrac{N}{d} z, s) ,$$

where $\mu(d)$ is the Möbius function and $E(z,s) = E_1(z,s)$ the Eisenstein series for $SL_2(\mathbb{Z})$, because for $SL_2(\mathbb{Z})$ all cusps are equivalent to ∞, where $E(z,s)$ has the well-known expansion

$$(2.17) \qquad E(z,s) = y^s + \phi(s)\, y^{1-s} + O(e^{-y}) \qquad (y = \mathrm{Im}(z) \to \infty) ,$$

$$(2.18) \qquad \phi(s) = \frac{\Gamma(\frac12)\,\Gamma(s-\frac12)}{\Gamma(s)} \frac{\zeta(2s-1)}{\zeta(2s)} .$$

(By $O(e^{-y})$ in (2.17) and below we mean a function which is not only $O(e^{-y})$ -- actually, $O(e^{-cy})$ for any $c < 2\pi$ -- for fixed $s > 1$ but is holomorphic in s at $s=1$ and is $O(e^{-y})$ uniformly in a neighborhood of $s=1$.) For $G_{N,s}$ we have the expansion

$$(2.19) \qquad G_{N,s}(z,z') = -\frac{4\pi}{2s-1} E_N(z',s)\, y^{1-s} + O(e^{-y}) \qquad (y = \mathrm{Im}(z) \to \infty)$$

at ∞ (see [20], (6.5); this expansion is obtained by calculating the Fourier-development of $G_{N,s}(z,z')$ with respect to z). At other cusps there is a similar expansion, so that $G_{N,s}(z,z') = \alpha(s)\, Y^{1-s} + O(e^{-Y})$ where $Y = \mathrm{Im}(\gamma z)$ for some $\gamma \in SL_2(\mathbb{R})$ transforming the cusp in question to ∞. Hence as z tends to any cusp other than 0, the expression in square brackets in (2.17) has the form $\alpha(s)\, Y^{1-s} + \beta(s) + O(e^{-Y})$, where $\alpha(s)$ and $\beta(s)$ have at most simple poles at $s=1$ and $\alpha(s) + \beta(s)$ is holomorphic there; letting $s \to 1$, we obtain a function of the form $\alpha \log Y + \beta + O(e^{-Y})$, and the harmonicity of this requires that $\alpha = 0$. Hence (2.15) is bounded as z tends to any cusp other than 0. At 0, we find from (2.16) and (2.17)

$$E_N(w_N z,s) = \mathrm{Im}(w_N z)^s + O(\mathrm{Im}(w_N z)^{1-s}) \qquad (z \to 0) ,$$

so the same argument shows that $G(z,z')$ has an expansion $4\pi Y + \alpha \log Y + \beta + O(e^{-Y})$

as $Y = \mathrm{Im}(w_N z) = \frac{y}{N|z|^2} \longrightarrow \infty$, where again α must be 0 (by direct computation or because G is harmonic). This proves the assertions of (2.3d) for z, and the assertions for z' are proved similarly or by noting the symmetry property

$$G(z,z') = G(w_N z', w_N z) \quad . \tag{2.20}$$

Finally, we must determine the constant in (2.15) so that $G(z,z')$ vanishes as $z \longrightarrow \infty$. By (2.19) we have

$$G(z,z') = \lim_{s\to 1} [\, 4\pi E_N(z',s) \, (1 - \frac{y^{1-s}}{2s-1}) \,] + \lim_{s\to 1} [\, 4\pi E_N(w_N z,s) + \frac{\kappa_N}{s-1} \,] + C + O(e^{-y})$$

as $y \longrightarrow \infty$. Since

$$4\pi E_N(z',s) = \frac{-\kappa_N}{s-1} + O(1) \;, \quad 1 - \frac{y^{1-s}}{2s-1} = (\log y + 2)\,(s-1) + O(s-1)^2$$

as $s \longrightarrow 1$, the first limit equals $-\kappa_N(\log y + 2)$. The second limit is evaluated by (2.16) - (2.18):

$$\begin{aligned} E_N(w_N z,s) &= N^{-s} \prod_{p|N} (1-p^{-2s})^{-1} \cdot \sum_{d|N} \frac{\mu(d)}{d^s} E(dz,s) \\ &= N^{-s} \prod_{p|N} (1-p^{-2s})^{-1} \left[\prod_{p|N} (1-p^{-2s+1})\, \phi(s)\, y^{1-s} + O(e^{-y}) \right] , \end{aligned}$$

$$\lim_{s\to 1} [\, 4\pi E_N(w_N z,s) + \frac{\kappa_N}{s-1} \,] = \kappa_N \log y + \lambda_N + O(e^{-y})$$

with

$$\begin{aligned} \lambda_N &= \lim_{s\to 1} [\, 4\pi N^{-s} \phi(s) \prod_{p|N} \frac{1-p^{-2s+1}}{1-p^{-2s}} + \frac{\kappa_N}{s-1} \,] \\ &= \kappa_N [\, \log N + 2\log 2 - 2\gamma + 2\frac{\zeta'}{\zeta}(2) - 2 \sum_{p|N} \frac{p \log p}{p^2-1} \,] \end{aligned} \tag{2.21}$$

(here γ = Euler's constant and we have used $\frac{\Gamma'}{\Gamma}(1) = -\gamma$, $\frac{\Gamma'}{\Gamma}(\frac{1}{2}) = -2\log 2 - \gamma$, $\zeta(2s-1) = \frac{1}{2s-2} + \gamma + O(s-1)$). Hence

$$G(z,z') = -2\kappa_N + \lambda_N + C + O(e^{-y})$$

as $y \longrightarrow \infty$, so we must have $C = 2\kappa_N - \lambda_N$. Summarizing, we have proved:

<u>Proposition 2.22</u>. <u>Let</u> x, x' <u>be distinct non-cuspidal points of</u> $X_0(N)(\mathbb{C})$. <u>Then</u>

$$\begin{aligned} \langle (x)-(\infty), (x')-(0) \rangle_{\mathbb{C}} = \lim_{s\to 1} [\, & G_{N,s}(z,z') + 4\pi E_N(w_N z,s) + 4\pi E_N(z',s) + \frac{\kappa_N}{s-1} \,] \\ & - \lambda_N + 2\kappa_N \;, \end{aligned}$$

<u>where</u> $z, z' \in H$ <u>are points representing</u> x <u>and</u> x' <u>and</u> $G_{N,s}$, E_N, κ_N, λ_N <u>are defined by</u> (2.10), (2.14), (2.13) <u>and</u> (2.21), <u>respectively</u>.

We would also like a formula of the same kind for $\langle (x)-(\infty), T_m((x')-(0)) \rangle$ where T_m is the m^{th} Hecke operator ($m > 0$ prime to N). Since T_m maps each cusp to itself, we have

$$\langle (x)-(\infty), T_m((x')-(0)) \rangle_{\mathbb{C}} = G(z,z')|_{z'} T_m = \sum_{\substack{\gamma \in \Gamma \backslash R_N \\ \det \gamma = m}} G(z,\gamma z')$$

(cf. (1.2)). The operator T_m acts on constants by multiplication with

$$\#\{\gamma \in \Gamma\backslash R_N \,,\, \det\gamma = m\} = \sigma_1(m) = \sum_{\substack{d|m \\ d>0}} d \;,$$

and on $E_N(z',s)$ by multiplication with

$$m^s \sigma_{-2s+1}(m) = m^s \sum_{d|m} d^{1-2s}$$

(this can be seen easily from the definition or from (2.16) and the corresponding statement for $SL_2(\mathbb{Z})$). Finally, it is clear from the definition of $G_{N,s}$ that

$$G_{N,s}(z,z')|_{z'} T_m = \sum_{\substack{\gamma \in R_N/\{\pm 1\} \\ \det \gamma = m}} g_s(z,\gamma z') \;.$$

Putting all this together, we obtain

<u>Proposition 2.23</u>. <u>Let</u> $m \geq 1$, $(m,N) = 1$, x, $x' \in X_0(N)(\mathbb{C})$ <u>non-cuspidal points with</u> $x \notin T_m x'$. <u>Then</u>

$$\begin{aligned} \langle (x)-(\infty), T_m((x')-(0)) \rangle_{\mathbb{C}} = \lim_{s\to 1} [\, & G^m_{N,s}(z,z') + 4\pi\sigma_1(m)\, E_N(w_N z,s) \\ & + 4\pi m^s \sigma_{1-2s}(m)\, E_N(z',s) + \frac{\sigma_1(m)\kappa_N}{s-1} \,] \\ & - \sigma_1(m)\lambda_N + 2\sigma_1(m)\kappa_N \end{aligned}$$

<u>with</u> z, z', E_N, κ_N, λ_N <u>as in Proposition 2.22</u>, $\sigma_\nu(m) = \sum_{d|m} d^\nu$, <u>and</u>

$$G^m_{N,s}(z,z') = \frac{1}{2} \sum_{\substack{a,b,c,d\in\mathbb{Z} \\ N|c,\ ad-bc=m}} g_s\left(z, \frac{az'+b}{cz'+d}\right) . \tag{2.24}$$

As a final remark, we observe that the functions $G_{N,s}$ and $G^m_{N,s}$ have the invariance property

$$G^m_{N,s}(w_d z, w_d z') = G^m_{N,s}(z,z') \tag{2.25}$$

for any $d\|N$, where w_d are the Atkin-Lehner operators as in (1.1). This property, which follows easily from (2.24) and the invariance of $g_s(z,z')$ under $z \to \gamma z$, $z' \to \gamma z'$ $(\gamma \in SL_2(\mathbb{R}))$, is compatible with the fact that the height pairing is invariant under automorphisms.

§3. Evaluation of the function $G^m_{N,s}$ at Heegner points

According to the results of §2, in order to compute the height pairing

$$\langle c, T_m d^\sigma \rangle_v, \quad c=(x)-(\infty), \quad d=(x)-(0), \quad \sigma\in \mathrm{Gal}(H/K) \quad (x = \text{Heegner point})$$

at an archimedean place v of H, we must evaluate the functions $G^m_{N,s}$ at the corresponding points of $X(H_v)=X(\mathbb{C})$. These points were described in §1 and shown to be parametrized by pairs $(A,\mathfrak{n})$, where $A\in Cl_K$ and $\mathfrak{n}\subset\mathcal{O}$ is a primitive ideal of norm N, the corresponding point $\tau_{A,\mathfrak{n}}\in\Gamma_0(N)\backslash H\subset X(\mathbb{C})$ (or rather, a representative of it in H) being a root of a quadratic equation as in (1.4). Since $\sigma=\sigma_A\in \mathrm{Gal}(H/K)$ acts by $\tau_{A_1,\mathfrak{n}} \longmapsto \tau_{A_1A^{-1},\mathfrak{n}}$, we need only consider values

$$G^m_{N,s}(\tau_{A_1,\mathfrak{n}}, \tau_{A_2,\mathfrak{n}}) \tag{3.1}$$

where the arguments are Heegner points associated to the <u>same</u> $\mathfrak{n}$ and to ideal classes A_1, A_2 satisfying $A_1A_2^{-1}=A$. Here we must assume $r_A(m)=0$ since otherwise the value (3.1) is not defined; we will discuss the modifications for the case $r_A(m)\neq 0$ in §5.

The expression (3.1) depends on the choice of $\mathfrak{n}$. On the other hand, the function $G^m_{N,s}$ is invariant under the action of the Atkin-Lehner operators w_d by (2.25), and we saw in §1 that these act on the Heegner points by

$$\tau_{A,\mathfrak{n}} \longmapsto \tau_{A[\mathfrak{d}]^{-1},\bar{\mathfrak{d}}\mathfrak{n}\mathfrak{d}^{-1}} \quad \text{where} \quad \mathfrak{d}|\mathfrak{n}, \quad N(\mathfrak{d})=d .$$

We can therefore replace A_1 and A_2 by $A_1[\mathfrak{d}]^{-1}$, $A_2[\mathfrak{d}]^{-1}$ and $\mathfrak{n}$ by $\mathfrak{n}\mathfrak{d}^{-1}\bar{\mathfrak{d}}$ in (3.1) without affecting the value of this expression. This substitution does not change either $A_1A_2^{-1}$ $(=A)$ or $A_1A_2[\mathfrak{n}]^{-1}$. Hence the sum

$$\gamma^m_{N,s}(A;\mathcal{B}) = \sum_{\substack{A_1,A_2\in Cl_K \\ A_1A_2^{-1}=A \\ A_1A_2[\mathfrak{n}]^{-1}=\mathcal{B}}} G^m_{N,s}(\tau_{A_1,\mathfrak{n}}, \tau_{A_2,\mathfrak{n}}) \qquad (r_A(m)=0) \tag{3.2}$$

is independent of $\mathfrak{n}$. The summation here is very small: If K has prime discriminant, so that $|Cl_K|$ is odd, it reduces to a single term (i.e. we have just re-indexed the quantities (3.1)), while in general it has 2^{t-1} terms if $\{A\}=\{\mathcal{B}\mathfrak{n}\}$ and is empty otherwise; here t is the number of prime factors of D and $\{A\}$ denotes the <u>genus</u> of A, i.e. the class of A in $Cl_K/2Cl_K \simeq (\mathbb{Z}/2\mathbb{Z})^{t-1}$. (Notice that all ideals $\mathfrak{n}$ with $N(\mathfrak{n})=N$ belong to the same genus, so the condition on A, $\mathcal{B}$ is independent of $\mathfrak{n}$, as it should be.) In this section we will obtain formulae for (3.1) and for the slightly cruder invariant (3.2); the latter will be much nicer (as can be expected since the dependence on the choice of $\mathfrak{n}$ has been eliminated). By summing further we obtain an even simpler expression for the yet cruder invariant

$$\gamma^m_{N,s}(A) = \sum_{\substack{A_1,A_2\in Cl_K \\ A_1A_2^{-1}=A}} G^m_{N,s}(\tau_{A_1,\mathfrak{n}}, \tau_{A_2,\mathfrak{n}}) = \sum_{\mathcal{B}\in Cl_K} \gamma^m_{N,s}(A;\mathcal{B}) . \tag{3.3}$$

Of course, (3.3) is all we need to compute the total contribution $\sum_{v|\infty} \langle c,d^\sigma\rangle_v$ to the global height pairing from all of the archimedean places of H, since these places are permuted transitively by $\mathrm{Gal}(H/K)\simeq Cl_K$. However, in Chapter V we will see that some interest attaches also to the individual terms (3.1).

We now start the calculation of (3.1). In (2.24), suppose that $z=\tau_1$ and $z'=\tau_2$ are Heegner points with the same $\mathfrak{n}$, i.e. that they satisfy quadratic equations $A_i\tau_i^2+B_i\tau_i+C_i$ as in (1.4) with the same β. Then for $\gamma=\begin{pmatrix} a & b \\ c & d\end{pmatrix}\in R_N$ we have

$$g_s(\gamma\tau_1,\tau_2) = -2\,Q_{s-1}\left(1+\frac{|\gamma\tau_1-\tau_2|^2}{2\,\mathrm{Im}(\gamma\tau_1)\,\mathrm{Im}(\tau_2)}\right) = -2\,Q_{s-1}\left(1+\frac{2nN}{|D|\det(\gamma)}\right)$$

with

$$n \;=\; \frac{A_1A_2}{N}\,|c\tau_1\tau_2 + d\tau_1 - a\tau_1 - b|^2 \quad . \tag{3.4}$$

Since n is a rational multiple of the norm of an element of K, it is rational. In fact, a direct calculation gives

$$\begin{aligned} n \;=\; \frac{1}{N}\Big[\, & c^2C_1C_2 + (ad-bc)\frac{D-B_1B_2}{2} + a^2C_1A_2 + d^2A_1C_2 - cdB_1C_2 \\ & + acC_1B_2 + b^2A_1A_2 + bdA_1B_2 - baB_1A_2 \,\Big] \ , \end{aligned} \tag{3.5}$$

and this is integer because A_1, A_2 and c are divisible by N and $B_1B_2 \equiv \beta^2 \equiv D \pmod{2N}$. Hence

$$G^m_{N,s}(\tau_1,\tau_2) \;=\; -2\sum_{n=1}^{\infty} \rho^m(n)\, Q_{s-1}\Big(1+\frac{2nN}{m|D|}\Big)$$

where $\rho^m(n)$ is the number of $\gamma = \begin{pmatrix} a & b \\ c & d\end{pmatrix} \in R_N/\{\pm 1\}$ satisfying $ad-bc=m$ and (3.4) or (3.5). To see what kind of an expression $\rho^m(n)$ is, consider the simplest case when $N=1$, $D=-4$ and $\tau_1=\tau_2=i$, so $A_1=A_2=C_1=C_2=1$, $B_1=B_2=0$. Then (3.5) becomes

$$n = a^2+b^2+c^2+d^2-2(ad-bc) \ ,$$

so $\rho^m(n)$ counts the number of 4-tuples $(a,b,c,d) \in \mathbf{Z}^4$ (up to sign) satisfying

$$(a-d)^2+(b+c)^2 = n \ , \quad (a+d)^2+(b-c)^2 = n+4m \ ,$$

i.e. (apart from a congruence condition modulo 2) $\rho^m(n)$ is the product of the numbers of representations of n and of $n+4m$ as sums of two squares. The answer in general will be similar. However, since (3.5) is so complicated we will stop using the language of quadratic forms and shift to that of ideals in quadratic fields. We start by redoing the proof that the number n defined by (3.4) is integral. Given $\gamma = \begin{pmatrix} a & b \\ c & d\end{pmatrix} \in R_N$ we define two numbers $\alpha,\ \beta \in K$ by

$$\alpha \;=\; c\tau_1\bar\tau_2 + d\bar\tau_2 - a\tau_1 - b \ , \quad \beta \;=\; c\tau_1\tau_2 + d\tau_2 - a\tau_1 - b \ . \tag{3.6}$$

From $\tau_i \in A_i^{-1}\bar{\mathfrak{a}}_i = \mathfrak{a}_i^{-1}$ (compare (1.5)), $c \in (N) = \mathfrak{n}\bar{\mathfrak{n}}$ and $\mathfrak{n}\,|\,\mathfrak{a}_i$ we have

$$\alpha \in \mathfrak{a}_1^{-1}\bar{\mathfrak{a}}_2^{-1} \ , \quad \beta \in \mathfrak{a}_1^{-1}\mathfrak{a}_2^{-1}\mathfrak{n} \ . \tag{3.7}$$

It follows that the two numbers

$$\ell = A_1A_2\,N(\alpha) \ , \quad n = N^{-1}A_1A_2\,N(\beta) \tag{3.8}$$

are in $\mathbf{Z}$. Also

$$\begin{aligned} \ell - Nn \;&=\; A_1A_2 \det\begin{pmatrix} \alpha & \beta \\ \bar\beta & \bar\alpha\end{pmatrix} \\ &=\; A_1A_2 \det\Big[\begin{pmatrix} -1 & \bar\tau_2 \\ -1 & \tau_2\end{pmatrix}\begin{pmatrix} a & b \\ c & d\end{pmatrix}\begin{pmatrix} \tau_1 & \bar\tau_1 \\ 1 & 1\end{pmatrix}\Big] \\ &=\; |D|\det(\gamma) \end{aligned} \tag{3.9}$$

and

$$A_1A_2\alpha \equiv A_1A_2\beta \pmod{\mathfrak{D}} \ , \tag{3.10}$$

where $\mathfrak{D} = (\sqrt{D})$ is the different of K (the last equation holds because $A_1\tau_1$, $A_2\tau_2$ are integral and $\lambda \equiv \bar\lambda \pmod{\mathfrak{D}}$ for any $\lambda \in \mathcal{O}$). Conversely, given any α and β in K, we can think of the real and imaginary parts of (3.6) as a system of 4 linear equations with rational coefficients in 4 unknowns a,b,c,d and solve for a,b,c,d. The simplest way is to notice that

$$c\tau_1 + d \;=\; \frac{\alpha-\beta}{\tau_2-\bar\tau_2} \;=\; \frac{A_2}{\sqrt{D}}(\alpha-\beta) \ ,$$

$$a\tau_1 + b \;=\; \tau_2(c\tau_1+d) - \alpha \;=\; \frac{\bar\tau_2\alpha - \tau_2\beta}{\tau_2-\bar\tau_2} \;=\; \frac{A_2}{\sqrt{D}}(\bar\tau_2\alpha - \tau_2\beta) \ .$$

If α and β satisfy (3.7) and (3.10) then the right-hand sides of these two equations are in $\mathfrak{n}\mathfrak{a}_1^{-1} = N\mathbf{Z}\tau_1 + \mathbf{Z}$ and $\mathfrak{a}_1^{-1} = \mathbf{Z}\tau_1 + \mathbf{Z}$, respectively, so $a,b,c,d \in \mathbf{Z}$ and $N|c$. If also the integers ℓ and n defined by (3.8) satisfy $\ell = nN + m|D|$ then (3.9) shows that $\det(\gamma) = m$. We have proved:

<u>Proposition 3.11</u>. <u>Let</u> A_1, A_2 <u>be two ideal classes of</u> K, $\mathfrak{n}$ <u>a primitive ideal of norm</u> N <u>and</u> $\mathfrak{a}_i$ $(i=1,2)$ <u>an integral ideal in</u> A_i <u>with</u> $\mathfrak{n}|\mathfrak{a}_i$, $N(\mathfrak{a}_i) = A_i$. <u>Then for</u> $m \in \mathbf{N}$, $r_{A_1A_2^{-1}}(m) = 0$ <u>we have</u>:

$$G^m_{N,s}(\tau_{A_1,\mathfrak{n}},\tau_{A_2,\mathfrak{n}}) \;=\; -2\sum_{n=1}^{\infty}\rho^m(n)\,Q_{s-1}\Big(1+\frac{2nN}{m|D|}\Big)$$

<u>where</u>

$$\rho^m(n) = \rho^m_{A_1,A_2,\mathfrak{n}}(n) \;=\; \#\Big\{(\alpha,\beta) \in (\mathfrak{a}_1^{-1}\bar{\mathfrak{a}}_2^{-1} \times \mathfrak{a}_1^{-1}\mathfrak{a}_2^{-1}\mathfrak{n})/\{\pm 1\} \;\Big|\; N(\alpha) = \frac{Nn+m|D|}{A_1A_2},\ N(\beta) = \frac{Nn}{A_1A_2},\ A_1A_2\alpha \equiv A_1A_2\beta \pmod{\mathfrak{D}}\Big\} \ .$$

(The condition $r_{A_1A_2^{-1}}(m)=0$ is required to ensure that n in (3.8) is strictly positive.)

To understand the expression $\rho^m(n)$ better, consider first the case when $n\equiv 0 \pmod D$. Then $A_1A_2\alpha$ and $A_1A_2\beta$ are automatically $0 \pmod D$, so $\rho^m(n)$ breaks up as a product

$$(3.12)\qquad \begin{aligned}\rho^m_{A_1,A_2,\mathfrak{n}}(n) &= \frac{1}{2}\#\{\alpha\in \mathfrak{a}_1^{-1}\bar{\mathfrak{a}}_2^{-1} \mid N(\alpha)=\frac{\ell}{A_1A_2}\}\\ &\quad\times \#\{\beta\in \mathfrak{a}_1^{-1}\mathfrak{a}_2^{-1}\mathfrak{n} \mid N(\beta)=\frac{Nn}{A_1A_2}\}\\ &= 2u^2\, r_{A_1A_2^{-1}}(\ell)\, r_{A_1A_2[\mathfrak{n}]^{-1}}(n) \qquad (n\equiv 0 \pmod D)\end{aligned}$$

where $u=\frac{1}{2}\#$ of units of K, $\ell = Nn+m|D|$ and, as usual, $r_A(n)$ denotes the number of integral ideals of norm n in the class A. Another easy case is when $n\not\equiv 0 \pmod D$ but D is prime. In this case, exactly half of the pairs $\alpha,\beta\in \mathfrak{a}_1^{-1}\bar{\mathfrak{a}}_2^{-1}\times \mathfrak{a}_1^{-1}\mathfrak{a}_2^{-1}\mathfrak{n}$ satisfying $A_1A_2N(\alpha)=nN+m|D|$, $A_1A_2N(\beta)=nN$ satisfy $A_1A_2\alpha\equiv A_1A_2\beta \pmod D$, namely exactly one of (α,β) and $(\alpha,-\beta)$ for any α, β (this is because a quadratic residue mod D has exactly two square roots mod D). Hence

$$(3.13)\qquad \rho^m_{A_1,A_2,\mathfrak{n}}(n) = u^2 r_{A_1A_2^{-1}}(nN+m|D|)\, r_{A_1A_2[\mathfrak{n}]^{-1}}(n)\times\begin{cases}1 & D\nmid n\\ 2 & D\mid n\end{cases} \qquad (D \text{ prime}).$$

A formula generalizing (3.12) and (3.13) is

$$(3.14)\qquad \sum_{\substack{A_1,A_2\in Cl_K\\ A_1A_2^{-1}=A\\ A_1A_2[\mathfrak{n}]^{-1}=B}} \rho_{A_1,A_2,\mathfrak{n}}(n) = \begin{cases} u^2\delta(n)r_A(nN+m|D|)r_B(n) & \text{if } \{A\}=\{B\mathfrak{n}\},\\ 0 & \text{otherwise,}\end{cases}$$

where now D is arbitrary, A and B are any two ideal classes of K, $\{A\}$ and $\{B\mathfrak{n}\}$ denote the genera to which A and $B[\mathfrak{n}]$ belong, and

$$(3.15)\qquad \delta(n) = \prod_{p\mid (n,D)} 2 .$$

Indeed, if D is prime then the sum in (3.14) reduces to a single term (since Cl_K has odd order) and (3.14) is identical with (3.13), while if $n\equiv 0 \pmod D$ the sum in (3.14) has 2^{t-1} or 0 terms according as $\{A\}=\{B\mathfrak{n}\}$ or not and these terms are all equal to the expression in (3.12) (note that $\delta(n)=2^t$ in this case). To prove (3.14) in general, we fix some A_1, A_2 satisfying the conditions on the left

(if there are no such then $\{A\}\neq\{B\mathfrak{n}\}$ and the formula is trivial). The other classes in the sum are obtained by replacing A_1 and A_2 by A_1C and A_2C with C^2 trivial, i.e. by replacing representatives $\mathfrak{a}_1$, $\mathfrak{a}_2$ of A_1, A_2 by $\mathfrak{a}_1\mathfrak{c}$, $\mathfrak{a}_2\mathfrak{c}$ with $\mathfrak{c}^2$ principal, say $\mathfrak{c}^2=(\gamma)$, $\gamma\in K^\times$. If we also replace α and β by $\alpha/N(\mathfrak{c})$ and β/γ we obtain a new solution of (3.7) and (3.8). Thus the only question is how many of the 2^{t-1} choices of $[\mathfrak{c}]$ lead to α, β satisfying the congruence (3.10). This congruence is equivalent to a congruence modulo p for each of the primes p dividing D; each of these t congruences is true if $p|n$ (both sides are 0) and true up to sign if $p\nmid n$ (both sides are non-0 and they have the same square). But the change of $\mathfrak{a}_1$, $\mathfrak{a}_2$, α, β described above changes the ratio $\alpha:\beta$ by a factor $\gamma/N(\mathfrak{c})$ of norm 1, i.e. by a number of the form $r+s\sqrt{D}$ with r and s p-integral and $r^2\equiv 1 \pmod p$ for all $p|D$. The 2^{t-1} classes of $\mathfrak{c}$ with $[\mathfrak{c}]^2$ trivial correspond in this way to the values $\pm r \pmod D$ with $r^2\equiv 1 \pmod D$. The formula (3.14) is now obvious. Combining it with Proposition 3.11, we find:

<u>Proposition 3.16.</u> <u>The invariant</u> $\gamma^m_{N,s}(A;B)$ <u>defined by</u> (3.2) <u>is given by</u>

$$\gamma^m_{N,s}(A;B) = -2u^2\sum_{n=1}^{\infty}\delta(n)r_A(nN+m|D|)r_B(n)Q_{s-1}\left(1+\frac{2nN}{m|D|}\right)$$

($\delta(n)$ <u>as in</u> (3.15)) <u>if</u> $\{A\}=\{B\mathfrak{n}\}$ <u>and is</u> 0 <u>otherwise</u>.

Summing over all B, we obtain:

<u>Corollary 3.17.</u> <u>The invariant</u> $\gamma^m_{N,s}(A)$ <u>defined by</u> (3.3) <u>is given by</u>

$$\gamma^m_{N,s}(A) = -2u^2\sum_{n=1}^{\infty}\delta(n)R_{\{A\mathfrak{n}\}}(n)r_A(nN+m|D|)Q_{s-1}\left(1+\frac{2nN}{m|D|}\right),$$

<u>where</u> $R_{\{A\mathfrak{n}\}}(n)$ <u>is the number of integral ideals of norm</u> n <u>in the genus</u> $\{A\mathfrak{n}\}$.

Since a number cannot be the norm of an ideal in more than one genus, $R_{\{A\mathfrak{n}\}}(n)$ is either $R(n)$ or 0, where

$$R(n) = \sum_{A\in Cl_K} r_A(n) = \sum_{m|n}\left(\frac{D}{m}\right)$$

is the total number of representations of n as the norm of an ideal of $\mathcal{O}$. Which of these two alternatives occurs depends only on values of genus characters. In particular, if $(n,D)=1$ then $R_{\{A\mathfrak{n}\}}(n)$ can be replaced by $R(n)$ in (3.17) because

$$r_A(nN+m|D|)\neq 0 \Rightarrow \left(\frac{A(nN+m|D|)}{p}\right)=+1 \quad (\forall p|D) \Rightarrow \left(\frac{AN\cdot n}{p}\right)=+1 \quad (\forall p|D)$$

$$\Rightarrow R_{\{A\mathfrak{n}\}}(n)=R(n)$$

(A = any integer prime to D which is the norm of an ideal in the genus $\{A\}$). In general, there will be one genus condition to be satisfied for each prime dividing (n,D), and we could replace the product

$$\delta(n)R_{\{A\mathfrak{n}\}}(n)r_A(nN+m|D|) = \Big(\prod_{p|(n,D)} 2\Big)\cdot R_{\{A\mathfrak{n}\}}(n)r_A(nN+m|D|)$$

by

$$\prod_{p|(n,D)}\Big(1+\hat{\varepsilon}_p\Big(\frac{nN+m|D|}{nN}\Big)\Big)\cdot R(n)r_A(nN+m|D|) \quad ,$$

where $\hat{\varepsilon}_p$ is the homomorphism from the group of norms of fractional ideals of K to $\{\pm 1\}$ defined by $\hat{\varepsilon}_p(N\mathfrak{a})=1$ for $\mathfrak{a}$ principal, $\hat{\varepsilon}_p(n)=\left(\frac{n}{p}\right)$ for $n\in\mathbb{Z}$, $p\nmid n$. However, for later purposes we will prefer to leave the formula for $\gamma^m_{N,s}(A)$ in the form given in 3.17.

§4. Final formula for the height ($r_A(m)=0$)

Let $c=(x)-(\infty)$, $d=(x)-(0)$, $\sigma=\sigma_A\in \mathrm{Gal}(H/K)$, m prime to N. We still assume that $r_A(m)=0$, so that the divisors c and $T_m d^\sigma$ have disjoint support. We want to compute

$$<c\,,T_m d^\sigma>_\infty \;:=\; \sum_{v|\infty} <c\,,T_m d^\sigma>_v \quad ,$$

where the sum is over the h_K archimedean places of H. Since these places are permuted simply transitively by $\mathrm{Gal}(H/K)\simeq Cl_K$, this equals

$$\sum_{\substack{A_1,A_2\in Cl_K\\ A_1A_2^{-1}=A}} <(\tau_{A_1,\mathfrak{n}})-(\infty)\,,T_m((\tau_{A_2,\mathfrak{n}})-(0))>_{\mathbb{C}} \quad ,$$

where $\mathfrak{n}$ is any integral ideal of K of norm N and the $\tau_{A,\mathfrak{n}}$ are the points in H described in §1. Applying Proposition 2.23, we find

$$<c\,,T_m d^\sigma>_\infty = \lim_{s\to 1}\Big[\gamma^m_{N,s}(A) + 4\pi\sigma_1(m)\sum_{A_1\in Cl_K} E_N(w_N\tau_{A_1,\mathfrak{n}},s)$$

$$+ 4\pi m^s\sigma_{1-2s}(m)\sum_{A_2\in Cl_K} E_N(\tau_{A_2,\mathfrak{n}},s) + \frac{h_K\sigma_1(m)\kappa_N}{s-1}\Big]$$

$$- h_K\sigma_1(m)\lambda_N + 2h_K\sigma_1(m)\kappa_N \quad .$$

Using (2.16), we have

$$\sum_{A\in Cl_K} E_N(w_N\tau_{A,\mathfrak{n}},s) = \sum_{A\in Cl_K} E_N(\tau_{A,\mathfrak{n}},s)$$

$$= N^{-s}\prod_{p|N}(1-p^{-2s})^{-1}\sum_{d|N}\frac{\mu(d)}{d^s}\sum_{A\in Cl_K} E\Big(\frac{N}{d}\tau_{A,\mathfrak{n}},s\Big)$$

where $E(z,s)$ is the Eisenstein series for $SL_2(\mathbb{Z})$. Since each $\tau_{A,\mathfrak{n}}$ solves a quadratic equation $a\tau^2+b\tau+c=0$ of discriminant D with $N|a$, the points $\frac{N}{d}\tau_{A,\mathfrak{n}}$ for $d|N$ also satisfy quadratic equations over $\mathbb{Z}$ of discriminant D. It is then easy to see that the inner sum on the right-hand side of (4.1) is independent of d and equals $\sum_A E(\tau_A,s)$, where τ_A is any point in H satisfying a quadratic equation of discriminant D corresponding to the ideal class A. As is well-known (and elementary), $E(\tau_A,s)$ is a simple multiple of the partial zeta-function

$$\zeta_K(A,s) = \sum_{\substack{\mathfrak{a}\text{ integral}\\ [\mathfrak{a}]=A}} \frac{1}{N(\mathfrak{a})^s} \quad ,$$

namely

$$E(\tau_A,s) = 2^{-s}|D|^{s/2}u\,\zeta(2s)^{-1}\zeta_K(A,s)$$

where u as usual is one-half the number of units of K. Since $\sum_A \zeta_K(A,s)=\zeta_K(s)$ the Dedekind zeta-function of K, we deduce

$$<c\,,T_m d^\sigma>_\infty = \lim_{s\to 1}\Big[\gamma^m_{N,s}(A) + \frac{2^{2-s}|D|^{s/2}\pi u}{N^s\prod_{p|N}(1+p^{-s})}\big(\sigma_1(m)+m^s\sigma_{1-2s}(m)\big)\frac{\zeta_K(s)}{\zeta(2s)}$$

$$+\frac{h_K\sigma_1(m)\kappa_N}{s-1}\Big] - h_K\sigma_1(m)\lambda_N + 2h_K\sigma_1(m)\kappa_N \quad .$$

Substituting into this the expansion

$$\zeta_K(s) = \zeta(s)L(s,\varepsilon) \qquad (\varepsilon(n) = (\tfrac{D}{n}))$$

$$= \left(\frac{1}{s-1} + \gamma + O(s-1)\right)\left(L(1,\varepsilon) + L'(1,\varepsilon)(s-1) + O(s-1)^2\right)$$

and the formula $L(1,\varepsilon) = \pi h_K/u\sqrt{|D|}$, we obtain

Proposition 4.2. Let $x \in X_0(N)$ be a Heegner point for the full ring of integers of an imaginary quadratic field K, $c = (x) - (\infty)$, $d = (x) - (0)$, $\sigma \in \mathrm{Gal}(H/K)$, $m \in \mathbb{N}$ prime to N, and $\mathcal{A} \in \mathrm{Cl}_K$ the ideal class corresponding to σ under the Artin isomorphism. Suppose m is not the norm of an integral ideal in $\mathcal{A}$. Then

$$\langle c, T_m d^\sigma\rangle_\infty = \lim_{s\to 1}\left[\gamma^m_{N,s}(\mathcal{A}) - \frac{h_K\sigma_1(m)\kappa_N}{s-1}\right]$$

$$+ h_K\kappa_N\left[\left(\log\frac{N}{|D|} + 2\sum_{p|N}\frac{\log p}{p^2-1} + 2 + 2\frac{\zeta'}{\zeta}(2) - 2\frac{L'}{L}(1,\varepsilon)\right)\sigma_1(m)\right.$$

$$\left. + \sum_{d|m} d \log\frac{m}{d^2}\right]$$

with $\gamma^m_{N,s}(\mathcal{A})$ as in Corollary 3.17. Here D, h_K and $L(s,\varepsilon)$ denote the discriminant, class number and L-function of K and κ_N the constant defined in (2.13).

§5. Modifications when $r_{\mathcal{A}}(m) \neq 0$.

Since the point x occurs with multiplicity $r_{\mathcal{A}}(m)$ in the divisor $T_m(x^\sigma)$, the divisors c and $T_m d^\sigma$ are not relatively prime in the case when $r_{\mathcal{A}}(m) \neq 0$. Although the global height pairing $\langle c, T_m d^\sigma\rangle$ is well-defined, Néron's theory does not give a canonical decomposition into local terms $\langle c, T_m d^\sigma\rangle_v$. We will first discuss how a local symbol can be defined by choosing a tangent vector at x, then calculate this symbol when v is an archimedean place of H.

We recall a procedure for defining a local symbol for two divisors a and b of degree zero on a general curve X over H, whose common support is equal to the point x [14]. Let g be any uniformizing parameter at x, i.e., any function on X with $\mathrm{ord}_x(g) = 1$, and define

$$(5.1) \qquad \langle a,b\rangle_v = \lim_{y\to x}\left\{\langle a_y,b\rangle_v - \mathrm{ord}_x(a)\,\mathrm{ord}_x(b)\log|g(y)|_v\right\},$$

where a_y is the divisor obtained from a by replacing every occurrence of the point x in a by a nearby point y which does not occur in b. This limit exists by the standard properties of local heights. If g' is another uniformizing parameter and g/g' has the value α at x, then

$$(5.2) \qquad \langle a,b\rangle'_v = \langle a,b\rangle_v + \mathrm{ord}_x(a)\,\mathrm{ord}_x(b)\log|\alpha|_v .$$

In particular, the sum $\sum_v \langle a,b\rangle_v$ is independent of the choice of g, by the product formula; this sum is equal to the global height pairing of the classes a and b [14].

Let $\frac{\partial}{\partial t}$ be the non-zero tangent vector at x which is determined by $\frac{\partial g}{\partial t} = 1$. Another consequence of (5.2) is that the local symbol $\langle a,b\rangle_v$ depends only on the tangent vector $\frac{\partial}{\partial t}$ and not by the full choice of g. By (5.2), this pairing is unchanged if we multiply $\frac{\partial}{\partial t}$ by a root of unity α, since $|\alpha|_v = 1$ for all v.

We now apply this procedure to the computation of the local symbols $\langle c,T_m d^\sigma\rangle_v$ on $X_0(N)$. We have $\mathrm{ord}_x(c) = 1$ and $\mathrm{ord}_x(T_m d^\sigma) = r_{\mathcal{A}}(m)$; if g is a uniformizing parameter at x, then

$$(5.3) \qquad \langle c,T_m d^\sigma\rangle_v = \lim_{y\to x}\left\{\langle c_y,T_m d^\sigma\rangle_v - r_{\mathcal{A}}(m)\log|g(y)|_v\right\},$$

where $c_y = (y) - (\infty)$. The trick is to normalize the function g at x so as to make the computation of each local symbol as simple as possible. To do this, we introduce the differential

$$(5.4) \qquad \omega = \eta^4(z)\,\frac{dq}{q} = 2\pi i\,\eta^4(z)\,dz ,$$

where $\eta(z) = q^{\frac{1}{24}}\prod_n(1-q^n)$ is the Dedekind eta-function. This differential is well-defined only up to a 6th root of unity, but this will be sufficient for our purposes by the remark above. If x is not an elliptic point on $X_0(N)$, so $u = 1$, then ω is non-zero at x and we may take our tangent vector $\frac{\partial}{\partial t}$ to be dual to ω. The uniformizing parameter g then satisfies

$$\omega = (g + a_2 g^2 + a_3 g^3 + \dots)\,\frac{dg}{g}$$

in a neighborhood of x. In general, ω has order $\frac{1}{u}-1$ at x and we may normalize g so that

$$\omega = (\, g^{1/u} + \text{higher degree terms}\,)\,\frac{dg}{g}$$

in a neighborhood of x. The reasons for this normalization will become clearer when we compute the heights at non-archimedean places in the next chapter. Here we observe that for a complex place v we have

$$\log|g(y)|_v - u\log|\,2\pi i\,\eta^4(z)\,(w-z)|_v \longrightarrow 0 \tag{5.5}$$

as $y\to x$, where z and w are points in the upper half-plane which map to x and y on $X_0(N)(\mathbb{C})$.

From Proposition 2.23 and the formulas (5.3), (5.5) we find

$$\begin{aligned} <c,T_m d^\sigma>_v = \lim_{s\to 1}\Bigg[& \sum_{\substack{\gamma\in R_N/\pm 1\\ \det\gamma=m\\ \gamma z'\neq z}} g_s(z,\gamma z') + 4\pi\sigma_1(m)E_N(w_N z,s) \\ & + u\,r_A(m)\lim_{w\to z}\Big\{ g_s(z,w) - \log|2\pi i\,\eta^4(z)\,(w-z)|_v\Big\} \\ & + 4\pi m^s\sigma_{1-2s}(m)E_N(z',s) + \frac{\sigma_1(m)\kappa_N}{s-1}\Bigg] - \sigma_1(m)(\lambda_N+2\kappa_N)\,, \end{aligned} \tag{5.6}$$

$$(\, z, z' \text{ points in } H \text{ mapping to } x, x^\sigma\,)$$

because in the terms $g_s(w,\gamma z')$ with $\gamma z'\neq z$ and in the term $E_N(w_N w,s)$ we can carry out the limit $w\to z$ simply by replacing w by z, and there are $u\,r_A(m)$ values of γ with $\gamma z'=z$. Formula (5.6) is identical to the formula in Proposition 2.23 if we define $G^m_{N,s}(z,z')$ (which was previously defined only if $z\notin T_m z'$) for all $z,z'\in H$ by

$$\begin{aligned} G^m_{N,s}(z,z') = & \sum_{\substack{\gamma\in R_N/\pm 1\\ \det\gamma=m\\ \gamma z'\neq z}} g_s(z,\gamma z') \\ & + \sum_{\substack{\gamma\in R_N/\pm 1\\ \det\gamma=m\\ \gamma z'=z}} \lim_{w\to z}\Big(g_s(z,w) - \log|2\pi i\,\eta(z)^4(z-w)|^2\Big)\,. \end{aligned} \tag{5.7}$$

Hence Proposition 4.2 is true without the restriction $r_A(m)=0$, provided that we define $\gamma^m_{N,s}(A)$ by (3.3) but with the new definition of $G^m_{N,s}$. In calculating this invariant, we find that the terms in (5.7) with $\gamma z'\neq z$ give exactly the expression in §3 and that their total contribution to $\gamma^m_{N,s}(A)$ is the infinite sum in Proposition 3.11 (the condition $\gamma z'\neq z$ translates into the condition $n>0$ in this sum). The second sum in (5.7) equals $t g_s(z)$, where t is the number of $\gamma\in R_N/\pm 1$ of determinant m with $\gamma z'=z$ (for z, z' as in (5.6) this number is $u r_A(m)$) and $g_s(z)$ is the renormalized value of $g_s(z,z)$ defined by the limit in (5.7). Using the asymptotic expansion

$$Q_{s-1}(t) = \frac{1}{2}\log\frac{t+1}{t-1} - \Big(\frac{\Gamma'}{\Gamma}(s) - \frac{\Gamma'}{\Gamma}(1)\Big) + o(1) \qquad (\, t\searrow 1\,)$$

we find

$$g_s(z) = -\log|2\pi\,(z-\bar z)\,\eta(z)^4|^2 + 2\frac{\Gamma'}{\Gamma}(s) - 2\frac{\Gamma'}{\Gamma}(1)\,.$$

By Kronecker's first limit formula, this is equivalent to

$$g_s(z) = -2\log 2\pi + 2\frac{\Gamma'}{\Gamma}(s) + 2\frac{\Gamma'}{\Gamma}(1) + \frac{2}{\pi}\lim_{\sigma\to 1}\Big[\, 2^\sigma\zeta(2\sigma)E(z,\sigma) - \frac{\pi}{\sigma-1}\Big]\,,$$

where $E(z,s)$ as usual denotes the Eisenstein series of weight zero on $SL_2(\mathbb{Z})$. The identity $2^s\zeta(2s)E(\tau_A,s)=u|D|^{s/2}\zeta_K(A,s)$ mentioned in §4 now gives

$$\begin{aligned} \sum_{A\in Cl_K} g_s(\tau_A) &= 2h\Big[\frac{\Gamma'}{\Gamma}(s) + \frac{\Gamma'}{\Gamma}(1) - \log 2\pi\Big] + \lim_{\sigma\to 1}\Big[\frac{2u}{\pi}|D|^{\sigma/2}\zeta_K(\sigma) - \frac{2h}{\sigma-1}\Big] \\ &= 2h\Big[\frac{\Gamma'}{\Gamma}(s) - \log 2\pi + \frac{L'}{L}(1,\varepsilon) + \frac{1}{2}\log|D|\ \Big]\,. \end{aligned}$$

The total contribution to $\gamma^m_{N,s}(A)$ of the terms with $\gamma z'=z$ is the product of this with the number $t=ur_A(m)$. Summarizing, we have:

<u>Proposition 5.8.</u> <u>Proposition 4.2 remains true when</u> m <u>is the norm of an ideal in</u> A, <u>provided that the local symbols</u> $<c,T_m d^\sigma>_v$ <u>in the definition of</u> $<c,T_m d^\sigma>_\infty$ <u>are defined by (5.3) with the choice of</u> g <u>explained above and the invariant</u> $\gamma^m_{N,s}(A)$ <u>is defined by (3.3) with</u> $G^m_{N,s}$ <u>as in (5.7). This invariant is given by</u>

$$\gamma^m_{N,s}(A) = \Big(\begin{matrix}\text{expression in}\\ \text{Corollary 3.17}\end{matrix}\Big) + 2hur_A(m)\Big(\frac{\Gamma'}{\Gamma}(s) - \log 2\pi + \frac{L'}{L}(1,\varepsilon) + \frac{1}{2}\log|D|\Big)\,.$$

Chapter III. Non-archimedean local heights

In this chapter we will compute the local symbols $\langle c,T_m d^{\sigma}\rangle_v$ for all non-rchimedean places v of H, always under the assumption that m is prime to N. Assume that v divides the rational prime p; let Λ_v denote the ring of ntegers in the completion H_v, π a uniformizing parameter in Λ_v, and $q = p^f$ the cardinality of the residue field Λ_v/π. Let W denote the comple-ion of the maximal unramified extension of Λ_v; then π is a prime element in W and $F = W/\pi$ is an algebraic closure of Λ_v/π.

We first reduce the calculation of Néron's local symbols $\langle a,b\rangle_v$ on rela-ively prime divisors of degree zero on X over H_v to a problem in arithmetic ntersection theory. Let $\underline{X}$ be a regular model for X over Λ_v, and let A nd B be divisors on $\underline{X}$ which restrict to a and b on the general fibre. f A has zero intersection with every fibre component of $\underline{X}$, we have the ormula [14]

$$(0.1) \qquad \langle a,b\rangle_v = -(A \cdot B)\log q .$$

In the next section we will describe a regular model $\underline{X}$ for X over $\mathbf{Z}$ hich has a modular interpretation; we will then discuss the reduction of eegner points on $\underline{X}$ and use (0.1) to obtain the intersection formula

$$(0.2) \qquad \langle c,T_m d^{\sigma}\rangle_v = -(\underline{x} \cdot \underline{T_m x}^{\sigma})\log q ,$$

where $\underline{x}$ and $\underline{x}^{\sigma}$ are the sections of $\underline{X} \otimes \Lambda_v$ corresponding to the points x and x^{σ} over H.

The rest of the chapter is devoted to a calculation of the intersection product $(\underline{x} \cdot \underline{T_m x}^{\sigma})$, which is unchanged if we extend scalars to W. We first identify the components of the divisor $\underline{T_m x}^{\sigma}$, then establish the formula

$$(0.3) \qquad (\underline{x} \cdot \underline{T_m x}^{\sigma}) = \frac{1}{2}\sum_{n\geq 1} \operatorname{Card} \operatorname{Hom}_{W/\pi^n}(\underline{x},\underline{x}^{\sigma})_{\text{degree } m}$$

where $\operatorname{Hom}_{W/\pi^n}(\underline{x},\underline{x}^{\sigma})$ is a suitable group of homomorphisms between the diagrams of elliptic curves representing $\underline{x}$ and $\underline{x}^{\sigma}$.

Using (0.3) and Deuring's results on singular liftings of ordinary elliptic curves, we show that $(\underline{x} \cdot \underline{T_m x}^{\sigma}) = 0$ when p is split in K. When p is non-split in K, the curves corresponding to $\underline{x}$ and $\underline{x}^{\sigma}$ have supersingular reduction and the groups $\operatorname{Hom}_{W/\pi^n}(\underline{x},\underline{x}^{\sigma})$ can be calculated using the arithmetic of certain orders in the definite quaternion algebra over $\mathbf{Q}$ of discriminant p. Next we discuss the modifications necessary in the computation of $\langle c,T_m d^{\sigma}\rangle_v$ when the divisors c and $T_m d^{\sigma}$ are <u>not</u> relatively prime. Finally, we make the orders in our quaternion algebras completely explicit and obtain a formula for $\sum_{v|p}\langle c,T_m d^{\sigma}\rangle_v$ in terms of the ideal theory of $\mathcal{O}$. For example, when $r_{\mathcal{A}}(m) = 0$ and p is inert in $\mathcal{O}$, our final formula is

$$\sum_{v|p}\langle c,T_m d^{\sigma}\rangle_v = -u^2\log p \sum_{\substack{0<n<\frac{m|D|}{N} \\ n\equiv 0 \pmod p}} \operatorname{ord}_p(pn)\, r_{\mathcal{A}}(m|D|-nN)\,\delta(n)\, R_{\{\mathcal{A}\mathfrak{q}\mathfrak{r}\}}(n/p)$$

where $\mathfrak{q}$ is an ideal of $\mathcal{O}$ with $\left(\frac{N\mathfrak{q}}{\ell}\right) = \left(\frac{-p}{\ell}\right)$ for all primes $\ell | D$.

Because we must treat all non-archimedean places of H , including those dividing N , m , or D where there are some complications, the argument often becomes fairly intricate. Here we will illustrate the main ideas in the case where $m = 1$ and v divides a rational prime p which is prime to ND . We shall also assume that $r_A(1) = 0$, so $\sigma \neq 1$ and the points x and x^σ are distinct over H .

By (0.2) and (0.3) we have

$$(0.4) \qquad \langle (x) - (\infty), (x^\sigma) - (0) \rangle_v = \langle c, d^\sigma \rangle_v$$

$$= -\frac{1}{2} \sum_{n \geq 1} \mathrm{Card}(\mathrm{Isom}_{W/\pi^n}(\underline{x}^\sigma, \underline{x})) \log q_v$$

The sum in (0.4) is zero unless $\underline{x}$ and $\underline{x}^\sigma$ intersect (mod π) . Deuring's theory shows $(\underline{x} \cdot \underline{x}^\sigma) = 0$ when p splits in K ; since we are assuming that $(p,D) = 1$ we must have p inert in K and hence $\log q_v = 2 \log p$. The endomorphism ring R of $\underline{x}$ (mod π) is an Eichler order of index N in the definite quaternion algebra B of discriminant p , and the group $\mathrm{Hom}_{W/\pi}(\underline{x}^\sigma, \underline{x})$ is isomorphic to the left R-module RA . The points $\underline{x}$ and $\underline{x}^\sigma$ will intersect (mod π) if and only if this module is principal; if this is so, the integer $\mathrm{Card}(\mathrm{Isom}_{W/\pi}(\underline{x}^\sigma, \underline{x}))$ is the number of generators.

Each generator gives a solution to a certain equation in ideals of $\mathcal{O}$, as we will now show. Let q be a prime with $q \equiv -p \pmod{D}$; then $(q) = \mathfrak{q} \cdot \bar{\mathfrak{q}}$ splits in the field K and B is the algebra $K + Kj$ with the relations $j\alpha = \bar{\alpha} j$ for $\alpha \in K$ and $j^2 = -pq$. Using reduction theory, one can show that for some place v dividing p the order R is given by the set of all $\alpha + \beta j \in B$ with $\alpha \in \mathcal{D}^{-1}$, $\beta \in \mathcal{D}^{-1}\mathfrak{q}^{-1}\mathfrak{n}$, and $\alpha - \beta$ is integral at all primes dividing $\mathcal{D}$. If $\mathfrak{a}$ is an ideal in the class of A , then

$$(0.5) \qquad \mathrm{Hom}_{W/\pi}(\underline{x}^\sigma, \underline{x}) \simeq R\mathfrak{a} = \{\alpha + \beta j : \alpha \in \mathcal{D}^{-1}\mathfrak{a},\ \beta \in \mathcal{D}^{-1}\mathfrak{q}^{-1}\mathfrak{n}\bar{\mathfrak{a}},\ \alpha - \beta \text{ integral at } \mathcal{D}\}.$$

This module is principal if and only if it contains an element $b = \alpha + \beta j$ with reduced norm $\mathrm{N}b = \mathrm{N}\alpha + pq\mathrm{N}\beta = \mathrm{N}\mathfrak{a}$. Assume b is a generator; if we define the integral ideals

$$(0.6) \qquad \begin{aligned} \mathfrak{c} &= (\alpha)\mathcal{D}\mathfrak{a}^{-1}, \\ \mathfrak{c}' &= (\beta)\mathcal{D}\mathfrak{q}\mathfrak{n}^{-1}\bar{\mathfrak{a}}^{-1}, \end{aligned}$$

these satisfy the identity

$$(0.7) \qquad \mathrm{N}\mathfrak{c} + pN\,\mathrm{N}\mathfrak{c}' = |D| .$$

Letting $n = pNr'$ and $\ell = Nr$, we have a solution to the equation $\ell + nN = |D|$ with $n \equiv 0 \pmod p$ and $r_A(\ell) \neq 0$. Conversely, such solutions will yield generators for $R\mathfrak{a}$ and contribute to the height in (0.4). We remark that this method is quite similar to that used in evaluating $G_{N,s}$ at Heegner points in Chapter II. Indeed the function $\rho^m(n)$ introduced in Proposition 3.11 of Chapter II counts certain elements of norm m in an Eichler order of discriminant N in the split quaternion algebra over $\mathbb{Q}$.

§1. The curve $X_0(N)$ over $\mathbb{Z}$

A model $\underline{X}$ for $X_0(N)$ over $\mathbb{Z}$ was proposed by Deligne-Rapoport [7], and given a modular interpretation when N was square-free. The general case was treated by Katz-Mazur [21], using ideas of Drinfeld [9]. We review this theory below.

Let $\mathcal{M}_{\Gamma_0(N)}$ be the algebraic stack classifying cyclic isogenies of degree N between generalized elliptic curves over S

$$\phi : E \to E' \tag{1.1}$$

such that the group scheme $A = \ker\phi$ meets every irreducible component of each geometric fibre. The condition that ϕ is cyclic of degree N means that locally on S there is a point P such that

$$A = \sum_{a=1}^{N} [aP] \tag{1.2}$$

as Cartier divisors on E. When N is invertible on S, this hypothesis is equivalent to the assumption that A is locally isomorphic to $\mathbb{Z}/N$; when N is square-free it is equivalent to the assumption that A is locally free of rank N.

Let $\underline{X}$ be the coarse moduli scheme associated to the stack $\mathcal{M}_{\Gamma_0(N)}$ ([9], 234-243, [21] 407ff). The scheme $\underline{X} \otimes \mathbb{Z}[1/N]$ is smooth and proper over $\mathbb{Z}[1/N]$. On the other hand, if p is a prime dividing N, the scheme $\underline{X} \otimes \mathbb{Z}/p$ is both singular and reducible over $\mathbb{Z}/p$. We will need a modular interpretation of its irreducible components. Write $N = p^n M$ with $(p,M) = 1$. Then

$\underline{X} \otimes \mathbb{Z}/p$ has (n+1)-irreducible components $\mathcal{F}_{a,b}$, indexed by pairs of non-negative integers with $a + b = n$. The component $\mathcal{F}_{a,b}$ is isomorphic to $\underline{X}_0(M) \otimes \mathbb{Z}/p$, and occurs with multiplicity $\phi(p^c)$ in $\underline{X} \otimes \mathbb{Z}/p$, where $c = \min(a,b)$. In terms of the modular equation, this decomposition of the fibre is reflected in Kronecker's congruence

$$\phi_N(j,j') \equiv \prod_{\substack{a+b=n \\ c=\min(a,b)}} \phi_M\left(j^{p^{a-c}}, j'^{p^{b-c}}\right)^{\phi(p^c)} \pmod p$$

All of the components $\mathcal{F}_{a,b}$ intersect at each supersingular point of $\underline{X}$ over F: these are the points $x = (\phi : E \to E')$ where E and E' are supersingular elliptic curves. The non-supersingular points of $\mathcal{F}_{a,b}$ over F correspond to diagrams where the groupscheme $A = \ker\phi$ is isomorphic to $\mu_{p^a} \times \mathbb{Z}/p^b \times \mathbb{Z}/M$.

For a geometric point $\underline{x} = (\phi : E \to E')$ of $\underline{X}$ over an algebraically closed field k, we define $\mathrm{Aut}_k(\underline{x})$ to be the group of all isomorphisms (f,f') which make the diagram

(1.3)
$$\begin{tikzcd} E \arrow[r, "\phi"] \arrow[d, "f"', "\wr"] & E' \arrow[d, "\wr", "f'"'] \\ E \arrow[r, "\phi'"] & E' \end{tikzcd}$$

commutative. This is a finite group, which contains $\langle \pm 1 \rangle$; it may also be de-

scribed as the automorphism group of the pair (E,A). The strict Henselization of $\underline{X}$ at the point $\underline{x}$ is isomorphic to the quotient of the strict Henselization of $\mathcal{M}_{\Gamma_0(N)}$ at the corresponding point m by the group $\mathrm{Aut}_k(\underline{x})/\langle \pm 1 \rangle$ [7, p. 172]. Using this fact, and results of Drinfeld [9] and Katz-Mazur [21, p. 166], one obtains the following

<u>Proposition 1.4</u> <u>$\underline{X}$ is regular over $\mathbb{Z}$, except at the supersingular points $\underline{x}$ in characteristics</u> $p|N$ <u>where</u> $\mathrm{Aut}_F(\underline{x}) \neq \langle \pm 1 \rangle$.

The subscheme <u>Cusps</u> of $\underline{X}$ is finite over $\mathbb{Z}$, with one irreducible component <u>Cusp</u>(d) for each positive divisor d of N. The component <u>Cusp</u>(d) corresponds to diagrams of Néron polygons where $A = \ker\phi$ is isomorphic to $\mu_d \times N\mathbb{Z}/d\mathbb{Z}$. It has $\phi(f)$ geometric points, where $f = \gcd(d,N/d)$, and one has an isomorphism <u>Cusp</u>(d) $\simeq \mathrm{Spec}\,\mathbb{Z}[\mu_f]$.

The section $\underline{\infty}$ of $\underline{X}$ is the component <u>Cusp</u>(N) and the section $\underline{0}$ is the component <u>Cusp</u>(1). These sections reduce to the components $\mathcal{F}_{n,0}$ and $\mathcal{F}_{0,n}$ in characteristic p respectively. In general, the reduction of the multi-section Cusp(d) lies on the component $\mathcal{F}_{a,b} \pmod p$, where $a = \mathrm{ord}_p(d)$ [21, Chapter 10].

§2. <u>Homomorphisms</u>

Let S be a complete local ring with algebraically closed residue field k, and let $\underline{x} = (\phi : E \to E')$ and $\underline{y} : (\psi : F \to F')$ be two S-valued points of $\underline{X}$ which are represented by diagrams of cyclic N-isogenies. Assume further that the points $\underline{x}$ and $\underline{y}$ have non-cuspidal reduction. We define the group $\mathrm{Hom}_S(\underline{y},\underline{x})$ to be set of all homomorphisms (f,f') over S which make the diagram

(2.1)
$$\begin{tikzcd} F \arrow[r, "\psi"] \arrow[d, "f"'] & F' \arrow[d, "f'"] \\ E \arrow[r, "\phi"'] & E' \end{tikzcd}$$

commutative. Addition of homomorphisms is defined using the group laws in E and E'. Then $\mathrm{Hom}_S(\underline{y},\underline{x})$ is a left module over the ring $\mathrm{End}_S(\underline{x}) = \mathrm{Hom}_S(\underline{x},\underline{x})$, and a right module over $\mathrm{End}_S(\underline{y})$; in these rings multiplication is defined by composition of homomorphisms. Using the fact that k is algebraically closed, one can check that the definition of $\mathrm{Hom}_S(\underline{y},\underline{x})$ is independent of the diagrams chosen to represent the points $\underline{x}$ and $\underline{y}$.

The ring $\mathrm{End}_S(\underline{x})$ is either $\mathbb{Z}$, an order in an imaginary quadratic field, or an order in a definite quaternion algebra of prime discriminant over $\mathbb{Q}$ [8]. We define the degree of a non-zero element (f,f') in $\mathrm{Hom}_S(\underline{y},\underline{x})$ to be the positive integer $\deg f = \deg f'$. Then the set of elements $\mathrm{Hom}_S(\underline{y},\underline{x})_{\deg m}$ of a fixed degree $m \geq 1$ is finite, and admits a faithful action by the finite group $\mathrm{Aut}_S(\underline{x}) = \mathrm{End}_S(\underline{x})_{\deg 1}$.

§3. Heights and intersection products

Let $x = (\phi : E \to E')$ be a Heegner point of discriminant D on X over H, and let $\underline{x}$ denote the corresponding section of $\underline{X} \otimes \Lambda_v$. We recall that Λ_v is the ring of integers in the completion H_v, and that the place v has residual characteristic p.

Since N is prime to $D^h = \mathrm{disc}(H/\mathbb{Q})$, the special fibre $\underline{X} \otimes \Lambda_v$ has the shape described in §1. Since elliptic curves with complex multiplication have potentially good reduction, the sections $\underline{x}$ and $\underline{x}^\sigma$ do not intersect the divisor Cusps in the special fibre. They reduce to supersingular points if and only if the rational prime p is not split in K [29].

Now suppose p divides N; then p is split in K and $\underline{x}$ and $\underline{x}^\sigma$ have ordinary reduction $(\mathrm{mod}\ \pi)$. We wish to determine the component $\mathcal{F}_{a,b}$ of the special fibre which contains the reduction of $\underline{x}$. Let $\mathfrak{n} \subset \mathcal{O}$ be the ideal annihilating $\ker\phi$; since this isogeny is cyclic of degree N, we have $\mathcal{O}/\mathfrak{n} \simeq \mathbb{Z}/N$. Hence the place v divides $\mathfrak{n}$ or $\bar{\mathfrak{n}}$, but not both.

<u>Proposition 3.1</u> <u>The sections $\underline{x}$ and $\underline{x}^\sigma$ reduce to ordinary points in the component</u> $\mathcal{F}_{0,n}$ <u>if</u> $v|\bar{\mathfrak{n}}$

$\mathcal{F}_{n,0}$ if $v|\mathfrak{n}$.

<u>Proof</u>. If $v|\bar{\mathfrak{n}}$ the group scheme $\ker\phi$ is étale over Λ_v, so is isomorphic to $\mathbb{Z}/N$ over F. Hence the reduction lies in $\mathcal{F}_{0,n}$, the component containing $\underline{\mathrm{Cusp}(1)} = \underline{0}$. If $v|\mathfrak{n}$ the group scheme $\ker\phi$ is isomorphic to $\mu_{p^n} \times \mathbb{Z}/M$ over F, so the reduction of $\underline{x}$ lies in the component $\mathcal{F}_{n,0}$ containing $\underline{\mathrm{Cusp}}(N) = \underline{\infty}$. Since σ fixes K, the kernel of the isogeny $(\phi^\sigma : E^\sigma \to E'^\sigma)$ defining $\underline{x}^\sigma$ is also annihilated by $\mathfrak{n}$. Hence $\underline{x}^\sigma$ reduces to the same component as $\underline{x}$.

<u>Corollary 3.2</u> <u>One of the divisors $\underline{c} = (\underline{x}) - (\underline{\infty})$, $\underline{d} = (\underline{x}^\sigma) - (\underline{0})$ has zero intersection with every fibral component</u> $\mathcal{F}_{a,b}$ of $\underline{X} \otimes \Lambda$.

<u>Proof</u>. Indeed, $\underline{c}$ has this property if $v|\mathfrak{n}$, and $\underline{d}$ has this property if $v|\bar{\mathfrak{n}}$. Since v divides $\mathfrak{n} \cdot \bar{\mathfrak{n}} = N$, one of these possibilities must occur.

We now return to the general case, and reduce the calculation of the local height symbol to that of an arithmetic intersection product.

Proposition 3.3 *Assume* $m \geq 1$ *is prime to* N and $r_A(m) = 0$. *Then we have the formula*

$$\langle c, T_m d^\sigma \rangle_v = -(\underline{x} \cdot T_m \underline{x}^\sigma) \log q$$

Proof. By resolving the quotient singularities at the supersingular points on $\underline{X}$ over $\mathbb{Z}$, we may obtain a regular model $\underline{X}^{reg}$. Neither the Heegner points nor the cusps are affected by this resolution, so by Corollary 3.2, one of the divisors $\underline{c}$ and $\underline{d}$ have zero intersection with each fibral component of $\underline{X}^{reg} \otimes \Lambda_v$. The same is true for $\underline{c}$ and $T_m \underline{d}$, as the Hecke operators preserve fibral components when m is prime to N . The general theory of heights then gives the identity (cf. (0.1))

$$\langle c, T_m d^\sigma \rangle_v = -(\underline{c} \cdot T_m \underline{d}^\sigma) \log q$$

We now use the additivity of the intersection product to obtain

$$(\underline{c} \cdot T_m \underline{d}^\sigma) = (\underline{x} \cdot T_m \underline{x}^\sigma) - (\underline{x} \cdot T_m \underline{0}) - (\underline{\infty} \cdot T_m \underline{x}^\sigma) + (\underline{\infty} \cdot \underline{0})$$

But $(\underline{x} \cdot T_m \underline{0}) = (\underline{\infty} \cdot T_m \underline{x}^\sigma) = 0$, as $\underline{x}$ and the points $\underline{y}$ in the divisor $T_m \underline{x}^\sigma$ have potentially good reduction, and $(\underline{\infty} \cdot \underline{0}) = 0$ as we have assumed that $N > 1$. This completes the proof.

§4. An intersection formula

In the computation of the product $(\underline{x} \cdot T_m \underline{x}^\sigma)$ in Proposition 3.3 , we may extend scalars to $\underline{X} \otimes_\Lambda W$, where W is the completion of the maximal unramified extension of Λ . We may then apply the considerations of §2 to the points $\underline{x}$ and $\underline{x}^\sigma$ over the complete local rings W and W/π^n for $n \geq 1$, as these have an algebraically closed residue field $\mathbb{F} = W/\pi$.

For example, we have

$$(4.1) \qquad \mathrm{End}_W(\underline{x}) = \mathrm{End}_W(\underline{x}^\sigma) = \mathcal{O}$$

$$(4.2) \qquad \mathrm{Hom}_W(\underline{x}^\sigma, \underline{x}) \simeq A \quad \text{as a left } \mathcal{O}\text{-module}$$

where A is the ideal class of K which corresponds to σ under the Artin isomorphism. Formula (4.2) is usually proved by embedding W into $\mathbb{C}$ and using the theory of lattices [23]. A direct algebraic proof was given by Serre [29] where the curves E^σ and E'^σ in $\underline{x}^\sigma$ are denoted $\mathrm{Hom}(\mathfrak{a}, E)$ and $\mathrm{Hom}(\mathfrak{a}, E')$ respectively, for an ideal $\mathfrak{a}$ in the class of A .

If we identify the elements g_α in $\mathrm{Hom}_W(\underline{x}^\sigma, \underline{x})$ with elements α in the ideal $\mathfrak{a}$, then the degree of the isogeny g_α is equal to $N\alpha/N\mathfrak{a}$. We have the following refinement of Proposition 8.1 of Chapter I. Assume as usual that m is prime to N .

Proposition 4.3 *The multiplicity of the point* x *in the divisor* $T_m x^\sigma$ *is equal to* $r_A(m)$.

<u>Proof</u>. By the definition of T_m ((2.3) of Chapter I), the multiplicity of x in $T_m x^\sigma$ is equal to the number of isogenies g_α of degree m in $\mathfrak{a} \simeq \mathrm{Hom}_W(\underline{x}^\sigma,\underline{x}) = \mathrm{Hom}_{\overline{H}}(x^\sigma,x)$, modulo the left action of the group $\mathcal{O}^* \simeq \mathrm{Aut}_W(\underline{x})$ which identifies isogenies with the same kernel C. This number is therefore equal to the number of integral ideals $\mathfrak{b} = (\alpha)/\mathfrak{a}$ of norm m in the class of A^{-1}, or equivalently to the number $r_A(m)$ of integral ideals $\bar{\mathfrak{b}} = (\bar{\alpha})/\bar{\mathfrak{a}}$ of norm m in the class of A.

In the next two sections we shall establish the following intersection formula (0.3).

<u>Proposition 4.4</u> <u>Assume</u> m <u>is prime to</u> N <u>and</u> $r_A(m) \neq 0$. <u>Then</u>

$$(\underline{x} \cdot T_m \underline{x}^\sigma) = \frac{1}{2} \sum_{n\geq 1} \mathrm{Card}(\mathrm{Hom}_{W/\pi^n}(\underline{x}^\sigma,\underline{x})_{\deg m})$$

Since the reduction of homomorphisms gives an injection ([30], [15])

$$(4.5)\qquad \begin{cases} \mathrm{Hom}_{W/\pi^{n+1}}(\underline{x}^\sigma,\underline{x}) \hookrightarrow \mathrm{Hom}_{W/\pi^n}(\underline{x}^\sigma,\underline{x}) & \text{for } n \geq 1, \\ \text{and } \mathrm{Hom}_W(\underline{x}^\sigma,\underline{x}) = \bigcap_{n\geq 1} \mathrm{Hom}_{W/\pi^n}(\underline{x}^\sigma,\underline{x}) & , \end{cases}$$

the terms in the sum (4.4) are all zero for n sufficiently large. We shall henceforth use the notation $h_n(\underline{y},\underline{x})_{\deg m}$ for the integer

$$\frac{1}{2}\mathrm{Card}\ \mathrm{Hom}_{W/\pi^n}(\underline{y},\underline{x})_{\deg m}\ .$$

§5. <u>The divisor</u> $T_m \underline{x}^\sigma$

To prove Proposition 4.4 we need a concrete description of the components of the divisor $T_m \underline{x}^\sigma$ over W, and some knowledge of their intersection products. To obtain this, we will use the theory of canonical and quasi-canonical liftings, as developed in [15].

Since m is prime to N, the points y in the divisor $T_m x^\sigma$ are all Heegner points over $\overline{H}$ in the sense of [13] and $\mathrm{End}_H(y) = \mathcal{O}_y$ is an order of conductor dividing m in K. When m is prime to p, the residual characteristic of v, the points y are all rational over $W \otimes \mathbb{Q}_p$ and each is the canonical lifting of its reduction $\underline{y}$ [15, 31]. In this case, we also have the formula

$$(5.1)\qquad h_n(\underline{x}^\sigma,\underline{x})_{\deg m} = \sum_{\underline{y}\in T_m \underline{x}^\sigma} h_n(\underline{y},\underline{x})_{\deg 1}\ ,$$

as any isogeny f of degree m between $\underline{x}^\sigma$ and $\underline{x}$ over W/π^n is determined by its kernel, which lefts uniquely to a group scheme C of order m on $\underline{x}^\sigma$ over W. Then f induces an isomorphism between $\underline{y} = \underline{x}_C^\sigma$ and $\underline{x}$ over W/π^n:

$$\begin{tikzcd} \underline{x}^\sigma \arrow[rr, "f"] \arrow[dr] & & \underline{x} \\ & \underline{x}_C^\sigma = \underline{y} \arrow[ur, "\wr"'] & \end{tikzcd}$$

Assume now that $m = p^t \cdot r$, where $t \geq 1$ and $(r,p) = 1$. The points z in the divisor $T_r x^\sigma$ are rational over $W \otimes \mathbb{Q}_p$ but the points y in the divisor $T_m x^\sigma = \sum_z T_{p^t}(z)$ are rational over ramified extensions of $W \otimes \mathbb{Q}_p$ and the corresponding sections $\underline{y}$ over the ring class extensions W_y are quasi-canonical liftings (of level p^s, with $0 \leq s \leq t$) of their reductions [15]. Let $\underline{y}(s)$ be the divisor over W obtained by taking the sum of a point of level s with all of its conjugates over W. We then have the decomposition

$$(5.2)\quad T_{p^t}\underline{z} = \begin{cases} \displaystyle\sum_{0\leq s\leq t}\ \sum_{j=1}^{t-s+1} \underline{y}(s)_j & \text{if } p \text{ splits in } K \\ & \deg \underline{y}(s) = p^s - p^{s-1} \qquad s \geq 1, \\ \displaystyle\sum_{\substack{0\leq s\leq t\\ s\equiv t(2)}} \underline{y}(s) & \text{if } p \text{ is inert in } K \\ & \deg \underline{y}(s) = p^s + p^{s-1} \qquad s \geq 1, \\ \displaystyle\sum_{0\leq s\leq t} \underline{y}(s) & \text{if } p \text{ is ramified in } K \\ & \deg \underline{y}(s) = p^s \qquad s \geq 0. \end{cases}$$

Eichler's congruence [11]

$$(5.3)\qquad T_{p^t} \equiv F^t + F^{t-1}F' + F^{t-2}F'^2 + \ldots + F'^t \pmod{p},$$

where F is the Frobenius correspondence and F' is its transpose, shows that each point $\underline{y}$ in the divisor $\underline{y}(s)$ is congruent $(\mathrm{mod}\ \pi_y)$ to a canonical lifting $\underline{y}_0$ of level zero over W. The fundamental negative congruence of

[15] then gives

$$(5.4)\qquad \underline{y} \not\equiv \underline{y}_0 \pmod{\pi_y^2} \quad \text{when } s \geq 1.$$

When p is split or ramified in K, the point y_0 occurs in $T_{p^t}z$.

§6. <u>Deformations and intersections</u>

<u>Proposition 6.1</u> <u>Let $\underline{x}$ and $\underline{y}$ be sections which intersect properly on X over W and reduce to regular, non-cuspidal points in the special fibre. Then</u>

$$(\underline{y}\cdot\underline{x}) = \sum_{n\geq 1} h_n(\underline{y},\underline{x})_{\deg 1}.$$

<u>Proof</u>. In the case when $\mathrm{Aut}_{W/\pi}(\underline{x}) = \langle\pm 1\rangle$, Proposition 6.1 follows from the fact that the completion of the local ring of $\underline{X}$ at $\underline{x}$ is the universal deformation space for the diagram $(\phi : E \to E')$ over W. Hence $(\underline{y}\cdot\underline{x}) = k$ if there is an isomorphism between $\underline{x}$ and $\underline{y}$ over W/π^k, but not over W/π^{k+1}. This agrees with the right hand side of (6.1), as

$$\tfrac{1}{2}\mathrm{Card}\ \mathrm{Hom}_{W/\pi^n}(\underline{y},\underline{x})_{\deg 1} = \begin{cases} 1 & n \leq k \\ 0 & n > k. \end{cases}$$

When $\mathrm{Aut}_{W/\pi}(\underline{x}) \neq \langle\pm 1\rangle$ one can modify the above using the local ring of the stack $\mathcal{M}_{\Gamma_0(N)}$. Alternatively, one can consider the pull-back of our situation to a modular cover $\underline{Y} \xrightarrow{f} \underline{X}$ over W where the corresponding objects are rigid. For example, $\underline{Y}$ could classify data of the type $(\phi : E \to E')$ together with a full level M structure, for an integer $M \geq 3$ which is prime to N and p. Here we do have the identity

$$(6.2) \qquad (\tilde{y} \cdot \tilde{x}) = \sum_{n\geq 1} \mathrm{Card}(\mathrm{Isom}_{W/\pi^n}(\tilde{y},\tilde{x}))$$

by the arguments above, where $\tilde{y}$ and $\tilde{x}$ are sections of $\underline{Y}$. Let $\tilde{y}$ be a section with $f(\tilde{y}) = \underline{y}$ and write $f^*(\underline{x}) = \sum_i (\tilde{x}_i)$ on $\underline{Y}$. By the general behavior of the intersection pairing under finite proper morphisms,

$$(\underline{y} \cdot \underline{x}) = (f_*\tilde{y},\underline{x}) = (\tilde{y},f^*\underline{x}) = \sum_i (\tilde{y},\tilde{x}_v).$$

Using (6.2) and re-arranging the sums, we find

$$(\underline{y} \cdot \underline{x}) = \sum_{n\geq 1} (\sum_i \mathrm{Card}(\mathrm{Isom}_{W/\pi^n}(\tilde{y},\tilde{x}_v)).$$

But $\sum_i \mathrm{Card}(\mathrm{Isom}_{W/\pi^n}(\tilde{y},x_i)) = \frac{1}{2}\mathrm{Card}(\mathrm{Hom}_{W/\pi^n}(\underline{y},\underline{x})_{\deg 1})$ which establishes the proposition.

The case $m = 1$ of Proposition 4.4 is an immediate corollary of 6.1, and the case where m is prime to p follows from Proposition 6.1 and formula (5.1). The real miracle occurs at the places v which divide m. Write $m = p^t \cdot r$ as in §5. We split into three cases, depending on the behavior of p in K.

When p splits in K, Proposition 4.4 follows from the fact that both sides of the identity are equal to zero. The right hand side vanishes because $\underline{x}$ and $\underline{x}^\sigma$ have ordinary reduction, so Deuring's theory [8] gives an isomorphism $\mathrm{Hom}_W(\underline{x}^\sigma,\underline{x}) \simeq \mathrm{Hom}_{W/\pi^n}(\underline{x}^\sigma,\underline{x})$ for all $n \geq 1$. Since we have assumed that $r_A(m) = 0$, these groups contain no elements of degree m. The left hand side is zero as every component $\underline{y}(s)_j$ in the decomposition (5.2) of $T_m\underline{x}^\sigma$ is congruent to a canonical section $\underline{y}_0$ of level zero in this divisor. If $\underline{x}$ intersects $\underline{y}(s)$, then $\underline{x} \equiv \underline{y}_0 \pmod{\pi}$. This forces $\underline{x}$ to be equal to $\underline{y}_0$, as they are both canonical liftings of their reductions. Hence $x = y_0$ occurs in $T_m x^\sigma$, which contradicts our hypothesis that $r_A(m) = 0$.

Now assume that p is inert in K, and let $\underline{y}(s)$ be the components in $T_{p^t}\underline{z}$ with $s \equiv t(2)$ as in (5.2). All of these components are congruent to a fixed $\underline{y}_0$ of level zero and by (5.4) we have

$$(T_{p^t}\underline{z} \cdot \underline{x}) = \begin{cases} \sum_{n\geq 1} h_n(\underline{z},\underline{x})_{\deg 1} + \frac{t}{2} h_1(\underline{z},\underline{x})_{\deg 1} & \left\{ \begin{array}{l} t \text{ even} \\ \underline{y}_0 = \underline{z} \end{array} \right. , \\ \\ \frac{t+2}{2} h_1(\underline{z},\underline{x})_{\deg p} & \left\{ \begin{array}{l} t \text{ odd} \\ \underline{y}_0 = \underline{z}^{(p)} \end{array} \right. . \end{cases}$$

Summing over all $z \in T_r x$ and using (5.1) for r prime to p, we obtain

$$(\underline{x}\cdot T_m\underline{x}^\sigma)=\begin{cases}\sum\limits_{n\ge 1}h_n(\underline{x}^\sigma,\underline{x})_{\deg r}+\frac{t}{2}h_1(\underline{x}^\sigma,\underline{x})_{\deg r} & t\ \text{even},\\[2ex] \frac{t+1}{2}h_1(\underline{x}^\sigma,\underline{x})_{\deg pr} & t\ \text{odd}.\end{cases}$$

In the first case, an isogeny $f:\underline{x}^\sigma\to\underline{x}$ of degree r over W/π^n yields an isogeny $p^{t/2}$ of degree m over $W/\pi^{n+t/2}$. In the second case, an isogeny $f:\underline{x}^\sigma\to\underline{x}$ of degree $r\,p$ over W/π yields an isogeny $p^{\frac{t-1}{2}}f$ of degree m $W/\pi^{\frac{t+1}{2}}$.

Finally, assume that p is ramified in K with prime factor $\mathfrak{p}$. For each $z\in T_r x^\sigma$ we have the decomposition $T_{p^t}\underline{z}=\sum\limits_{0\le s\le t}\underline{y}(s)$ as in (5.2); each $\underline{y}(s)$ is congruent $(\bmod\ \pi_y)$ to $\underline{z}$ if t is even, and to $\underline{z}^{\mathfrak{p}}$ if t is odd. Thus

$$(T_{p^t}\underline{z}\cdot\underline{x})=\begin{cases}\sum\limits_{n\ge 1}h_n(\underline{z},\underline{x})_{\deg 1}+t\,h_1(\underline{z},\underline{x})_{\deg 1} & t\ \text{even},\\[2ex] \sum\limits_{n\ge 1}h_n(\underline{z}^{\sigma},\underline{x})_{\deg 1}+t\,h(\underline{z}^{\sigma},\underline{x})_{\deg 1} & t\ \text{odd}.\end{cases}$$

Summing over all $z\in T_r x^\sigma$ and using (5.1) for r prime to p, we obtain

$$(\underline{x}\cdot T_m\underline{x}^\sigma)=\begin{cases}\sum\limits_{n\ge 1}h_n(\underline{x}^\sigma,\underline{x})_{\deg r}+t\,h_1(\underline{x}^\sigma,\underline{x})_{\deg r} & t\ \text{even},\\[2ex] \sum\limits_{n\ge 1}h_n(\underline{x}^{\sigma\sigma_{\mathfrak{p}}},\underline{x})_{\deg r}+t\,h_1(\underline{x}^{\sigma\sigma_{\mathfrak{p}}},\underline{x})_{\deg r} & t\ \text{odd}.\end{cases}$$

In the first case, an isogeny $f:\underline{x}^\sigma\to\underline{x}$ of degree r over W/π^n yields an isogeny $\mathfrak{p}^t f=p^{t/2}f$ of degree m over W/π^{n+t}. In the second case, an isogeny $f:\underline{x}^{\sigma\sigma_{\mathfrak{p}}}\to\underline{x}$ of degree r over W/π^n yields an isogeny $\mathfrak{p}^t f:\underline{x}^\sigma\to\underline{x}$ of degree m over W/π^{n+t}.

§7. Quaternionic formulae

We now turn to the calculation of the right hand side of Proposition 4.4. First, we record an important result which was established in its proof.

Proposition 7.1 If p splits in K and $r_A(m)=0$, then $(\underline{x}\cdot T_m\underline{x}^\sigma)=0$.

Proof. In this case, $\mathrm{Hom}_{W/\pi^n}(\underline{x}^\sigma,\underline{x})=\mathrm{Hom}_W(\underline{x}^\sigma,\underline{x})$ for all $n\ge 1$. This group contains no elements of degree m, by the assumption that $r_A(m)=0$.

Henceforth in this section, we will assume p has a unique prime factor $\mathfrak{p}$ in K (in particular, p does not divide N). Then $\underline{x}$ and $\underline{x}^\sigma$ have supersingular reduction $(\bmod\ \pi)$ and $\mathrm{End}_{W/\pi}(\underline{x})=R$ is an order in the quaternion algebra B over Q which is ramified at ∞ and p. The reduced discriminant of R is equal to Np ; $R \otimes \mathbb{Z}_p$ is maximal in $B \otimes \mathbb{Q}_p$, and for all $\ell \neq p$ $R \otimes \mathbb{Z}_\ell$ is conjugate to the Eichler order $\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} : c \equiv 0 \pmod N\right\}$ in $B \otimes \mathbb{Q}_\ell$.

The embedding $\mathcal{O} = \mathrm{End}_W(\underline{x}) \to R = \mathrm{End}_{W/\pi}(\underline{x})$ given by reduction of endormorphisms extends to a $\mathbb{Q}$-linear map $K \to B$. This in turn yields a decomposition

(7.2) $$B = B_+ + B_- = K + Kj$$

where j is an element in the non-trivial coset of $N_{B^*}(K^*)/K^*$. The decomposition (7.2) is respected by the reduced norm: $\mathbb{N}(b) = \mathbb{N}(b_+) + \mathbb{N}(b_-)$.

<u>Proposition 7.3</u> 1) $\mathrm{End}_{W/\pi^n}(\underline{x}) = \{b \in R : D \cdot \mathbb{N}b_- \equiv 0 \mod p(\mathbb{N}\mathfrak{p})^{n-1}\}$.

2) $\mathrm{Hom}_{W/\pi^n}(\underline{x}^\sigma, \underline{x}) \cong \mathrm{End}_{W/\pi^n}(\underline{x}) \cdot \mathfrak{a}$ <u>in</u> B , <u>where</u> $\mathfrak{a}$ <u>is any ideal in the class of</u> A . <u>If the isogeny</u> $\phi : \underline{x}^\sigma \to \underline{x}$ <u>corresponds to</u> $b \in B$, <u>then</u> $\deg\phi = \mathbb{N}b/\mathbb{N}\mathfrak{a}$.

<u>Proof</u>. Let $\hat{\underline{x}} = (\hat{\phi} : \hat{E} \to \hat{E}')$ be the diagram of p-divisible groups over W corresponding to $\underline{x}$. Since $\underline{x}$ has supersingular reduction the p-divisible groups $\hat{E}$ and $\hat{E}'$ are both formal groups of dimension 1 and height 2 . Since p is prime to N , $\hat{\phi}$ is an isomorphism and $\mathrm{End}_{W/\pi^n}(\hat{\underline{x}}) = \mathrm{End}_{W/\pi^n}(\hat{E})$ for all $n \geq 1$.

The ring $\mathrm{End}_{W/\pi}(\hat{\underline{x}}) = R_{\mathfrak{p}} = R \otimes \mathbb{Z}_p$ is the maximal order in the quaternion division algebra $B_{\mathfrak{p}} = B \otimes \mathbb{Q}_p$ over $\mathbb{Q}_p$. By the results of [15] we have

$$\mathrm{End}_{W/\pi^n}(\hat{\underline{x}}) = \{b \in R_{\mathfrak{p}} : D\mathbb{N}b_- \equiv 0 \mod p(\mathbb{N}\mathfrak{p})^{n-1}\} .$$

But a fundamental theorem of Serre and Tate [31] states that:

$$\mathrm{End}_{W/\pi^n}(\underline{x}) = \mathrm{End}_{W/\pi}(\underline{x}) \cap \mathrm{End}_{W/\pi^n}(\hat{\underline{x}}) ,$$

which gives 1). Part 2) follows from the fact that $\underline{x}^\sigma \cong \mathrm{Hom}(\mathfrak{a}, \underline{x})$ for any ideal $\mathfrak{a}$ in the class of A .

<u>Corollary 7.4</u>. <u>Assume</u> $r_A(m) = 0$. 1) <u>If</u> p <u>is inert in</u> K <u>and</u> v <u>is a place dividing</u> p <u>in</u> H, <u>then</u> $q_v = p^2$ <u>and</u>

$$(\underline{x}, T_m \underline{x}^\sigma) = \sum_{\substack{b \in R\alpha/\pm 1 \\ Nb = mN\alpha}} \frac{1}{2}(1 + \mathrm{ord}_p(Nb\_))$$

2) <u>If</u> p <u>is ramified in</u> K <u>and</u> v <u>is a place dividing</u> p <u>in</u> H, <u>then</u> $q_v = p^k$ <u>where</u> k <u>is the order of</u> $[\mathfrak{p}]$ <u>in</u> $C\ell_K$ <u>and</u>

$$(\underline{x} \cdot T_m \underline{x}^\sigma) = \sum_{\substack{b \in R\alpha/\pm 1 \\ Nb = mN\alpha}} \mathrm{ord}_p(DNb\_) .$$

<u>Proof</u>. We will use Propositions 4.4 and 7.3. Combining these results yields

$$(\underline{x} \cdot T_m \underline{x}^\sigma) = \frac{1}{2} \sum_{n \geq 1} \mathrm{Card}\{b \in R\alpha,\ Nb = mN\alpha,\ DNb\_ \equiv 0 \mod p N\mathfrak{p}^{n-1}\}$$

$$= \sum_{\substack{b \in R\alpha/\pm 1 \\ Nb = mN\alpha}} \begin{cases} \frac{1}{2}(1 + \mathrm{ord}_p(Nb\_)) & p \nmid D, \\ \mathrm{ord}_p(DNb\_) & p \mid D. \end{cases}$$

We remark that when $p \nmid D$, $\mathrm{ord}_p(Nb\_)$ is always odd.

§8. <u>Modifications when</u> $r_A(m) \neq 0$

In this case, the divisors c and $T_m d^\sigma$ are not relatively prime, and the computation of the local symbol $\langle c, T_m d^\sigma \rangle$ uses the tangent vector $\partial/\partial t$ at x which is defined in §5 of Chapter II. Recall that $\partial/\partial t$ is defined up to a 6th root of unity, and is dual to the 1-form $\omega = \eta^4(q)\frac{dq}{q}$ at x when $u = 1$.

We will adopt the convention that

$$(8.1) \qquad (x \cdot x) = \mathrm{ord}_v(\alpha)$$

where $\alpha\, \partial/\partial t$ is a basis for the free W-module $T_{\underline{x}} \underline{X}$. Then the intersection formula (0.2) continues to hold. The reason for our particular choice of tangent vector is the following.

<u>Lemma 8.2</u>. <u>If</u> v <u>does not divide</u> N, <u>then</u>

$$\mathrm{ord}_v(\alpha) = \frac{1}{2} \sum_{n \geq 1} \mathrm{Card}(\mathrm{Aut}_{W/\pi^n}(\underline{x})) - \mathrm{Card}(\mathrm{Aut}_W(\underline{x}))$$

$$= \frac{1}{2} \sum_{n \geq 1} \mathrm{Card}(\mathrm{Aut}^{\mathrm{new}}_{W/\pi^n}(\underline{x})) .$$

In particular, we see that $\partial/\partial t$ generates $T_{\underline{x}} \underline{X}$ if and only if $\mathrm{Aut}_{W/\pi^n}(\underline{x}) = \mathrm{Aut}_W(\underline{x})$. This is a completely general fact, which like (6.1), has noting to do with $\underline{x}$ being a Heegner point. It only requires that $\underline{x}$ reduce to a non-cuspidal point of the special fibre.

<u>Proof</u>. The differential ω is defined on a cyclic cover Y' of degree 6 of the curve $Y = X_0(1)$, which corresponds to the commutator subgroup of $PSL_2(\mathbb{Z})$. The compositum X' over X still is cyclic of degree 6, as it is totally

ramified over the rational cusp ∞ .

$$\begin{tikzcd} & X' \arrow[dl, "6"'] \arrow[dr] & \\ X \arrow[dr] & & Y' \arrow[dl, "6"] \\ & Y & \end{tikzcd}$$

Over $\mathbb{Z}[1/6]$, $\underline{Y}'$ is an elliptic curve with good reduction and ω is a Néron differential. Since the covering $\underline{X}' \to \underline{Y}'$ is ramified only at the cusp of $\underline{Y}'$ and the fibres dividing N , we may calculate the relationship between $\omega \cdot W$ and $T_{\underline{x}}X$ for primes $v \nmid 6N$ via an analysis of the ramification in the cover $\underline{X}' \to \underline{X}$ over the section $\underline{x}$. This comes from extra automorphisms $(\mathrm{mod}\ \pi)$, and we recover the formula of (8.2) exactly as in (6.1),

The argument for primes dividing 2 and 3 is more involved, and we will not give it here. We simply note that when $N = 1$, so $X = Y$ and $X' = Y'$, we have the explicit formulae

$$(8.3) \qquad \alpha \underset{\mathrm{mod}\,\mu_6}{\equiv} j(x)^{2/3}(j(x) - 1728)^{1/2} \qquad j(x) \neq 0,\ 1728,$$

$$\equiv 2^6 \cdot 3^4 \qquad j(x) = 1728,$$

$$\equiv 2^9 \cdot 3^{3/2} \qquad j(x) = 0 .$$

If v does not divide mN , then Proposition 4.4 and Lemma 8.2 give

$$(8.4) \qquad (x \cdot T_m x^\sigma) = \frac{1}{2} \sum_{n \geq 1} \mathrm{Card}(\mathrm{Hom}^{\mathrm{new}}_{W/\pi^n}(\underline{x}^\sigma, \underline{x})_{\deg m}) \ .$$

The quaternionic formulae for the right hand side Corollary 7.4 remain true, provided we sum over those $b \in R$ with $b \notin \mathcal{O}$. Another way to express this condition is to insist that $b_- \neq 0$; this is necessary if the terms $\mathrm{ord}_p(\mathrm{N}b_-)$ in Corollary 7.4 are to make sense!

When $v|m$, formula (8.4) must be modified slightly, as the $u\, r_A(m)$ elements in $\mathrm{Hom}_W(x^\sigma, x)_{\deg m}/(\pm 1)$ which do not appear on the right hand side actually contribute to intersections of $\underline{x}$ with its quasi-canonical liftings $\underline{y}$ which occur in $T_m \underline{x}^\sigma$. A count of these liftings, together with their levels, as in §5 gives the correction term.

<u>Proposition 8.5</u>. <u>Assume that</u> v <u>does not divide</u> N .

1) <u>If</u> p <u>is inert in</u> K <u>then</u>

$$(\underline{x} \cdot T_m \underline{x}^\sigma) = \frac{1}{2} \sum_{\substack{b \in R\mathfrak{a}/\pm 1 \\ \mathrm{N}b = m\mathrm{N}\mathfrak{a} \\ b_- \neq 0}} (1 + \mathrm{ord}_p(\mathrm{N}b_-)) + \frac{1}{2}\, u\, r_A(m) \mathrm{ord}_p(m)$$

2) <u>If</u> p <u>is ramified in</u> K <u>then</u>

$$(\underline{x} \cdot T_m \underline{x}^\sigma) = \sum_{\substack{b \in R\mathfrak{a}/\pm 1 \\ \mathrm{N}b = m\mathrm{N}\mathfrak{a} \\ b_- \neq 0}} \mathrm{ord}_p(D\mathrm{N}b_-) + u\, r_A(m) \mathrm{ord}_p(m)$$

3) <u>If</u> $p = \mathfrak{p} \cdot \bar{\mathfrak{p}}$ <u>is split in</u> K <u>and</u> $v|\mathfrak{p}$ <u>then</u>

$$(x \cdot T_m x^{\sigma}) = u\, r_A(m) k_{\mathfrak{p}}$$

where $k_{\mathfrak{p}} \geq 0$ and $k_{\mathfrak{p}} + k_{\bar{\mathfrak{p}}} = \operatorname{ord}_p(m)$.

When $v|N$ Lemma 8.2 remains true, <u>provided</u> $\underline{x}$ reduces to the same component as the cusp ∞ . In our case, this occurs when $v|\mathfrak{N}$. Using the action of w_N on ω , one can show that the tangent vector $\partial/\partial t$ spans the submodule $(N)^u T_{\underline{x}} \underline{X}$ when $v|\bar{\mathfrak{N}}$. Hence

<u>Proposition 8.6</u>. <u>Assume that</u> $v|N$. <u>Then</u>

$$(\underline{x} \cdot T_m \underline{x}^{\sigma}) = \begin{cases} 0 & \text{if } v|\mathfrak{N} \\ -u\, r_A(m) \operatorname{ord}_p(N) & \text{if } v|\bar{\mathfrak{N}} . \end{cases}$$

§9. <u>Explicit quaternion algebras</u>

We now seek a formula for the sum

$$(9.1) \qquad \langle c, T_m d^{\sigma}\rangle_p \overset{\text{defn.}}{=} \sum_{v|p} \langle c, T_m d^{\sigma}\rangle_v .$$

The case when p splits in K can be handled immediately.

<u>Proposition 9.2</u> <u>If</u> p <u>splits in</u> K , <u>then</u>

$$\langle c, T_m d^{\sigma}\rangle_p = -u\, r_A(m) h \operatorname{ord}_p(m/N) \log p .$$

<u>Proof</u>. By Propositions 8.5 and 8.6, $\langle c, T_m d^{\sigma}\rangle_v = -u\, r_A(m) j_{\mathfrak{p}} \log q_v$ with $j_{\mathfrak{p}} + j_{\bar{\mathfrak{p}}} = \operatorname{ord}_p(m/N)$. On the other hand $\sum_{v|\mathfrak{p}} \log q_v = h \log p$.

We now assume that v divides a prime p which remains inert in K . Fix an auxiliary prime q with $(\frac{q}{\ell}) = (\frac{-p}{\ell})$ for all primes $\ell|D$. Such primes exist by Dirichlet's theorem and must split $(q) = \mathfrak{q} \cdot \bar{\mathfrak{q}}$ in K . The quaternion algebra B with Hilbert symbol $(D,-pq)$ is ramified only at ∞ and p , and we have a splitting: $B = K + Kj$ with $j^2 = -pq$.

We wish to find a convenient model for the order $R = \operatorname{End}_{W/\pi}(\underline{x})$ of Corollary 7.4 as a subring of B . Recall that R has reduced discriminant Np and is locally an Eichler order at all finite $\ell \neq p$. A global order S with this local behavior is given by

$$S = \{\alpha + \beta j : \alpha \in \mathcal{D}^{-1}, \beta \in \mathcal{D}^{-1}\mathfrak{q}^{-1}\mathfrak{n}, \alpha \equiv \beta \mod \mathcal{O}_{\mathfrak{f}}\}$$

where the congruence is for all primes $\mathfrak{f}$ of $\mathcal{O}$ dividing $\mathcal{D}$. By a fundamental result of Eichler [10, p. 118] there is an ideal $\mathfrak{b}$ of $\mathcal{O}$ such that $R\mathfrak{b} = \mathfrak{b}S$ inside B. If $\mathfrak{a}$ is an ideal in the class A corresponding to σ (as in 7.4), we have

$$(9.3) \quad R\mathfrak{a} = \{\alpha + \beta j : \alpha \in \mathcal{D}^{-1}\mathfrak{a}, \beta \in \mathcal{D}^{-1}\mathfrak{q}^{-1}\mathfrak{n}\bar{\mathfrak{f}}\mathfrak{b}^{-1}\bar{\mathfrak{a}}, \alpha \equiv (-1)^{\mathrm{ord}_{\mathfrak{f}}(\mathfrak{b})}\beta \mod \mathcal{O}_{\mathfrak{f}}\} .$$

The class $\mathcal{B}$ of the ideal $\mathfrak{b}$ depends on the place v which divides p. If $v' = v^{\sigma_{\mathfrak{c}}}$ we find $\mathfrak{b}' = \mathfrak{b}\mathfrak{c}$, so $\mathcal{B}' = \mathcal{B}\cdot\mathcal{C}$. Hence the different classes of ideals which arise are permitted simply transitively by $\mathrm{Gal}(H/K)$. If we sum over all primes v dividing p, this class will drop out of the final formulas.

We now consider the local sums in Corollary 7.4. Assume $b = \alpha + \beta j \in R\mathfrak{a}$ satisfies

$$(9.4) \quad \begin{cases} \mathrm{N}b = \mathrm{N}\alpha + pq\mathrm{N}\beta = m\mathrm{N}\mathfrak{a}. \\ \mathrm{N}b\_ = pq\mathrm{N}\beta \neq 0 . \end{cases}$$

If we define the integral ideals of $\mathcal{O}$

$$(9.5) \quad \begin{cases} \mathfrak{c} = (\alpha)\mathcal{D}\mathfrak{a}^{-1} \\ \mathfrak{c}' = (\beta)\mathcal{D}\mathfrak{q}\mathfrak{n}^{-1}\bar{\mathfrak{b}}^{-1}\mathfrak{b}\bar{\mathfrak{a}}^{-1} \end{cases}$$

then $\mathfrak{c}$ is in the class A^{-1} and $\mathfrak{c}'$ is in the class $A\mathcal{B}^2[\mathfrak{q}\mathfrak{n}^{-1}]$. Furthermore, we have the identity:

$$(9.6) \quad \mathrm{N}\mathfrak{c} + \mathrm{N}_p\mathrm{N}\mathfrak{c}' = m|D|$$

The integer $n = p\mathrm{N}\mathfrak{c}'$ is non-zero and $\mathrm{ord}_p(n) = \mathrm{ord}_p(\mathrm{N}b\_)$. Recall that $u = \mathrm{Card}(\mathcal{O}^*/\pm 1)$ and for any integer n define $\delta(n) = 2^{\mathrm{Card}\{\ell | (n,D)\}}$. We shall prove

<u>Proposition 9.7</u> <u>If</u> p <u>is inert in</u> K, <u>then</u>

$$\langle c, T_m d^{\sigma}\rangle_p = - r_A(m) h\, u\, \mathrm{ord}_p(m) \log p$$
$$- u^2 \log p \sum_{\substack{0<n<\frac{m|D|}{N} \\ n\equiv 0 \pmod p}} \mathrm{ord}_p(pn) r_A(m|D|-nN)\delta(n)R_{\{A\mathfrak{q}\mathfrak{n}\}}(n/p) .$$

<u>Proof.</u> We will use Proposition 8.5 and the fact that $\langle c, T_m d^{\sigma}\rangle_v = -2\log p(\underline{x} \cdot T_m \underline{x}^{\sigma})$, as $q_v = p^2$. The first term is clear, so it remains to calculate the sum over b

in the different $R\mathfrak{a}$.

Let us start with a pair of ideals $\mathfrak{c}$ and $\mathfrak{c}'$ in the classes of A^{-1} and $A[\mathfrak{q}\mathfrak{n}^{-1}]\mathcal{B}^2$ which satisfy (9.6). If $n = pN\mathfrak{c}' = p^{2k-1}n'$ then $N\mathfrak{c} = m|D| - nN$.

We will try to construct elements $b = \alpha + \beta j$ in R satisfying (9.4) by reversing formulas (9.5). This defines α and β up to units in $\mathcal{O}^*$; whatever generators we take, the fact that $mN\mathfrak{a} = N\alpha + pqN\beta$ is integral implies that $\alpha \equiv \pm\beta \mod \mathcal{O}_{\mathfrak{f}}$ for all $\mathfrak{f} | \mathcal{D}$. If we may adjust the signs so that $\alpha \equiv (-1)^{\mathrm{ord}_{\mathfrak{f}}(\mathfrak{b})}\beta$ we will obtain an element in $R\mathfrak{a}$. But we will <u>always</u> get an element in $R'\mathfrak{a}$, at a place v' conjugate to v by an element of order 2 in $\mathrm{Gal}(H/K)$. Thus each pair $(\mathfrak{c}, \mathfrak{c}')$ contributes to the sum $\sum_{v|p} (\underline{x} \cdot T_m \underline{x}^{\sigma})$ some elements of weight $\frac{1}{2}(1 + \mathrm{ord}_p(Nb_-))$. The total number of elements which arise from this pair is equal to $2 \cdot u^2 \cdot \delta(n)$ since we only count b up to sign, this gives Proposition 9.7.

The case when v divides a prime p which is ramified in K is quite similar. Let $\mathfrak{p}$ be the prime which divides (p) in K and let f be the order of $[\mathfrak{p}]$ in $C\ell(K)$. There are h/f factors v of $\mathfrak{p}$ in H, each of residual degree p^f. To obtain models for the orders $R = \mathrm{End}_{W/\pi}(\underline{x})$ in (7.4), we let q be a rational prime with $(\frac{q}{p'}) = (\frac{-1}{p'})$ for all $p' \neq p$ which divide D and $(\frac{-q}{p}) = -1$. Then $q = \mathfrak{q} \cdot \bar{\mathfrak{q}}$ splits in K and B has Hilbert symbol $(D, -q)$. We have a splitting $B = K + Kj$ with $j^2 = -q$.

Here we find that

(9.8)

$$R\mathfrak{a} = \{\alpha + \beta j : \alpha \in \mathfrak{p}\mathcal{D}^{-1}\mathfrak{a}, \beta \in \mathfrak{p}\mathcal{D}^{-1}\mathfrak{q}^{-1}\mathfrak{n}\bar{\mathfrak{b}}\mathfrak{b}^{-1}\bar{\mathfrak{a}}, \alpha \equiv (-1)^{\mathrm{ord}_{\mathfrak{f}}(\mathfrak{b})} \mod \mathcal{O}_{\mathfrak{f}}\}$$

where $\mathfrak{f}$ divides $\mathcal{D}$. The class of $\mathfrak{b}$ is well defined in the quotient group $C\ell(K)/[\mathfrak{p}]$ by the place v. An element $\alpha + \beta j = b \in R\mathfrak{a}$ with $Nb = mN\mathfrak{a}$ and $Nb_- \neq 0$ gives integral ideals

$$(9.9) \qquad \begin{cases} \mathfrak{c} = (\alpha)\mathcal{D}\mathfrak{a}^{-1}, \\ \mathfrak{c}' = (\beta)\mathcal{D}\mathfrak{q}\mathfrak{n}^{-1}\bar{\mathfrak{b}}^{-1}\mathfrak{b}\bar{\mathfrak{a}}^{-1}, \end{cases}$$

which lie in the classes of A^{-1} and $A[\mathfrak{q}\mathfrak{n}^{-1}]\mathcal{B}^2$ respectively. Both are divisible by $\mathfrak{p}$, and their norms satisfy

$$(9.10) \qquad N\mathfrak{c} + N\,N\mathfrak{c}' = m|D|.$$

The integer $n = N\mathfrak{c}'$ is non-zero, and $\mathrm{ord}_p(n) = \mathrm{ord}_p(DNb_-)$. Arguing as in the proof of Proposition 9.7, we find:

<u>Proposition 9.11</u>. <u>If</u> p <u>is ramified in</u> K, <u>then</u>

$$\langle c, T_m d^{\sigma}\rangle_p = - r_A(m) h\, u\, \mathrm{ord}_p(m) \log p$$

$$-u^2 \log p \sum_{\substack{0 < n < \frac{m|D|}{N} \\ n \equiv 0 \ (\mathrm{mod}\ p)}} \mathrm{ord}_p(n) r_A(m|D| - nN)\delta(n) R_{\{A\mathfrak{q}\mathfrak{p}\mathfrak{n}\}}(n/p)$$

Chapter IV. Derivatives of Rankin L-series at the center of the critcal strip

In this chapter we will study the values of a certain L-series of Rankin type and of its first derivative. This L-series is determined by the following data:

i) An ideal class A in an imaginary quadratic field K. We fix the following notations: D is the discriminant of K, $\varepsilon(n) = (\frac{D}{n})$ the associated Dirichlet character (an odd primitive character of conductor $|D|$), Cl_K the class group and $h = Cl_K$ the class number of K, w ($=2$, 4 or 6) the number of units of K, $r_A(n)$ the number of integral ideals of norm n in the class A if $n \geq 1$, $r_A(0) = \frac{1}{w}$.

ii) A cusp form $f \in S_{2k}^{new}(\Gamma_0(N))$, where k is any positive integer and N is a positive integer which we assume prime to D. Here $S_{2k}^{new}(\Gamma_0(N))$ is the space of cusp forms of weight $2k$ and level N which are orthogonal (w.r.t. the Petersson product) to all oldforms (= forms $g(dz)$ with g of level $M<N$, $dM|N$); it is spanned by newforms (Hecke eigenforms) but we do not assume that f is a newform. We write $\sum_{n=1}^{\infty} a(n)\, e^{2\pi i n z}$ for the Fourier expansion of $f(z)$ and $L(f,s)$ for the Hecke L-series $\sum_{1}^{\infty} a(n)\, n^{-s}$.

Given this data, we define a Dirichlet series $L_A(f,s)$ by

$$(0.1) \qquad L_A(f,s) = L^{(N)}(2s-2k+1,\varepsilon) \sum_{n=1}^{\infty} a(n)\, r_A(n)\, n^{-s},$$

i.e. as the product of the Dirichlet L-function $L^{(N)}(2s-2k+1,\varepsilon) = \sum_{(n,N)=1} \varepsilon(n)\, n^{-2s+2k-1}$ and the convolution of $L(f,s)$ with the zeta-function $\sum r_A(n)\, n^{-s}$ of the ideal class A. We will show that $L_A(f,s)$ extends analytically to an entire function of s (this is the reason for the inclusion of the factor $L^{(N)}(2s-2k+1,\varepsilon)$ in (0.1)) and satisfies the functional equation

$$(0.2) \qquad L_A^*(f,s) := (2\pi)^{-2s} N^s |D|^s \Gamma(s)^2\, L_A(f,s) = -\varepsilon(N)\, L_A^*(f,2k-s).$$

In particular, if $\varepsilon(N) = +1$ then $L_A(f,s)$ vanishes at $s=k$; the main result of this chapter will be a formula for the derivative $L'_A(f,k)$ in this case. We will also obtain a formula for the value of $L_A(f,k)$ if $\varepsilon(N)=-1$

(and more generally for all the values $L_A(f,r)$, $r = 1,2,\ldots,2k-1$); this case is much simpler. The case which is related to Heegner points on $X_0(N)$ is $k=1$ and $\varepsilon(p) = 1$ for all primes p dividing N (i.e. D a square modulo $4N$). However, doing the computations for arbitrary even weight not only involves no extra work, but actually simplifies things, since for forms of weight 2 there are extra technical difficulties (connected with the non-absolute convergence of Eisenstein series and Poincaré series in this weight) which obscure the exposition, so that it is convenient to first treat the general case and then discuss the modifications necessary when $k=1$. The case when $k=1$ and $\varepsilon(N)=1$ but $\varepsilon(p)$ is not 1 for all $p|N$ is also interesting, since it turns out that the formula we obtain for $L'_A(f,1)$ in that case is related to the height of a Heegner point on a modular curve associated to a group of units in the indefinite quaternion algebra over $\mathbb{Q}$ ramified at the set of primes p with $\mathrm{ord}_p(N)$ odd and $\varepsilon(p)=-1$. The case $k=1$, $\varepsilon(N)=-1$ is related to special points on a curve associated to a definite quaternion algebra over $\mathbb{Q}$. (For details, see §3 of Chapter V.)

One case of the theorem is particularly striking and should be mentioned, especially as it permits one to understand the presence of the factor $L^{(N)}(2s+2k-1$ in (0.1) and the form of the functional equation (0.2). If $\chi: Cl_K \to \mathbb{C}^*$ is an ideal class character of K, then we can form the function

$$(0.3) \qquad L_K(f,\chi,s) = \sum_{\mathfrak{a}} \chi(\mathfrak{a})\, a(N(\mathfrak{a}))N(\mathfrak{a})^{-s} = \sum_{A \in Cl_K} \chi(A)\, L_A(f,s),$$

and clearly the properties of these functions (analytic continuation, functional equation, derivative at $s=k$) can be read off from those of the functions (0.1) and conversely. Now suppose that χ is a genus character, i.e. a character with values ± 1. Recall that such characters correspond to decompositions of D as a product of two discriminants of quadratic fields (one real and one imaginary), the character $\chi_{D_1 \cdot D_2}$ corresponding to the decomposition $D = D_1 \cdot D_2$ being characterized by the property $\chi(\mathfrak{a}) = \varepsilon_{D_1}(N(\mathfrak{a})) = \varepsilon_{D_2}(N(\mathfrak{a}))$ for integral ideals $\mathfrak{a}$ prime to D (here ε_{D_i} is the Dirichlet character associated to $\mathbb{Q}(\sqrt{D_i})$). The L-series $L_K(s,\chi)$ of such a character is equal to the product of the two

Dirichlet L-series $L(s,\varepsilon_{D_i})$. On the other hand, if $f \in S_{2k}(\Gamma_0(N))$ is a Hecke eigenform, then the L-series of f has the form

$$L(f,s) = \prod_p \frac{1}{(1-\alpha_p p^{-s})(1-\beta_p p^{-s})}, \quad \alpha_p+\beta_p = a(p), \quad \alpha_p\beta_p = \begin{cases} p^{2k-1} & (p\nmid N), \\ 0 & (p|N), \end{cases}$$

and a simple calculation shows that the convolution of this with $L_K(s,\chi)$ equals $L^{(N)}(2s+2k-1,\varepsilon)^{-1}$ times the product of the two "twisted" Hecke L-series $L(f,\varepsilon_{D_i},s) = \sum_n \varepsilon_{D_i}(n)\,a(n)\,n^{-s}$. Hence we have the identity

$$(0.4) \qquad L_K(f,\chi_{D_1\cdot D_2},s) = L(f,\varepsilon_{D_1},s)\,L(f,\varepsilon_{D_2},s) \qquad (f \text{ an eigenform}).$$

On the other hand, it is well-known that the twisted L-series $L(f,\varepsilon_{D_i},s)$ has an analytic continuation and a functional equation with gamma-factor $(2\pi)^{-s}N^{s/2}|D_i|^s\Gamma(s)$ and sign $(-1)^k\varepsilon_{D_i}(-N)w$, where $w=\pm 1$ is the eigenvalue of f with respect to the Atkin-Lehner involution W_N: $f(z)\to N^{-k}z^{-2k}f(\frac{-1}{Nz})$. When we multiply these two functional equations we obtain a functional equation for $L_K(f,\chi,s)$ with gamma-factor and sign as in (0.2), independent both of the value of w and of the choice of (genus) character. (The fact that the sign of the functional equation does not depend on the eigenform chosen shows that this functional equation is true for any element of $S_{2k}^{new}(\Gamma_0(N))$, unlike the situation for the Hecke L-series $L(f,s)$ which has a functional equation only if f is an eigenfunction of W_N.) If $\varepsilon(N)=1$ then one of the two L-series on the right-hand side of (0.4), say the first, will have a functional equation with a minus sign and the other a functional equation with a plus sign, and our main result will specialize to a formula for the product $L'(f,\varepsilon_{D_1},k)L(f,\varepsilon_{D_2},k)$. If $k=1$ and the eigenform f has integral Fourier coefficients, then the value of this product will be related to the height of a point defined over $\mathbb{Q}$ on the twist by D_1 of the elliptic curve associated to f. This is the situation which was studied extensively (numerically) by Birch and Stephens [4,5].

The plan of this chapter is as follows. In §1 we will apply "Rankin's method"

to obtain a formula for $L_A(f,s)$ as the Petersson scalar product of f with the product of a theta series and a non-holomorphic Eisenstein series. This product is a modular form on $\Gamma_0(ND)$ and must be traced down to $\Gamma_0(N)$ to get a (non-holomorphic) modular form Φ_s of level N whose Petersson product with f also gives the desired L-function. This is carried out in §2, while §3 contains the calculation of the Fourier coefficients of Φ_s. In §4 we check that each of these Fourier coefficients satisfies a functional equation in s and calculate their value or derivative (depending on the sign of the functional equation) at the symmetry point. This establishes the functional equation (0.2) and gives a formula for $L_A(f,k)$ or $L'_A(f,k)$ as the scalar product of f with a certain non-holomorphic modular form $\tilde{\Phi}$ of level N. The final step, carried out in §5, is to replace $\tilde{\Phi}$ by a holomorphic modular form Φ having the same scalar product with f; this is done by means of the holomorphic projection operator of Sturm [33]. The modifications needed to treat the case $k=1$ are described in §6. It is suggested that, at least on a first perusal, the reader mentally restrict to the case $N=1$, $k>1$, $|D|$ prime, since the ideas of the proof are the same here as in the general case but many of the calculations (e.g. those of §2 and §6) can be omitted or drastically shortened. Even the case $N=1$, $k=1$ is interesting, for even though there are no cusp forms f in this case, the function Φ still makes sense and the fact that its Fourier coefficients are identically zero gives non-trivial information about the value of the classical modular function $j(z)$ at quadratic imaginary arguments; this simplest case is discussed in [18].

Conventions. For $z \in \mathfrak{H}$ we write x, y for the real and imaginary parts of z and q for $e^{2\pi i z}$. The functions $e^{2\pi i x}$ $(x\in\mathbb{C})$ and $e^{2\pi i a/n}$ $(a\in\mathbb{Z}/n\mathbb{Z})$ will be denoted $e(x)$ and $e_n(a)$, respectively. If a is an integer being considered modulo another integer n to which it is prime, then a^* denotes the inverse of $a \pmod n$; thus the notation $e_n(a^*b)$ implies that $(a,n)=1$

and means $e^{2\pi i c/n}$ with $ac \equiv b \pmod n$. If f is a function on $\mathfrak{H}$, $k \in \mathbb{Z}$ and $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2^+(\mathbb{R})$, then $f|_k\gamma$ has the usual meaning in the theory of modular forms: $(f|_k\gamma)(z) = (ad-bc)^{k/2}(cz+d)^{-k} f(\frac{az+b}{cz+d})$. If N is a natural number and χ a Dirichlet character modulo N, then we denote by $\widetilde{M}_k(\Gamma_0(N),\chi)$ the space of functions $f: \mathfrak{H} \to \mathbb{C}$ satisfying $f|_k\gamma = \chi(d)\, f$ for all $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$ and having at most polynomial growth at the cusps (i.e. $(f|_k\gamma)(z) = O(y^C)$ as $y \to \infty$ for all $\gamma \in SL_2(\mathbb{Z})$ and some $C > 0$) and by $M_k(\Gamma_0(N),\chi)$ and $S_k(\Gamma_0(N),\chi)$ the subspaces of holomorphic modular forms and holomorphic cusp forms, respectively; the character χ is omitted from these notations if it is trivial.

§1. Rankin's method

The assumptions are as in §0: D is a fundamental discriminant, $\mathcal{A}$ an ideal class of $\mathbb{Q}(\sqrt{D})$, and $f(z) = \sum a(n)\, q^n$ a cusp form in $S_{2k}^{new}(\Gamma_0(N))$ for some integer N prime to D. Let $\theta_{\mathcal{A}}$ denote the theta-series

$$(1.1) \qquad \theta_{\mathcal{A}}(z) = \sum_{n=0}^{\infty} r_{\mathcal{A}}(n)\, q^n = \frac{1}{w} \sum_{\lambda \in \mathfrak{a}} q^{N(\lambda)/A} ,$$

where $\mathfrak{a}$ is any ideal in the class $\mathcal{A}$ and $A = N(\mathfrak{a})$. It is known that $\theta_{\mathcal{A}}$ belongs to $M_1(\Gamma_0(D),\varepsilon)$. (In §2 we will give the transformation behavior of $\theta_{\mathcal{A}}$ under all of $SL_2(\mathbb{Z})$.) Hence we have (for $\mathrm{Re}(s)$ large)

$$\frac{\Gamma(s+2k-1)}{(4\pi)^{s+2k-1}} \sum_{n=1}^{\infty} \frac{a(n)\, r_{\mathcal{A}}(n)}{n^{s+2k-1}} = \int_0^\infty \sum_{n=1}^{\infty} a(n)\, r_{\mathcal{A}}(n)\, e^{-4\pi n y}\, y^{s+2k-2}\, dy$$

$$= \int_0^\infty \int_0^1 f(x+iy)\, \overline{\theta_{\mathcal{A}}(x+iy)}\, dx\; y^{s+2k-2}\, dy$$

$$= \iint_{\Gamma_\infty \backslash \mathfrak{H}} f(z)\, \overline{\theta_{\mathcal{A}}(z)}\, y^{s+2k} \frac{dx\,dy}{y^2} ,$$

where $\Gamma_\infty = \{\pm\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix},\ n \in \mathbb{Z}\}$, acting on $\mathfrak{H}$ by integer translation. A fundamental domain for this action can be chosen to be $\bigcup_\gamma \gamma F$, where F is a fundamental domain for the action of $\Gamma_0(M)$, $M = N|D|$, and γ runs over a set of right coset representatives of $\Gamma_0(M)$ modulo Γ_∞. Hence the last expression can be rewritten as

$$\sum_{\gamma \in \Gamma_\infty \backslash \Gamma_0(M)} \iint_{\gamma F} f(z)\, \overline{\theta_{\mathcal{A}}(z)}\, y^{s+2k} \frac{dx\,dy}{y^2} = \sum_\gamma \iint_F f(\gamma z)\, \overline{\theta_{\mathcal{A}}(\gamma z)}\, \mathrm{Im}(\gamma z)^{s+2k} \frac{dx\,dy}{y^2}$$

$$= \sum_{\gamma = \pm\begin{pmatrix} \cdot & \cdot \\ c & d \end{pmatrix} \in \Gamma_\infty \backslash \Gamma_0(M)} \iint_F f(z)\, \overline{\theta_{\mathcal{A}}(z)}\, \frac{\varepsilon(d)}{(c\bar{z}+d)^{2k-1}} \frac{y^s}{|cz+d|^{2s}}\, y^{2k} \frac{dx\,dy}{y^2} ,$$

where we have used the invariance of $\frac{dx\,dy}{y^2}$ under $SL_2(\mathbb{R})$ and the transformation properties of f and $\theta_{\mathcal{A}}$ under $\Gamma_0(M)$. In the last expression we can interchange the summation and integration. We obtain:

$$\frac{\Gamma(s+2k-1)}{(4\pi)^{s+2k-1}} L_{\mathcal{A}}(f,s+2k-1) = \iint_F f(z)\, \overline{\theta_{\mathcal{A}}(z)\, E_{\bar{s}}(z)}\, y^{2k} \frac{dx\,dy}{y^2}$$

$$= (f, \theta_{\mathcal{A}} E_{\bar{s}})_{\Gamma_0(M)} ,$$

where E_s denotes the Eisenstein series

$$E_s(z) = E_{M,\varepsilon,2k-1,s}(z) = L^{(N)}(2s+2k-1,\varepsilon) \sum_{\pm\begin{pmatrix} \cdot & \cdot \\ c & d \end{pmatrix} \in \Gamma_\infty \backslash \Gamma_0(M)} \frac{\varepsilon(d)}{(cz+d)^{2k-1}} \frac{y^s}{|cz+d|^{2s}}$$

$$= \frac{1}{2} \sum_{\substack{c,\ d \in \mathbb{Z} \\ c \equiv 0 \ (\mathrm{mod}\ M) \\ (d,M) = 1}} \frac{\varepsilon(d)}{(cz+d)^{2k-1}} \frac{y^s}{|cz+d|^{2s}}$$

in $\widetilde{M}_{2k-1}(\Gamma_0(M),\varepsilon)$ and $(\ ,\ )_{\Gamma_0(M)}$ the Petersson scalar product on $\Gamma_0(M)$. (The reason for including the factor $L^{(N)}(s-2k+1,\varepsilon)$ in the definition (0.1) is now clear.) The process we just used to express the convolution of the L-series of two modular forms as a scalar product involving an Eisenstein series was first used by Rankin and Selberg in 1939 and is commonly referred to as "Rankin's method

We now use the principle $(f,g)_{\Gamma_0(M)} = (f, \mathrm{Tr}_N^M g)_{\Gamma_0(N)}$ for any $f \in S_{2k}(\Gamma_0(N))$ and $g \in \widetilde{M}_{2k}(\Gamma_0(M))$, where Tr_N^M is the trace map

$$\mathrm{Tr}_N^M : \widetilde{M}_{2k}(\Gamma_0(M)) \to \widetilde{M}_{2k}(\Gamma_0(N)) , \quad g \mapsto \sum_{\gamma \in \Gamma_0(M) \backslash \Gamma_0(N)} g|_{2k}\gamma .$$

This gives

$$(4\pi)^{-s-2k+1} \Gamma(s+2k-1)\ L_{\mathcal{A}}(f,s+2k-1) = (f, \mathrm{Tr}_N^M(\theta_{\mathcal{A}} E_{\bar{s}})) ,$$

where now the scalar product is taken on $\Gamma_0(N)$. In the definition of E_s, the condition $(d,M)=1$ can be replaced by $(d,N)=1$ since $\varepsilon(d)=0$ otherwise, and this condition in turn can be dropped if we insert a factor $\sum_{e|(d,N)}\mu(e)$ (μ = Möbius function) which vanishes if $(d,N)>1$. Hence

$$E_s(z) = \frac{1}{2}\sum_{e|N}\mu(e)\sum_{\substack{c,d\in\mathbb{Z}\\ M|c,\ e|d}}\frac{\varepsilon(d)}{(cz+d)^{2k-1}}\,\frac{y^s}{|cz+d|^{2s}}$$

$$= \sum_{e|N}\frac{\mu(e)\varepsilon(e)}{e^{2s+2k-1}}\,(N/e)^{-s}\,E_s^{(1)}\left(\frac{N}{e}z\right),$$

where $E_s^{(1)}$ is defined like E_s but with N replaced by 1 (i.e. M by D); the last line is obtained by replacing c, d by c/N', d/e. Note that the only non-trivial terms are those with e square-free and prime to D. Now when we form $Tr_N^M(\theta_A E_s)$ the terms with $e>1$ contribute terms of level $N/e<N$, because any system of representatives of $\Gamma_0(M)\backslash\Gamma_0(N)$ is also a system of representatives for $\Gamma_0(\frac{M}{e})\backslash\Gamma_0(\frac{N}{e})$. Since f is orthogonal to modular forms of level smaller than N, these terms contribute nothing to the scalar product and can be omitted. (Actually, the definition of S_{2k}^{new} involves only the scalar products with holomorphic forms, but the scalar product of f with any non-holomorphic form $\tilde g$ is equal to its scalar product with a holomorphic form g of the same level, as we will see in §5, so this doesn't matter.) We have proved:

Proposition 1.2. Let D be a fundamental discriminant, $N\geq 1$ prime to D, and define a function $\Phi_s = \Phi_{s,A}\in\tilde{M}_{2k}(\Gamma_0(N))$ by

$$\tilde{\Phi}_s(z) = Tr_N^{ND}(\theta_A(z)E_s^{(1)}(N z)),$$

where θ_A is the theta-series defined in (1.1) and

$$E_s^{(1)}(z) = \frac{1}{2}\sum_{\substack{c,d\in\mathbb{Z}\\ D|c}}\frac{\varepsilon(d)}{(cz+d)^{2k-1}}\,\frac{y^s}{|cz+d|^{2s}}$$

the non-holomorphic Eisenstein series of level $|D|$, weight $2k-1$ and Nebentypus ε. Then for any $f\in S_{2k}^{new}(\Gamma_0(N))$ we have

$$(4\pi)^{-s-2k+1}N^s\Gamma(s+2k-1)\;L_A(f,s+2k-1) = (f,\tilde{\Phi}_{\bar{s}}).$$

Remark. The proof used only the orthogonality of f with modular forms g of level strictly dividing N and not the orthogonality of f with functions $g(dz)$ with $d>1$ and g a form of level dividing N/d. The effect of this second property of $f\in S_{2k}^{new}$ is that in Proposition 1.2 only the Fourier coefficients of $\tilde{\Phi}_s$ with index prime to N are relevant. Thus to prove the functional equation (0.2), for instance, it suffices to prove the corresponding functional equation for the coefficients $A_m(s,y)$ defined by

$$(1.3)\qquad \tilde{\Phi}_s(z) = \sum_{m=-\infty}^{\infty}A_m(s,y)\,e(mx)$$

for m prime to N, since then the difference between $\tilde{\Phi}_s$ and its image under the asserted functional equation is automatically orthogonal to f. In the same way, in giving formulas for the values of $L_A(f,s)$ at special points or for its derivative at $s=k$ it will suffice to study the corresponding values or derivatives of $A_m(s,y)$ for $(m,N)=1$. It would not, in fact, be difficult to study the coefficients with $(m,N)>1$ as well, or to retain the terms with $e>1$ which were omitted in the proof of 1.2, and thus obtain formulas valid for all $f\in S_{2k}(\Gamma_0(N))$, but this would complicate the notations and calculations and is pointless since one can always reduce to the case of newforms.

§2. Computation of the trace

The function $\tilde{\Phi}_s(z)$ is defined as a trace from $\Gamma_0(ND)$ to $\Gamma_0(N)$. To compute its Fourier development, we will need the expansions of $\theta_A(z)$ and $E_s^{(1)}(z)$ at the various cusps of $\Gamma_0(D)$. These cusps are in 1:1 correspondence with the positive divisors of D. (This is because D is not divisible by 16 or the square of an odd prime; in general, to describe a cusp of $\Gamma_0(n)$ one must specify a divisor n' of n and an element of $(\mathbb{Z}/(n',\frac{n}{n'})\mathbb{Z})^*$.) We write δ for $|D|$, δ_1 for the divisor, $\delta_2=\delta/\delta_1$ for the complementary divisor. The numbers δ_1 and δ_2 can be written uniquely as the norms of integral ideals $\mathfrak{d}_1$ and $\mathfrak{d}_2$ of K which are products of ramified primes. If $(\delta_1,\delta_2)=1$, then we can uniquely write $\delta_i=|D_i|$ with D_1 and D_2 discriminants of quadratic fields and $D_1D_2=D$; we then have the associated Dirichlet characters $\varepsilon_i=\varepsilon_{D_i} \pmod{\delta_i}$ and genus character $\chi_{D_1\cdot D_2}$ as in §0. For odd D this is always the case, while for even D we can also have $(\delta_1,\delta_2)=2$. Since the latter case is more complicated, we restrict our attention in the next several sections to the case D odd, and discuss briefly what happens for even D in §8.

It will be most convenient for our purposes to have formulas for the behavior of θ_A and $E_s^{(1)}$ for all matrices in $SL_2(\mathbb{Z})$, not just a system of representatives for $\Gamma_0(ND)\backslash\Gamma_0(N)$, since later on we will need information about the Fourier development of $\widetilde{\Phi}_s$ at all cusps of $\Gamma_0(N)$ rather than just at ∞. We begin with $E_s^{(1)}$. For each decomposition $D=D_1\cdot D_2$ we define, with the notations just introduced,

$$E_s^{(D_1)}(z) = \frac{1}{2}\sum_{\substack{m,n\in\mathbb{Z}\\ D_2|m}} \frac{\varepsilon_1(m)\varepsilon_2(n)}{(mz+n)^{2k-1}}\,\frac{y^s}{|mz+n|^{2s}}\;; \tag{2.1}$$

this is compatible with the notation $E_s^{(1)}$ and belongs, as is easily checked, to $\widetilde{M}_{2k-1}(\Gamma_0(D),\varepsilon)$. For $\gamma=\begin{pmatrix}a&b\\c&d\end{pmatrix}\in SL_2(\mathbb{Z})$ with $(c,D)=\delta_2$ we have

$$\begin{aligned} E_s^{(1)}|_{2k-1}\gamma &= \frac{1}{2}\sum_{\substack{m,n\in\mathbb{Z}\\ D|m}} \frac{\varepsilon(n)}{[m(az+b)+n(cz+d)]^{2k-1}}\,\frac{y^s}{|m(az+b)+n(cz+d)|^{2s}}\\ &= \frac{1}{2}\sum_{\substack{m,n\in\mathbb{Z}\\ md\equiv nc\ (D)}} \frac{\varepsilon(an-bm)}{(mz+n)^{2k-1}}\,\frac{y^s}{|mz+n|^{2s}}\,, \end{aligned}$$

where in the second line we have replaced (m,n) by $\gamma^{-1}(m,n)$. Now

$md\equiv nc \pmod D \qquad d(an-bm)\equiv(ad-bc)n=n\,,\quad c(an-bm)\equiv(ad-bc)m=m \pmod D$

and hence, since $(c,d)=1$ and $(c,D)=\delta_2$ imply $(c,D_1)=(d,D_2)=1$,

$$\varepsilon(an-bm) = \varepsilon_1(an-bm)\varepsilon_2(an-bm) = \varepsilon_1(c)\varepsilon_1(m)\varepsilon_2(d)\varepsilon_2(n)\,.$$

The condition $md\equiv nc \pmod D$ is equivalent to the two conditions $D_2|m$ and $n\equiv c^*md \pmod{D_1}$, where c^* is an inverse of $c \pmod{D_1}$. Replacing n by $c^*md+n\delta_1$, and choosing c^* to satisfy $c^*\equiv 0 \pmod{D_2}$, so that $\varepsilon_2(mc^*d+\delta_1 n)=\varepsilon_2(\delta_1)\varepsilon_2(n)$, we find

$$\begin{aligned} E_s^{(1)}|_{2k-1}\gamma &= \frac{1}{2}\sum_{\substack{m,n\in\mathbb{Z}\\ D_2|m}} \frac{\varepsilon_1(c)\varepsilon_1(m)\varepsilon_2(d)\varepsilon_2(\delta_1)\varepsilon_2(n)\,y^s}{(mz+mc^*d+\delta_1 n)^{2k-1}|mz+mc^*d+\delta_1 n|^{2s}}\\ &= \varepsilon_{D_1}(c)\,\varepsilon_{D_2}(d\delta_1)\,\delta_1^{-s-2k+1}\,E_s^{(D_1)}\Big(\frac{z+c^*d}{\delta_1}\Big) \end{aligned} \tag{2.2}$$

$$\Big(\gamma=\begin{pmatrix}a&b\\c&d\end{pmatrix}\in SL_2(\mathbb{Z})\,,\quad (c,D)=|D_2|,\quad D_1D_2=D\Big)\,.$$

We now turn to θ_A. Here the corresponding formula is :

<u>Lemma 2.3.</u> <u>For</u> $\gamma=\begin{pmatrix}a&b\\c&d\end{pmatrix}\in PSL_2(\mathbb{Z})$, $(c,D)=|D_2|, D_1\cdot D_2=D$ <u>we have</u>

$$\theta_A|_1\gamma = \varepsilon_{D_1}(c/\delta_2)\varepsilon_{D_2}(d)\kappa(D_1)^{-1}\delta_1^{-\frac{1}{2}}\chi_{D_1\cdot D_2}(A)\,\theta_{A\mathcal{D}_1}\Big(\frac{z+c^*d}{\delta_1}\Big)\,,$$

<u>where</u> $\kappa(D_1)$ <u>denotes</u> 1 <u>or</u> i <u>according as</u> $D_1>0$ <u>or</u> $D_1<0$ <u>and</u> $\mathcal{D}_1$ is <u>the ideal class of the ideal</u> $\mathfrak{d}_1$ <u>with</u> $\mathfrak{d}_1^2=(D_1)$.

<u>Proof</u>: It will suffice to treat the case $c=\delta_2$. Indeed, let $\gamma=\begin{pmatrix}a&b\\c&d\end{pmatrix}$ be an

it will suffice to treat the case $c=\delta_2$. Indeed, let $\gamma=\begin{pmatrix}a&b\\c&d\end{pmatrix}$ be an arbitrary element of $SL_2(\mathbb{Z})$ with $(c,D)=\delta_2$ and choose $x\in\mathbb{Z}$ so that $cx\equiv d\delta_2 \pmod{D_1}$ and $(x,D_2)=1$. Then we can find a matrix $\gamma_1=\begin{pmatrix}\cdot&\cdot\\\delta_2&x\end{pmatrix}$ in $SL_2(\mathbb{Z})$, and the matrix $\gamma_0=\gamma\gamma_1^{-1}=\begin{pmatrix}ax-b\delta_2&\cdot\\cx-d\delta_2&\cdot\end{pmatrix}$ is in $\Gamma_0(D)$, so

$$\begin{aligned} \theta_A|_1\gamma &= \theta_A|_1\gamma_0\gamma_1 = (ax-b\delta_2)\;\theta_A|_1\gamma_1\\ &= \varepsilon_1(c)\varepsilon_1(\delta_2)\varepsilon_2(a)\varepsilon_2(x)\cdot\varepsilon_2(x)\kappa(D_1)^{-1}\delta_1^{-\frac{1}{2}}\,\chi_{D_1\cdot D_2}(A)\,\theta_{A\mathcal{D}_1}\Big(\frac{z+\delta_2^*x}{\delta_1}\Big) \end{aligned}$$

by the special case $c=\delta_2$ of (2.3), and this proves (2.3) in general. So assume $c=\delta_2$ and write

$$\theta_A\left(\frac{az+b}{cz+d}\right) = \theta_A\left(\frac{a}{c}+\zeta\right) = \frac{1}{w}\sum_{\lambda\in\mathfrak{a}} e\left(\frac{N(\lambda)}{A}\left(\frac{a}{c}+\zeta\right)\right), \quad \zeta = \frac{-1}{c(cz+d)}$$

ith A, w as in (1.1). The number $N(\lambda)/A$ is integral and its value modulo $=\delta_2$ depends only on $\lambda \pmod{\mathfrak{a}\mathfrak{d}_2}$. Hence

$$\theta_A\left(\frac{az+b}{cz+d}\right) = \frac{1}{w}\sum_{\lambda\in\mathfrak{a}/\mathfrak{a}\mathfrak{d}_2} e_c\left(a\frac{N(\lambda)}{A}\right)\sum_{\mu\in\mathfrak{a}\mathfrak{d}_2} e\left(N(\lambda+\mu)\frac{\zeta}{A}\right).$$

n the other hand, the Poisson summation formula gives

$$\sum_{\mu\in\mathfrak{b}} e(N(\lambda+\mu)z) = \frac{i\,\delta^{-\frac12}}{N(\mathfrak{b})\,z}\sum_{\nu\in\mathfrak{b}^{-1}\mathfrak{d}^{-1}} e\left(-\frac{N(\nu)}{z}\right) e(\mathrm{Tr}\,\lambda\nu)$$

or any $z\in\mathfrak{H}$ and any fractional ideal $\mathfrak{b}$ of K (consider the left-hand side s a periodic function of $\lambda\in\mathbb{C}/\mathfrak{b}$ and compute its Fourier development), so this an be rewritten

$$\theta_A\left(\frac{az+b}{cz+d}\right) = \frac{-i\,(cz+d)}{w\,\delta^{\frac12}}\sum_{\lambda\in\mathfrak{a}/\mathfrak{a}\mathfrak{d}_2} e_c\left(a\frac{N(\lambda)}{A}\right)\sum_{\nu\in\mathfrak{a}^{-1}\mathfrak{d}_2^{-1}\mathfrak{d}^{-1}} e(AN(\nu)c(cz+d))\; e(\mathrm{Tr}\;\lambda\nu)$$

r, replacing ν by ν/δ_2,

$$\theta_A|_1\gamma = \frac{-i}{w\delta^{\frac12}}\sum_{\nu\in\mathfrak{a}^{-1}\mathfrak{d}_1^{-1}} C(\nu)\; e\left(AN(\nu)\left(z+\frac{d}{c}\right)\right)$$

ith

$$C(\nu) = \sum_{\lambda\in\mathfrak{a}/\mathfrak{a}\mathfrak{d}_2} e_c\left(a\frac{N(\lambda)}{A}\right) e_c(\mathrm{Tr}\;\lambda\nu).$$

hoose $\lambda_0\in\mathfrak{a}$ so that the ideal $(\lambda_0)\mathfrak{a}^{-1}$ is prime to $\mathfrak{d}_2$. Then as μ runs ver a set of representatives for $\mathcal{O}/\mathfrak{d}_2$ ($\mathcal{O}$ = ring of integers of K) the numbers $_0\mu$ give a system of representatives for $\mathfrak{a}/\mathfrak{a}\mathfrak{d}_2$, so

$$C(\nu) = \sum_{\mu\in\mathcal{O}/\mathfrak{d}_2} e_{\delta_2}(RN(\mu))\; e_{\delta_2}(\mathrm{Tr}\;\lambda_0\nu\mu)$$

ith $R = aN(\lambda_0)/A$. Note that $\mathrm{Tr}(\lambda_0\nu\mu)\in\mathbb{Z}$ because $\lambda_0\nu\mu\in\mathfrak{d}_1^{-1}\subset\mathfrak{d}^{-1}$, and that is prime to δ_2. Hence, choosing an inverse R^* of $R \pmod{\delta_2}$ which is ivisible by D_1, we find

$$e_{\delta_2}(RN(\mu)+\mathrm{Tr}(\lambda_0\nu\mu)) = e_{\delta_2}(RN(\mu)+RR^*\mathrm{Tr}(\lambda_0\nu\mu))$$

$$= e_{\delta_2}(RN(\mu+R^*\lambda_0'\nu'))\; e_{\delta_2}(-R^*N(\lambda_0\nu)),$$

so

$$C(\nu) = e_{\delta_2}(-R^*N(\lambda_0\nu))\cdot\sum_{\mu\in\mathcal{O}/\mathcal{O}\mathfrak{d}_2} e_{\delta_2}(R\,N(\mu)).$$

Because δ_2 is square-free and completely ramified, one can choose the integers modulo δ_2 as a system of representatives for $\mathcal{O}/\mathfrak{d}_2$, so

$$\sum_{\mu\in\mathcal{O}/\mathfrak{d}_2} e_{\delta_2}(RN(\mu)) = \sum_{n\in\mathbb{Z}/\delta_2} e_{\delta_2}(Rn^2) = \kappa(D_2)\,\delta_2^{\frac12}\,\varepsilon_{D_2}(R)$$

by the usual evaluation of Gauss sums. Also,

$$e\left(AN(\nu)\left(z+\frac{d}{c}\right)\right) e_c(-R^*N(\lambda_0\nu)) = e\left(AN(\nu)\left(z+\frac{d-R^*N(\lambda_0)/A}{\delta_2}\right)\right)$$

$$= e\left(N(\mathfrak{a}\mathfrak{d}_1)\,N(\nu)\,\frac{z+c^*d}{\delta_1}\right)$$

because $d-R^*N(\lambda_0)/A$ is $\equiv 0 \pmod{\delta_2}$ and $\equiv d \pmod{\delta_1}$, and $\varepsilon_{D_2}(R) = \varepsilon_{D_2}(d)\,\chi_{D_1\cdot D_2}(A)$ because $R = aN(\mathfrak{b})$ with $\mathfrak{b} = (\lambda_0)\mathfrak{a}^{-1}$ in the class A^{-1}. Therefore

$$\theta_A|_1\gamma = \frac{-i\kappa(D_2)}{\delta_1^{1/2}}\,\varepsilon_{D_2}(d)\,\chi_{D_1\cdot D_2}(A)\,\frac{1}{w}\sum_{\nu\in\mathfrak{a}^{-1}\mathfrak{d}^{-1}} e\left(N(\mathfrak{a}\mathfrak{d}_1)N(\nu)\,\frac{z+c^*d}{\delta_1}\right),$$

and this completes the proof of (2.3) since $\kappa(D_1)\kappa(D_2)=i$ and $\theta_{A^{-1}\mathcal{D}_1^{-1}}=\theta_{A\mathcal{D}_1}$.

From (2.3) and (2.4) we find for $\gamma=\begin{pmatrix}a&b\\c&d\end{pmatrix}\in\Gamma_0(N)$ with $(c,D)=\delta_2$

$$E_s^{(1)}(Nz)\;\theta_A(z)|_{2k}\gamma = \left(E_s^{(1)}|_{2k-1}\begin{pmatrix}a&bN\\c/N&d\end{pmatrix}\right)(Nz)\;\left(\theta_A|_1\begin{pmatrix}a&b\\c&d\end{pmatrix}\right)(z)$$

$$= \varepsilon_1(c/N)\varepsilon_2(d\delta_1)\delta_1^{-s-2k+1}\varepsilon_1(c/\delta_2)\varepsilon_2(d)\kappa(D_1)^{-1}\delta_1^{-\frac12}\chi_{D_1\cdot D_2}(A)\cdot$$

$$\cdot E_s^{(D_1)}\left(\frac{Nz+(c/N)^*d}{\delta_1}\right)\quad\theta_{A\mathcal{D}_1}\left(\frac{z+c^*d}{\delta_1}\right)$$

$$= \varepsilon_1(N)\kappa(D_1)^{-1}\delta_1^{-s-2k+\frac12}\chi_{D_1\cdot D_2}(A)\;E_s^{(D_1)}\left(N\frac{z+c^*d}{\delta_1}\right)\quad\theta_{A\mathcal{D}_1}\left(\frac{z+c^*d}{\delta_1}\right)$$

where we have used $\varepsilon_{D_1}(\delta_2)\varepsilon_{D_2}(\delta_1)=1$. The trace from $\Gamma_0(ND)$ to $\Gamma_0(N)$ is given by summing over $\sum_{\delta_1|D}\delta_1$ representatives $\begin{pmatrix}a&b\\c&d\end{pmatrix}$ of $\Gamma_0(ND)\backslash\Gamma_0(N)$, the representatives being characterized by the value $\delta_2=(c,D)$ and by the residue class of c^*d modulo $\delta_1 = \delta/\delta_2$. Hence

$$\begin{aligned}\tilde{\Phi}_s(z) &= Tr_N^{ND}(E_s^{(1)}(Nz)\ \theta_A(z)) \\ &= \sum_{D=D_1\cdot D_2} \frac{\varepsilon_{D_1}(N)\,\chi_{D_1\cdot D_2}(a)}{\kappa(D_1)\,\delta_1^{s+2k-1/2}} \sum_{j \pmod{\delta_1}} E_s^{(D_1)}\Big(N\frac{z+j}{\delta_1}\Big)\ \theta_{AD_1}\Big(\frac{z+j}{\delta_1}\Big) \\ &= \sum_{D=D_1\cdot D_2} \frac{\varepsilon_{D_1}(N)\,\chi_{D_1\cdot D_2}(a)}{\kappa(D_1)\,\delta_1^{s+2k-3/2}} \Big(E_s^{(D_1)}(Nz)\quad \theta_{AD_1}(z)\Big)\Big|\,U_{D_1},\end{aligned}$$

where U_n $(n\in\mathbb{N})$ is the usual operator

$$U_n:\ f(z) \mapsto \frac{1}{n}\sum_{j \,(\mathrm{mod}\, n)} f\Big(\frac{z+j}{n}\Big), \qquad \sum_{m\in\mathbb{Z}} A_m(y)\, e(mx) \mapsto \sum_{m\in\mathbb{Z}} A_{mn}(y/n)\, e(mx)$$

on functions on $\mathcal{H}$ of period 1. But for any function f on $\mathcal{H}$ of period 1 we have

$$(f(z)\,\theta_{AD_1}(z))\,|U_{\delta_1} = (f(\delta_2 z)\,\theta_{AD_1}(\delta_2 z))\,|U_\delta = (f(\delta_2 z)\,\theta_A(z))\,|U_\delta\,.$$

because $\theta_{AD_1}(\delta_2 z)$ and $\theta_A(z)$ have the same n-th Fourier coefficient for any n divisible by δ_2 (since $AD_1 = AD_2$ and any integral ideal of norm n is $\mathfrak{d}$ times an integral ideal of norm n/δ_2). Hence we obtain finally:

<u>Proposition 2.4.</u> <u>Assume</u> $(D,2N)=1$. <u>Then the function</u> $\tilde{\Phi}_s(z)$ <u>defined in Proposition 1.2 is given by</u> $\tilde{\Phi}_s = (E_s(Nz)\theta_A(z))|U_{|D|}$, <u>where</u>

$$E_s(z) = \sum_{D=D_1\cdot D_2} \frac{\varepsilon_{D_1}(N)\,\chi_{D_1\cdot D_2}(A)}{\kappa(D_1)\,|D_1|^{s+2k-3/2}}\, E_s^{(D_1)}(|D_2|z)\,.$$

<u>Here the sum is over all decompositions of</u> D <u>as a product of two fundamental discriminants</u> D_1 <u>and</u> D_2, $\chi_{D_1\cdot D_2}$ <u>is the corresponding genus character,</u> $\kappa(D_1) = 1$ <u>or</u> i <u>according as</u> $D_1>0$ <u>or</u> $D_1<0$, <u>and</u> $E_s^{(D_1)}$ <u>is the Eisenstein series (2.1).</u>

Note that E_s depends on N and A (or at least on N modulo D and on the genus of A); however, we omit this dependence in our notation. In the case $k=2$, $|D|=p$ prime and $\varepsilon(N)=1$, $E_s(z)$ is simply $E_s^{(1)}(pz) - ip^{-s-\frac{1}{2}}E_s^{(p)}(z)$.

§ 3. <u>Fourier expansions</u>

Let $E_s(z)$ be the combination of Eisenstein series defined in Proposition 2.4 and write

$$E_s(z) = \sum_{n\in\mathbb{Z}} e_s(n,y)\, e(nx) \qquad (z=x+iy\in\mathcal{H})\,.$$

Then Proposition 2.4 gives the Fourier expansion

$$(3.1)\qquad \tilde{\Phi}_{s,A}(z) = \sum_{\substack{n\in\mathbb{Z}\\ \ell\geq 0\\ Nn+\ell\equiv 0 \,(\mathrm{mod}\, D)}} e_s\Big(n,\frac{Ny}{\delta}\Big)\, r_A(\ell)\, e^{-2\pi\ell y/\delta}\, e\Big(\frac{Nn+\ell}{\delta}x\Big)$$

($\delta=|D|$ as before). The coefficients $e_s(n,y)$ are described by the following two propositions.

<u>Proposition 3.2.</u> <u>The</u> n^{th} <u>Fourier coefficient of</u> $E_s(z)$ <u>is given by</u>

$$e_s(0,y) = L(2s+2k-1,\varepsilon)\,(\delta y)^s + \frac{\varepsilon(N)}{i\sqrt{\delta}}\, V_s(0)\, L(2s+2k-2,\varepsilon)\,(\delta y)^{-s-2k+2}$$

<u>if</u> $n=0$ <u>and by</u>

$$e_s(n,y) = \frac{\varepsilon(N)}{i\sqrt{\delta}}\,(\delta y)^{-s-2k+2}\, V_s(ny) \sum_{\substack{d|n\\ d>0}} \frac{\varepsilon(n,d)}{d^{2s+2k-2}}$$

<u>if</u> $n\neq 0$, <u>where</u> $\varepsilon(n,d) = \varepsilon_A(n,d)$ <u>is defined by</u>

$$\varepsilon(n,d) = \begin{cases} 0 & \text{if } (d,\frac{n}{d},D) \neq 1 \\ \varepsilon_{D_1}(d)\,\varepsilon_{D_2}(-N\frac{n}{d})\,\chi_{D_1\cdot D_2}(A) & \text{if } (d,\frac{n}{d},D) = 1, \\ & (d,D)=|D_2|,\ D_1D_2=D, \end{cases}$$

and $V_s(t)$ $(s \in \mathbb{C},\ t \in \mathbb{R})$ is defined by

$$V_s(t) = \int_{-\infty}^{\infty} \frac{e^{-2\pi i x t}\,dx}{(x+i)^{2k-1}(x^2+1)^s} \qquad (\mathrm{Re}(s) > 1-k) .$$

Proposition 3.3. The function $V_s(t)$ ocurring in 3.2 has the following properties:

a) $V_s(0) = (-1)^k \pi i 2^{-2s-2k+3}\ \Gamma(2s+2k-2)/\Gamma(s)\Gamma(s+2k-1)$.

b) For $t \neq 0$ the function $V_s(t)$ continues holomorphically to all s and satisfies a locally uniform (in s) estimate $V_s(t) = |t|^{O(1)} e^{-2\pi|t|}$ $(|t| \to \infty)$.

c) For $t \neq 0$, set $V_s^*(t) = (\pi|t|)^{-s-2k+1}\ \Gamma(s+2k-1)\ V_s(t)$.

Then $V_s^*(t)$ is entire in s and satisfies $V_s^*(t) = \mathrm{sgn}(t) V_{2-2k-2s}^*(t)$.

d) Let r be an integer satisfying $0 \le r \le k-1$. Then

$$V_{-r}(t) = \begin{cases} 0 & (t<0) , \\ 2\pi i(-1)^{k-r} p_{k,r}(4\pi t) e^{-2\pi t} & (t>0) , \end{cases}$$

where $p_{k,r}(t)$ is the polynomial $(t/2)^{2k-2-2r} \sum_{j=0}^{r} \binom{r}{j} \frac{(-t)^j}{(2k-2r-2+j)!}$.

e) For $t<0$, the derivative with respect to s of $V_s(t)$ at the symmetry point of the functional equation is given by

$$\frac{\partial}{\partial s} V_s(t)\Big|_{s=1-k} = -2\pi i q_{k-1}(4\pi|t|) e^{-2\pi t} \qquad (t<0) ,$$

where

$$q_{k-1}(t) = \int_1^{\infty} \frac{(x-1)^{k-1}}{x^k} e^{-xt}\,dx \qquad (t>0) .$$

Proof. We have

$$e_s(n,y) = \sum_{\substack{D=D_1\cdot D_2 \\ D_2|n}} \frac{\varepsilon_{D_1}(N)\chi_{D_1\cdot D_2}(A)}{\kappa(D_1)\delta_1^{s+2k-3/2}} e_s^{(D_1)}(n/\delta_2, \delta_2 y) ,$$

where $e_s^{(D_1)}$ is defined by

$$E_s^{(D_1)}(n,y) = \sum_{n \in \mathbb{Z}} e_s^{(D_1)}(n,y) e(nx) .$$

The computation of the Fourier development is standard. The terms with $m=0$ in (2.1) give 0 unless $D_1=1$ (since $|D_1|>1 \Rightarrow \varepsilon_1(0)=0$), while if $D_1=1, D_2=D$ they give $L(2s+2k-1,\varepsilon)y^s$. On the other hand, the Poisson summation formula gives the identity

$$\sum_{\ell \in \mathbb{Z}} \frac{1}{(z+\ell)^{2k-1}|z+\ell|^{2s}} = y^{-2s-2k+2} \sum_{r \in \mathbb{Z}} V_s(ry) e^{2\pi i r x}$$

with $V_s(t)$ as in Proposition 3.2, so

$$E_s^{(D_1)}(z) - \begin{cases} L(2s+2k-1,\varepsilon)y^s & \text{if } D_1=1 \\ 0 & \text{otherwise} \end{cases}$$

$$= \frac{y^s}{\delta_2^{2s+2k-1}} \sum_{m=1}^{\infty} \varepsilon_1(m\delta_2) \sum_{n (\mathrm{mod}\,\delta_2)} \varepsilon_2(n) \sum_{\ell \in \mathbb{Z}} \left(mz+\frac{n}{\delta_2}+\ell\right)^{-2k+1} \left|mz+\frac{n}{\delta_2}+\ell\right|^{-2s}$$

$$= \frac{\varepsilon_1(\delta_2) y^{-s-2k+2}}{\delta_2^{2s+2k-1}} \sum_{m=1}^{\infty} \frac{\varepsilon_1(m)}{m^{2s+2k-2}} \sum_{n (\mathrm{mod}\,\delta_2)} \varepsilon_2(n) \sum_{r \in \mathbb{Z}} V_s(rmy) e\left(rmx+\frac{rn}{\delta_2}\right) .$$

But

$$\sum_{n(\mathrm{mod}\ \delta_2)} \varepsilon_2(n)\, e(\tfrac{rn}{\delta_2}) = \varepsilon_2(r)\kappa(D_2)\delta_2^{1/2}$$

(Gauss sum), so this equals

$$\frac{\varepsilon_1(\delta_2)\kappa(D_2)}{\delta_2^{2s+2k-3/2}}\, y^{-s-2k+2} \sum_{\substack{m>0\\ r\in\mathbb{Z}}} \frac{\varepsilon_1(m)\varepsilon_2(r)}{m^{2s+2k-2}}\, V_s(rmy)\, e(rmx)\ .$$

Hence

$$e_s^{(D_1)}(0,y) = \begin{cases} L(2s+2k-1,\varepsilon)y^s & \text{if } D_1=1,\ D_2=D,\\ V_s(0)L(2s+2k-2,\varepsilon)y^{-s-2k+2} & \text{if } D_1=D,\ D_2=1,\\ 0 & \text{otherwise,}\end{cases}$$

while

$$e_s^{(D_1)}(n,y) = \frac{\varepsilon_1(\delta_2)\kappa(D_2)}{\delta_2^{2s+2k-3/2}} \left(\sum_{\substack{m|n\\ m>0}} \frac{\varepsilon_1(m)\varepsilon_2(n/m)}{m^{2s+2k-2}}\right) y^{-s-2k+2}\, V_s(ny)$$

for $n \neq 0$. For the coefficients of E_s this gives

$$e_s(0,y) = L(2s+2k-1,\varepsilon)(\delta y)^s + \frac{\varepsilon(N)}{i\sqrt{\delta}}\, V_s(0)L(2s+2k-2,\varepsilon)(\delta y)^{-s-2k+2}\quad ,$$

$$e_s(n,y) = i\delta^{-s-2k+\frac{3}{2}}\left(\sum_{\substack{D=D_1\cdot D_2\\ D_2|n}} \varepsilon_{D_1}(-N)\chi_{D_1\cdot D_2}(A) \sum_{\substack{m|n/\delta_2\\ m>0}} \frac{\varepsilon_{D_1}(m\delta_2)\varepsilon_{D_2}(n/m\delta_2)}{(m\delta_2)^{2s+2k-2}}\right) y^{-s-2k+2} V_s(ny) \qquad (n\neq 0)\ ,$$

where we have used $\kappa(D_2)/\kappa(D_1) = i\varepsilon_{D_1}(-1)$. The inner sum can be rewritten $\sum_{0<d|n} \varepsilon_{D_1}(d)\varepsilon_{D_2}(n/d)d^{-2s-2k+2}$, since the only non-zero terms here are those of the form $d=md_2$ ($D_2|n$ and D_2 must be prime to n/d). This gives the formula stated in Proposition 3.2.

We now give the proof of Proposition 3.3. The integral defining $V_s(t)$ can be found in several standard tables, where it is expressed in terms of Whittaker functions, but the results found in various tables do not agree and we prefer to give direct proofs of all the properties needed. We start with a). We have

$$V_s(0) = \int_{-\infty}^{\infty} \frac{(x-i)^{2k-1}dx}{(x^2+1)^{s+2k-1}} = -2i\sum_{j=0}^{k-1}(-1)^j\binom{2k-1}{2j+1}\int_0^{\infty}\frac{x^{2k-2j-2}dx}{(x^2+1)^{s+2k-1}}\ ,$$

where we have expanded $(x-i)^{2k-1}$ by the binomial theorem and discarded the odd terms in the integrand. The integral occurring in the sum equals $\frac{1}{2}\Gamma(k-j-\frac{1}{2})\,\Gamma(s+k+j-\frac{1}{2})/\Gamma(s+2k-1)$ (beta function) so using the duplication formula for the gamma function, we find

$$V_s(0) = \frac{(-1)^k 2^{3-2k-2s}\pi i\Gamma(2s+2k-2)}{\Gamma(s+2k-1)\Gamma(s+k-1)} \sum_{j=0}^{k-1} \frac{(-1/4)^{k-1-j}(2k-1)!}{(2j+1)!(k-1-j)!}(s+k-\tfrac{1}{2})\cdots(s+k+j-\tfrac{3}{2})\ .$$

That the sum equals $s(s+1)\dots(s+k-2)$ can be checked by hand for small valves of k and by a tedious induction argument in general. A different method, which is less elementary but works directly for all k , uses the Henkel integral formula for $1/\Gamma(s)$:

$$\begin{aligned} V_s(0) &= (-1)^{k-1} i\int_{-\infty}^{\infty}\frac{dx}{(1+ix)^s(1-ix)^{s+2k-1}}\\ &= \frac{(-1)^{k-1}i}{\Gamma(s+2k-1)}\int_{-\infty}^{\infty}\frac{1}{(1+ix)^s}\int_0^{\infty}e^{-u(1-ix)}u^{s+2k-2}du\,dx\\ &= \frac{(-1)^{k-1}}{\Gamma(s+2k-1)}\int_0^{\infty}e^{-2u}u^{s+2k-2}\left(\int_{-1-i\infty}^{-1+i\infty}(-z)^{-s}e^{-uz}dz\right)du \end{aligned}$$

$(z=-1-ix)$

$$= \frac{(-1)^k}{\Gamma(s+2k-1)} \int_0^\infty e^{-2u} u^{s+2k-2} \left(\frac{2\pi i}{\Gamma(s)} u^{s-1}\right) du$$

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

This proves a) and the meromorphic continuation of $V_s(t)$ when $t=0$.

Now suppose $t>0$ and define $V_s^*(t)$ as in c).

Then

$$V_s^*(t) = \int_{-\infty}^{\infty} (x-i)^{2k-1} \left(\int_0^\infty u^{s+2k-2} e^{-\pi t(x^2+1)u} du\right) e^{-2\pi itx} dx$$

$$= \int_0^\infty u^{s+2k-2} e^{-\pi t(u+1/u)} \int_{-\infty}^{\infty} e^{-\pi tu(x+i/u)^2} (x-i)^{2k-1} dx\, du .$$

In the inner integral we move the path of integration from $\mathrm{Im}(x) = 0$ to $\mathrm{Im}(x) = -\frac{1}{u}$ and make the substitution $x=-\frac{i}{u}+\frac{v}{\sqrt{u}}$ $(v\in\mathbb{R})$ to obtain

$$V_s^*(t) = \int_0^\infty u^{s+k-1} e^{-\pi t(u+1/u)} \int_{-\infty}^{\infty} e^{-\pi tv^2}\left(v+\frac{u^{1/2}+u^{-1/2}}{i}\right)^{2k-1} dv \frac{du}{u} .$$

This integral converges for all s and is clearly an even function of $s+k-1$ (replace u by $1/u$) , so we have obtained the meromorphic continuation and functional equation of $V_s(t)$ for $t>0$; the proof for $t<0$ is exactly similar. If we wish, we can use the last formula to write $V_s^*(t)$ in terms of standard

functions: expanding $\left(v+\frac{u^{\frac12}+u^{-\frac12}}{i}\right)^{2k-1}$ by the trinomial theorem we obtain the expression

$$V_s^*(t) = i \sum_{\substack{a,b,c\geq 0\\ 2a+b+c=2k-1}} \frac{(-1)^{k-a}(2k-1)!}{(2a)!b!c!} \frac{\Gamma(a+1/2)}{(\pi t)^{a+\frac12}} \int_0^\infty u^{s+k+\frac{b-c}{2}-1} e^{-\pi t(u+\frac{1}{u})} du$$

$$= \frac{2(-1)^k i}{t^{1/2}} \sum_{\substack{a,b,c\geq 0\\ 2a+b+c=2k-1}} \frac{(2k-1)!}{a!b!c!} \left(\frac{-1}{4\pi t}\right)^a K_{s+k-1+(b-c)/2}(2\pi t) \qquad (t>0)$$

for $V_s^*(t)$ as a linear combination of K-Bessel functions, the functional equation now following from $K_\nu(z)=K_{-\nu}(z)$ by interchanging b and c . For $k=1$ the formula simplifies to

$$V_s^*(t) = \frac{-2i}{\sqrt{t}} \left(K_{\frac12+s}(2\pi t) + K_{\frac12-s}(2\pi t)\right) \quad (k=1, t>0) .$$

In any case, we have proved the functional equation c). The estimate $V_s^*(t)=|t|^{O(1)}e^{-2\pi|t|}$ in b) follows easily from the above integral representations or from the explicit formulas in terms of $K_\nu(2\pi t)$.

For d), we note that

$$V_{-r}(t) = \int_{-\infty}^{\infty} \frac{(x-i)^r}{(x+i)^{2k-1-r}} e^{-2\pi ixt} dx$$

for $r\in\mathbb{Z}$, $0\leq r\leq k-1$ (for $r=k-1$ the integral is only conditionally convergent; we could also treat the cases $r=k,k+1,\ldots,2k-2$ by using the functional equation). The integrand has a pole only at $x=-i$, so if $t<0$ we can move the path of integration up to

$+i\infty$ to get $V_{-r}(t) = 0$, while if $t > 0$ we can move it down to $-i\infty$ to get

$$V_{-r}(t) = -2\pi i \ \mathrm{Res}_{x=-i}\left(\frac{(x-i)^r}{(x+i)^{2k-1-r}}\, e^{-2\pi ixt}\right)$$

$$= -2\pi i \sum_{j=0}^{r} \binom{r}{j} (-2i)^j \ \mathrm{Res}_{x=-i}\left(\frac{e^{-2\pi ixt}}{(x+i)^{2k-1-2r+j}}\right)$$

$$= (-1)^{k-r} 2\pi i \ p_{k,r}(4\pi t)\ e^{-2\pi t} .$$

Finally, suppose $t < 0$ and consider the integral defining $V_s(t)$ near $s = 1-k$. The integrand is well-defined in the x-plane cut along the imaginary axis from $-i\infty$ to $-i$ and from $+i$ to $+i\infty$, and we can deform the path of integration upwards to a path C circling the half-line $[i,i\infty)$ in a counterclockwise direction (from $-\varepsilon+i\infty$ to $i-i\varepsilon$ to $+\varepsilon+i\infty$). The new integrand converges for all s (this, by the way, shows that $V_s(t)$, and not only $V_s^*(t)$, is entire in s for $t < 0$, and a similar argument applies for $t > 0$ if we deform the path of integration downwards to circle $(-i\infty,-i]$; this completes the proof of 3.3b, which up to now we had only established with "meromorphically" in place of "holomorphically"), and we can differentiate under the integral sign to obtain

$$\frac{\partial}{\partial s} V_s(t)\Big|_{s=1-k} = -\int_C \frac{(x-i)^{k-1}}{(x+i)^k} \log(x^2+1)\, e^{-2\pi itx} dx \quad (t<0) .$$

The function $\log(x^2+1)$ is continuous on C and changes by $2\pi i$ as one passes from one side of C to the other across the branch cut $[i,i\infty)$. Therefore

$$\frac{\partial}{\partial s} V_s(t)\Big|_{s=1-k} = -2\pi i \int_i^{i\infty} \frac{(x-i)^{k-1}}{(x+i)^k}\, e^{-2\pi itx} dx \quad (t<0) ,$$

and replacing x by $2ix-i$ we obtain the formula given in e). This completes the proof of Proposition 3.3.

From equation (3.1) and Propositions 3.2 and 3.3d we obtain a finite formula for the Fourier coefficients of $\tilde{\Phi}_s(z)$ at arguments $s=-r$ $(r = 0, 1, \ldots, k-1)$ as polynomials in $\frac{1}{y}$ of degree r:

<u>Corollary 3.4.</u> <u>For</u> $r \in \mathbb{Z}$, $0 \le r \le k-1$, <u>we have</u>

$$\tilde{\Phi}_{-r}(z) = \sum_{m=0}^{\infty} \left(\sum_{0\le n\le \frac{m\delta}{N}} e_{n,r}(y)\, r_{\mathcal{A}}(m\delta-nN)\right) e^{2\pi imz} ,$$

<u>where</u>

$$e_{0,r}(y) = \begin{cases} L(2k-2r-1,\varepsilon)\ (Ny)^{-r} & \text{if } r<k-1, \\ [L(1,\varepsilon) - \varepsilon(N)\frac{\pi}{\sqrt{\delta}}L(0,\varepsilon)]\ (Ny)^{1-k} & \text{if } r=k-1, \end{cases}$$

$$e_{n,r}(y) = (-1)^{k-r}\varepsilon(N)\frac{2\pi}{\sqrt{\delta}}(Ny)^{r-2k+2} p_{k,r}\left(\frac{4\pi Nny}{\delta}\right) \sum_{\substack{d|n\\ d>0}} \varepsilon_{\mathcal{A}}(n,d)\, d^{2r-2k+2} \qquad (n>0)$$

<u>with</u> $p_{k,r}$ <u>as in 3.3d</u>, $\varepsilon_{\mathcal{A}}(n,d)$ <u>as in 3.2</u>. (We have written $e_{n,r}(y)$ for $e_{-r}(n,\frac{Ny}{\delta})\, e^{2\pi Nny/\delta}$.)

In particular, $\tilde{\Phi}_{0,\mathcal{A}}$ is a holomorphic modular form; this, of course, was clear *a priori* since the definition of the Eisenstein series $\mathcal{E}_s(z)$ shows that it is holomorphic in z at $s=0$.

§4. Functional equation; preliminary formulae for $L_{\mathcal{A}}(f,k)$ and $L'_{\mathcal{A}}(f,k)$

We wish to prove the functional equation for $L_{\mathcal{A}}(f,s)$ given in (0.2). In view of Proposition 1.2 and equation (3.1), this will follow from the identity

$$(4.1)\qquad e_s^*(n,y) \;:=\; \pi^{-s}\delta^s\,\Gamma(s+2k-1)\,e_s(n,y) \;=\; -\varepsilon(N)\,e^*_{2-2k-s}(n,y)$$

for $n\in\mathbb{Z}$ satisfying

$$(4.2)\qquad Nn+\ell\equiv 0 \pmod{D} \quad \text{for some } \ell=N(\mathfrak{a}),\quad \mathfrak{a}\text{ integral ideal in } \mathcal{A}.$$

From the first equation of Proposition 3.2 and (a) of Proposition 3.3 we obtain

$$\begin{aligned} e_s^*(0,y) \;=\;& (s+k)(s+k+1)\ldots(s+2k-2)[\,\pi^{-s}\delta^s\Gamma(s+k)L(2s+2k-1,\varepsilon)\,]\,(\delta y)^s \\ &-\varepsilon(N)(2-k-s)(3-k-s)\ldots(-s)[\,\pi^{\frac12-s}\delta^{s-\frac12}\Gamma(s+k-\tfrac12)L(2s+2k-2,\varepsilon)]\,(\delta y)^{2-2k-s}\,, \end{aligned}$$

and this proves (4.1) for $n=0$ since the two expressions in square brackets are interchanged under $s\to 2-2k-s$ by the functional equation of $L(s,\varepsilon)$. For $n\neq 0$ we have

$$e_s^*(n,y) = -i\varepsilon(N)\,|n|^k\,\pi^{2k-1}\,\delta^{-2k+\frac32}\,y\,V_s^*(ny)\sum_{\substack{d\mid n\\ d>0}}\varepsilon_{\mathcal{A}}(n,d)\,(|n|/d^2)^{s+k-1}$$

with $V_s^*(t)$ as in (c) of Proposition 3.3. In view of the functional equation of $V_s^*(ny)$, therefore, (4.1) will follow from the identity

$$(4.3)\qquad \varepsilon_{\mathcal{A}}(n\,,\,|n|/d\,) \;=\; -\varepsilon(N)\,\mathrm{sgn}(n)\;\varepsilon_{\mathcal{A}}(n,d)$$

for n satisfying (4.2) and d a positive divisor of n. We can assume that $(d,\frac{n}{d},D)=1$ since otherwise both sides of (4.3) are zero. Then D decomposes as

$$D=D_0D'D''\,,\qquad |D'|=(d,D)\,,\qquad |D''|=(\tfrac{n}{d},D)$$

with D_0, D', D'' discriminants and D_0 prime to n. The discriminants D_1 and D_2 in the definition of $\varepsilon(n,d)$ are then D_0D'' and D', respectively, while the corresponding discriminants for $\varepsilon(n,|n|/d)$ are D_0D' and D''. Hence

$$\begin{aligned} \varepsilon(n,d) \;&=\; \varepsilon_{D_0}(d)\varepsilon_{D''}(d)\varepsilon_{D'}(-N\tfrac{n}{d})\;\chi_{D_0D''\cdot D'}(\mathcal{A})\,, \\ \varepsilon(n,\tfrac{|n|}{d}) \;&=\; \varepsilon_{D_0}(\tfrac{|n|}{d})\varepsilon_{D'}(\tfrac{|n|}{d})\varepsilon_{D''}(-N\,\mathrm{sgn}(n)\,d)\;\chi_{D_0D'\cdot D''}(\mathcal{A})\,. \end{aligned}$$

All terms in these two expressions take on values in $\{\pm1\}$, and the product is

$$\varepsilon(n,d)\,\varepsilon(n,\tfrac{|n|}{d}) \;=\; \varepsilon_{D_0}(|n|)\;\varepsilon_{D'D''}(-N\,\mathrm{sgn}(n))\;\chi_{D_0\cdot D'D''}(\mathcal{A})\,,$$

which equals $\varepsilon_D(-N)\,\mathrm{sgn}(n)$ because (4.2) implies that $\chi_{D_0\cdot D'D''}(\mathcal{A})=\varepsilon_{D_0}(\ell)=\varepsilon_{D_0}(-Nn)$. This completes the proof of the functional equation.

The functional equation suggests that we look at the symmetry point $s=1-k$ or, more specifically, at the value or derivative of $L_{\mathcal{A}}(f,s)$ there, depending whether $\varepsilon(N)=-1$ or $\varepsilon(N)=1$. We consider first the former case. Here we can apply Proposition 1.2 and Corollary 3.4 with $r=k-1$ to find:

Proposition 4.4. *Suppose $\varepsilon(N)=-1$. Then the value of $L_{\mathcal{A}}(f,s)$ at the symmetry point of the functional equation is given by*

$$L_{\mathcal{A}}(f,k) \;=\; \frac{2^{2k+1}\pi^{k+1}}{(k-1)!\,\sqrt{\delta}}\;(f\,,\,\tilde{\Phi})$$

where $\tilde{\Phi}\in\widetilde{M}_{2k}(\Gamma_0(N))$ has the Fourier expansion

$$\tilde{\Phi}(z) \;=\; \sum_{m=0}^{\infty}\Big(\sum_{0<n\le\frac{m\delta}{N}}\sigma_{\mathcal{A}}(n)\,r_{\mathcal{A}}(m\delta-Nn)\,p_{k-1}\big(\tfrac{4\pi Nny}{\delta}\big)+\frac{h}{u}\,r_{\mathcal{A}}(m)\Big)\,y^{1-k}\,e^{2\pi imz}$$

with

$$\sigma_{\mathcal{A}}(n) \;=\; \sum_{\substack{d\mid n\\ d>0}}\varepsilon_{\mathcal{A}}(n,d)\,,\qquad\qquad p_{k-1}(t) \;=\; \sum_{j=0}^{k-1}\binom{k-1}{j}\frac{(-t)^j}{j!}\,.$$

Note that the coefficients of $\tilde{\Phi}$ are polynomials in y^{-1} of degree $k-1$. For $k=1$ the function $\tilde{\Phi}$ is a holomorphic modular form (but not a cusp form).

Now consider the case $\varepsilon(N)=1$. Here we have to compute the derivative of $e_s(n,y)$ with respect to s at $s=1-k$. There are three cases, according to the sign of n. If $n=0$ then the formulas at the beginning of this section give

$$\begin{aligned} \frac{\partial}{\partial s}e_s(0,y)\Big|_{s=1-k} \;&=\; \frac{\pi^{1-k}\delta^{k-1}}{(k-1)!}\;\frac{\partial}{\partial s}\,e_s^*(0,y)\Big|_{s=1-k} \\ &=\; 2\,\frac{\pi^{1-k}\delta^{k-1}}{(k-1)!}\;\frac{\partial}{\partial s}[\,\Gamma(s+2k-1)\pi^{-s}\delta^{2s}y^{s}L(2s+2k-1,\varepsilon)]\Big|_{s=1-k} \\ &=\; 2\,L(1,\varepsilon)\,(\delta y)^{1-k}\Big[\,\frac{\Gamma'}{\Gamma}(k)+\log\frac{\delta^2y}{\pi}\;+\;2\,\frac{L'}{L}(1,\varepsilon)\,\Big]\,. \end{aligned}$$

If n is positive, then the sum $\sum_{d|n} \varepsilon(n,d)\, d^{-2s-2k+2}$ in Proposition 3.2 vanishes at $s=1-k$, so

$$\frac{\partial}{\partial s} e_s(n,y)\Big|_{s=1-k} = 2i\, \delta^{-k+\frac12} y^{-k+1} V_{1-k}(ny) \sum_{d|n} \varepsilon(n,d) \log d \quad .$$

If n is negative, then it is instead the factor $V_s(ny)$ in 3.2 which vanishes at $s=1-k$, so

$$\frac{\partial}{\partial s} e_s(n,y)\Big|_{s=1-k} = -i\, \delta^{-k+\frac12} y^{-k+1} \frac{\partial}{\partial s} V_s(n,y)\Big|_{s=1-k} \cdot \sum_{d|n} \varepsilon(n,d) \quad .$$

Substituting for $V_{1-k}(ny)$ $(n>0)$ and $\frac{\partial}{\partial s} V_s(ny)\big|_{s=1-k}$ $(n<0)$ from parts (d) and (e) of Proposition 3.3, and combining with (3.1) and Proposition 1.2, we find:

Proposition 4.5. Suppose $\varepsilon(N)=1$. Then the derivative of $L_{\mathcal{A}}(f,s)$ at the symmetry point of the functional equation is given by

$$L'_{\mathcal{A}}(f,k) = \frac{2^{2k+1}\pi^{k+1}}{(k-1)!\sqrt{\delta}} \ (f\,,\,\Phi)$$

where $\tilde{\Phi} \in \tilde{M}_{2k}(\Gamma_0(N))$ has the Fourier expansion

$$\tilde{\Phi}(z) = \sum_{m=-\infty}^{\infty} \Bigg(- \sum_{0<n\le\frac{m\delta}{N}} \sigma'_{\mathcal{A}}(n)\, r_{\mathcal{A}}(m\delta-Nn)\, p_{k-1}\Big(\frac{4\pi nNy}{\delta}\Big)$$
$$+ \frac{h}{u} r_{\mathcal{A}}(m) \Big(\log y + \frac{\Gamma'}{\Gamma}(k) + \log N\delta - \log \pi + 2\frac{L'}{L}(1,\varepsilon) \Big)$$
$$- \sum_{n=1}^{\infty} \sigma_{\mathcal{A}}(n)\, r_{\mathcal{A}}(m\delta+Nn)\, q_{k-1}\Big(\frac{4\pi nNy}{\delta}\Big) \Bigg)\, y^{1-k} e^{2\pi i m z}$$

with $\sigma_{\mathcal{A}}(n)$ and $p_{k-1}(t)$ as in Proposition 4.4, q_{k-1} as in Proposition 3.3e, and

$$\sigma'_{\mathcal{A}}(n) = \sum_{\substack{d|n \\ d>0}} \varepsilon_{\mathcal{A}}(n,d) \log \frac{n}{d^2} \qquad (n>0) \quad .$$

(The function $\tilde{\Phi}$ is $\frac{N^{k-1}\sqrt{\delta}}{2\pi} \frac{\partial}{\partial s} \tilde{\Phi}_s\big|_{s=1-k}$. In the formula for its m^{th} Fourier coefficient we have replaced n by $-n$ in the third term; the first two terms are absent if $m<0$.)

Propositions 4.4 and 4.5 are the preliminary formulas for $L_{\mathcal{A}}(f,k)$ and $L'_{\mathcal{A}}(f,k)$ referred to in the section heading. We now make them more explicit by

giving a simple closed formula for the arithmetical functions $\sigma_{\mathcal{A}}(n)$ and $\sigma'_{\mathcal{A}}(n)$. Let $\{n\}$ be the genus of any integral ideal of K satisfying

$$N(n) \equiv \varepsilon(N)\, N \pmod{D}$$

(this is independent of the choice of n), $\{\mathcal{A}n\}$ its product with the genus of the ideal class $\mathcal{A}$, and (as in Chapter II)

$R_{\{\mathcal{A}n\}}(n)$ = number of integral ideals of norm n in the genus $\{\mathcal{A}n\}$

$\delta(n) = 2^s$, s = number of prime factors of (n,D).

Then we have

Proposition 4.6. a) Let n be an integer satisfying (4.2) and $\varepsilon(N)n<0$. Then

$$\sigma_{\mathcal{A}}(n) = \delta(n)\, R_{\{\mathcal{A}n\}}(|n|) \quad .$$

b) Suppose $n>0$ and $\varepsilon(N)=1$. Then

$$\sigma'_{\mathcal{A}}(n) = \sum_{p|n} a_p(n) \log p$$

with

$$a_p(n) = \begin{cases} 0 & \text{if } \varepsilon(p)=1\,, \\ (\mathrm{ord}_p(n)+1)\, \delta(n)\, R_{\{\mathcal{A}nc\}}(\frac{n}{p}) & \text{if } \varepsilon(p)=-1\,, \\ \mathrm{ord}_p(n)\, \delta(n)\, R_{\{\mathcal{A}nc\}}(\frac{n}{p}) & \text{if } \varepsilon(p)=0\,, \end{cases}$$

where in the last two cases $\{c\}$ is the genus of any integral ideal with $N(c) \equiv -p \pmod{D}$.

Remarks. 1. The genus of c in b) is well-defined, since if $\varepsilon(p)=-1$ then $-p$ is prime to N and determines a genus by the usual correspondence

$$\{\text{genera of } K\} \xleftrightarrow{1:1} \{x \in (\mathbb{Z}/D\mathbb{Z})^* \mid \varepsilon(x)=1\}/(\mathbb{Z}/D\mathbb{Z})^{*2} \ ,$$

while if $\varepsilon(p)=0$ then the genus characters of c corresponding to all prime divisors $p' \ne p$ of D are determined (we must have $(\frac{N(c)}{p'}) = (\frac{-p}{p'})$) and the genus character corresponding to p is therefore also fixed (the product of the genus characters corresponding to all prime divisors of D is the trivial character).

Explicitly, we could take $\mathfrak{C} = \mathfrak{q}$ when $\varepsilon(p) = -1$ and $\mathfrak{C} = \mathfrak{q}\mathfrak{p}$ when $\varepsilon(p) = 0$, where $\mathfrak{q}$ is a prime ideal satisfying $N(\mathfrak{q}) \equiv -p \pmod{D}$ in the first case and in the second case $\mathfrak{p}$ is the prime divisor of p in K and $\mathfrak{q}$ any prime ideal with $N(\mathfrak{q}) \equiv -1 \pmod{D/p}$.

2. The numbers $a_p(n)$ in (b) are all even, since $\delta(n)$ is even if n is divisible by a ramified prime and $\mathrm{ord}_p(n)+1$ is even if n is divisible by an inert prime p with $R(n/p) \neq 0$. This is of course as it should be, because under the assumptions of (b) we have $\sum_{d|n} \varepsilon_{\mathcal{A}}(n,d) = 0$, as shown at the beginning of this section, and consequently $\sigma'_{\mathcal{A}}(n) = -2 \sum_{d|n} \varepsilon_{\mathcal{A}}(n,d) \log d$.

<u>Proof</u>. a) We assume for definiteness that $\varepsilon(N) = -1$ and n is positive (i.e. the case needed for Proposition 4.4); the opposite case is exactly similar. If n is prime to D then the formula is very easy: in this case we have $\varepsilon_{\mathcal{A}}(n,d) = \varepsilon(d)$ for all divisors d of n (since $D_2 = 1$, $D_1 = D$ in the definition of $\varepsilon_{\mathcal{A}}$) and consequently $\sigma_{\mathcal{A}}(n) = \sum_{d|n} \varepsilon(d) = R(n)$, the total number of representations of n as the norm of an integral ideal of K; from (4.2) it follows that any such representation belongs to the genus $\{\mathcal{A}\mathfrak{n}\}$. In general, write $n = p_1^{\nu_1} \cdots p_s^{\nu_s} n_0$ with $(n_0, D) = 1$. Any divisor d of n with $(d, \frac{n}{d}, D) = 1$ has the form $d = p_1^{\mu_1} \cdots p_s^{\mu_s} d_0$ with $d_0 | n_0$ and $\mu_i = 0$ or ν_i for each i. The function $\varepsilon_{\mathcal{A}}(n,d)$ is multiplicative in d for n fixed, i.e. $\varepsilon_{\mathcal{A}}(n,d'd'') = \varepsilon_{\mathcal{A}}(n,d')\,\varepsilon_{\mathcal{A}}(n,d'')$ for $d'd''|n$, $(d',d'') = 1$. Indeed, let $D = D_1' \cdot D_2' = D_1'' \cdot D_2'' = D_1 \cdot D_2$ be the splittings of D occurring in the definition of $\varepsilon_{\mathcal{A}}$ for d', d'' and d'd'', respectively; then $D_2 = D_2' D_2''$ and consequently

$$\begin{aligned}
\varepsilon_{\mathcal{A}}(n,d')\,\varepsilon_{\mathcal{A}}(n,d'') &= \varepsilon_{D_1'}(d')\varepsilon_{D_2'}(-N\tfrac{n}{d'})\,\chi_{D_1' \cdot D_2'}(\mathcal{A}) \cdot \varepsilon_{D_1''}(d'')\varepsilon_{D_2''}(-N\tfrac{n}{d''})\,\chi_{D_1'' \cdot D_2''}(\mathcal{A}) \\
&= \varepsilon_{D_1 D_2''}(d')\varepsilon_{D_2'}(d'')\varepsilon_{D_2'}(-N\ell\tfrac{n}{d'd''}) \cdot \varepsilon_{D_1 D_2'}(d'')\varepsilon_{D_2''}(d')\varepsilon_{D_2''}(-N\ell\tfrac{n}{d'd''})
\end{aligned}$$

(ℓ any norm from the ideal class $\mathcal{A}$ prime to D)

$$= \varepsilon_{D_1}(d'd'')\varepsilon_{D_2}(-N\ell\tfrac{n}{d'd''}) = \varepsilon_{\mathcal{A}}(n,d'd'') .$$

Hence

$$\begin{aligned}
\sigma_{\mathcal{A}}(n) &= \sum_{\mu_1 \in \{0,\nu_1\}} \cdots \sum_{\mu_s \in \{0,\nu_s\}} \sum_{d_0 | n_0} \varepsilon_{\mathcal{A}}(n,p_1^{\mu_1}) \cdots \varepsilon_{\mathcal{A}}(n,p_s^{\mu_s})\varepsilon_{\mathcal{A}}(n,d_0) \\
&= \prod_{i=1}^{s} (1 + \varepsilon_{\mathcal{A}}(n,p_i^{\nu_i})) \cdot \sum_{d_0 | n_0} \varepsilon(d_0) .
\end{aligned}$$

The sum equals $R(n_0)$, and this in turn equals $R(n)$ because there is a 1:1 correspondence between integral ideals of norm n_0 and of norm n given by multiplication with $\mathfrak{p}_1^{\nu_1} \cdots \mathfrak{p}_s^{\nu_s}$, where $\mathfrak{p}_i^2 = (p_i)$. If $R(n) = 0$ then both sides of our identity are zero and we are done. If not, then the ideals of norm n all belong to the same genus. To complete the proof, we must show that $\varepsilon_{\mathcal{A}}(n,p_i^{\nu_i}) = 1$ for all i if and only if this genus coincides with $\{\mathcal{A}\mathfrak{n}\}$, i.e. if and only if the values of every genus character χ on these two genera agree. It suffices to consider χ associated to prime divisors p of D, since these generate the group of genus characters. If $p \nmid n$, then the condition to be checked is just $(\frac{n}{p}) = (\frac{-N\ell}{p})$ for some ℓ prime to p representable as the norm of an ideal in $\mathcal{A}$, and this follows from (4.2). If p divides n, then p is one of the p_i. Every ideal of norm n has the form $\mathfrak{p}_i^{\nu_i}\mathfrak{m}$ with $N(\mathfrak{m}) = n/p_i^{\nu_i}$, and the value of χ on this ideal is given by

$$\chi(\mathfrak{p}_i^{\nu_i}\mathfrak{m}) = \chi(\mathfrak{p}_i^{\nu_i})\,\chi(\mathfrak{m}) = \varepsilon_{D_1}(p_i^{\nu_i})\,\varepsilon_{D_2}(n/p_i^{\nu_i}) ,$$

where D_2 is the prime discriminant associated to p_i (i.e. $|D_2| = p_i$, $D_1 \equiv 1$ (mod and $D_1 = D/D_2$. But these are the same D_1 and D_2 as occur in the definition of $\varepsilon_{\mathcal{A}}(n,d)$ for $d = p_i^{\nu_i}$, so

$$\varepsilon_{\mathcal{A}}(n,p_i^{\nu_i}) = \varepsilon_{D_1}(p_i^{\nu_i})\varepsilon_{D_2}(-Nn/p_i^{\nu_i})\,\chi_{D_1 \cdot D_2}(\mathcal{A}) = \chi(\mathfrak{p}_i^{\nu_i}\mathfrak{m})\,\chi(\mathfrak{n}\mathcal{A})$$

and we are done.

b) This case is rather similar. By Remark 2, we have $\sigma'_{\mathcal{A}}(n) = \sum_{p|n} a_p(n) \log p$ with $a_p(n) = -2 \sum_{d|n} \varepsilon_{\mathcal{A}}(n,d)\,\mathrm{ord}_p(d)$. Write $n = p^{\nu} n_1$ with $p \nmid n_1$. The divisors of n have the form $p^{\mu} d_1$ with $0 \le \mu \le \nu$, $d_1 | n_1$, so using the multiplicativity proved in part (a) we find

$$a_p(n) = -2 \sum_{\mu=0}^{\nu} \mu\, \varepsilon_{\mathcal{A}}(n,p^{\mu}) \cdot \sum_{d_1 | n_1} \varepsilon_{\mathcal{A}}(n_1,d_1) .$$

If $\varepsilon(p)=+1$ then $\varepsilon_{\mathcal{A}}(n,p^{\mu})=\varepsilon(p^{\mu})=1$ for all μ, so

$$\nu\cdot\sum_{d_1|n_1}\varepsilon_{\mathcal{A}}(n,d_1) = \sum_{\mu=0}^{\nu}\varepsilon_{\mathcal{A}}(n,p^{\mu})\sum_{d_1|n_1}\varepsilon_{\mathcal{A}}(n,d_1) = \sigma_{\mathcal{A}}(n),$$

and this was shown at the beginning of the section to be zero under the hypotheses of (b). Hence $a_p(n)=0$ in this case. If $\varepsilon(p)=-1$, then the same argument shows that $\sum_{d_1|n_1}\varepsilon_{\mathcal{A}}(n,d_1)=0$, and consequently $a_p(n)=0$, if ν is even, since then $\sum_{\mu=0}^{\nu}\varepsilon_{\mathcal{A}}(n,p^{\mu})=\sum_{\mu=0}^{\nu}(-1)^{\mu}\neq 0$. If ν is odd, then $\sum_{\mu=0}^{\nu}\mu\,\varepsilon_{\mathcal{A}}(n,p^{\mu})=-1+2-3+\ldots-\nu$ $=-\frac{1}{2}(\nu+1)$, so $a_p(n)=(\nu+1)\sum_{d_1|n_1}\varepsilon_{\mathcal{A}}(n,d_1)$. If d_1 is a divisor of n_1 and $D=D_1D_2$ the corresponding decomposition of D, then

$$\varepsilon_{\mathcal{A}}(n,d_1)=\varepsilon_{\mathcal{A}}(n_1p^{\nu},d_1)=\varepsilon_{D_2}(p^{\nu})\,\varepsilon_{\mathcal{A}}(n_1,d_1)=\chi_{D_1\cdot D_2}(\mathfrak{c})\,\varepsilon_{\mathcal{A}}(-n_1,d_1)=\varepsilon_{\mathcal{A}\mathfrak{c}}(-n_1,d_1),$$

with $\mathfrak{c}$ as in the statement of the proposition. Therefore $\sum_{d_1|n_1}\varepsilon_{\mathcal{A}}(n,d_1)=\sigma_{\mathcal{A}\mathfrak{c}}(-n_1)$ $=\delta(n_1)R_{\{\mathcal{A}\mathfrak{c}n\}}(n_1)$ by part (a), and this is what we want since $\delta(n_1)=\delta(n)$ and $R_{\{\mathcal{A}\mathfrak{c}n\}}(n_1)=R_{\{\mathcal{A}\mathfrak{c}n\}}(n/p)$. Finally, suppose $p|D$. Then $\varepsilon_{\mathcal{A}}(n,p^{\mu})$ vanishes for $0<\mu<\nu$, so

$$a_p(n) = -2\nu\,\varepsilon_{\mathcal{A}}(n,p^{\nu})\sum_{d_1|n_1}\varepsilon_{\mathcal{A}}(n,d_1) = -2\nu\sum_{d_1|n_1}\varepsilon_{\mathcal{A}}(n,p^{\nu}d_1) = 2\nu\sum_{d_1|n_1}\varepsilon_{\mathcal{A}}(n,d_1),$$

where for the last equality we have used the identity $\varepsilon_{\mathcal{A}}(n,d)=-\varepsilon_{\mathcal{A}}(n,n/d)$ proved at the beginning of the section and replaced d_1 by n_1/d_1. A computation like the one above gives $\varepsilon_{\mathcal{A}}(n,d_1)=\varepsilon_{\mathcal{A}\mathfrak{c}\mathfrak{p}^{\nu-1}}(-n_1,d_1)$ in this case, so using part (a) again we find

$$a_p(n) = 2\nu\,\sigma_{\mathcal{A}\mathfrak{c}\mathfrak{p}^{\nu-1}}(-n_1) = 2\nu\,\delta(n_1)\,R_{\{\mathcal{A}n\mathfrak{c}\mathfrak{p}^{\nu-1}\}}(n_1),$$

and the desired result follows in this case because $\delta(n)=2\delta(n_1)$ and $R_{\{\mathcal{A}n\mathfrak{c}\mathfrak{p}^{\nu-1}\}}(n_1)=R_{\{\mathcal{A}n\mathfrak{c}\}}(n/p)$. This completes the proof of Proposition 4.6.

We remark that the formula in b) implies that $\sigma'_{\mathcal{A}}(n)$ is always a multiple of the logarithm of a single prime number. [Specifically: It is 0 if n is divisible to an odd power by more than one prime inert in K and equals

$(\mathrm{ord}_p(n)+1)\,\delta(n)R_{\{\mathcal{A}n\}}(p)\log p$ if there is a unique such prime p. If there is no such prime, then n is the norm of some ideal; let Q be the norm of an ideal prime to D lying in the genus of the product of this ideal with $\{\mathcal{A}n\}$; then $(\frac{-Q}{p})=-1$ for an odd number of prime divisors p of D, and $\sigma'_{\mathcal{A}}(n)$ equals $\delta(n)\,\mathrm{ord}_p(n)\,R(n)\log p$ if there is exactly one such p and 0 if there is more than one.] Actually, this property of $\sigma'_{\mathcal{A}}$ can be seen <u>a priori</u>: under the hypothesis of b), the sum $\sum_{d|n}\varepsilon_{\mathcal{A}}(n,d)\,d^{-s}$ vanishes at $s=0$ and has derivative equal to $\frac{1}{2}\sigma'_{\mathcal{A}}(n)$ there, and since this sum has an Euler product (by the multiplicativity of $d\mapsto\varepsilon_{\mathcal{A}}(n,d)$ proved above), we see that $\sigma'_{\mathcal{A}}(n)$ can be non-zero only if exactly one Euler factor of this sum vanishes at $s=0$, and is then an integer multiple of the corresponding $\log p$.

§5. Holomorphic projection and final formulae for $L_{\mathcal{A}}(f,r)$ and $L'_{\mathcal{A}}(f,k)$, $k>1$

In Sections 3 and 4 we obtained formulae for special values of $L_{\mathcal{A}}(f,s)$ and of its derivative in the critical strip as the scalar products of f with certain non-holomorphic modular forms. We would like to have instead formulae expressing these values as scalar products of f with something holomorphic. To do this we will use a "holomorphic projection lemma" due to Sturm [33] which we now state and (since our hypotheses are slightly different from Sturm's) prove.

<u>Proposition 5.1.</u> *Let $\tilde{\Phi}\in\tilde{M}_{2k}(\Gamma_0(N))$ be a non-holomorphic modular form of weight $2k>2$ and level N with the Fourier expansion $\tilde{\Phi}(z)=\sum_{m=-\infty}^{\infty}a_m(y)\,e^{2\pi imz}$, and suppose that $(\tilde{\Phi}|_{2k}\alpha)(z)=O(y^{-\varepsilon})$ as $y=\mathrm{Im}(z)\to\infty$ for some $\varepsilon>0$ and every $\alpha\in SL_2(\mathbb{Z})$. Define*

$$a_m = \frac{(4\pi m)^{2k-1}}{(2k-2)!}\int_0^{\infty}a_m(y)\,e^{-4\pi my}\,y^{2k-2}\,dy \qquad (m>0).$$

Then the function $\Phi(z)=\sum_{m=1}^{\infty}a_m\,e^{2\pi imz}$ is a holomorphic cusp form of weight $2k$ and level N and satisfies $(f,\Phi)=(f,\tilde{\Phi})$ for all $f\in S_{2k}(\Gamma_0(N))$.

<u>Proof.</u> For $m>0$ define the Poincaré series $P_m(z)$ by

$$P_m(z) = \sum_{\gamma\in\Gamma_\infty\backslash\Gamma_0(N)} e^{2\pi imz}|_{2k}\gamma = \sum_{\binom{a\ b}{c\ d}\in\Gamma_\infty\backslash\Gamma_0(N)} (cz+d)^{-2k}\, e^{2\pi im\frac{az+b}{cz+d}}$$

where $\Gamma_\infty = \pm\binom{1\ \mathbf{Z}}{0\ 1}$ as earlier. The series is absolutely convergent because $k>1$, and the function P_m belongs to $S_{2k}(\Gamma_0(N))$. Let P_m^* be the series obtained by replacing every term in the series defining P_m by its absolute value. Then we have the estimate

$$P_m^*(z) \le \sum_{\binom{a\ b}{c\ d}\in\Gamma_\infty\backslash SL_2(\mathbb{Z})} \left|(cz+d)^{-2k}\, e^{2\pi im\frac{az+b}{cz+d}}\right|$$

$$\le |e^{2\pi iz}| + \sum_{\substack{\binom{a\ b}{c\ d}\in\Gamma_\infty\backslash SL_2(\mathbf{Z})\\ c\ne 0}} |cz+d|^{-2k}$$

$$= e^{-2\pi y} + y^{-k}(E(z,k)-y^k)$$

$$= O(y^{1-2k}) \qquad (y\to\infty)$$

since for any $s>1$ the Eisenstein series $E(z,s)$ for $SL_2(\mathbb{Z})$ satisfies $E(z,s) = y^s + O(y^{1-s})$ as $y\to\infty$. Moreover, since we have replaced $\Gamma_0(N)$ by $SL_2(\mathbf{Z})$ in the above estimate, we automatically have the same estimate on $P_m^*|_{2k}\alpha$ for any $\alpha\in SL_2(\mathbb{Z})$. It follows that the $\Gamma_0(N)$-invariant function $P_m^*(z)|\tilde\Phi(z)|y^{2k}$ is bounded by $O(y^{1-\epsilon})$ as $y\to\infty$ and similarly for its composition with any element of $SL_2(\mathbf{Z})$. Hence in the integral defining the Petersson scalar product of P_m and $\tilde\Phi$ it is legitimate to replace P_m by its definition as a series and interchange the summation and integration. This gives

$$(\tilde\Phi, P_m) = \int_{\Gamma_\infty\backslash H} \overline{e^{2\pi imz}}\,\tilde\Phi(z)\, y^{2k-2}\,dy = \int_0^\infty e^{-4\pi my}\, a_m(y)\, y^{2k-2}\,dy$$

by the standard unfolding trick. On the other hand, the map $f\mapsto(\tilde\Phi,f)$ is an antilinear map from $S_{2k}(\Gamma_0(N))$ to $\mathbb{C}$, so is represented by $(\Phi,\cdot)$ for some holomorphic cusp form $\Phi = \sum b_m q^m$. The above computation with $\tilde\Phi$ replaced by Φ shows that

$$(\Phi, P_m) = \int_0^\infty e^{-4\pi my}\, b_m\, y^{2k-2}\,dy = \frac{(2k-2)!}{(4\pi m)^{2k-1}}\, b_m ,$$

so the equality $(\Phi,P_m) = (\tilde\Phi,P_m)$ gives $b_m = a_m$ as desired.

As a special case of Proposition 5.1, if $\tilde\Phi$ is a non-holomorphic modular form of weight $2k$ which is small at the cusps in the sense of the proposition (i.e. $(\tilde\Phi|\alpha)(x+iy) = O(y^{-\epsilon})$ as $y\to\infty$ for all α), and if the Fourier coefficients of $\tilde\Phi$ are polynomials of degree $\le 2k-2$ in $\frac{1}{y}$, then we obtain a holomorphic modular form having the same scalar product with all $f\in S_{2k}(\Gamma_0(N))$ by dropping any terms y^{-j} and replacing any term $y^{-j}e^{2\pi imz}$ $(m>0,\ 0\le j\le 2k-2)$ by $\frac{(2k-2-j)!}{(2k-2)!}(4\pi m)^j e^{2\pi imz}$. We can apply this special case to the functions of Corollary 3.4 and Proposition 4.4.

In Corollary 3.4, the function $\tilde\Phi_{-r}$ is already holomorphic if $r=0$, as we remarked there, so there is nothing to do. If $r\ge 1$, then $k>1$ (since $0\le r\le k-1$) and $\tilde\Phi_{-r}$ is small at the cusps in the above sense (this is clear at ∞ since the constant term of $\tilde\Phi_{-r}$ is a multiple of y^{-r} and the other terms are $O(e^{-2\pi y})$; at the other cusps it can be seen by going back to the definition of $\tilde\Phi_{-r}$ as the trace of the product of a theta function and an Eisenstein series and looking at the expressions for their Fourier developments at the cusps). Hence Proposition 5.1 applies to show that the holomorphic projection of $\tilde\Phi_{-r}$ is the function $\Phi_{-r} = \sum_{m\ge 1} a_{m,r}\, q^m$ with

$$a_{m,r} = \frac{(4\pi m)^{2k-1}}{(2k-2)!} \sum_{n=0}^{[m\delta/N]} r_A(m\delta-nN) \int_0^\infty e_{n,r}(y)\, e^{-4\pi my}\, y^{2k-2}\,dy .$$

Since $e_{n,r}(y)$ is a polynomial in $1/y$ of degree $\le 2k-2$, the integral is a sum of ordinary gamma integrals. Performing the calculation we find

$$a_{m,r} = \frac{(-1)^{k-r}\, 2^{2k-1}\, \epsilon(N)\, r!\, \pi^{2k-1-r}}{(2k-2)!\, N^r\, |D|^{2k-r-3/2}}\, b_{m,r} ,$$

where

$$(5.2)\qquad b_{m,r} = \sum_{0\le n\le m|D|/N} r_A(m|D|-nN)\, P_{k,r}(Nn, m|D|)\, \sigma_{2k-2r-2,A}(n)$$

with

$$(5.3)\qquad P_{k,r}(x,y) = \sum_{j=0}^{r} \binom{r}{j}\binom{2k-2+j-r}{r}(-x)^j\, y^{r-j} ,$$

$$(5.4)\qquad \sigma_{2\ell,A}(n) = \begin{cases} -\frac{1}{2}\varepsilon(N)\,L(-2\ell,\varepsilon) & \text{if } n=0\,, \\ \sum\limits_{n|d} \varepsilon_A(n,d)\,(n/d)^{2\ell} & \text{if } n>0\,. \end{cases}$$

(We have used the functional equation of $L(s,\varepsilon)$.) Now Proposition 1.2 gives:

Theorem 5.5. *Let* A *be an ideal class in an imaginary quadratic field of discriminant* D , N *an integer prime to* D , *and* r *and* k *two integers satisfying* $0 \le r < k-1$. *For* $m \ge 0$ *define* $b_{m,r}$ *by equations (5.2)-(5.4). Then* $\sum_{m\ge0} b_{m,r}\,q^m$ *is a modular form of weight* $2k$ *and level* N (*and a cusp form if* $r \ne 0$) *and*

$$L_A(f,2k-1-r) = \frac{(-1)^{k-r}(2\pi)^{2(2k-1-r)}}{(2k-2-2r)!}\,\frac{2^{2k-1}}{(2k-2)!}\,\frac{\varepsilon(N)\,r!}{|D|^{2k-r-1/2}}\,(f, \textstyle\sum b_{m,r}\,q^m)$$

for any f *in the space spanned by newforms of weight* $2k$ *and level* N .

Here we have omitted the case $r=k-1$, since the formula is slightly different (cf. Proposition 3.2) and we will treat this case in a moment, but we have included the case $r=0$, which, as just observed, can be treated without holomorphic projection. Note that the coefficients $b_{m,r}$ are rational numbers and in fact that all summands in (5.2) except the end terms $n=0$ and $n=m|D|/N$ are integers, and even the end terms are not too far from being integers (we have $r_A(0) = \frac{1}{2u} = \frac{1}{2}$ for any $D<-4$ and $\sigma_{2\ell,A}(0) \in \mathbb{Z}$ for any $D<-4\ell-3$).

For $r=k-1$, corresponding to the central point of the critical strip, the formula is similar but there are various simplifications. We can suppose that $\varepsilon(N)=-1$ since otherwise $L_A(f,k)=0$ by the functional equation. Then Proposition 3.2, and consequently Theorem 5.5, are the same as before except that the terms with $n=0$ must be doubled. However, the function $\sigma_{0,A}(n)$ can be evaluated by the formula in Proposition 4.6, and the polynomial $P_{k,k-1}$ is expressible in terms of a well-known function, namely

$$P_{k,k-1}(x,y) = y^{k-1}\,P_{k-1}(1-2x/y)\ ,$$

where P_{k-1} denotes the (k-1)st Legendre polynomial. (Actually, the polynomials $P_{k,r}$ can always be expressed in terms of standard orthogonal polynomials, namely $P_{k,r}(x,y) = y^r\,P_r^{(2k-2-2r,0)}(1-2x/y)$, where $P_n^{(\alpha,\beta)}$ are

Jacobi polynomials, but these are much less familiar functions.) Thus Theorem 5.5 for $r=k-1$ takes on the form:

Theorem 5.6. *Let* D, A, N *be as in the last theorem,* $\varepsilon(N)=-1$, *and let* k *be any integer* ≥ 1 . *For* $m \ge 0$ *define*

$$b_{m,A} = (m|D|)^{k-1}\Big[\, r_A(m|D|)\,\frac{h}{u} + \sum_{0<n\le m|D|/N} \delta(n)\,R_{\{An\}}(n)\,r_A(m|D|-nN)\,P_{k-1}\big(1-\tfrac{2nN}{m|D|}\big)\Big]$$

with $\delta(n)$, $R_{\{An\}}(n)$ *as in Proposition 4.6. Then* $\sum_{m\ge0} b_{m,A}q^m$ *is a modular form of weight* $2k$ *and level* N (*and a cusp form if* $k \ne 1$) *and*

$$L_A(f,k) = \frac{(2\pi)^{2k}\,2^{2k-1}\,(k-1)!}{(2k-2)!\ |D|^{k-1/2}}\,(f, \textstyle\sum_m b_{m,A}\,q^m)$$

for any f *in the space spanned by newforms of weight* $2k$ *and level* N .

Theorems 5.5 and 5.6 give all values of $L_A(f,s)$ at integral points within the critical strip, since the points to the left of $s=k$ can be obtained by applying the functional equation. Note that the expression for $b_{m,A}$ in Theorem 5.6 can be simplified by dropping the term $r_A(m|D|)\frac{h}{u}$ and changing the summation conditions to $0 \le n \le m|D|/N$, since $\delta(0)=2^t$ (t = number of prime factors of D) and $R_{\{An\}}(0) = h/2^t u$ (each genus contains $h/2^{t-1}$ ideal classes, and $r_A(0) = 1/2u$ for each ideal class).

As an example of Theorem 5.6, take $N=5$, $k=2$ and $D=-p$, where p is a prime satisfying $p \equiv 3 \pmod 4$, $(\frac{5}{p}) = -1$, and sum over all ideal classes A . Since $S_4(\Gamma_0(5))$ is spanned by a unique eigenform $f = q-4q^2+2q^3+8q^4-\dots$ we have $(f, \sum b_m q^m) = b_1(f,f)$ for any form $\sum_m b_m q^m$ in this space. Also $\sum_A L_A(f,s) = L(f,s)\,L_\varepsilon(f,s)$, where $\varepsilon = (\frac{-}{p})$. Hence Theorem 5.6 gives

$$\frac{p^{3/2}}{64\pi^2}\,\frac{L(f,2)\,L_\varepsilon(f,2)}{(f,f)} = \sum_A b_{1,A} = ph(-p) + \sum_{1\le n<\frac{p}{5}} (p-10n)R(n)R(p-5n)$$

where $R(n) = \sum_{d|n} (\frac{d}{p})$ and $h(-p)$ must be replaced by $\frac{1}{3}$ for $p=3$. The first values of the expression on the right-hand side of this formula are

p	3	7	23	43	47	67	83	103	107	127	163	167	223	227	263	283
b_1	1	1	1	49	25	121	361	25	289	25	169	81	121	2025	1	121

;

in accordance with the theorem of Waldspurger-Vignéras [36], they are all squares.

In general, there is some simplification in Theorem 5.6 if we sum over A. Indeed, for any $n, \ell \in \mathbb{N}$ we have

$$\sum_A R_{\{A\mathfrak{n}\}}(n)\, r_A(\ell) = \sum_{\{A\}} R_{\{A\mathfrak{n}\}} R_{\{A\}}(\ell) = R(n)R(\ell) \text{ or } 0,$$

where $R(n) = \sum_{d|n} \varepsilon(d)$ is the total number of representations of n as the norm of an integral ideal of K and we must take $R(n)R(\ell)$ or 0 depending whether the genus of an ideal of norm $n\ell$ (if there is one) is $\{\mathfrak{n}\}$ or not. This is a question of the values of genus characters associated to the primes p dividing N. For $\ell = m|D| - nN$, $-N \equiv N(\mathfrak{n}) \pmod D$ these conditions are automatic for $p\nmid n$ since $\ell \equiv N(\mathfrak{n})n \pmod p$. Hence we have

$$\delta(n) \sum_A R_{\{A\mathfrak{n}\}}(n)\, r_A(m|D| - nN) = R(n)\, R(m|D| - nN) \prod_{p|(n,D)} \left(1 + \hat{\varepsilon}_p\left(\frac{nN - m|D|}{nN}\right)\right)$$

where $\hat{\varepsilon}_p$ is the homomorphism $\mathbb{Q}^\times \to \{\pm 1\}$ defined by $\hat{\varepsilon}_p(n) = \left(\frac{n}{p}\right)$ for $p \nmid n$, $\varepsilon_p(p) = \left(\frac{|D|/p}{p}\right)$ (cf. remarks at the end of §3 of Chapter II). Thus the formula for $\sum_A L_A(f,k) = L(f,k)L_\varepsilon(f,k)$ is a little simpler than the formula for the individual $L_A(f,k)$, as might be expected.

This completes our discussion of the values of $L_A(f,s)$ at integer points in the critical strip. We turn now to the derivative at $s=k$, under the assumption that $\varepsilon(N) = 1$, so that $L_A(f,k)$ vanishes. We must apply Proposition 5.1 to the function $\tilde{\Phi}$ of Proposition 4.5. We assume $k > 1$ (the case $k=1$ will be the subject of the next section). Then the growth conditions at the cusps required in Proposition 5.1 are satisfied. Indeed, at ∞ this follows from the Fourier expansion given in Proposition 4.5, since (denoting by $a_m(y)$ the coefficient of $e^{2\pi i m z}$ and using the estimates $P_{k-1}(t) = O(t^{k-1})$, $q_{k-1}(t) = O(t^{k-1}e^{-t})$, $\sigma_A'(n) = O(n^\varepsilon)$, $r_A(n) = O(n^\varepsilon)$) we have

$$a_m(y) = \begin{cases} O(m^{k+\varepsilon}) & (m > 0), \\ O(y^{1-k}\log y) & (m = 0), \\ O(|m|^{k+\varepsilon} e^{-4\pi|m|y}) & (m < 0) \end{cases}$$

and hence $\tilde{\Phi}(z) = O(y^{1-k}\log y)$. At the other cusps, $\tilde{\Phi}$ has an expansion of

the same type and satisfies the same estimate, as we can see by going back to the definition of $\tilde{\Phi}$ in terms of theta and Eisenstein series. Hence we can apply Proposition 5.1 to get $(f,\tilde{\Phi}) = (f, \sum_{m\geq 1} a_m q^m)$ with

$$\frac{(2k-2)!}{(4\pi m)^{2k-1}} a_m = \int_0^\infty a_m(y)\, e^{-4\pi m y}\, y^{2k-2}\, dy$$
$$= -\sum_{0<n\leq \frac{m\delta}{N}} \sigma_A'(n)\, r_A(m\delta - Nn) \int_0^\infty P_{k-1}\left(\frac{4\pi n N y}{\delta}\right) y^{k-1} e^{-4\pi m y}\, dy$$
$$+ \frac{h}{u} r_A(m) \left[\int_0^\infty y^{k-1} \log y\, e^{-4\pi m y} dy + \left(\frac{\Gamma'}{\Gamma}(k) + \log\frac{N\delta}{\pi} + 2\frac{L'}{L}(1,\varepsilon)\right) \int_0^\infty y^{k-1} e^{-4\pi m y}\, dy \right]$$
$$- \sum_{n=1}^\infty \sigma_A(n)\, r_A(m\delta + nN) \int_0^\infty q_{k-1}\left(\frac{4\pi n N y}{\delta}\right) y^{k-1} e^{-4\pi m y}\, dy .$$

The first integral is elementary and was already evaluated for the proof of Theorem 5.6:

$$\int_0^\infty P_{k-1}\left(\frac{4\pi n N y}{\delta}\right) y^{k-1} e^{-4\pi m y}\, dy = \frac{(k-1)!}{(4\pi m)^k} P_{k-1}\left(1 - 2\frac{nN}{m\delta}\right),$$

where P_{k-1} is the $(k-1)$st Legendre polynomial. The values of the next two integrals follow immediately from the definition of the gamma function:

$$\int_0^\infty y^{k-1} \log y\, e^{-4\pi m y}\, dy = \frac{\partial}{\partial s}\left(\frac{\Gamma(s)}{(4\pi m)^s}\right)\Big|_{s=k} = \frac{(k-1)!}{(4\pi m)^k}\left(\frac{\Gamma'}{\Gamma}(k) - \log 4\pi m\right),$$

$$\int_0^\infty y^{k-1} e^{-4\pi m y}\, dy = \frac{(k-1)!}{(4\pi m)^k} .$$

Finally, substituting into the last integral the formula for q_{k-1} given in Proposition 3.3e, we find

$$\int_0^\infty q_{k-1}\left(\frac{4\pi n N y}{\delta}\right) y^{k-1} e^{-4\pi m y}\, dy = \int_0^\infty y^{k-1} e^{-4\pi m y} \int_1^\infty \frac{(x-1)^{k-1}}{x^k} e^{-\frac{4\pi n N y x}{\delta}}\, dx\, dy$$
$$= \frac{(k-1)!}{(4\pi m)^k} \int_1^\infty \frac{(x-1)^{k-1}\, dx}{x^k \left(1 + \frac{nN}{m\delta}x\right)^k} .$$

The last integral is clearly elementary, since we can write the integrand by a partial fraction decomposition as a linear combination of terms x^{-j} and

$(1+\frac{nN}{m\delta}x)^{-j}$ with $1\le j\le k$. Explicitly, if we set $z=1+2\frac{nN}{m\delta}$, then the substitution $x = 1+\sqrt{\frac{z-1}{z+1}}\,e^t$ gives

$$\int_1^\infty \frac{(x-1)^{k-1}\,dx}{x^k\left(1+\frac{z-1}{2}x\right)^k} = \int_{-\infty}^{\infty} \frac{dt}{(z+\sqrt{z^2-1}\cosh t)^k},$$

and this is the standard integral representation of $2\,Q_{k-1}(z)$, where Q_{k-1} is the Legendre function of the second kind as in Chapter II. This function is indeed elementary; it is defined by the properties

$$(5.7)\quad \begin{cases} Q_{k-1}(z) = \frac{1}{2}P_{k-1}(z)\log\frac{z+1}{z-1} + (\text{polynomial in } z), \\ Q_{k-1}(z) = O(z^{-k}) \qquad (z\to\infty) \end{cases}$$

Putting all this together, and renormalizing slightly by writing $\frac{(4\pi)^{k-1}(k-1)!}{(2k-2)!}a_{m,A}$ for a_m, we obtain the following theorem; since this is the basic result of this chapter (for $k>1$), we have repeated our assumptions and notations.

Theorem 5.8. Suppose $k>1$, $N\ge 1$, and A an ideal class in an imaginary quadratic field K of discriminant D with $\varepsilon(N)=1$ ($\varepsilon=(\frac{D}{\cdot})$). For each $m>0$ define

$$a_{m,A} = m^{k-1}\Big[-\sum_{0<n\le\frac{m|D|}{N}} \sigma_A'(n)\, r_A(m|D|-Nn)\, P_{k-1}\Big(1-\frac{2nN}{m|D|}\Big)$$
$$+\frac{h}{u}r_A(m)\Big(2\frac{\Gamma'}{\Gamma}(k) - 2\log 2\pi + \log\frac{N|D|}{m} + 2\frac{L'}{L}(1,\varepsilon)\Big)$$
$$-2\sum_{n=1}^{\infty}\sigma_A(n)\, r_A(m|D|+nN)\, Q_{k-1}\Big(1+\frac{2nN}{m|D|}\Big)\Big],$$

where h, u and $r_A(n)$ are defined as usual, $\sigma_A(n)$ and $\sigma_A'(n)$ are the arithmetical functions occurring in Propositions 4.4-4.6,

$$P_{k-1}(z) = 2^{1-k}\sum_{0\le n\le (k-1)/2} (-1)^n\binom{k-1}{n}\binom{2k-2-2n}{k-1} z^{k-1-2n}$$

is the $(k-1)$st Legendre polynomial, and $Q_{k-1}(z)$ is the $(k-1)$st Legendre function of the second kind, defined by the properties (5.7). Then the function $\sum_{m\ge 1} a_{m,A}q^m$ is a cusp form of weight $2k$ and level N and we have

$$L_A(f,k) = 0,$$

$$L_A'(f,k) = \frac{2^{4k-1}\pi^{2k}}{(2k-2)!\sqrt{|D|}}\Big(f,\sum_{m\ge 0} a_{m,A}q^m\Big)$$

for all f in the space spanned by newforms of weight $2k$ and level N.

§6. The case $k=1$: final formula for $L_A'(f,1)$

Theorem 5.8 breaks down for forms of weight 2 for several reasons: Proposition 5.1 is not true for $k=1$, the function $\tilde\Phi$ of Proposition 4.5 is not small at the cusps, and the infinite series in the definition of $a_{m,A}$ is no longer convergent (because the function $Q_0(z) = \frac{1}{2}\log\frac{z+1}{z-1}$ is only $O(z^{-1})$ as $z\to\infty$). In this section we will discuss the modifications needed to take care of these difficulties.

In the Fourier expansion of $\tilde\Phi$ in Proposition 4.5, all terms with $m\ne 0$ are exponentially small as $y=\mathrm{Im}(z)$ goes to infinity, while the $m=0$ term has the form $(A\log y+B)y^{1-k}+O(e^{-cy})$ for suitable constants A, B and $c>0$. Thus when $k=1$ the function $\tilde\Phi$ grows like $A\log y+B$ rather than having the decay behavior $O(y^{-\varepsilon})$ required in Propostion 5.1. The same is true at the other cusps, as we shall see, i.e. we have

$$(6.1)\qquad (\tilde\Phi|_2\alpha)(z) = A_\xi\log y + B_\xi + O(y^{-\varepsilon}) \qquad \text{as } y\to\infty$$
$$(\alpha\in SL_2(\mathbb{Z}),\quad \alpha(\infty)=\xi,\quad \varepsilon>0)$$

at a cusp $\xi\in\mathbb{Q}\cup\{\infty\}$. A priori, for a function $\tilde\Phi\in\tilde M_2(\Gamma_0(N))$ satisfying this growth condition there are $2H$ constants A_ξ and B_ξ to deal with, where H is the number of cusps of $\Gamma_0(N)$. This number is the sum over all positive divisors N_1 of N of $\phi((N_1,N/N_1))$ (ϕ = Euler function), the invariants of a cusp $\xi=\frac{a}{c}$ being $N_1=(c,N)$ and the class of $(c/N_1)^{-1}a$ modulo $(N_1,N/N_1)$. However, for our particular function $\tilde\Phi$ the coefficients A_ξ and B_ξ will turn out to depend only on the first invariant N_1. We now formulate the analogue of Proposition 5.1 for functions of this type.

Proposition 6.2. Let $\tilde\Phi(z) = \sum_{m=-\infty}^{\infty} a_m(y)e^{2\pi imz}$ be a function in $\tilde M_2(\Gamma_0(N))$

satisfying the growth condition (6.1) at all cusps ξ, and suppose that the coefficients A_ξ and B_ξ depend only on the greatest common divisor N_1 of N and the denominator of ξ, say $A_\xi = A(N_1)$, $B_\xi = B(N_1)$. Let $\{\alpha(M),\ \beta(M) : M|N\}$ be the solution of the non-singular system of linear equations

$$(6.3)\qquad \sum_{M|N} \frac{(M,N_1)^2}{M^2}\,\alpha(M) = A(N_1) \qquad (N_1|N),$$

$$(6.4)\qquad \sum_{M|N} \frac{(M,N_1)^2}{M^2}\,\{\beta(M) + \alpha(M)\log\frac{(M,N_1)^2}{M}\} = B(N_1) \qquad (N_1|N).$$

Then there is a holomorphic cusp form $\Phi = \sum_{m=1}^{\infty} a_m e^{2\pi i m z} \in S_2(\Gamma_0(N))$ satisfying $(\Phi, f) = (\tilde{\Phi}, f)$ for all $f \in S_2(\Gamma_0(N))$ and with a_m given by

$$(6.5)\qquad a_m = \lim_{s\to 0}\,[\,4\pi m\int_0^\infty a_m(y)\,e^{-4\pi m y}\,y^s\,dy + 24\,\alpha(1)\,\sigma_1(m)\,s^{-1}\,]$$
$$+\,24\,\beta(1)\,\sigma_1(m) + 48\,\alpha(1)\,[\sigma_1'(m) - \sigma_1(m)\,(\log 2m + \tfrac{1}{2} + \tfrac{\zeta'}{\zeta}(2)\,)]$$

for $(m,N)=1$ ($\sigma_1(m) = \sum_{d|m} d$, $\sigma_1'(m) = \sum_{d|m} d\log d$).

Proof: Suppose first that $A(N_1) = B(N_1) = 0$ for all $N_1|N$, i.e. that $\tilde{\Phi}$ satisfies the growth conditions of Proposition 5.1. The proof of Proposition 5.1 goes wrong for $k=1$ because the series defining the majorant P_m^* diverges (due to the pole of $E(z,s)$ at $s=1$). To get around this, we use "Hecke's trick": we replace P_m ($m\ge 1$) by the absolutely convergent series

$$P_{m,s}(z) = \sum_{\Gamma_\infty\backslash\Gamma_0(N)} y^s e^{2\pi i m z}\big|_2\gamma = \sum_{\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)\in\Gamma_\infty\backslash\Gamma_0(N)} \frac{1}{(cz+d)^2}\,\frac{y^s}{|cz+d|^{2s}}\,e^{2\pi i m\frac{az+b}{cz+d}}$$
$$(\,\mathrm{Re}(s) > 0\,)$$

and then continue analytically to $s=0$. The series $P_{m,s}^* = P_{m,\sigma}^*$ ($\sigma = \mathrm{Re}(s)$) obtained by replacing every term of $P_{m,s}$ by its absolute value is majorized by $O(y^{-1-\sigma})$ by the same calculation as in the case $k>1$, the $O(\ )$-constant being itself $O(\frac{1}{\sigma})$ as $\sigma\to 0$. Hence if $0<\sigma<\varepsilon$, $\tilde{\Phi} = O(y^{-\varepsilon})$ at each cusp, then the calculation used for 5.1 is justified and gives

$$(\tilde{\Phi}, P_{m,\bar{s}}) = \int_{\Gamma_\infty\backslash H} e^{-2\pi i m\bar{z}}\,\tilde{\Phi}(z)\,y^s\,dy = \int_0^\infty e^{-4\pi m y}\,a_m(y)\,y^s\,dy$$

(we have replaced s by $\bar{s}$ in the Petersson scalar product to get a holomorphic function of s). As before, we know *a priori* that there is a holomorphic cusp form $\Phi = \sum_{m\ge 1} a_m q^m$ having the same scalar products with holomorphic forms as $\tilde{\Phi}$, and replacing $\tilde{\Phi}$ by Φ in the last formula gives

$$(\Phi, P_{m,\bar{s}}) = a_m\int_0^\infty e^{-4\pi m y}\,y^s\,dy = \frac{\Gamma(1+s)}{(4\pi m)^{1+s}}\,a_m\,.$$

Furthermore, the function $P_m = \lim_{s\to 0} P_{m,s}$ is known to be a holomorphic cusp form of weight 2 (this is proved by computing the Fourier coefficients of $P_{m,s}$ as functions of s), so by the defining property of Φ we have

$$a_m = 4\pi m\lim_{s\to 0}(\Phi, P_{m,\bar{s}}) = 4\pi m\,(\Phi, P_m) = 4\pi m\,(\tilde{\Phi}, P_m)$$
$$= 4\pi m\lim_{s\to 0}\int_0^\infty e^{-4\pi m y}\,a_m(y)\,y^s\,dy\,,$$

where the limit is taken through values of s tending to 0 with $\mathrm{Re}(s)$ positive. This is equivalent with (6.5) since all $\alpha(M)$ and $\beta(M)$ are 0 in this case.

We now turn to the general case, where $\tilde{\Phi}$ satisfies (6.1). Consider the Eisenstein series

$$E_{2,s}(z) = \sum_{\gamma\in\Gamma_\infty\backslash SL_2(\mathbb{Z})} y^s\big|_2\gamma = \frac{1}{2}\sum_{(c,d)=1}\frac{1}{(cz+d)^2}\,\frac{y^s}{|cz+d|^{2s}}$$

which is absolutely convergent for $\mathrm{Re}(s) > 2$ and defines a non-holomorphic modular function of weight 2 on $SL_2(\mathbb{Z})$. This function is orthogonal to holomorphic cusp forms by the calculation above ($E_{2,s}$ is just the function $P_{m,s}$ for $N=1$ with $m=0$) and has the form $y^s + c(s)\,y^{-1-s} + O(e^{-y})$ as $y\to\infty$, where $c(s)$ and the coefficients in the $O(\ )$-term are holomorphic near $s=0$. Hence the two functions

$$E(z) = E_{2,s}(z)\big|_{s=0}\,, \qquad F(z) = \frac{\partial}{\partial s}E_{2,s}(z)\big|_{s=0}\,,$$

where $|_{s=0}$ is defined by holomorphic continuation or simply as the limit for $s\searrow 0$, belong to $\tilde{M}_2(SL_2(\mathbb{Z}))$, are orthogonal to cusp forms, and satisfy

$$E(z) = 1 + O(\tfrac{1}{y})\,, \qquad F(z) = \log y + O(\tfrac{1}{y}\log y)$$

as $y \to \infty$. Hence if we have a function $\tilde{\Phi}$ in $\tilde{M}_2(SL_2(\mathbb{Z}))$ satisfying $\tilde{\Phi}(z) = A\log y + B + O(y^{-\varepsilon})$ for some constants A and B, then we can subtract $AF(z) + BE(z)$ from $\tilde{\Phi}$ to obtain a new function having the same scalar products with holomorphic forms as $\tilde{\Phi}$ and which is $O(y^{-\varepsilon})$ at infinity, so we can find the holomorphic projection of $\tilde{\Phi}$ by applying the result already obtained to this function. For a function of higher level satisfying (6.1) with arbitrary A_ξ and B_ξ, we would in general have to subtract off the analogues of $E(z)$ and $F(z)$ defined using the analogue of $E_{2,s}(z)$ for all cusps of $\Gamma_0(N)$. However, under the hypothesis of 6.2 that A_ξ and B_ξ depend only on the g.c.d. of N and the denominator of ξ, we need only work with the functions $E(Mz)$ and $F(Mz)$, where M runs over the positive divisors of N. To see this, we must compute their behaviour at the various cusps. Let $\xi = \frac{a}{c}$, $(a,c) = 1$, $(c,N) = N_1$. Then for $M|N$ we have $M\frac{a}{c} = \frac{a'}{c'}$ with $a' = \frac{M}{(M,N_1)}a$, $c' = \frac{1}{(M,N_1)}c$, $(a',c') = 1$. Complete $\binom{a}{c}$ and $\binom{a'}{c'}$ to matrices $\alpha = \begin{pmatrix} a & b \\ c & d\end{pmatrix}$, $\alpha' = \begin{pmatrix} a' & b' \\ c' & d'\end{pmatrix}$ in $SL_2(\mathbb{Z})$ and let z, z' be related by $c'z'+d' = \frac{(M,N_1)}{M}(cz+d)$. Then $\frac{a'z'+b'}{c'z'+d'} = M\frac{az+b}{cz+d}$ and $y' = \frac{(M,N_1)^2}{M}y$, so as $y \to \infty$ we have $y' \to \infty$ also and

$$\begin{aligned}
E_{2,s}(Mz)|_2\alpha &= (cz+d)^{-2}\, E_{2,s}\left(M\frac{az+b}{cz+d}\right) \\
&= \frac{(M,N_1)^2}{M^2}\,(c'z'+d')^{-2} E_{2,s}\left(\frac{a'z'+b'}{c'z'+d'}\right) \\
&= \frac{(M,N_1)^2}{M^2}\, E_{2,s}(z') \\
&= \frac{(M,N_1)^2}{M^2}\,(y'^s + O(y'^{-1-s})) \\
&= \frac{(M,N_1)^{2+2s}}{M^{2+s}}\, y^s + O(y^{-1-s}) .
\end{aligned}$$

Setting $s = 0$, or differentiating in s and then setting $s = 0$, we find

$$E(Mz)|_2\alpha = \frac{(M,N_1)^2}{M^2} + O\left(\frac{1}{y}\right), \quad F(Mz)|_2\alpha = \frac{(M,N_1)^2}{M^2}\left(\log y + \log\frac{(M,N_1)^2}{M}\right) + O\left(\frac{1}{y}\log y\right)$$

as $y \to \infty$. It follows that the function $\sum_{M|N}\{\alpha(M)F(Mz) + \beta(M)E(Mz)\}$, which is orthogonal to cusp forms, has the expansion $A(N_1)\log y + B(N_1) + O(y^{-1}\log y)$ at ξ if $\alpha(M)$ and $\beta(M)$ satisfy equations (6.3) and (6.4), and hence that we have a decomposition

$$\tilde{\Phi}(z) = \tilde{\Phi}^*(z) + \sum_{M|N}\{\alpha(M)F(Mz) + \beta(M)E(Mz)\}$$

where $\tilde{\Phi}^* \in \tilde{M}_2(\Gamma_0(N))$ has the same Petersson scalar products with holomorphic cusp forms as $\tilde{\Phi}$ does and is small at the cusps. Hence $\tilde{\Phi}$ and $\tilde{\Phi}^*$ have the same holomorphic projection Φ, and, by what has already been proved, the m^{th} Fourier coefficient of Φ is given by

$$a_m = 4\pi m \lim_{s\to 0}\int_0^\infty e^{-4\pi my}\, a_m^*(y)\, y^s\, dy$$

where $\tilde{\Phi}^*(z) = \sum_m a_m^*(y)\, e^{2\pi imz}$. Let

$$E(z) = \sum_{m=-\infty}^{\infty} e(m,y)\, e^{2\pi imz}, \qquad F(z) = \sum_{m=-\infty}^{\infty} f(m,y)\, e^{2\pi imz}$$

be the Fourier developments of $E(z)$ and $F(z)$. Then for m prime to N we have $a_m^*(y) = a_m(y) - \alpha(1)f(m,y) - \beta(1)e(m,y)$. Hence to establish (6.5) we must show that for $m > 0$

$$\int_0^\infty e(m,y)\, e^{-4\pi my}\, y^s\, dy = -\frac{6}{\pi m}\sigma_1(m) + o(1),$$

$$\int_0^\infty f(m,y)\, e^{-4\pi my}\, y^s\, dy = -\frac{6}{\pi m}\sigma_1(m)\, s^{-1} - \frac{12}{\pi m}\sigma_1'(m) + \frac{12}{\pi m}\sigma_1(m)\left(\log 2m + \tfrac{1}{2} + \frac{\zeta'}{\zeta}(2)\right) + o(1)$$

as $s \to 0$. The first equation is trivial since $e(m,y) = -24\sigma_1(m)$ for $m > 0$. To prove the second we need to know the Fourier coefficients $f(m,y)$, which we compute by working out the Fourier expansion of $E_{2,s}$. The identity

$$\frac{1}{(cz+d)}\,\frac{y^s}{|cz+d|^{2s}} = \frac{2i}{s+1}\,\frac{\partial}{\partial z}\left(\frac{y^{s+1}}{|cz+d|^{2s+2}}\right)$$

implies $E_{2,s}(z) = \frac{2i}{s+1}\frac{\partial}{\partial z}E(z,s+1)$, where $E(z,s)$ is the Eisenstein series of weight 0 on $SL_2(\mathbb{Z})$; the well-known Fourier expansion

$$E(z,s) = y^s + \frac{\pi^{\frac{1}{2}}\Gamma(s-\frac{1}{2})\zeta(2s-1)}{\Gamma(s)\zeta(2s)}\,y^{1-s} + \frac{2\pi^s y^{\frac{1}{2}}}{\Gamma(s)\zeta(2s)}\sum_{m\neq 0}|m|^{\frac{1}{2}-s}\sigma_{2s-1}(m)K_{s-\frac{1}{2}}(2\pi|m|y)e^{2\pi i}$$

(where $\sigma_\nu(m) = \sum_{d|m} d^\nu$, $K_\nu(x)$ = K-Bessel function) then gives

$$E_{2,s}(z) = y^s - \frac{\pi^{\frac{1}{2}}s\Gamma(s+\frac{1}{2})\zeta(2s+1)}{\Gamma(s+2)\zeta(2s+2)}\,y^{-1-s} + \sum_{m\neq 0} e_{2,s}(m,y)\, e^{2\pi imz},$$

$$e_{2,s}(m,y) = \frac{2\pi^{s+1}|m|^{-s-\frac{1}{2}}}{\Gamma(s+2)\zeta(2s+2)} \sigma_{2s+1}(m)\, e^{2\pi my} \left(\frac{\partial}{\partial y} - 2\pi m\right)\left(\sqrt{y}\, K_{s+\frac{1}{2}}(2\pi|m|y)\right).$$

Integration by parts gives

$$\int_0^\infty e_{2,t}(m,y)\, e^{-4\pi my} y^s\, dy = -\frac{2\pi^{1+t} m^{-\frac{1}{2}-t}}{\Gamma(2+t)\zeta(2+2t)} \sigma_{1+2t}(m)\, s \int_0^\infty y^{s-\frac{1}{2}} K_{\frac{1}{2}+t}(2\pi my)\, e^{-2\pi my}\, dy$$

for $m \geq 1$ and $0 < t < \mathrm{Re}(s)$. The integral is tabulated and equals $\frac{\Gamma(s+t+1)\Gamma(s-t)\pi^{\frac{1}{2}}}{\Gamma(s+1)(4\pi m)^{s+\frac{1}{2}}}$. Since $f(m,y) = \frac{\partial}{\partial t} e_{2,t}(m,y)\big|_{t=0}$, we get

$$\int_0^\infty f(m,y)\, e^{-4\pi my} y^s\, dy = \frac{\partial}{\partial t}\left[\frac{-2\pi^{\frac{3}{2}+t} m^{-\frac{1}{2}-t}\, \Gamma(s+t+1)\Gamma(s-t)}{(4\pi m)^{s+\frac{1}{2}}\Gamma(2+t)\Gamma(s)\zeta(2+2t)} \sigma_{1+2t}(m)\right]\Bigg|_{t=0}$$

$$= -24 \frac{\Gamma(s+1)}{(4\pi m)^{s+1}}\left[2\sigma_1'(m) + \sigma_1(m)\left(\log\frac{\pi}{m} + \gamma - 1 - 2\frac{\zeta'}{\zeta}(2) + \frac{1}{s}\right)\right]$$

(γ = Euler's constant), and the Laurent expansion of this near $s=0$ begins as given above.

This completes the proof of Proposition 6.2, except that we still have to verify that the system of equations (6.3) and (6.4) always has a solution, i.e. that the $\sigma_0(N) \times \sigma_0(N)$ matrix

$$\underline{C}_N = \{C_N(N_1,M)\}_{N_1,M|N}, \qquad C_N(N_1,M) = \frac{(M,N_1)^2}{M^2}$$

is invertible. Since the coefficients $C_N(N_1,M)$ are multiplicative (i.e. $C_{\Pi p^{\nu_p}}(\Pi p^{\lambda_p}, \Pi p^{\mu_p}) = \Pi C_{p^{\nu_p}}(p^{\lambda_p}, p^{\mu_p})$), the matrix $\underline{C}_N$ for $N = \Pi p^{\nu_p}$ is the Kronecker product of the matrices $\underline{C}_{p^{\nu_p}}$, so it suffices to check this for $N = p^\nu$. But

$$\underline{C}_{p^\nu} = \begin{pmatrix} 1 & p^{-2} & p^{-4} & p^{-6} & \cdots & p^{-2\nu} \\ 1 & 1 & p^{-2} & p^{-4} & \cdots & p^{-2\nu+2} \\ 1 & 1 & 1 & p^{-2} & \cdots & p^{-2\nu+4} \\ & & & \vdots & & \\ 1 & 1 & 1 & 1 & \cdots & p^{-2} \\ 1 & 1 & 1 & 1 & \cdots & 1 \end{pmatrix},$$

and one sees by inspection that this is invertible with inverse given by the tridiagonal matrix

$$(6.6) \qquad \underline{C}_{p^\nu}^{-1} = \frac{1}{p^2-1}\begin{pmatrix} p^2 & -1 & 0 & 0 & \cdots & & 0 \\ -p^2 & p^2+1 & -1 & 0 & \cdots & & 0 \\ 0 & -p^2 & p^2+1 & -1 & \cdots & & 0 \\ & & & \vdots & & & \\ 0 & 0 & 0 & \cdots & -p^2 & p^2+1 & -1 \\ 0 & 0 & 0 & \cdots & 0 & -p^2 & p^2 \end{pmatrix}.$$

This completes the proof of 6.2. Moreover, since we know the inverse of $\underline{C}_N$ we can solve the equations (6.3) and (6.4) explicitly and in particular give a formula for the numbers $\alpha(1)$ and $\beta(1)$ occurring in (6.5):

<u>Proposition 6.7.</u> <u>Let the notations be as in Proposition 6.2. Then</u>

$$\alpha(1) = \delta^{-1} \sum_{N_1|N} \frac{\mu(N_1)}{N_1^2} A(N_1),$$

$$\beta(1) = \delta^{-1} \sum_{N_1|N} \frac{\mu(N_1)}{N_1^2}\left(B(N_1) - 2A(N_1)\log N_1\right) - 2\alpha(1)\sum_{p|N} \frac{\log p}{p^2-1},$$

<u>where</u> $\mu(\ )$ <u>is the Möbius function and</u> $\delta = \prod_{p|N}(1-p^{-2}) = \sum_{N_1|N} \frac{\mu(N_1)}{N_1^2}$.

<u>Proof:</u> We have $C_N^{-1}(1,N_1) = \delta^{-1}\frac{\mu(N_1)}{N_1^2}$ by (6.6) and the multiplicativity property of $\underline{C}_N$, so the formula for $\alpha(1)$ follows immediately from (6.3). Rewrite (6.4) in the form

$$\sum_{M|N} C_N(N_1,M)\,\beta(M) = B(N_1) - \sum_{M|N} C_N(N_1,M)\,\alpha(M)\log\frac{(M,N_1)^2}{M} = B(N_1) + \sum_p s_p(N_1)\log p,$$

where $\sum_p$ denotes a sum over all primes dividing N and

$$s_p(N_1) = \sum_{M|N} C_N(N_1,M)\,\alpha(M)\left(v_p(M) - 2\min\{v_p(N_1), v_p(M)\}\right).$$

The formula for $C_N^{-1}(1,N_1)$ just given yields

$$\beta(1) = \delta^{-1}\sum_{N_1|N}\frac{\mu(N_1)}{N_1^2}\left[B(N_1) + \sum_p s_p(N_1)\log p\right]$$

We must show

$$\sum_{N_1|N}\frac{\mu(N_1)}{N_1^2} s_p(N_1) = -2\sum_{N_1|N}\frac{\mu(N_1)}{N_1^2} A(N_1)\left(v_p(N_1) + \frac{1}{p^2-1}\right).$$

By definition of $\alpha(M)$ we have

$$s_p(N_1) = \sum_{M|N}\sum_{N_2|M} C_N(N_1,M)\, C_N^{-1}(M,N_2)\left(v_p(M) - 2\min\{v_p(M), v_p(N_1)\}\right) A(N_2).$$

Write $N = p^\nu N'$ with $p \nmid N'$ and $N_1 = p^\lambda N_1'$ with $N_1' | N'$; then the multiplicativity property of $\underline{C}_N$ and $\underline{C}_N^{-1}$ gives

$$s_p(N_1) = \sum_{\substack{N_2'|N' \\ 0\le\kappa\le\nu}} \Big[\sum_{M'|N'} C_{N'}(N_1',M')\, C_{N'}^{-1}(M',N_2') \Big]$$

$$\times\Big[\sum_{1\le\mu\le\nu} C_{p^\nu}(p^\lambda,p^\mu)\, C_{p^\nu}^{-1}(p^\mu,p^\kappa)\, (\mu - 2\min\{\mu,\lambda\})\Big]\, A(p^\kappa N_2')\,.$$

The first expression in square brackets is $\delta_{N_1'N_2'}$ (Kronecker delta) by definition. Hence

$$\sum_{N_1|N} \frac{\mu(N_1)}{N_1^2}\, s_p(N_1) = \sum_{N_1'|N'} \frac{\mu(N_1')}{N_1'^2}\Big\{ s_p(N_1') - \frac{1}{p^2}\, s_p(pN_1')\Big\}$$

$$= \sum_{\substack{N_1'|N' \\ 0\le\kappa\le\nu}} \frac{\mu(N_1')}{N_1'^2} A(p^\kappa N_1') \sum_{\mu=1}^{\nu} \Big[\, \mu\, C_{p^\nu}(1,p^\mu) - \frac{1}{p^2}(\mu-2)C_{p^\nu}(p,p^\mu)\,\Big] C_{p^\nu}^{-1}(p^\mu,p^\kappa)\,.$$

The expression in square brackets equals $2p^{-2\mu}$, and

$$\sum_{\mu=1}^{\nu} p^{-2\mu} C_{p^\nu}^{-1}(p^\mu,p^\kappa) = \begin{cases} \dfrac{-1}{p^2-1} & (\kappa=0) \\ \dfrac{1}{p^2-1} & (\kappa=1) \\ 0 & (\kappa>1) \end{cases} = -\frac{\mu(p^\kappa)}{p^{2\kappa}}\Big(\kappa + \frac{1}{p^2-1}\Big)$$

by (6.6). This completes the proof.

To apply Propositions 6.2 and 6.7 we need the coefficients $A(N_1)$ and $B(N_1)$ for our particular function $\widetilde{\Phi}$. They are given by the following:

<u>Proposition 6.8. Let $\widetilde{\Phi}$ be the function of Proposition 4.5 for</u> $k=1$, $\varepsilon(N)=1$. <u>Then $\widetilde{\Phi}$ satisfies the hypotheses of Proposition 6.2 with</u>

$$A(N_1) = \frac{h}{2u^2}\,\frac{\varepsilon(N_1)N_1}{N}\,, \quad B(N_1) = A(N_1)\Big(\log\frac{N_1^2\delta}{N\pi} - \gamma + 2\frac{L'}{L}(1,\varepsilon)\Big) \quad (N_1|N),$$

<u>where</u> h, u, ε <u>have the usual meaning</u>, γ = <u>Euler's constant</u>.

<u>Proof</u>: The case $N_1=N$ follows directly from the Fourier expansion at infinity given in Proposition 4.5, since, as remarked already, all terms in this expansion except the term $\frac{h}{u}r_A(m)\big(\log\frac{N\delta y}{\pi} - \gamma + 2\frac{L'}{L}(1,\varepsilon)\big)e^{2\pi imz}$ for $m=0$ are exponentially small as $y\to\infty$. To obtain the corresponding result at other cusps, we must go back to the definition of $\widetilde{\Phi}$ as $\frac{\sqrt{\delta}}{2\pi}\frac{\partial}{\partial s}\widetilde{\Phi}_s\big|_{s=0}$, with $\widetilde{\Phi}_s = \mathrm{Tr}_N^{ND}(\theta_A(z)E_s^{(1)}(Nz))$ as in Proposition 1.2, and use the formulas given in §§2-3 for the Fourier

expansions of θ_A and $E_s^{(1)}$ in the various cusps.

Let $\xi\in\mathbb{P}^1(\mathbb{Q})$ be a cusp, N_1 the greatest common divisor of N and the denominator of ξ, and choose a matrix $\alpha\in SL_2(\mathbb{Z})$ sending ∞ to ξ. By definition of the trace operator we have

$$\widetilde{\Phi}_s|_2\alpha = \sum_{\gamma\in\Gamma_0(ND)\backslash\Gamma_0(N)\alpha} \theta_A(z)E_s^{(1)}(Nz)|_2\gamma\,.$$

For each $\gamma = \left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right)$ in the sum we have $(c,N)=N_1$ since $\gamma\alpha^{-1}\in\Gamma_0(N)$. Let $a'=N_2a$, $c'=c/N_1$, where $N_2=N/N_1$; then $\frac{a'}{c'} = N\frac{a}{c}$ and $(a',c')=1$. Choose a matrix $\gamma' = \left(\begin{smallmatrix} a' & b' \\ c' & d'\end{smallmatrix}\right)\in SL_2(\mathbb{Z})$ and define z' by $N\gamma z = \gamma' z'$, $c'z'+d' = \frac{1}{N_2}(cz+d)$ as in the proof of Proposition 6.2. Then

$$\theta_A(z)E_s^{(1)}(Nz)|_2\gamma = (\theta_A(z)|_1\gamma)(E_s^{(1)}(Nz)|_1\gamma) = (\theta_A|_1\gamma)(z)\cdot\frac{1}{N_2}(E_s^{(1)}|_1\gamma')(z')$$

By Lemma 2.3 and formula (2.2) we have

$$(\theta_A|_1\gamma)(z) = \varepsilon_{D_1}\Big(\frac{c}{\delta_2}\Big)\varepsilon_{D_2}(d)\kappa(D_1)^{-1}\delta_1^{-\frac12}\chi_{D_1\cdot D_2}(A)\theta_{AD_1}(z)\,,$$
$$(E_s^{(1)}|_1\gamma')(z') = \varepsilon_{D_1}(c')\varepsilon_{D_2}(d'\delta_1)\,\delta_1^{-s-1}E_s^{(D_1)}\Big(\frac{z'+c^*d}{\delta_1}\Big)\,,$$

where $D=D_1\cdot D_2$ is the decomposition of D into fundamental discriminants with $(c,D)=|D_2|$ and $\delta_i=|D_i|$. Note that $(c',D)=(c,D)$ because N is prime to D. As $y\to\infty$ we have

$$\theta_{AD_1}(z) = \frac{1}{2u} + \dots\,,$$

$$E_s^{(1)}(z) = \begin{cases} L(2s+1,\varepsilon)\,y^s + \dots & \text{if } D_1=1\,, \\ V_s(0)L(2s,\varepsilon)y^{-s} + \dots & \text{if } D_2=1\,, \\ \dots & \text{otherwise,} \end{cases}$$

(here "..." denotes exponentially small terms), the first by definition of the theta-series and the second by the calculations in the proof of Proposition 3.2. If $D_1=1$ then c and c' are divisible by D, so $d\equiv a^{-1}\equiv N_2a'^{-1}\equiv N_2d'$ (mod D) and $\varepsilon_{D_2}(dd')=\varepsilon(N_2)$. If $D_2=1$ then c and c' are prime to D and $\varepsilon_{D_1}(cc')=\varepsilon(c^2/N_1)=\varepsilon(N_1)$. Also $\varepsilon(N_1)=\varepsilon(N_2)$ since we are assuming $\varepsilon(N)=1$, and $\kappa(1)=1$, $\kappa(D)=i$. Hence

$$(\theta_A(z)E_s^{(1)}(Nz))|_2\gamma = \begin{cases} \frac{1}{2u}\frac{\varepsilon(N_1)}{N_2} L(2s+1,\varepsilon)(N_1y/N_2)^s + \dots & \text{if } D|c\ , \\ \frac{\delta^{-3/2}}{2ui}\frac{\varepsilon(N_1)}{N_2} V_s(0)\, L(2s,\varepsilon)\,(N_1y/N_2)^{-s} + \dots & \text{if } (c,D)=1\,, \\ \dots & \text{otherwise}\,. \end{cases}$$

Since the collection of left cosets $\Gamma_0(ND)\backslash\Gamma_0(N)\alpha$ contains one coset of elements γ with $D|c$ and $|D|$ cosets of γ with $(c,D)=1$, we deduce

$$(\tilde{\Phi}_s|_2\alpha)(z) = \frac{1}{2u}\frac{\varepsilon(N_1)}{N_2}\,[\,L(2s+1,\varepsilon)(N_1y/N_2)^s - \frac{iV_s(0)}{|D|^{1/2}}L(2s,\varepsilon)\,(N_1y/N_2)^{-s}\,] + \dots$$

as $y\to\infty$, and the result follows by substituting $V_s(0) = -\frac{\pi^{\frac12}\Gamma(s+\frac12)}{\Gamma(s+1)}i$ and computing the derivative at $s=0$.

Combining Propositions 6.7 and 6.8, we find

$$\alpha(1) = \frac{h}{2u^2}N^{-1}\delta^{-1}\sum_{N_1|N}\frac{\mu(N_1)\varepsilon(N_1)}{N_1} = \frac{h}{2u^2}N^{-1}\prod_{p|N}(1+\frac{\varepsilon(p)}{p})^{-1},$$

$$\beta(1) = \alpha(1)\left(\log\frac{\delta}{N\pi} - \gamma + 2\frac{L'}{L}(1,\varepsilon) - 2\sum_{p|N}\frac{\log p}{p^2-1}\right)$$

for our function $\tilde{\Phi}$. We still have to calculate the integral in (6.5). From Proposition 4.5 we have

$$a_m(y) = A_m\log y + B_m + \sum_{n=1}^{\infty} C_{mn}\, q_0(\frac{4\pi nNy}{\delta})$$

for $m>0$, where we have made the abbreviations

$$A_m = \frac{h}{u}\, r_A(m)\ ,$$

$$B_m = A_m\left(\log\frac{N\delta}{\pi} - \gamma + 2\frac{L'}{L}(1,\varepsilon)\right) - \sum_{1\le n\le\frac{m\delta}{N}}\sigma_A'(n)\, r_A(m\delta-Nn)\ ,$$

$$C_{mn} = -\,\sigma_A(n)\, r_A(m\delta+Nn)\ .$$

Hence

$$\int_0^\infty a_m(y)\, e^{-4\pi my}\, y^s\, dy = \frac{\Gamma(s+1)}{(4\pi m)^{s+1}}\, A_m\frac{\Gamma'}{\Gamma}(s+1) - A_m\log 4\pi m + B_m)$$
$$+ \sum_{n=1}^\infty C_{mn}\int_0^\infty q_0(\frac{4\pi nNy}{\delta})\, e^{-4\pi my}\, y^s\, dy\ .$$

The first term has the finite limit $\frac{1}{4\pi m}(-A_m\gamma - A_m\log 4\pi m + B_m)$ as $s\to 0$. The integral in the infinite sum is given by

$$\int_0^\infty\left(\int_1^\infty\frac{1}{x}e^{-\frac{4\pi nNy}{\delta}x}dx\right)e^{-4\pi my}y^s\,dy = \frac{\Gamma(s+1)}{(4\pi m)^{s+1}}\int_1^\infty\left(1+\frac{nN}{m\delta}x\right)^{-s-1}\frac{dx}{x}\ .$$

At $s=0$ this equals

$$\frac{1}{4\pi m}\int_1^\infty\left(\frac{1}{x} - \frac{1}{x+m\delta/nN}\right)dx = \frac{1}{4\pi m}\log(1+\frac{m\delta}{nN})\ ,$$

while as $n\to\infty$ it equals

$$\frac{\Gamma(s+1)}{(4\pi m)^{s+1}}\int_1^\infty[\,(\frac{nN}{m\delta}x)^{-s-1} + O(n^{-s-2}x^{-s-2})\,]\frac{dx}{x} = \frac{1}{s+1}\frac{\Gamma(s+1)}{(4\pi nN/\delta)^{s+1}} + O(n^{-s-2})\ ,$$

the $O(\ )$-constant being uniform near $s=0$. On the other hand, the Legendre function $Q_s(x)$ satisfies

$$Q_0(1+2t) = \frac{1}{2}\log(1+\frac{1}{t})\ ,$$

$$Q_s(1+2t) = \frac{\Gamma(s+1)^2}{2\Gamma(2s+2)}[t^{-s-1} + O(t^{-s-2})] \qquad \text{as } t\to\infty\ ,$$

so we can write

$$\int_0^\infty q_0(\frac{4\pi nNy}{\delta})\, e^{-4\pi my}\, y^s\, dy = \frac{2\Gamma(2s+2)}{(4\pi m)^{s+1}\Gamma(s+2)}\, Q_s(1+\frac{2nN}{m\delta}) + \varepsilon_n(s)$$

with $\varepsilon_n(s) = O(n^{-s-2})$ as $n\to\infty$ and $\varepsilon_n(0)=0$. Since $C_{mn} = O(n^c)$ for any $c>0$, the series $\sum_n C_{mn}\varepsilon_n(s)$ converges uniformly near $s=0$ and vanishes at $s=0$. Hence

$$4\pi m\int_0^\infty a_m(y)\, e^{-4\pi my}\, y^s\, dy = B_m - A_m(\gamma+\log 4\pi m) + \frac{2\Gamma(2s+2)}{(4\pi m)^s\Gamma(s+2)}\sum_{n=1}^\infty C_{mn}Q_s(1+\frac{2nN}{m\delta}) + o(1)$$

as $s\to 0$, and putting this into (6.5) we obtain

$$a_m = B_m - A_m(\gamma+\log 4\pi m) + \lim_{s\to 0}\left[\frac{2\Gamma(2s+2)}{(4\pi m)^s\Gamma(s+2)}\sum_{n=1}^\infty C_{mn}\, Q_s(1+\frac{2nN}{m\delta}) + \frac{24\alpha(1)\sigma_1(m)}{s}\right]$$
$$+ 24\,\beta(1)\,\sigma_1(m) + 48\,\alpha(1)\,\sigma_1'(m) - 48\,\alpha(1)\,\sigma_1(m)(\log 2m + \frac{1}{2} + \frac{\zeta'}{\zeta}(2))\ ,$$

an expression which can be further simplified by multiplying the expression in square brackets by $\frac{(4\pi m)^s\Gamma(s+2)}{\Gamma(2s+2)}$ to replace the $\lim\limits_{s\to 0}$ term by

$$\lim_{s\to 0}\left[2\sum_{n=1}^\infty C_{mn}\, Q_s(1+\frac{2nN}{m\delta}) + \frac{24\alpha(1)\sigma_1(m)}{s}\right] + 24\,\alpha(1)\,\sigma_1(m)(\log 4\pi m + \gamma - 1)\ .$$

(The argument just described was already used in the case $N=m=1$ in [18], p. 218.) Putting into this the expressions for $\alpha(1)$, $\beta(1)$, A_m, B_m and C_{mn} given above, and combining the resulting formula with the assertion of Proposition 4.5, obtain our main result:

Theorem 6.9. *Let* D, A, h, u, ε *have their usual meanings,* N *a natural number with* $\varepsilon(N) = 1$. *Then there exists a holomorphic cusp form* $\Phi_A(z) = \sum_{m=1}^{\infty} a_{m,A}\, e^{2\pi i m z}$ *of weight* 2 *and level* N *such that*

i) $L_A(f,1) = 0$, $L_A'(f,1) = \frac{8\pi^2}{\sqrt{\delta}}(f, \Phi_A)$ *for any cusp form* f *in the space spanned by newforms of weight* 2 *and level* N, *and*

ii) *the* m^{th} *Fourier coefficient of* Φ_A *for* m *prime to* N *is given by*

$$\begin{aligned} a_{m,A} = &- \sum_{1 \le n \le \frac{m|D|}{N}} \sigma_A'(n)\, r_A(m|D|-nN) + \frac{h}{u} r_A(m) \left[\log \frac{N|D|}{4\pi^2 m} - 2\gamma + 2\frac{L'}{L}(1,\varepsilon)\right] \\ &+ \lim_{s \to 0} \left[-2 \sum_{n=1}^{\infty} \sigma_A(n)\, r_A(m|D|+nN)\, Q_s\!\left(1 + \frac{2nN}{m|D|}\right) - \frac{h\kappa}{u^2} \sigma_1(m) \frac{1}{s} \right] \\ &+ \frac{h\kappa}{u^2} \left[\sigma_1(m) \left(\log \frac{N}{|D|} + 2 \sum_{p|N} \frac{\log p}{p^2-1} + 2 + 2\frac{\zeta'}{\zeta}(2) - 2\frac{L'}{L}(1,\varepsilon) \right) + \sum_{d|m} d \log \frac{m}{d^2} \right], \end{aligned}$$

where $\sigma_1(m) = \sum_{d|m} d$, $\kappa = -12/N \prod_{p|N}\left(1 + \frac{\varepsilon(p)}{p}\right)$, σ_A *and* σ_A' *as in Proposition 4.6.*

Chapter V. Main identity, consequences and generalizations

In the first section of this chapter we combine the results of Chapters II – IV to prove the theorems stated in §6 of Chapter I. The proofs of their various consequences for the Birch – Swinnerton-Dyer conjecture are given in §2. The application to the problem of estimating class numbers of imaginary quadratic fields was described in Chapter I and will not be discussed again.

These results involve only the special case of the calculations of Chapter IV when the weight of the modular form f is 2 and its level is a norm in the imaginary quadratic field K. The corresponding results when these assumptions are dropped are discussed in §3 (weight 2 but arbitrary level) and §4 (higher weight). The results described in §3, relating the values of $L_A(f,1)$ or $L_A'(f,1)$ to heights of Heegner points of more general types than those discussed so far in this paper, have been proved, but their proofs will be postponed to a later paper. The case $k > 1$ is discussed in §4, where we describe a conjectural interpretation of the formula for $L_A'(f,k)$ in terms of heights of higher-dimensional "Heegner cycles" and state a conjecture according to which certain combinations of special values at Heegner points of the resolvent kernel function $G_{N,s}^{m}(z,z')$ of Chapter II are logarithms of algebraic numbers belonging to the Hilbert class field of K.

§1. Heights of Heegner points and derivatives of L-series

The notations and assumptions are again as in Chapters II and III: it is assumed that every prime divisor of N splits in our imaginary quadratic field K, $x \in X_0(N)(H)$ is one of the Heegner points associated to K (H as usual the Hilbert class field of K), c denotes the class of $(x) - (\infty)$ in $\mathrm{Jac}(X_0(N))(H)$, A is an ideal class of K and σ the corresponding element of $G = \mathrm{Gal}(H/K)$. The first assertion of Theorem 6.1 of Chapter I was that the function $g_A(z) = \sum_{m \ge 1} \langle c, T_m c^{\sigma} \rangle q^m$ is a cusp form of weight 2 on $\Gamma_0(N)$.

This in fact has nothing at all to do with Heegner points: if y and z are any two points of $J_0(N)(\bar{\mathbb{Q}})$, then $\sum_{m\geq 1} \langle y, T_m z\rangle q^m$ is a cusp form of weight 2 and level N. In fact, if α is any $\mathbb{Q}$-linear map from the Hecke algebra $\mathbb{T}$ to $\mathbb{C}$, then $\sum_{m\geq 1} \alpha(T_m) q^m$ is such a cusp form. The proof of this is a simple formal argument; since it may not be familiar to all readers, we give it here.

If J is any abelian variety over $\mathbb{Q}$ and S its cotangent space at the origin, then endomorphisms of J act faithfully on S. Take J to be the Jacobian of $X_0(N)$; then S can be identified with the space of cusp forms of weight 2 and level N having rational Fourier coefficients. Hence the map $\mathbb{T} \to \mathrm{End}_{\mathbb{Q}}(S)$ is injective (recall that $\mathbb{T}$ is defined as the subalgebra of $\mathrm{End}_{\mathbb{Q}} J$ spanned by the Hecke operators T_m). In particular, $\dim_{\mathbb{Q}} \mathbb{T}$ is finite and bounded by d^2, where $d = \dim_{\mathbb{Q}} S = \dim_{\mathbb{C}} S_2(\Gamma_0(N))$. For each $m \in \mathbb{N}$ let $a_m : S \to \mathbb{Q}$ be the map sending a cusp form to its mth Fourier coefficient, and define a map $\beta : \mathbb{T}\times S \to \mathbb{Q}$ by $\beta(T,f) = a_1(Tf)$. We claim that β is a perfect pairing (and hence that $\dim_{\mathbb{Q}} \mathbb{T} = d$). Indeed, if for some $f \in S$ the map $\beta(\cdot, f)$ vanishes identically then $a_m(f) = a_1(T_m f) = \beta(T_m, f) = 0$ for all m, so $f = 0$; conversely, if for some $T \in \mathbb{T}$ the map $\beta(T,\cdot)$ vanishes identically then for any $f \in S$ we have $a_m(Tf) = a_1(T_m Tf) = a_1(TT_m f) = \beta(T, T_m f) = 0$ for all m and consequently $Tf = 0$, so the injectivity of $\mathbb{T} \to \mathrm{End}_{\mathbb{Q}}(S)$ implies $T = 0$. The fact that β is a perfect pairing means in particular that any $\alpha \in \mathrm{Hom}_{\mathbb{Q}}(\mathbb{T}, \mathbb{C})$ can be represented as $\beta(\cdot, f)$ for some $f \in S\otimes\mathbb{C}$, and then $\sum_{m\geq 1} \alpha(T_m) q^m = f$.

This proves that g_A is a cusp form on $\Gamma_0(N)$ as claimed. To identify it, we must look at the formulas for its Fourier coefficients. With $d = (x) - (0)$ as usual we have $\langle c, T_m c^\sigma\rangle = \langle c, T_m d^\sigma\rangle$ because c and d give the same class in $J(H)\otimes\mathbb{Q}$ by the Manin-Drinfeld theorem. For the latter symbol we have the decomposition $\langle c, T_m d^\sigma\rangle = \sum_v \langle c, T_m d^\sigma\rangle_v$ where if $|c| \cap |T_m d^\sigma| \neq \emptyset$ the local symbols $\langle c, T_m d^\sigma\rangle_v$ must be defined as in §5 of Chapter II. The formula for the sum of the archimedean local symbols given in Propositions 4.2 and 5.6 of Chapter II can be written more simply by using the first part of Proposition 4.6 of Chapter IV as

$$\begin{aligned}\langle c, T_m d^\sigma\rangle_\infty = \lim_{s\to 1}\Bigg[& -2u^2 \sum_{n=1}^{\infty} \sigma_A(n)\, r_A(nN+m|D|)\, Q_{s-1}\Big(1+\frac{2nN}{m|D|}\Big) - \frac{h\kappa\sigma_1(m)}{s-1}\Bigg] \\ & + h\kappa\Bigg[\sigma_1(m)\Big(\log\frac{N}{|D|} + 2\sum_{p|N}\frac{\log p}{p^2-1} + 2 + 2\frac{\zeta'}{\zeta}(2) - 2\frac{L'}{L}(1,\varepsilon)\Big) + \sum_{d|m} d\log\frac{m}{d^2}\Bigg] \\ & + hur_A(m)\Big[2\frac{L'}{L}(1,\varepsilon) - 2\gamma - 2\log 2\pi + \log|D|\Big]\end{aligned}$$

for $(m,N) = 1$, where $\sigma_A(n) = \sum_{d|n} \varepsilon_A(n,d)$ with $\varepsilon_A(n,d)$ ($= 0$, 1 or -1) as in Proposition 3.2 of Chapter IV and

$h = h_K$, $D = D_K$, $u = u_K$ the class number, discriminant, $\frac{1}{2}$ number of units of K;
$\kappa = \kappa_N = \frac{-12}{N}\prod_{p|N}\frac{p}{p+1}$, $\sigma_1(m) = \sum_{d|m} d$, γ = Euler's constant;
$Q_{s-1}(t)$ = Legendre function of the second kind.

Similarly, we can combine the formulas for $\sum_{v|p}\langle c, T_m d^\sigma\rangle_v$ given in Propositions 9.2, 9.7 and 9.11 of Chapter III for all p and rewrite the result using the second part of Proposition 4.6 of Chapter IV as

$$\langle c, T_m d^\sigma\rangle_{\text{finite}} = -u^2 \sum_{0<n\leq m|D|/N} \sigma_A'(n)\, r_A(m|D| - nN) + hur_A(m)\log\frac{N}{m}$$

for $(m,N) = 1$, where $\sigma_A'(n) = \sum_{d|n} \varepsilon_A(n,d)\log\frac{n}{d^2}$. Adding the last two formulae, we find the identity $\langle c, T_m c^\sigma\rangle = u^2 a_{m,A}$ for $(m,N) = 1$, where $a_{m,A}$ is the m^{th} Fourier coefficient of the cusp form defined in Theorem 6.9 of Chapter IV. But this means that g_A and $u^2\sum a_{m,A} q^m$ differ by an old form in $S_2(\Gamma_0(N))$, so they have the same Petersson scalar product with any f in the space spanned by newforms of weight 2 and level N, which is just assertion of Theorem 6.1 of Chapter I.

As an aside, we mention that the function g is not quite independent of the choice of Heegner point x (as erroneously asserted in our announcement [17]), but this is true up to the addition of an old form, which is all we need. That $\langle c, T_m c^\sigma\rangle$ is independent of the choice of x when $(m,N) = 1$ follows from the fact that any two choices of x are related by the action of an element of $G\times W$, where W is the group of Atkin-Lehner involutions, and this action commutes with that of T_m for $(m,N) = 1$. (It also follows, of course, from our computation of the height.)

We now turn to the second main result of §6 of Chapter I, Theorem 6.3, which is a consequence of the first and of the formalism at the beginning of this section. For χ a character of G set $c_\chi = \sum_{\sigma\in G}\chi^{-1}(\sigma)c^\sigma$; then

$$\begin{aligned}<c_\chi, T_m c_\chi> &= <\sum_\tau \chi^{-1}(\tau)c^\tau, \sum_\sigma \chi^{-1}(\sigma)\, T_m c^\sigma> \\ &= \sum_{\sigma,\tau}\chi(\tau^{-1}\sigma) <c^\tau, T_m c^\sigma> \\ &= h\sum_\sigma \chi(\sigma) <c, T_m c^\sigma>\end{aligned}$$

by the invariance under G of the height pairing on $J(H)$ (which we have extended to $J(H)\otimes\mathbb{C}$ as a hermitian pairing). Now let $f\in S_2(\Gamma_0(N))$ be a normalized newform. In our basic identity $L_A'(f,1) = 8\pi^2u^{-2}|D|^{-1/2}(f,g_A)$ we can replace (f,g_A) by (g_A,f) because both f and g_A have real Fourier coefficients. Hence

$$L'(f,\chi,1) = \sum_A \chi(A)\, L_A'(f,1) = \frac{8\pi^2}{u^2|D|^{1/2}}\left(\sum_A \chi(A)g_A\, ,\, f\right) .$$

On the other hand, $\sum_A \chi(A)\, g_A = \frac{1}{h}\sum_{m\geq 1}<c_\chi, T_m c_\chi>q^m$ by the calculation just given. Extend $\{f\}$ to a basis $f_1=f, f_2,\dots,f_d$ of $S_2(\Gamma_0(N))$ consisting of the normalized newforms together with a basis of the space of oldforms (chosen for convenience to have real Fourier coefficients). Then the formalism at the beginning of this section implies that c_χ (or any element of $J(H)\otimes\mathbb{C}$) can be written as a sum of components transforming like the f_j, say $c_\chi = \sum_{j=1}^d c_\chi^{(j)}$ with $T_m c_\chi^{(j)} = a_m(f_j)\, c_\chi^{(j)}$ (in particular, $c_\chi^{(1)}$ is the f-isotypical component $c_{\chi,f}$ of c_χ). Then $<c_\chi, T_m c_\chi> = \sum_{i,j} a_m(f_j) <c_\chi^{(i)}, c_\chi^{(j)}>$, so $\sum_A \chi(A)\, g_A = \frac{1}{h}\sum_{i,j} <c_\chi^{(i)}, c_\chi^{(j)}>\, f_j$. Combining this with the last identity and observing that $(f_j,f)=0$ for $j\neq 1$, we find

$$L'(f,\chi,1) = \frac{8\pi^2}{hu^2|D|^{1/2}}\sum_{i=1}^d <c_\chi^{(i)}, c_\chi^{(1)}>\, (f,f) .$$

But $<c_\chi^{(i)}, c_\chi^{(1)}> = 0$ for $i\neq 1$ since $c_\chi^{(i)}$ and $c_\chi^{(1)}$ are eigenvectors with different eigenvalues of some T_m, $(m,N)=1$, so the sum reduces to a single

term $\hat{h}(c_{\chi,f})\,(f,f)$. This gives Theorem 6.3 of Chapter I.

We end this section by giving three important corollaries of the main theorem which were already mentioned in our announcement [17].

<u>Corollary 1.1.</u> <u>Let</u> $f\in S_2(\Gamma_0(N))$ <u>be any newform and</u> χ <u>any character of</u> $\mathrm{Gal}(H/K)$. <u>Then</u> $L'(f,\chi,1)\geq 0$.

This follows immediately from the formula for $L'(f,\chi,1)$ since both the Petersson product and the global height pairing are positive definite. Notice that Corollary 1.1 is what would be predicted by the Riemann hypothesis for $L(f,\chi,s)$, according to which the largest zero of the real function $L(f,\chi,s)$ on the real axis should occur at $s=1$.

<u>Corollary 1.2.</u> <u>Let</u> $f\in S_2(\Gamma_0(N))$ <u>be any newform and</u> χ <u>any character of</u> $\mathrm{Gal}(H/K)$. <u>Then either all conjugates</u> $L(f^\alpha,\chi^\alpha,s)$ $(\alpha\in\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}))$ <u>have a simple zero at</u> $s=1$ <u>or else all have a zero of order</u> ≥ 3.

Indeed, each $L(f^\alpha,\chi^\alpha,s)$ has an odd order zero at $s=1$ by the functional equation, and $L'(f^\alpha,\chi^\alpha,1)=0$ iff the Heegner point $c_{\chi^\alpha,f^\alpha}\in J(H)\otimes\mathbb{C}$ vanishes (again by the formula for $L'(f,\chi,1)$ together with the positive-definiteness of the height pairing). But c_{χ^α,f^α} equals $c_{\chi,f}^\alpha$ and hence vanishes if and only if $c_{\chi,f}$ does.

A consequence of Corollary 1.2, also mentioned in [17], is the analogous statement for the ordinary Hecke L-series:

<u>Corollary 1.3.</u> <u>Let</u> f <u>be any newform of weight</u> 2 <u>and</u> f^α $(\alpha\in\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}))$ <u>any conjugate of</u> f. <u>Then</u>

$$\begin{aligned}\mathrm{ord}_{s=1}L(f,s) = 0 &\longleftrightarrow \mathrm{ord}_{s=1}L(f^\alpha,s) = 0 ,\\ \mathrm{ord}_{s=1}L(f,s) = 1 &\longleftrightarrow \mathrm{ord}_{s=1}L(f^\alpha,s) = 1 ,\\ \mathrm{ord}_{s=1}L(f,s) \geq 2 &\longleftrightarrow \mathrm{ord}_{s=1}L(f^\alpha,s) \geq 2 ,\\ \mathrm{ord}_{s=1}L(f,s) \geq 3 &\longleftrightarrow \mathrm{ord}_{s=1}L(f^\alpha,s) \geq 3 .\end{aligned}$$

Indeed, $L(f,1)$ is known to be equal to the product of a non-vanishing period with an algebraic number which is conjugated by α when f is, so the first statement is clear. Since $L(f,s)$ and $L(f^{\alpha},s)$ satisfy the same functional equation, their orders of vanishing at $s=1$ have the same parity. Hence all the statements of Corollary 1.3 will follow if we show that $L(f,1)=0$, $L'(f,1)\neq 0 \Rightarrow L'(f^{\alpha},1)\neq 0$. The assumption implies that $L(f,s)$ (and hence $L(f^{\alpha},s)$) has a functional equation with a sign -1. Then for any $K=\mathbb{Q}(\sqrt{D})$ as in this paper the twisted function $L_{\varepsilon}(f,s)=\sum \varepsilon(n)\,a(n)\,n^{-s}$, where $\varepsilon(n)=(\frac{D}{n})$ as usual, will have an even order zero by virtue of the functional equation of $L(f,s)L_{\varepsilon}(f,s)=L(f,1,s)$. According to a theorem of Waldspurger ([36], Th. 2.3, [37], Th. 4), we can choose K so that $L_{\varepsilon}(f,1)$ (and hence also $L_{\varepsilon}(f^{\alpha},1)$) is non-zero. Then the result follows from Corollary 1.2 and the identity $L'(f,1)L_{\varepsilon}(f,1)=L'(f,1,1)$.

Corollaries 1.2 and 1.3 are interesting in view of a general conjecture that the order of vanishing of an odd-weight motivic L-function at the symmetry point of its functional equation should be invariant under Galois conjugation [6].

§2. Comparison with the conjecture of Birch and Swinnerton-Dyer

In §7 of Chapter I we described several applications of our main theorem to the Birch - Swinnerton-Dyer conjecture for an elliptic curve E over $\mathbb{Q}$, under the assumption that the L-series of E coincides with that of a modular form f. We recall that this condition can be verified by a finite computation for any given elliptic curve $E/\mathbb{Q}$. If it is satisfied, the modular form f is necessarily a Hecke eigenform of weight 2 with Fourier coefficients in $\mathbb{Z}$; conversely, given any such f, the periods of the elliptic differential $\omega_f=2\pi i\, f(z)\,dz=\sum_{n\geq 1} a_n q^n \frac{dq}{q}$ define an elliptic curve ("strong Weil curve") $E_0/\mathbb{Q}$ with $L(E_0,s)=L(f,s)$ [25], and by Faltings' theorem any elliptic curve with $L(E,s)=L(f,s)$ is isogenous to E_0 and hence admits a covering map $\pi: X_0(N)\to E$ (N = level of f) defined over $\mathbb{Q}$ and sending the cusp ∞ to $0\in E(\mathbb{Q})$. For the rest of this section we suppose given a newform f of weight 2 and level N and an elliptic curve E over $\mathbb{Q}$ related in this way.

The assertion of Theorem 7.3 of Chapter I was that under these circumstances the quotient of $L'(E,1)$ by the real period of a regular differential of $E/\mathbb{Q}$ is a non-zero rational multiple of the height of some point in $E(\mathbb{Q})$. This implied in particular that $\mathrm{rk}\, E(\mathbb{Q})>0$ if $L'(E,1)\neq 0$ and showed that, if $L'(E,1)\neq 0$ and $\mathrm{rk}\, E(\mathbb{Q})=1$, then the Birch - Swinnerton-Dyer conjectural formula for $L'(E,1)$ holds up to a non-zero rational factor. In this section we show how to prove this by applying the results of the last section to the trivial character $\chi=1$. Since $L(f,\chi,s)$ in this case is equal to the L-series of E over the imaginary quadratic field K, we will actually be working over K rather than $\mathbb{Q}$, and here our result will be even more precise: if $\mathrm{ord}_{s=1} L(E/K,s)=1$, then $\mathrm{rk}\, E(K)\geq 1$, and if $\mathrm{ord}_{s=1} L(E/K,s)=\mathrm{rk}\, E(K)=1$ then the Birch - Swinnerton-Dyer conjectural formula for $L'(E/K,1)$ holds up to a non-zero rational *square*. This last result will suggest a conjecture relating various arithmetical invariants of E/K which can sometimes be verified by descent arguments.

Finally, we will give some consequences of our main identity for the Birch - Swinnerton-Dyer conjecture for certain abelian varieties over $\mathbb{Q}$ of dimension larger than 1, as stated in our announcement [17].

Let E, f, ω_f and π be as above and let ω be a Néron differential on E (this is unique up to sign). Then $\pi^*(\omega)=c\,\omega_f$ for some non-zero integer c, and we normalize the choice of ω so that $c>0$. It is generally conjectured [25] that c divides the index of $\pi_* H_1(X_0(N),\mathbb{Z})$ in $H_1(E,\mathbb{Z})$ (for the strong Weil parametrization, this is the conjecture that $c_0=1$), but we will not assume this here.

Let x be a Heegner point of discriminant D on $X_0(N)$. Then the point

$$P_K = \sum_{\sigma\in \mathrm{Gal}(H/K)} \pi(x^{\sigma}) = \sum_{\sigma\in \mathrm{Gal}(H/K)} \pi(x)^{\sigma},$$

where the sum is taken with respect to the group law on $E(H)$, belongs to $E(K)$. Up to sign, it is independent of the choice of the Heegner point x, and we have the formula

$$\hat{h}(P_K) = \hat{h}(c_{1,f}) \cdot \deg(\pi) ,$$

where the canonical heights are taken on the abelian varieties E and $\mathrm{Jac}(X_0(N))$ over K. The degree of π also appears when we compare periods:

$$\|\omega\|^2 \underset{\text{defn.}}{=} \iint_{E(\mathbb{C})} |\omega \wedge \bar{\omega}| = c^2 \|\omega_f\|^2/\deg(\pi) .$$

Consequently, Theorem 6.3 of Chapter I with $\chi = 1$ gives the identity

Theorem 2.1. $L'(E/K,1) = \|\omega\|^2 \hat{h}(P_K)/c^2 u_K^2 |D|^{1/2}$.

Now assume that P_K has infinite order, so $L'(E/K,1) \neq 0$. The conjecture of Birch and Swinnerton-Dyer then predicts that $E(K)$ has rank 1 over $\mathbb{Z}$ and gives an exact formula for the first derivative in terms of arithmetic invariants of E. For each place $\mathfrak{p}$ of K which divides N, let $m_{\mathfrak{p}}$ be the order of the finite group of connected components in the Néron model for E over $\mathcal{O}_{\mathfrak{p}}$. Since $\mathfrak{p} \cdot \bar{\mathfrak{p}} = p$ is a rational prime, we have $m_{\mathfrak{p}} = m_{\bar{\mathfrak{p}}}$ and hence (writing m_p for this common value) $m_{\mathfrak{p}} \cdot m_{\bar{\mathfrak{p}}} = m_p^2$. Put $m = \prod_{p|N} m_p$. Finally, let $|Ш_K|$ denote the order of the Tate-Shafarevitch group of E over K; this integer is conjecturally finite and, if so, is a square [35]. Then the conjecture of Birch and Swinnerton-Dyer predicts the identity

$$L'(E/K,1) \overset{?}{=} \|\omega\|^2 \cdot m^2 \cdot \hat{h}(P_K) \cdot |Ш_K| / |D|^{1/2} [E(K):\mathbb{Z}P_K]^2$$

[35]. Theorem 2.1 confirms this up to a rational square and suggests:

Conjecture 2.2. If P_K has infinite order in $E(K)$, then it generates a subgroup of finite index and this index equals $c \cdot m \cdot u_K \cdot |Ш_K|^{1/2}$.

Notice that in Conjecture 2.2 the integer m is an invariant of E over $\mathbb{Q}$, the integer $u_K = \mathrm{Card}(\mathcal{O}^*/\pm 1)$ is an invariant of K, and the group $Ш_K$ is an invariant of E over K. The integer c is an invariant of the parametrization π of E over $\mathbb{Q}$, which also enters into the definition of the point P_K. However, if π' is another parametrization of E we have

$n'_E \circ \pi' = n_E \circ \pi$ for some integers $n, n' \geq 1$. Hence $n'c' = nc$ and $n'P'_K = nP_K$, so Conjecture 2.2 is independent of the parametrization chosen. We henceforth assume that π is the parametrization of minimal degree for E; this minimizes the index of $\mathbb{Z} P_K$ in $E(K)$.

Since the index of $\mathbb{Z}P_K$ in $E(K)$ is certainly divisible by $t = |E(\mathbb{Q})_{tor}|$, Conjecture 2.2 implies the simpler

Conjecture 2.3. If $E(K)$ has rank 1, then the integer $c \cdot m \cdot u_K \cdot |Ш_K|^{1/2}$ is divisible by t.

(Notice that this makes sense even without knowing that $Ш_K$ is finite, since in considering the divisibility of $|Ш_K|$ by a natural number n we may replace $Ш_K$ by its n-torsion subgroup, which is known to be finite.)

Conjecture 2.3 can be attacked using descent techniques. In many cases, t divides the term $c \cdot m$, which depends only on E over $\mathbb{Q}$. For example, when $N = 11$ there are 3 curves to consider.

E	c	m	t
$E_0 = J_0(11)$	1	5	5
$E_0/\mu_5 = J_1(11)$	5	1	5
$E_0/(\mathbb{Z}/5)$	1	1	1

However, the identity $t = cm$ does not always hold; when $N = 65 = 5 \cdot 13$ we have 2 curves, with invariants:

E	c	m	t
$E_0 = J_0(65)/\langle w_5, w_{13}\rangle$	1	1	2
$E_0/(\mathbb{Z}/2)$	1	4	2

Conjecture 2.3 for the curve $E = E_0$ predicts that if K is imaginary quadratic where 5 and 13 are split, then either

$$\begin{cases} \text{a)} & K = \mathbb{Q}(i) \ (\text{so } u_K = 2), \text{ or} \\ \text{b)} & Ш(E/K)_2 \neq 0 , \text{ or} \\ \text{c)} & \operatorname{rank}(E(K)) > 1 . \end{cases}$$

Using results of Kramer [22], one can show that for $K \neq \mathbb{Q}(i)$ the 2-Selmer group of E over K has rank ≥ 4 over $\mathbb{Z}/2$. Hence either b) or c) is true.

We now show how these results concerning the Birch - Swinnerton-Dyer conjecture over K can be used to prove the statements concerning the same conjecture over $\mathbb{Q}$ stated in Theorem 7.3 of Chapter I. This theorem is trivial if $L'(E,1) = 0$ (take $P = 0$), so we can assume $\operatorname{ord}_{s=1} L(E,s) = 1$. In particular, the sign of the functional equation of $L(E,s) = L(f,s)$ is -1, so $f|w_N = f$. As in §1 we choose a K by Waldspurger's theorem so that $L_\varepsilon(f,1) \neq 0$. The function $L_\varepsilon(f,s)$ is the L-series of E' over $\mathbb{Q}$, where E' is the twist of E by K (i.e. the elliptic curve defined by $Dy^2 = x^3 + ax + b$, where $y^2 = x^3 + ax + b$ is a Weierstrass equation for E). By the theory of modular symbols [25], we have

$$L(E',1) = \alpha' \Omega' ,$$

where Ω' is the fundamental real period of the Néron differential $\omega' = \omega/\sqrt{D}$ on E' and α' is a rational number, which by our choice of K is non-zero. We also have the identity

$$\frac{\|\omega\|^2}{|D|^{1/2}} = [E(\mathbb{R}):E(\mathbb{R})^0] \cdot \Omega \cdot \Omega' .$$

If we take $P = P_K + \overline{P_K} \in E(\mathbb{Q})$, and combine Theorem 2.1 and the last two formulas, we obtain the desired formula $L'(E,1) = \alpha\Omega\hat{h}(P)$ with $\alpha \in \mathbb{Q}^\times$.

Finally, we recall that the Birch - Swinnerton-Dyer conjecture applies to abelian varieties defined over number fields, not just to elliptic curves; our result says something about this more general case. Namely, let $f = \sum a_n q^n$ be a Hecke eigenform of weight 2 and level N whose Fourier coefficients do not lie in $\mathbb{Q}$ but instead generate a totally real number field K_f of degree m (i.e. f lies in an m-dimensional irreducible representation of the Hecke algebra over $\mathbb{Q}$). Then one can associate to f an m-dimensional abelian variety $A_0/\mathbb{Q}$ which is a quotient of the Jacobian of $X_0(N)$. The L-series of A_0, or of any abelian variety A isogenous to A_0 over $\mathbb{Q}$, is given by

$$(2.4) \qquad L(A/\mathbb{Q},s) = \prod_{\alpha:K_f \hookrightarrow \mathbb{R}} L(f^\alpha, s) .$$

Now assume that $f|w_N = f$, so that the sign of the functional equation of $L(f,s)$ is -1. Then by Corollary 1.3 we know that the order of vanishing of $L(A/\mathbb{Q},s)$ at $s = 1$ is either m or $\geq 3m$, depending whether $L'(f,1)$ is non-zero or zero. Moreover, (2.4) gives the identity $L^{(m)}(A,s) = \prod_\alpha L'(f^\alpha,1)$. We now imitate the argument for the case $m = 1$ to show that $\operatorname{ord}_{s=1} L(A/\mathbb{Q},s) = m$ implies that $\operatorname{rk} A(\mathbb{Q}) \geq m$ (the space $A(\mathbb{Q}) \otimes \mathbb{R}$ contains the m-dimensional subspace spanned by the c_{1,f^α}) and that if equality holds the Birch - Swinnerton-Dyer formula for $L^{(m)}(A/\mathbb{Q},1)$ is true up to a non-zero rational multiple.

§3. Generalized Heegner points and their relation to L-series

In §1 we related the main theorem of Chapter IV, under the assumptions $k=1$ and

$$(3.1) \qquad \varepsilon(p) = 1 \quad \text{for all } p|N ,$$

to the computations in Chapters II and III of heights of Heegner points on $X_0(N)$. However, a glance at Theorem 6.9 of Chapter IV shows that the formula for $L'_A(f,1)$ when $k=1$ and $\varepsilon(N)=1$ is of essentially the same nature when (3.1) is not fulfilled as when it is. Moreover, Theorem 5.6 of Chapter IV (for k=1), giving $L_A(f,1)$ when $\varepsilon(N)=-1$, also has a similar (though much simpler) form. We would therefore expect that there is again a connection with the heights of Heegner-like points on some algebraic curve. This is indeed the case and will now be described briefly. The detailed proofs, which follow the lines of the height computations in this paper, will be given in a later paper; the simplest case, when N is prime and $\varepsilon(N)=-1$, is worked out in detail in [16].

Let S be the finite set

$$S = \{\, p \mid p \text{ prime},\ \operatorname{ord}_p(N) \text{ odd},\ \varepsilon(p)=-1 \,\}\ .$$

Then $(-1)^{|S|}=\varepsilon(N)$, so the parity of $|S|$ corresponds to the sign of the functional equation of $L_A(f,s)$. If $|S|$ is even, so that $L_A(f,s)$ has an odd order zero at $s=1$, we define B to be the indefinite quaternion algebra over $\mathbb{Q}$ ramified at S ("indefinite case"), while if $|S|$ is odd, so that $\operatorname{ord}_{s=1} L_A(f,s)$ is even, we take for B the definite quaternion algebra over $\mathbb{Q}$ ramified at $S\cup\{\infty\}$ ("definite case"). Since every prime which ramifies in B is inert in K, there is an embedding $j:K\to B$. Let R be an order in B which contains $j(\mathcal{O})$ and has reduced discriminant N. Such global orders exist [15]; in the indefinite case they are unique up to conjugacy whereas in the definite case there are finitely many conjugacy classes. The group $\Gamma = R^\times/\{\pm 1\}$ embeds as a discrete subgroup of the real Lie group $G=(B\otimes\mathbb{R})^\times/\mathbb{R}^\times$.

In the indefinite case, the group G is isomorphic to $PGL_2(\mathbb{R})$ and $\Gamma^+ = \Gamma\cap PGL_2^+(\mathbb{R})$ is an infinite Fuchsian group which acts discretely on $\mathfrak{H}$. If (3.1) holds then $\Gamma^+ \cong \Gamma_0(N)$ and we are in the case studied in this paper; in all other cases the curve $\Gamma^+\backslash\mathfrak{H}$ is a compact Riemann surface. An important theorem of Shimura [32] states that this curve has a canonical model X over $\mathbb{Q}$. This model is characterized by the fields of rationality of its special points and has a modular description as the coarse moduli of polarized abelian surfaces with endomorphisms by R. The Hecke correspondences are rational over $\mathbb{Q}$ and determine the zeta-function. The embedding $j:\mathcal{O}\to R$ gives rise to a Heegner point x of discriminant D on X, rational over the Hilbert class field H of K.

The group $\operatorname{Pic}(\mathcal{O})$ acts freely on the set of Heegner points of discriminant D, the action being described via conjugation in $\operatorname{Gal}(H/K)$ by Shimura's reciprocity law. The generalization of our main identity says that the coefficients $a_{m,A}$ in Theorem 6.9 of Chapter IV are given by a fixed multiple of $\langle x, T_m x^{\sigma_A}\rangle$, where $\langle\ ,\ \rangle$ is the height pairing on $\operatorname{Pic}(X)$ defined using the Néron-Tate theory. The necessary height computations are similar to those in Chapters II and III of this paper. For instance, the number $\kappa = -\frac{12}{N}\prod_{p\mid N}\left(1+\frac{\varepsilon(p)}{p}\right)^{-1}$ which occurs in Theorem 6.9 of Chapter IV arises (just as in the special case, (2.13) of Chapter II) as the residue of the resolvent kernel function G_s for $X(\mathbb{C})$ at $s=1$.

In the definite case, $G\simeq SO_3(\mathbb{R})\subset PGL_2(\mathbb{C})$ and Γ is a finite group which acts on $\mathbb{P}^1(\mathbb{C})$. The quotient $\Gamma\backslash\mathbb{P}^1(\mathbb{C})$ is again a compact Riemann surface, now always of genus 0, and one can again construct a canonical model of this curve over $\mathbb{Q}$: it is simply $\Gamma\backslash Y$, where Y is the curve of genus 0 over $\mathbb{Q}$ which corresponds to the quaternion algebra B. To define Hecke operators one must work with the disjoint union $X=\coprod_{i=1}^{n}\Gamma_i\backslash Y$ where n is the class number of R and Γ_i is the projective unit group of the right order of the i^{th} left ideal class. (This union is a natural double coset space in the adèlic point of view.) The representation of the Hecke algebra on $\operatorname{Pic}(X)\simeq\mathbb{Z}^n$ then gives rise to the classical theory of Brandt matrices [16]. Again $j:\mathcal{O}\to R$ gives a Heegner point x of discriminant D on X, this time defined already over K, and $\operatorname{Pic}(\mathcal{O})$ acts freely on the set of such Heegner points. We define a height pairing $\langle\ ,\ \rangle$ on $\operatorname{Pic}(X)$ by setting $\langle x,y\rangle$ equal to 0 if x and y are on different components of X and to $|\Gamma_i|$ if x and y are both on the component $\Gamma_i\backslash Y$. Our main identity in this case says that the coefficients $b_{m,A}$ occurring in Theorem 5.6 of Chapter IV (for k=1) are fixed multiples of $\langle x, T_m x^{\sigma_A}\rangle$. An argument like that in §1 of this chapter permits us to deduce a relationship between $L(f,\chi,1)$ and $\langle x_{\chi,f}, x_{\chi,f}\rangle$ for a newform $f\in S_2(\Gamma_0(N))$ and character $\chi: Cl_K\to\mathbb{C}^\times$, where $x_{\chi,f}$ is the obvious eigencomponent. Since $x_{1,f}$ lies in a fixed 1-dimensional space as K varies, the theorem of Waldspurger and Vignéras (cf. [36]) that $L(f,1,1)$ is proportional to the square of an element of K_f follows immediately.

§4. The case $k>1$: higher weight cycles and an algebraicity conjecture

We now return to the hypothesis (3.1), but assume that $k>1$. Recall that for $s \in \mathbb{C}$ and $m \in \mathbb{N}$ prime to N we defined an invariant $\gamma^m_{N,s}(A)$ in Chapter II by $\gamma^m_{N,s}(A) = \sum_{\tau \in G} G^m_{N,s}(x^\tau, x^{\tau\sigma})$, where

x is a Heegner point of discriminant D,

σ is the element of $G = \mathrm{Gal}(H/K)$ corresponding to A, and

$G^m_{N,s} = G_{N,s}|T_m$, $G_{N,s}$ the resolvent kernel function for $\Gamma_0(N)$.

If $r_A(m) \neq 0$, then some of the terms in the sum defining $\gamma^m_{N,s}(A)$ become infinite and the definition of $\gamma^m_{N,s}(A)$ has to be modified as explained in §5 of Chapter II. The final formula obtained for $\gamma^m_{N,s}(A)$ (Proposition 5.8 of Chapter II) can be expressed using Proposition 4.6(a) of Chapter IV as

$$\gamma^m_{N,s}(A) = -2u^2 \sum_{n=1}^{\infty} \sigma_A(n)\, r_A(nN+m|D|)\, Q_{s-1}\left(1+\frac{2nN}{m|D|}\right) + 2hu\, r_A(m)\left(\frac{\Gamma'}{\Gamma}(s) - \log 2\pi + \frac{1}{2}\log|D| + \frac{L'}{L}(1,\varepsilon)\right).$$

Comparing this with the formula for $a_{m,A}$ in Theorem 5.8 of Chapter IV, we see that we have the following analogue for higher weight of the main identity proved in §1 :

Theorem 4.1. Suppose (3.1) is satisfied, k an integer greater than 1. Then there is a holomorphic cusp form $\Phi = \sum_{m \geq 1} a_{m,A} q^m \in S_{2k}(\Gamma_0(N))$ satisfying

$$L'_A(f,k) = \frac{2^{4k-1}\pi^{2k}}{(2k-2)!\sqrt{|D|}}\,(f,\Phi) \quad \text{for all } f \in S^{new}_{2k}(\Gamma_0(N))$$

and with $a_{m,A}$ (m prime to N) given by

$$(4.2) \qquad a_{m,A} = \frac{m^{k-1}}{u^2}\gamma^m_{N,k}(A) + \frac{h}{u} r_A(m)\, m^{k-1} \log\frac{N}{m} - m^{k-1} \sum_{0<n\leq \frac{m|D|}{N}} \sigma'_A(n)\, r_A(m|D|-nN)\, P_{k-1}\left(1-\frac{2nN}{m|D|}\right).$$

Since $P_{k-1}\left(1-\frac{2nN}{m|D|}\right) r_A(m|D|-nN)$ is rational and $\sigma'_A(n)$ is a rational linear

combination of logarithms of primes (indeed, by the remark following Proposition 4.6 of Chapter IV, a nonnegative even integral multiple of the logarithm of a single prime), equation (4.2) expresses $a_{m,A}$ as a finite sum of values of $G^m_{N,k}$ at Heegner points plus a finite sum of rational multiples of logarithms of prime numbers. This is reminiscent of the situation for $k=1$ and suggests that there should be an interpretation of the right-hand side of (4.2) as some sort of a height. In fact such an interpretation has been provided by Deligne, who found a definition of Heegner vectors s_x in the stalks above Heegner points x of the local coefficient system $\mathrm{Sym}^{2k-2}(\underline{H}^1)$ ($\underline{H}^1$ = first cohomology group of the universal elliptic curve over $X_0(N)$) and of a height pairing $\langle\ ,\ \rangle$ such that $\langle s_x, T_m s_{x^\sigma}\rangle = a_{m,A}$. The height pairing is defined as the sum of local heights characterized by axioms similar to those of §4 of Chapter I, and these can be calculated using intersection theory at the finite places and values of a certain eigenfunction of the Laplace operator (which turns out to be $G_{N,k}$) at the archimedean places. Moreover, the definitions can be carried over to the case when (3.1) is not satisfied (now with $X_0(N)$ replaced by the curve discussed in §3 and $\mathrm{Sym}^{2k-2}(\underline{H}^1)$ by the local coefficient system $\Gamma^+\backslash \mathfrak{H}\times W$ or $\coprod_i \Gamma_i\backslash \mathbb{P}^1(\mathbb{C})\times W$, where W is the unique $(2k-1)$-dimensional irreducible representation of $B^\times/\mathbb{Q}^\times$), and one again gets a formula relating the heights of the Heegner vectors to the values of $L_A(f,k)$ or $L'_A(f,k)$ as calculated in Chapter IV. However, the global significance of the sum of the local heights is not yet understood (e.g.: under what circumstances does the height pairing vanish?), so that we do not get applications of the sort given for $k=1$.

However, even in the absence of a complete height theory, the identity (4.2) is not devoid of interest. Suppose, for instance, that there are no non-zero cusp forms of weight $2k$ on $\Gamma_0(N)$. Then $a_{m,A}$ must vanish for each m, and (4.2) gives us an explicit formula for $\gamma^m_{N,k}(A)$ as a rational linear combination of logarithms of rational primes. If $S_{2k}(\Gamma_0(N))$ is not 0, we replace $G^m_{N,k}$ by the function

$$G_{N,k,\underline{\lambda}}(z_1,z_2) = \sum_{m=1}^{\infty} \lambda_m\, m^{k-1}\, G^m_{N,k}(z_1,z_2),$$

where $\underline{\lambda} = \{\lambda_m\}_{m\geq 1}$ with

i) $\lambda_m \in \mathbb{Z}$, $\lambda_m = 0$ for all but finitely many m,

ii) $\sum_{m\geq 1} \lambda_m a_m = 0$ for any cusp form $\sum a_m q^m \in S_{2k}(\Gamma_0(N))$,

and (for convenience)

iii) $\lambda_m = 0$ for m not prime to N

(we call such a $\underline{\lambda}$ a relation for $S_{2k}(\Gamma_0(N))$). Then (4.1) implies that the invariant

$$\gamma_{N,k,\underline{\lambda}}(A) = \sum_{m=1}^{\infty} m^{k-1} \lambda_m \gamma^m_{N,k}(A) = \sum_{\tau\in G} G_{N,k,\underline{\lambda}}(x^\tau, x^{\tau\sigma})$$

is a rational linear combination of logarithms of prime numbers:

Corollary 4.3. Suppose (3.1) is satisfied, $k>1$. Let λ be a relation for $S_{2k}(\Gamma_0(N))$ and A an ideal class of K. Then

$$\gamma_{N,k,\underline{\lambda}}(A) = \sum_{m>0} \lambda_m m^{k-1} \mathrm{hur}_A(m) \log\frac{m}{N} + u^2 \sum_{\substack{m,\, n\in\mathbb{Z}\\ m|D|\geq nN>0}} \lambda_m m^{k-1} \sigma'_A(n)\, r_A(m|D|-nN)\, P_{k-1}\left(1-\frac{2nN}{m|D|}\right).$$

In particular, $\exp\left(\frac{D^{k-1}}{u^2}\gamma_{N,k,\underline{\lambda}}(A)\right)$ is a rational number, and in fact a rational square unless $|D|$ is prime.

To prove the last statement, multiply both sides of the formula by D^{k-1}/u^2. Then the terms in the second sum with $m|D|>nN>0$ are even integral combinations of logarithms of rational primes, because $m^{k-1}D^{k-1}P_{k-1}(1-\frac{2nN}{m|D|})$, $r_A(m|D|-nN)$ and λ_m are integers and $\sigma'_A(n)$ is an even multiple of the logarithm of a prime. In the terms with $m|D|=nN$ (these can occur only for $N=1$, since we are assuming both m and D prime to N) we lose a factor $2u$ because $r_A(0)=\frac{1}{2u}$ but gain a factor of $m^{k-1}D^{k-1}$ (cancelling at least the u) because $P_{k-1}(-1)$ $(=(-1)^{k-1})$ has no denominator. If D has more than one prime factor, then the extra factor of 2 in these terms is gained because the numbers $a_p(n)$ in Proposition 4.6 of Chapter IV are divisible by 4 rather than just 2 when $D|n$ (because $4|\delta(n)$). Similarly, the first sum in 4.3 multiplied by D^{k-1}/u^2 is always an integral multiple of $\log\frac{m}{n}$ and this multiple is even if $|D|$ is not prime because $2|h$.

Let us return for a moment to the case $k=1$, and consider the interpreta-

tion of the formula for $\gamma_{N,k,\underline{\lambda}}(A)$ there. We know from Chapter II that the individual terms $G_{N,1,\underline{\lambda}}(x^\tau,x^{\sigma\tau})$ in the definition of $\gamma_{N,1,\underline{\lambda}}(A)$ are the local height pairings at archimedean places of the divisors $\sum_{m\geq 1}\lambda_m T_m((x)-(\infty))$ and $(x^\sigma)-(0)$. On the other hand, the action of the Hecke operators on $J_0(N)$ is the same as that on $S_2(\Gamma_0(N))$, so the fact that $\underline{\lambda}$ is a relation for $S_2(\Gamma_0(N))$ means that $\sum_m \lambda_m T_m a$ is a principal divisor for any divisor a of degree 0. In particular, $\sum_m \lambda_m T_m((x)-(\infty)) = (\phi)$ for some rational function ϕ on $X_0(N)$ defined over H, and then the axioms for the local height pairings imply

$$\langle \sum_{m\geq 1}\lambda_m T_m((x)-(\infty))\, ,(x^\sigma)-(0)\rangle_v = \log\left|\frac{\phi(x^\sigma)}{\phi(0)}\right|_v$$

for any place v of H. In particular, the numbers $G_{N,1,\underline{\lambda}}(x^\tau,x^{\sigma\tau})$ are the logarithms of the absolute values of the conjugates of an algebraic number lying in the class field H. It is then natural to expect that the same thing happens for $k>1$:

Conjecture 4.4. Let the hypotheses be as in Corollary 4.3 and fix a Heegner point x and an embedding $H\hookrightarrow\mathbb{C}$. Then there exists a number $\alpha\in H^\times$ such that $G_{N,k,\underline{\lambda}}(x^\tau,x^{\sigma\tau}) = u^2 D^{1-k}\log|\alpha^\tau|$ for all $\tau\in G=\mathrm{Gal}(H/K)$.

This conjecture is at least compatible with Corollary 4.3, which, if the conjecture is true, gives an explicit formula for the prime decomposition of the absolute norm of the number α. In fact, one can give a more precise version of Conjecture 4.4, based on the form of the expression for $\gamma_{N,k,\underline{\lambda}}(A)$ in 4.3, which predicts which ideal α generates and hence specifies α up to a unit. (The details will be given in a later paper.) Together with 4.4, which specifies the absolute values of α at archimedean places, this determines α up to a root of unity and also allows numerical computations to check the conjecture. We end with numerical examples to illustrate 4.3 and 4.4. We take the simplest case: $D=-p$ with $p>3$ a prime congruent to 3 (mod 4), $A=[\mathcal{O}]$ the trivial ideal class, $N=1$, $k=2$ and $\underline{\lambda}=(1,0,0,\ldots)$ (this is permissible since $S_4(SL_2(\mathbb{Z}))=\{0\}$). Then

$\gamma_{N,k,\underline{\lambda}}(A)$ equals $\sum_z G(z)$ where the sum is over all $h(-p)$ points $z \in H/SL_2(\mathbb{Z})$ satisfying a quadratic equation of discriminant $-p$ over $\mathbb{Z}$ and $G(z) = G_{1,2}(z,z)$ (defined as in §5 of Chapter II by a limiting procedure). For primes with $h(-p) = 1$, Corollary 4.3 gives a fomula for $G(\frac{1+i\sqrt{p}}{2})$, e.g.

$$G\left(\frac{1+i\sqrt{7}}{2}\right) = -\log 7 - 2\log 3 - \frac{12}{7}\log 5 ,$$

$$G\left(\frac{1+i\sqrt{43}}{2}\right) = -\log 43 + \frac{2}{43}\log\frac{5^6 7^{29}}{2^{127}3^{54}} ,$$

$$G\left(\frac{1+i\sqrt{163}}{2}\right) = -\log 163 + \frac{2}{163}\log\frac{2^{233}5^6 7^{37}19^{125}}{3^{163}11^{35}23^{42}29^{138}127^{91}} .$$

The reader can check these numerically using the expansion (to be proved in a later paper)

$$(4.5)\qquad \begin{aligned} G\left(\tfrac{1}{2}+iy\right) &= -\frac{2\pi}{3}y - \frac{119\zeta(3)}{2\pi^2}y^{-2} - \left(8 - \frac{480}{\pi y} - \frac{240}{\pi^2 y^2}\right)e^{-2\pi y} \\ &\quad - \left(282876 + \frac{283968}{\pi y} + \frac{70992}{\pi^2 y^2}\right)e^{-4\pi y} + O(e^{-6\pi y}) \end{aligned}$$

(with an $O(\ )$-constant of about 10^8). For the prime $p = 31$ with class number $h(-p) = 3$, Corollary 4.3 gives

$$G\left(\frac{1+i\sqrt{31}}{2}\right) + G\left(\frac{1+i\sqrt{31}}{4}\right) + G\left(\frac{-1+i\sqrt{31}}{4}\right) = -\log 31 - \frac{2}{31}\log 3^{116}11^8 17^6 23^{30}$$

and Conjecture 4.4 (or rather, the more precise form of it mentioned above) predicts

$$G\left(\frac{1+i\sqrt{31}}{2}\right) = -\log \pi_{31} - \frac{2}{31}\log\frac{\pi_3^{54}\pi_9^{31}\pi_{121}^{13}\pi_{17}^{6}\pi_{23}^{30}}{\pi_{11}^{18}\theta^n} ,$$

for some $n \in \mathbb{Z}$, where $\theta \approx 1.465571232$ is the real root of $\theta^3 - \theta^2 - 1 = 0$ and the π_q are the prime elements (of norm q)

$$\pi_3 = \theta+1 ,\quad \pi_9 = 3/\pi_3,\quad \pi_{11} = 3\theta-4 ,\quad \pi_{121} = 11/\pi_{11} ,\quad \pi_{17} = -\theta+3 ,\quad \pi_{23} = -3\theta+5 ,\quad \pi_{31} = 3\theta+1$$

in the field $\mathbb{Q}(\theta)$ (which equals $\mathbb{Q}(j(\frac{1+i\sqrt{31}}{2}))$, the real subfield of the Hilbert class field of $\mathbb{Q}(\sqrt{-31})$). Using (4.5), the reader can check that this holds numerically to at least 15 places with $n = 61$.

Bibliography

[1] Atkin, A.O.L. and Lehner, J.: Hecke operators on $\Gamma_0(m)$. Math. Ann. 185, 134-160 (1970).

[2] Birch, B.J.: Elliptic curves and modular functions. Symp. Math. Ist. Alta Mat. 4, 27-32 (1970).

[3] Birch, B.J.: Heegner points of elliptic curves. Symp. Math. Ist. Alta Mat. 15, 441-445 (1975).

[4] Birch, B.J. and Stephens, N.: Heegner's construction of points on the curve $y^2 = x^3 - 1728e^3$. Séminaire de Théorie des Nombres, Paris 1981-82, Progress in Math. 38, pp. 1-19. Boston: Birkhäuser 1983.

[5] Birch, B.J. and Stephens, N.: Computation of Heegner points. In Modular Forms (ed. R.A. Rankin), pp. 13-41. Chichester: Ellis Horwood 1984.

[6] Deligne, P.: Valeurs de fonctions L et périodes d'intégrales. Symp. Pure Math. A.M.S. 33, II, 313-346 (1979).

[7] Deligne, P. and Rapoport, M.: Les schémas de modules de courbes elliptiques. In Modular Functions of One Variable II (ed. P. Deligne, W. Kuyk), Lecture Notes in Math. 349, pp. 143-316. Berlin-Heidelberg-New York: Springer 1973.

[8] Deuring, M.: Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. Abh. Math. Sem. Hamburg 14, 197-272 (1941).

[9] Drinfeld, V.G.: Elliptic modules (Russian). Math. Sbornik 94, 596-627 (1974). English translation: Math. USSR, Sbornik 23 (4), 1973.

[10] Eichler, M.: Lectures on modular correspondences. Lecture Notes of the Tata Institute 9 (1956), Bombay.

[11] Eichler, M.: Quaternäre quadratische Formen und die Riemannsche Vermutung für die Kongruenzzetafunktion. Arch. Math. 5, 355-366 (1954).

[12] Goldfeld, D.: The conjectures of Birch and Swinnerton-Dyer and the class numbers of quadratic fields. In Journées Arithmétiques de Caen, Astérisque 41-42, pp. 219-227. Soc. math. de France 1977.

[13] Gross, B.: Heegner points on $X_0(N)$. In Modular Forms (ed. R.A. Rankin), pp. 87-106. Chichester: Ellis Horwood 1984.

[14] Gross, B.: Local heights on curves. To appear in Proceedings of the Conference on Arithmetic Algebraic Geometry, Storrs.

[15] Gross, B.: On canonical and quasi-canonical liftings. This journal, pp. ?? .

[16] Gross, B.: Heights and the special values of L-series. To appear in Sém. Math. Sup., Presses Univ. Montréal.

[17] Gross, B. and Zagier, D.: Points de Heegner et dérivées de fonctions L. C.R. Acad. Sci. Paris 297, 85-87 (1983).

[18] Gross, B. and Zagier, D.: On singular moduli. J. reine u. angew. Math. 355, 191-220 (1985).

[19] Hecke, E.: Analytische Arithmetik der positiven quadratischen Formen. In Mathematische Werke, pp. 789-918. Göttingen: Vandenhoeck & Ruprecht 1959.

[20] Hejhal, D.: The Selberg Trace Formula for PSL(2,$\mathbb{R}$). Lecture Notes in Math. 1001. Berlin-Heidelberg-New York: Springer 1983.

[21] Katz, N. and Mazur, B.: Arithmetic Moduli of Elliptic Curves. Annals of Math. Studies 108. Princeton at the Univ. Press 1985.

[22] Kramer, K.: Arithmetic of elliptic curves upon quadratic extension. Trans. A.M.S. 264, 121-135 (1981).

[23] Lang, S.: Elliptic Functions. Reading: Addison-Wesley 1973.

[24] Lang, S.: Les formes bilinéaires de Néron et Tate. Sém. Bourbaki No. 274 (1964).

[25] Mazur, B. and Swinnerton-Dyer, H.P.F.: Arithmetic of Weil curves. Inv. math. 25, 1-61 (1974).

[26] Mestre, J.-F.: Courbes de Weil de conducteur 5077. C.R. Acad. Sc. Paris 300, 509-512 (1985).

[27] Néron, A.: Quasi-fonctions et hauteurs sur les variétés abéliennes. Ann. of Math. 82, 249-331 (1965).

[28] Oesterlé, J.: Nombres de classes des corps quadratiques imaginaires. Sém. Bourbaki No. 631 (1984).

[29] Serre, J.-P.: Complex multiplication. In Algebraic Number Theory (ed. J.W.S. Cassels, A. Fröhlich), pp. 292-296. London-New York: Academic Press 1967.

[30] Serre, J.-P. and Tate, J.: Good reduction of abelian varieties. Annals of Math. 88, 492-517 (1968).

[31] Serre, J.-P. and Tate, J. (Mimeographed notes from the AMS Summer Institute at Woods Hole, 1964.)

[32] Shimura, G.: Construction of class fields and zeta functions of algebraic curves. Ann. of Math. 85, 58-159 (1967).

[33] Sturm, J.: Projections of C^∞ automorphic forms. Bull. A.M.S. 2, 435-439 (1980).

[34] Swinnerton-Dyer, H.P.F. and Birch, B.J.: Elliptic curves and modular functions. In Modular Functions of One Variable IV (ed. B.J. Birch, W. Kuyk), Lecture Notes in Math. 476, pp. 2-32. Berlin-Heidelberg-New York: Springer 1975.

[35] Tate, J.: The arithmetic of elliptic curves. Inv. math. 23, 179-206 (1974).

[36] Vignéras, M.-F.: Valeur au centre de symétrie des fonctions L associées aux formes modulaires. Séminare de Théorie des Nombres, Paris 1979-80, Progress in Math. 12, pp. 331-356. Boston: Birkhäuser 1981.

[37] Waldspurger, J.-L.: Correspondances de Shimura et quaternions. Preprint.

[38] Weil, A.: Über die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen. Math. Ann. 168, 149-156 (1967).

[39] Zagier, D.: L-series of elliptic curves, the Birch-Swinnerton-Dyer conjecture, and the class number problem of Gauss. Notices A.M.S. 31, 739-743 (1984).

On canonical and quasi-canonical liftings

Benedict H. Gross

1. Let F be a field complete with respect to a discrete valuation, with finite residue class field. Let A be the ring of integers in F, let π be a prime element in A, and let q be the number of elements in the residue field $A/\pi A$.

Let k be an A-algebra, with structural map $i : A \to k$. A formal A-module (G,g) of dimension 1 over k is, by definition [1,§1]:

(1.1) a commutative formal group G of dimension 1 over k

(1.2) a homomorphism $g : A \to \mathrm{End}_k(G)$ which induces the map i on the tangent space: $\mathrm{End}_k(\mathrm{Lie}\ G) \simeq k$.

If k is a field and $\ker i = \pi A$, the endomorphism $g(\pi)$ is either zero or a purely inseparable isogeny of degree q^h for some integer $h \geq 1$. In the latter case, we say (G,g) has height h. If (G,g) and (G',g') are two formal A-modules over the A-algebra k, we define:

$$(1.3)\quad \mathrm{Hom}_k((G,g),(G',g')) = \{f \in \mathrm{Hom}_k(G,G') : f\circ g = g'\circ f\}.$$

If k is a separably closed field, the height is a complete isomorphism invariant of a formal A-module, and any value $h \geq 1$ can occur. The ring $\mathrm{End}_k(G,g)$ of a formal A-module of height h over a separably closed field is isomorphic to the maximal order in the division algebra B of invariant $1/h$ over F [1,Prop.1.7].

Henceforth we will usually drop the g in our notation.

2. Let K denote a separable quadratic extension of F, let $\mathcal{O}$ be the ring of integers in K, let p be a prime element in $\mathcal{O}$, and let q^f denote the cardinality of the residue field $\mathcal{O}/p\mathcal{O}$. We have $f = 2$ if $\mathcal{O}$ is unramified over A; otherwise $f = 1$. Let W be the ring of integers in the maximal unramified extension M of K. Then p is a prime of W and $W/pW = k$ is algebraically closed.

Let G denote the unique formal A-module of height $h = 2$ over k. The ring $R = \mathrm{End}_k(G)$ is isomorphic to the maximal order in the quaternion division algebra B over F. Fix an embedding

$$(2.1)\qquad \alpha : \mathcal{O} \hookrightarrow R$$

such that the action on $\mathrm{Lie}_k(G) = k$ is the reduction map $\pmod p$. Via α, the formal A-module G inherits the structure of a formal $\mathcal{O}$-module of height 1.

<u>Proposition 2.1</u> <u>There is a formal $\mathcal{O}$-module $\underline{G}$ over W, unique up to W-isomorphism, which reduces to $G \pmod p$.</u>

<u>Proof</u>. Lubin and Tate [4] construct a formal $\mathcal{O}$-module $\underline{G}$ over $\mathcal{O}$ with $g(p)\ [x] = px + x^{q^f}$. Since $\underline{G}$ has height 1 over $\mathcal{O}/p\mathcal{O}$, it becomes isomorphic to G over $W/pW = k$, which is separably closed. Since height 1 $\mathcal{O}$-modules have a trivial deformation space [5;1,prop.4.2] the lifting $\underline{G}$ is unique up to W-isomorphism.

3. We shall henceforth consider the formal $\mathcal{O}$-module $\underline{G}$ constructed in (2.1) as a formal A-module over W, with reduction G of height 2 over k. We will refer to $\underline{G}$ as the canonical lifting of the pair (G,α); we note that $\mathrm{End}_W(\underline{G}) = \mathcal{O}$ and $\mathrm{End}_{W/pW}(\underline{G}) = R$.

For $n \geq 1$ we define $R_{n-1} = \mathrm{End}_{W/p^nW}(\underline{G})$, so $R_0 = R$. The reduction of homomorphisms $(\bmod\ p^n)$ gives injections:

$$(3.1) \qquad R_n \hookrightarrow R_{n-1} \hookrightarrow R_{n-2} \hookrightarrow \cdots \hookrightarrow R_1 \hookrightarrow R$$

Since W is Henselian, we also have:

$$(3.2) \qquad \bigcap_{n\geq 0} R_n = \mathcal{O}\ .$$

<u>Proposition 3.3</u> <u>For $n \geq 1$ we have $R_n = \mathcal{O} + p^n R$.</u>

<u>Proof</u>: We shall first show that R_{n-1}/R_n is isomorphic to $\mathcal{O}/p\mathcal{O}$ as an $\mathcal{O}$-module.

Choosing co-ordinates, we may assume $\underline{G}$ is given by a formal group law $\underline{G}(x,y)$ over $W[[x,y]]$, and appeal to the formal cohomology theory developed by Lubin-Tate [5,§2] and Drinfeld [1,§4]. Let $G_1(x,y)$ be the partial derivative of $G(x,y) \in k[[x,y]]$ with respect to x. Then G_1 has constant term 1, so $G_1(0,y)$ is an invertible power series in $k[[y]]$.

For an endomorphism $f(x) \in R_{n-1}$ we define the series:

$$\alpha_f(x,y) = G_1(0,G(f(x),f(y)))^{-1} \quad \text{in } k[[x,y]]\ .$$

$$\beta_f(x) = G_1(0,f(x))^{-1} \quad \text{in } k[[x]]\ .$$

The data:

$$(3.4) \qquad \begin{cases} \Delta(f)(x,y) = \alpha_f(x,y)[f(\underline{G}(x,y)) - \underline{G}(f(x),f(y))] \\ \delta_a(f)(x) \;\;= \beta_f(x) \quad [f(a(x)) - a(f(x))] \qquad a \in A \end{cases}$$

define a symmetric 2-cocycle of the formal A-module $\underline{G}$ [1,pg 571] with coefficients in p^n/p^{n+1}. The cohomology class of (Δ,δ_a) depends only on the class of f $(\bmod\ R_n)$, we denote the resulting map:

$$(3.5) \qquad \alpha_n : R_{n-1}/R_n \hookrightarrow H^2(\underline{G},p^n/p^{n+1})$$

Applying α_n to the endomorphism $p \circ f$, we find:

$$\Delta(p\circ f)(x,y) = \alpha_{p\circ f}(x,y)[p\circ f(\underline{G}(x,y)) - \underline{G}(p\circ f(x),p\circ f(y))]$$

$$= \alpha_{p\circ f}(x,y)[p\circ f(\underline{G}(x,y)) - p\circ\underline{G}(f(x),f(y))]$$

as p is an endomorphism of $\underline{G}$ over W. Writing $\alpha_{p\circ f}(x,y) = c_p(x,y)\alpha_f(x,y)$ and recalling that $p(x) = px + x^{q^f}$, we find:

$$\Delta(p\circ f)(x,y) = c_p(x,y)\cdot p\cdot \Delta(f)(x,y) + \alpha_{p\circ f}\left[f(\underline{G}(x,y))^{q^f} - \underline{G}(f(x),f(y))^{q^f}\right]$$

$$\equiv c_p(x,y)\cdot p\cdot \Delta(f)(x,y) \qquad \pmod{p^{n+2}}$$

Similar arguments apply to $\delta_a(p\circ f)$, so by (3.5) the $\mathcal{O}$-module R_{n-1}/R_n is annihilated by p. Furthermore, we have a commutative diagram:

(3.6)
$$\begin{tikzcd}
\alpha_n : R_{n-1}/R_n \arrow[r, hook] \arrow[d, "p"] & H^2(\underline{G}, p^n/p^{n+1}) \arrow[d, "\wr\, p"] \\
\alpha_{n+1} : R_n/R_{n+1} \arrow[r, hook] & H^2(\underline{G}, p^{n+1}/p^{n+2})
\end{tikzcd}$$

Since R_n and R_{n-1} are both free $\mathcal{O}$-modules of rank 2 which contain $\mathcal{O}$, R_{n-1}/R_n is a cyclic $\mathcal{O}$-module. Hence it is isomorphic to $\mathcal{O}/p\mathcal{O}$ or is trivial. We will show that $R_{n-1}/R_n \simeq \mathcal{O}/p$ for all $n \geq 1$; by (3.6) it suffices to show that R/R_1 is a non-trivial $\mathcal{O}$-module.

First assume that $\mathcal{O}$ is unramified over A. In this case we take $p = \pi$ so $p(x) = \pi x + x^{q^2}$ and the formal module $\underline{G}$ is defined over A. Hence $\underline{G}$ (mod p) is rational over the finite field A/π of q elements,

and $j(x) = x^q$ defines an endomorphism (mod p). To show that $j(x)$ does not come from the reduction of an endomorphism (mod p^2), we compute (cf. (3.4))

$$\delta_\pi(j) = (\pi^q - \pi)x^q + \text{terms of higher degree.}$$

Since the coefficient of x^q is non-zero (mod p^2), this shows that $\alpha_1(j) \neq 0$ in $H^2(\underline{G}, p/p^2) \simeq pW/p^2W$ [5]. In this case we have $R = \mathcal{O} + \mathcal{O}j$.

Next assume that $\mathcal{O}$ is tamely ramified over A, so the characteristic of A/π is odd and $\mathcal{O} = A[p]$ with $p^2 = \pi$. Since $p(x) = px + x^q$ we have $\pi(x) = \pi x + (p+p^q)x^q + x^{q^2}$. In this case, $R = \mathcal{O} + \mathcal{O}j$ where $j^2 = u$ is a unit of A which is not a square in $(A/\pi)^*$. Hence $j(x) = vx + \ldots$ where $v^2 \equiv u$ in W/p and $v^q \not\equiv v$ (mod p). Then

$$\delta_\pi(j) = (v - v^q)(p + p^q)x^q + \text{terms of higher degree.}$$

Since the coefficient of x^q is non-zero (mod p^2), this shows that $\alpha_1(j) \neq 0$.

Finally, assume that $\mathcal{O}$ is wildly ramified over A with different ideal $\mathcal{D} = (p^e)$. Then the residue characteristic of A/π is equal to 2. If $\mathcal{O} = A[p]$ then p satisfies the Eisenstein equation $x^2 - ax + \pi = 0$ with $\mathrm{ord}_p(2p-a) = e$. Since $2p$ has odd valuation and a has even valuation, there is no cancellation and $2 \equiv 0$ (mod p^{e-1}). In this case the group F^*/NK^* is generated by a unit u with $\mathrm{ord}_\pi(u-1) = e-1$ and $B = K + Kj$ with $j^2 = u$. The maximal order R is given by $R = \mathcal{O} + p^{1-e}(1+j)$ and the element $p^{1-e}(1+j)$ is a unit whose residue class does not lie in $(A/\pi)^*$. An argument similar to the tamely ramified case now shows that $\delta_\pi(p^{1-e}(1+j)) \not\equiv 0$ (mod p^2)

By the remarks preceding (3.6) we have $R_n \supseteq \mathcal{O} + p^n R$. Since both of these rings have the same index in R , they are equal.

4. There is a further description of the subrings R_n , which is quite useful. By the theorem of Skolem-Noether, there is an element $j \in B^*/K^*$ such that conjugation by j induces the non-trivial automorphism of K over F . When $\mathcal{O}$ is unramified over A we may choose j to be a Frobenius element satisfying $j^2 = \pi$. When $\mathcal{O}$ is ramified over A we may choose j with $j^2 \equiv 1 \ (\pi^{e-1})$, where $D = (\pi^e)$ is the discriminant. In any case, we obtain a decomposition

$$B = K + Kj = B_+ + B_- \tag{4.1}$$

The reduced trace and reduced norm of an element $b = b_+ + b_-$ are given by:

$$\begin{cases} \mathrm{Tr}(b) = \mathrm{Tr}(b_+) \\ \mathbb{N}(b) = \mathbb{N}(b_+) + \mathbb{N}(b_-) \ , \end{cases} \tag{4.2}$$

and we have the following characterization of the rings R_n .

<u>Proposition 4.3</u> <u>For $n \geq 0$ we have</u>

$$\underline{R_n = \{b \in B : \mathrm{Tr}(b) \in A \ , \ \mathbb{N}(b) \in A \ , \ \mathbb{N}(b_-) \equiv 0 \mod \pi^{1-e+nf}\}}$$

$$\underline{= \{b \in R : D \cdot \mathbb{N}(b_-) \equiv 0 \mod \pi \cdot (\mathbb{N}p)^n\}}$$

<u>Proof</u>: We first observe that R is the subring of all $b \in B$ with $\mathrm{Tr}(b)$ and $\mathbb{N}(b)$ in A . Thus the two descriptions above are equivalent.

If $\mathcal{O}$ is unramified over A , $e = 0$ and $f = 2$. Then $R = \mathcal{O} + \mathcal{O}j$ and by (3.3) we have $R_n = \mathcal{O} + p^n j$. Since $\mathbb{N}(p^n j)$ has valuation $1 + 2n$, this gives the result.

If $\mathcal{O}$ is ramified over A , $e \geq 1$ and $f = 1$. Then $R = \mathcal{O} + p^{1-e}(1+j)$ and $R_n = \mathcal{O} + p^{1-e+n}(1+j)$ by (3.3). Since $\mathbb{N}(p^{1-e+n})$ has valuation $1 - e + n$, this gives the result.

5. Recall that M is the quotient field of W , the maximal unramified extension of $\mathcal{O}$. Let T denote the Tate module of the formal $\mathcal{O}$-module $\underline{G}$ over W : $T = \varprojlim_n \underline{G}_{p^n}(\overline{M})$. Then T is a free $\mathcal{O}$-module of rank 1 with an action of $\mathrm{Gal}(\overline{M}/M)$. Put $V = T \otimes_{\mathcal{O}} K$.

If $T \subset T' \subset V$ is an A-submodule of V with T'/T finite, then T' gives rise to an isogenous formal A- module $\underline{G}'$ over $\overline{M}$. If we let Γ be the finite A-module associated to T'/T in $V/T \cong \underline{G}(\overline{M})_{\mathrm{torsion}}$, then an explicit isogeny $f : \underline{G} \to \underline{G}'$ is given by Serre's formula [3, pg 298]:

$$f(x) = \prod_{\Gamma} \underline{G}(x,\gamma) \tag{5.1}$$

From this we can conclude that $\underline{G}'$ and f are both rational over the integers W' of the finite extension M' fixed by the subgroup of $\mathrm{Gal}(\overline{M}/M)$ stabilizing T' . Since each γ lies in the maximal ideal of $\overline{M}$, we have:

(5.2) $\underline{G}' \equiv \underline{G} \pmod{p'}$

where p' is a prime element of W' .

The endomorphism ring $\mathcal{O}' = \mathrm{End}_{W'}(\underline{G}')$ is the order of all $\alpha \in \mathcal{O}$ which stabilize the A-lattice T' . Since this contains A , there are two possibilities:

a) $\mathcal{O}' = \mathcal{O}$

b) $\mathcal{O}' = A + \pi^s \mathcal{O} = \mathcal{O}_s$ for some $s \geq 1$.

In the first case, $\underline{G}'$ is isomorphic to $\underline{G}$ and $W' = W$. In the second case we say that $\underline{G}'$ is a quasi-canonical lifting of level s of the pair (G,α) .

Proposition 5.3 1) Quasi-canonical liftings $\underline{G}'$ exist for all levels $s \geq 1$.

2) The liftings of level s are rational over the integers W' of the abelian extension M' of K with norm group $\mathcal{O}_s^*$ in K^* . They are permuted simply transitively under the action of the Galois group $\mathrm{Gal}(M'/M) \simeq (\mathcal{O}/\pi^s\mathcal{O})^*/(A/\pi^s A)^*$, which has order $q^{s-1}(q+1)$ if $\mathcal{O}$ is unramified over A and q^s if $\mathcal{O}$ is ramified over A .

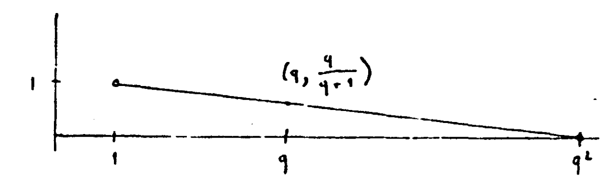
3) The formal modulus of the height 2 A-module $\underline{G}'$ has valuation 1 in W' . In particular, the A-modules $\underline{G}$ and $\underline{G}'$ are not isomorphic $\pmod{p'^2}$.

Proof: 1) To construct a lifting level s , write $T = \mathcal{O}t$ and take

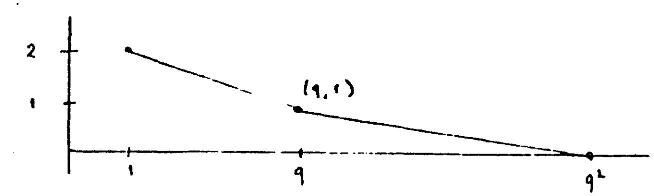
$T' = \pi^{-s}(\mathcal{O}_s \cdot t) = \pi^{-s}At + T$. Then $T'/T \simeq A/\pi^s A$ and clearly $\{\alpha \in \mathcal{O} : \alpha T' \subset T'\} = \mathcal{O}_s$.

2) The theory of Lubin-Tate [4] shows that M' is the ring class field with norm group $\mathcal{O}_s^*$. Since multiplication by $\mathcal{O}^*$ permutes the choices for T' transitively, the Galois group $(\mathcal{O}/\pi^s\mathcal{O})^*/(A/\pi^s A)^*$ permutes the different quasi-canonical liftings of level s simply transitively

3) The Newton polygon for $\pi_{\underline{G}}(x)$ looks like:



if $\mathcal{O}$ is unramified over A , and like:



if $\mathcal{O}$ is ramified over A . We may factor the cyclic isogeny f as a composition:

$$\underline{G} \xrightarrow[f_0]{} \underline{G}_1 \xrightarrow[f_1]{} \underline{G}_2 \rightarrow \cdots \rightarrow \underline{G}_s = \underline{G}'$$

where $\ker f_i \simeq A/\pi A$ is a non-canonical A-submodule of the π-torsion of G_i . By Lubin's theory [2], the Newton polygon for π_{G_i} has a break at the point $(q, \frac{1}{q^{i-1}(q+1)})$ if $\mathcal{O}$ is unramified over A , and at the point $(q, \frac{1}{q^i})$ if

$\mathcal{O}$ is ramified over A. Since the y-coordinate is the reciprocal of the degree $[W':W]$, the formal modulus of $\underline{G}'$ has p'-valuation one [5].

Since the formal modulus of the lifting $\underline{G}$ lies in pW, it has p'-valuation greater than or equal to $\deg[W':W] \geq 2$. Hence the groups $\underline{G}$ and $\underline{G}'$ are not isomorphic $(\bmod\ p'^2)$.

6. One can extend the results of the proceeding 3 sections to liftings of divisible A-modules of height 2, in the sense of Drinfeld [1,§4]. When $A = \mathbb{Z}_p$ this theory was developed for the p-divisible groups of ordinary elliptic curves by Serre and Tate [6]; we sketch the general theory here in the hope that it may clarify some of our terminology.

Over a separably closed field k the divisible A-modules of height 2 are either formal modules or isomorphic to $H \times (F/A)$, where H is the unique formal A-module of height 1 and (F/A) is the unique étale A-module of height 1. The canonical lifting $\underline{G} = \underline{H} \times (F/A)$ to W has $\mathrm{End}_W(\underline{G}) = \mathrm{End}_{W/pW}(\underline{G}) = \mathcal{O} = A \times A$.

By Serre-Tate [6], the other liftings of $G = H \times (F/A)$ to W are classified by elements in the A-module $\mathrm{Ext}^1(F/A,\underline{H}) = \underline{H}(W)$. The quasi-canonical liftings $\underline{G}'$ correspond to A-torsion points h in $\underline{H}(W)$. If h has order π^s the lifting $\underline{G}'$ of level s is rational over the abelian extension $W' = W[h]$ of degree $q^{s-1}(q-1)$. All of the quasi-canonical liftings of this level are permuted simply transitively by the Galois group and have endomorphism ring $\mathrm{End}_{W'}(\underline{G}') = \mathcal{O}_s = \{(a,b) \in A \times A : a \equiv b \pmod{\pi^s}\}$. Finally, $\underline{G}'$ is congruent to $\underline{G} \pmod{p'}$ but not $(\bmod\ p'^2)$; this follows from the fact that h is a uniformizing parameter in W'.

Bibliography

1. Drinfeld, V. G., Elliptic Modules, Math USSR Sbornik Vol 23 (1974), pg 561-592.

2. Lubin, J., Canonical subgroups of formal groups. Trans. AMS 251 (1979), pg 103-127.

3. Lubin, J., Finite subgroups and isogenies of one-parameter formal Lie groups. Annals Math. 85 (1967), pg 296-302.

4. Lubin, J. and Tate, J., Formal complex multiplication in local fields. Annals of Math. 81 (1965), pg 380-387.

5. Lubin, J. and Tate, J., Formal moduli for one-parameter formal Lie groups, Bull. Soc. math France 94 (1966), pg 49-60.

6. Lubin, J., Serre, J.-P., and Tate, J., Seminar at Woods Hole Institute on algebraic geometry, 1964.