Heegner Points on $X_0(N)$

Benedict H. Gross

In his work on the class-number problem for imaginary quadratic fields, Heegner [7] introduced a remarkable collection of points on certain modular curves. These points always form a subset of the singular moduli; on the curve $X_0(N)$ they correspond to the moduli of N-isogenous elliptic curves with the *same* ring of complex multiplication. Birch [1] was the first to recognize the significance of the divisor classes supported on these points in the arithmetic of the Jacobian $J_0(N)$. Using them, he was able to construct points of infinite order in certain elliptic quotients of $J_0(N)$ possessing a cuspidal group of even order [2]. Mazur [11] later found an interesting method to construct points of infinite order in Eisenstein quotients of $J_0(N)$, when N is prime.

In this paper, I would like to show how to obtain some of the above results via the theory of modular, elliptic, and circular units. This method will be exposed in Section II, after a review of the basic material on Heegner points in Section I. These theoretical results, although fragmentary, fit in nicely with the extensive computations which Birch and Stephens have made on this subject [3]. On the basis of this evidence, I was led to conjecture a simple identity relating the height of a Heegner divisor class to the first derivative at $s = 1$ of the L-series of an automorphic form on $\mathrm{PGL}(2) \times \mathrm{GL}(2)$. Zagier and I have obtained a proof of this identity in many cases: I will discuss this work briefly in Section III. In Section IV I will present a general program of work on other modular curves.

I would like to thank Joe Buhler for helping me with some computation of Heegner points, as well as John Tate for his constant support. Finally, I would like to dedicate this paper to Bryan Birch, whose work in this field has been a great source of inspiration to me.

I. HEEGNER POINTS AND DIVISORS

1. Let $N \geqslant 1$ be an integer, and let $Y = Y_0(N)$ be the open modular curve over $\mathbb{Q}$ which classifies ordered pairs (E, E') of elliptic curves together with a cyclic

isogeny $\phi: E \to E'$ of degree N. The complex points of Y have the structure of a Riemann surface, which is analytically isomorphic to the quotient space $\mathscr{H}/\Gamma_0(N)$. Here $\mathscr{H}$ is the upper half-plane and $\Gamma_0(N)$ is the subgroup of matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $\mathrm{SL}_2(\mathbb{Z})$ with $c \equiv 0 \pmod N$. The isomorphism between $Y(\mathbb{C})$ and $\mathscr{H}/\Gamma_0(N)$ is affected as follows.

To each point $y = (E, E')$ in $Y(\mathbb{C})$ we associate a pair of N-isogenous tori $\phi: \mathbb{C}/M \to \mathbb{C}/M'$. Changing M by a homothety, we may assume $M \subset M'$ and the isogeny ϕ is given by the identity map on the covering spaces. Since M'/M is cyclic of order N, there is an oriented basis $\langle \omega_1, \omega_2 \rangle$ of M such that $M' = \langle \omega_1, \omega_2/N \rangle$ and $\tau = \omega_1/\omega_2$ is in $\mathscr{H}$. The $\Gamma_0(N)$-orbit of τ is well determined by the point y. To see that the map is surjective, to each orbit τ in $\mathscr{H}/\Gamma_0(N)$ we associate the lattices $M = \langle \tau, 1 \rangle$ and $M' = \langle \tau, 1/N \rangle$. The tori $E(\mathbb{C}) = \mathbb{C}/M$ and $E'(\mathbb{C}) = \mathbb{C}/M'$ are then related by the obvious cyclic N-isogeny.

Let $X = X_0(N)$ be the natural compactification of Y; this is the modular curve which classifies N-isogenous generalized elliptic curves. The complex points $X(\mathbb{C})$ may be identified with the quotient $\mathscr{H}^*/\Gamma_0(N)$, where $\mathscr{H}^* = \mathscr{H} \cup \mathbb{P}^1(\mathbb{Q})$. The finite set $\mathbb{P}^1(\mathbb{Q})/\Gamma_0(N) = X(\mathbb{C}) - Y(\mathbb{C})$ consists of the 'cusps' of X.

2. The Heegner points of $Y(\mathbb{C}) \subset X(\mathbb{C})$, as defined by Birch [2], correspond to pairs (E, E') of N-isogenous curves with the *same* ring $\mathcal{O}$ of complex multiplications. The ring $\mathcal{O} = \operatorname{End} E = \operatorname{End} E'$ is an order in an imaginary quadratic field K, and our first task will be to determine which orders can occur.

Orders in quadratic fields are somewhat special, as they are completely determined by their discriminants. The discriminant D of $\mathcal{O}$ has the form $D = d \cdot c^2$, where d is the discriminant of K and c is the conductor of $\mathcal{O}$ (its index in the ring of integers $\mathcal{O}_K$ of K). The integer c^2 is the largest square factor of D such that $D/c^2 \equiv 0, 1 \pmod 4$.

If $y = (E, E')$ is a complex Heegner point with endomorphism ring $\mathcal{O}$, then the associated lattices M and M' are both projective $\mathcal{O}$-modules of rank 1. Modifying by a homothety, we may assume that $M = \mathfrak{a}$ and $M' = \mathfrak{b}$ are both invertible $\mathcal{O}$-submodules of K with $\mathfrak{a} \subset \mathfrak{b}$. The module $\mathfrak{n} = \mathfrak{a}\mathfrak{b}^{-1}$ is then a proper (= invertible) $\mathcal{O}$-ideal with quotient $\mathcal{O}/\mathfrak{n}$ cyclic of order N. Such an ideal will exist if and only if there is a primitive binary quadratic form of discriminant D which properly represents N, or equivalently – if and only if the equation $D = B^2 - 4NC$ can be solved in integers with $\gcd(N, B, C) = 1$.

If such ideals $\mathfrak{n}$ exist in $\mathcal{O}$, we can construct Heegner points with $\mathcal{O} = \operatorname{End} E = \operatorname{End} E'$ as follows. Let $\mathfrak{a}$ be an invertible $\mathcal{O}$-submodule of K, and let $[\mathfrak{a}]$ denote the class of $\mathfrak{a}$ in the group $\operatorname{Pic}(\mathcal{O})$. Let $\mathfrak{n}$ be a proper $\mathcal{O}$-ideal with cyclic quotient of order N, and put $E(\mathbb{C}) = \mathbb{C}/\mathfrak{a}$, $E'(\mathbb{C}) = \mathbb{C}/\mathfrak{a}\mathfrak{n}^{-1}$. These curves are related by the obvious isogeny, with kernel isomorphic to

$\mathfrak{a}\mathfrak{n}^{-1}/\mathfrak{a} \simeq \mathfrak{a}/\mathfrak{a}\mathfrak{n} \simeq \mathbb{Z}/N$, so determine a point $y=(E,E')$ in $Y(\mathbb{C})$. We describe this point by the data $y=(\mathcal{O},\mathfrak{n},[\mathfrak{a}])$, as the curves E and E' depend only on the class of $\mathfrak{a}$ in $\mathrm{Pic}(\mathcal{O})$. By our previous remarks, all Heegner points in $Y(\mathbb{C})$ can be described in this manner.

To find the image of $y=(\mathcal{O},\mathfrak{n},[\mathfrak{a}])$ in $\mathscr{H}$, choose an oriented basis $\langle\omega_1,\omega_2\rangle$ of $\mathfrak{a}$ such that $\mathfrak{a}\mathfrak{n}^{-1}=\langle\omega_1,\omega_2/N\rangle$. Then y corresponds to the orbit of $\tau=\omega_1/\omega_2$ in $\mathscr{H}/\Gamma_0(N)$. Since τ is in K, it satisfies a quadratic equation $A\tau^2+B\tau+C=0$ over $\mathbb{Z}$ with $\gcd(A,B,C)=1$. It is easy to check that $D=B^2-4AC$, $A=NA'$, and $\gcd(A',B,NC)=1$.

3. We define the conductor of the Heegner point $y=(\mathcal{O},\mathfrak{n},[\mathfrak{a}])$ to be the integer $c=[\mathcal{O}:\mathcal{O}_K]$. Henceforth in this paper, we shall restrict our attention to Heegner points of *conductor c prime to N*. This condition, which is fairly natural from the point of view of L-series (§20), is automatic whenever N is square-free.

With this assumption on the conductor, the invertible ideal $N\mathcal{O}$ has a factorization which mirrors the factorization of (N) in K. An invertible ideal $\mathfrak{n}\subseteq\mathcal{O}$ with cyclic quotient of order N will exist if and only if every prime p dividing N in split or ramified in K, and every prime p with p^2 dividing N is split in K.

Thus, every prime p which divides $\gcd(D,N)$ is relatively prime to c, ramifies in K, and *exactly* divides N (which we write $p\,\|\,N$). If $p\neq 2$, then $p\,\|\,d$ also.

4. The Heegner points of conductor c for K are stable under the action of $\mathrm{Aut}(\mathbb{C})$ on $X(\mathbb{C})$. This group is the semi-direct product of its normal subgroup $\mathrm{Aut}_K(\mathbb{C})$ with the group $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C})$ of order 2 generated by complex conjugation τ. Since τ is a continuous automorphism of $\mathbb{C}$ we have the formula

$$(\mathcal{O},\mathfrak{n},[\mathfrak{a}])^{\tau}=(\mathcal{O},\mathfrak{n}^{\tau},[\mathfrak{a}^{\tau}]). \tag{4.1}$$

We remark that $[\mathfrak{a}^{\tau}]=[\mathfrak{a}]^{-1}$ in $\mathrm{Pic}(\mathcal{O})$.

The action of the non-continuous automorphisms σ of $\mathrm{Aut}_K(\mathbb{C})$ lies somewhat deeper, although one clearly has the formula $(\mathcal{O},\mathfrak{n},[\mathfrak{a}])^{\sigma}=(\mathcal{O},\mathfrak{n},[\mathfrak{a}'])$ for some $[\mathfrak{a}']$ in $\mathrm{Pic}(\mathcal{O})$ – depending on both $[\mathfrak{a}]$ and σ. The exact formula for $[\mathfrak{a}']$ is given by the theory of complex multiplication. This asserts that the points of level c are all rational over the subfield $H=K(j(\mathcal{O}))$ of $\mathbb{C}$; this is an abelian extension of K – the ring class-field of conductor c – with Galois group $G=\mathrm{Gal}(H/K)$ canonically isomorphic to $\mathrm{Pic}(\mathcal{O})$ by class-field theory. If $\mathfrak{b}$ is an ideal of $\mathcal{O}$ not dividing c, and $\sigma[\mathfrak{b}]$ denotes the Artin symbol of $[\mathfrak{b}]$ in G, we have the formula [13]

$$(\mathcal{O},\mathfrak{n},[\mathfrak{a}])^{\sigma(\mathfrak{b})}=(\mathcal{O},\mathfrak{n},[\mathfrak{a}\mathfrak{b}^{-1}]). \tag{4.2}$$

Finally, we remark that H is a normal extension of $\mathbb{Q}$, with Galois group a generalized dihedral group. Its irreducible representations over $\mathbb{C}$ have degree 1 or 2.

5. The Heegner points of conductor c for K are also stable under the action of the Atkin–Lehner involutions w_p of X, for those primes p dividing N. Write $N = p^k m$ with $(m, p) = 1$. If $\mathfrak{p}$ is the unique factor of p in $\mathcal{O}$ which divides the ideal $\mathfrak{n}$, we have a similar factorization $\mathfrak{n} = \mathfrak{p}^k \cdot \mathfrak{m}$ with $(\mathfrak{m}, p) = 1$.

Let $\mathfrak{n}'$ be the ideal $(\mathfrak{p}^\tau)^k . \mathfrak{m}$ of $\mathcal{O}$; this is invertible with cyclic quotient of order N, and we have the formula

$$w_p(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}]) = (\mathcal{O}, \mathfrak{n}', [\mathfrak{a}\mathfrak{p}^{-k}]). \tag{5.1}$$

In particular, the canonical involution $w_N = \prod_{p|N} w_p$ of X acts on Heegner points via the formula

$$w_N(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}]) = (\mathcal{O}, \mathfrak{n}^\tau, [\mathfrak{a}\mathfrak{n}^{-1}]). \tag{5.2}$$

6. The Hecke correspondences T_l of X, for those primes l not dividing N, also stabilize the divisors supported on the Heegner points of K with conductor prime to N. We have the formula

$$T_l(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}]) = \sum_{\mathfrak{a}/\mathfrak{b} = \mathbb{Z}/l} (\mathcal{O}_\mathfrak{b}, \mathfrak{n}_\mathfrak{b}, [\mathfrak{b}]), \tag{6.1}$$

where the sum is taken over the $(l+1)$ sub-lattices $\mathfrak{b}$ of index l in $\mathfrak{a}$, $\mathcal{O}_\mathfrak{b} = \mathrm{End}(\mathfrak{b})$ and $\mathfrak{n}_\mathfrak{b} = \mathfrak{n}, \mathcal{O}_\mathfrak{b} \cap \mathcal{O}_\mathfrak{b}$.

7. Let $J = J_0(N)$ be the Jacobian of X over $\mathbb{Q}$. This is an abelian variety of dimension $g = \text{genus}(X)$; over the number field H its group of points $J(H)$ is finitely generated, by the Mordell–Weil theorem.

The points of J in H can be described as follows. Let Div denote the group of divisors on X which are rational over H, and let P denote the subgroup of principal divisors – those of the form $\mathrm{Div}(f)$, where f is a non-zero function on X over H. Then P is actually a subgroup of D_0, the divisors of degree zero, and we have an isomorphism of $G = \mathrm{Gal}(H/K)$-modules: $J(H) \simeq D_0/P$.

Let $\chi: G \to \mathbb{C}^*$ be a complex character of the Galois group, and let $R = \mathbb{Z}[\chi]$ be the cyclotomic ring generated by its values. If M is a $\mathbb{Z}[G]$-module, we define

$$M^\chi = \{m \in M \otimes R : m^\sigma = \chi(\sigma).m \text{ for all } \sigma \in G\};$$

this eigenspace is a sub R-module of $M \otimes R$. The sequence of R-modules

$$0 \to P^\chi \to D_0^\chi \xrightarrow[\alpha]{} J(H)^\chi \tag{7.1}$$

is then exact, and coker α is a finite R-module annihilated by the order of χ.

8. We now use Heegner points to define classes in $J(H)^\chi$. Let $x = (\mathcal{O}, \mathfrak{n}, [\mathfrak{a}])$ be a point rational over H, and let x_0 denote the cusp ∞ on $X_0(N)$ – which is rational over $\mathbb{Q}$. The divisor $y = (x) - (x_0)$ has degree zero over H; if $\chi: G \to \mathbb{C}^*$ is a ring class character we define

$$y_\chi = \sum_G \bar{\chi}(\sigma) y^\sigma \quad \text{in} \quad D_0^\chi. \tag{8.1}$$

We will also use the symbol y_χ for the image of this divisor in $J(H)^\chi$. By (4.2) we have the identity

$$y_\chi = \sum_{\operatorname{Pic}\mathcal{O}} \chi(\mathfrak{b})(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}\mathfrak{b}]) - \sum_{\operatorname{Pic}\mathcal{O}} \chi(\mathfrak{b}).(x_0), \tag{8.2}$$

so this divisor is supported on the Heegner points and the cusp ∞; it is entirely supported on the Heegner points when $\chi \neq 1$.

9. Let $W = H^0(X(\mathbb{C}), \Omega^1)$ denote the complex cotangent space of X, which may be identified with the vector space of holomorphic cusp forms of weight 2 for $\Gamma_0(N)$. Since W is a sub-space of $H^1(X, \mathbb{C})$, cup-product gives a Hermitian pairing:

$$(\omega_1, \omega_2) = \int_{X(\mathbb{C})} \omega_1 \wedge \overline{i\omega_2}. \tag{9.1}$$

By Hodge theory, this is positive definite.

Let $\mathbb{T}$ be the commutative sub-algebra of $\operatorname{End}_{\mathbb{Q}}(J)$ generated over $\mathbb{Z}$ by the Hecke correspondences T_l, for l prime to N, and by the involutions w_p, for p dividing N. Since W may also be identified with the cotangent space of J, the algebra $\mathbb{T}$ acts as linear endomorphisms of W. This action is *faithful* and self-adjoint with respect to the above inner product. We thus obtain a spectral decomposition

$$W = \bigoplus_f W^f \tag{9.2}$$

where $f: \mathbb{T} \to \mathbb{R}$ ranges over all characters of $\mathbb{T}$ and W^f is the corresponding eigenspace.

An important subset of the characters occurring is given by the newforms of level N. In this case W^f is one-dimensional, with normalized basis the differential $\omega_f = 2\pi i f(z)dz = q^{-1}f(q)dq$. Here $f = \sum_{n \geq 1} a_n q^n$ is a newform, with normalization $a_1 = 1$. The corresponding character of $\mathbb{T}$ is given by $f(T_l) = a_l$ for $(l, N) = 1$ and $f(w_p) = -a_p$ for $p \| N$.

10. Let $V = J(H) \otimes \mathbb{C}$; this finite-dimensional complex vector space also has a Hermitian inner product, which is given by the formula

$$\langle e_1 \otimes z_1, e_2 \otimes z_2 \rangle = z_1 \bar{z}_2 . \langle e_1, e_2 \rangle_J. \tag{10.1}$$

Here e_1 and e_2 are elements of $J(H)$, and $\langle\,,\rangle_J$ is the normalized height pairing on the Mordell–Weil group.

The algebra $\mathbb{T} \subset \mathrm{End}_{\mathbb{Q}}(J)$ acts as linear endomorphisms on V, and this action is self-adjoint with respect to the above inner product. Since the endomorphisms in $\mathbb{T}$ are defined over $\mathbb{Q}$, they commute with the action of G on V, and we obtain a spectral decomposition for each eigenspace:

$$V^\chi = \bigoplus_f V^{\chi,f}. \tag{10.2}$$

We let $v_{\chi,f}$ denote the projection of y_χ into the subspace $V^{\chi,f}$.

Henceforth in this paper, we will only consider the elements y_χ when χ is a *primitive* character of G (i.e. the conductor of χ is equal to c). We will only consider the elements $v_{\chi,f}$ when χ is primitive and f is a *newform* of level N.

11. When $\gcd(N,D) \neq 1$, there are certain cases where the element $v_{\chi,f}$ is forced to be equal to zero. We want to identify these cases here, and exclude them from what follows.

Suppose p divides $\gcd(N,D)$. Since $(N,c)=1$ we must have $p|d$, and so p is ramified in K. Write $p\mathcal{O} = \mathfrak{p}^2$; the value $b_p = \chi([\mathfrak{p}])$ is then equal to ± 1.

Since p is ramified in K, p exactly divides N. Hence $w_p|f = -a_p \cdot f$ with $a_p = \pm 1$.

Lemma 11.1 *If $a_p = b_p$ then $v_{\chi,f} = 0$.*

Proof Put $v = v_{\chi,f}$; since v lies in V^f we have $w_p(v) = -a_p v$. But formula (5.1) shows that we also have the formula $w_p(v) = b_p v$. If $a_p = b_p$ this implies that $v = -v$, hence $v = 0$.

Henceforth we will only consider the elements $v_{\chi,f}$ if for every prime p dividing $\gcd(N,D)$ we have $a_p b_p = -1$. With these restrictions, we present our first conjecture – which was motivated by some computations of Birch and Stephens [3].

Conjecture 11.2 *The element $v_{\chi,f}$ is non-zero in $V^{\chi,f}$ if and only if* $\dim V^{\chi,f} = 1$.

We note that if α is any automorphism of $\mathbb{C}$, we have $\dim V^{\chi,f} = \dim V^{\chi^\alpha,f^\alpha}$ and $v_{\chi,f} \neq 0$ if and only if $v_{\chi^\alpha,f^\alpha} \neq 0$. Therefore this conjecture is compatible with the action of $\mathrm{Aut}(\mathbb{C})$ on pairs (χ,f).

II. HEEGNER DIVISORS AND MODULAR UNITS

12. In this Section, we will study the classes y_χ in $J(H)^\chi$, when the ring class character χ satisfies $\chi = \chi^{-1}$. These are precisely the ring class characters which arise from the restriction of characters of $\mathbb{Q}$. We let L denote the fixed field of $\ker \chi \subset G$ on H. If $\chi = 1$, then $L = K$; if χ is quadratic, the field L is a biquadratic extension of $\mathbb{Q}$. In all cases, y_χ lies in the subgroup $J(L)^\chi$ of $J(L)$; we will see that it frequently has infinite order in the Jacobian.

The quadratic ring class characters of K of conductor c correspond bijectively to factorings of $D = d_K c^2$ into the product of two quadratic discriminants:

$$D = d.d' \quad \text{with} \quad d > 0. \tag{12.1}$$

If k and k' are the associated quadratic fields, with discriminants d and d' and Dirchlet characters ψ and ψ', we have

$$L = Kk = Kk', \qquad \chi = \operatorname{Res}\psi = \operatorname{Res}\psi'.$$

Since $d > 0$, the field k is real and k' is imaginary. We let h and h' denote the class-numbers of these fields, w' denote the order of the unit group of k', and $0 < u < 1$ be a fundamental unit for k when $d > 1$.

13. We begin with the case where N is prime. Let $m = \gcd(N-1, 12)$ and put $n = (N-1)/m$. The function $f(z) = \{\Delta(z)/\Delta(Nz)\}^{1/m}$ is a modular unit in the rational function field of $X = X_0(N)$. Its divisor is given by $\operatorname{div}(f) = n\{(0) - (\infty)\}$.

Let F be a subfield of $\mathbb{C}$, and let D_0' denote the divisors of degree 0 on X over F, relatively prime to the cusps (0) and (∞). Define the homomorphism

$$\delta : D_0' \to F^* \tag{13.1}$$

by the formula

$$\delta(\textstyle\sum a_i(x_i)) = \prod f(x_i)^{a_i}.$$

On principal divisors we find $\delta((g)) = g((f)) = (g(0)/g(\infty))^n$ by reciprocity. Hence δ induces a homomorphism

$$\delta : J(F) \to F^*/F^{*n} = F^* \otimes \mathbb{Z}/n\mathbb{Z}, \tag{13.2}$$

which commutes with the action of $\operatorname{Aut}(F)$.

Recall that $\mathbb{T}$ is the commutative sub-algebra of $\operatorname{End}_{\mathbb{Q}}(J)$ generated by the Hecke operators T_l for $l \neq N$ and the involution w_N. Let I denote the Eisenstein ideal of $\mathbb{T}$ [10]; this may be defined as the annihilator of the divisor class (0)–(∞), or equivalently, as the ideal generated by $T_l - l - 1$ for $l \neq N$ and $1 + w_N$. The quotient $\mathbb{T}/I$ is isomorphic to $\mathbb{Z}/n\mathbb{Z}$; with this identification it is easy to check that the map δ in (13.2) is a homomorphism of Hecke modules. In particular, δ is trivial on the subgroup $IJ(F)$.

Let p be a prime divisor of n, and let $\mathfrak{P} = (p, I)$ denote the corresponding Eisenstein prime of $\mathbb{T}$. Let $\mathbb{T}_{\mathfrak{P}}$ denote the completion of $\mathbb{T}$ at $\mathfrak{P}$, and let $J^{(p)}$ denote the pth-Eisenstein factor of $J = J_0(N)$ over $\mathbb{Q}$. The map δ induces a homomorphism

$$\delta_p : J(F) \otimes_{\mathbb{T}} \mathbb{T}_{\mathfrak{P}}/I\mathbb{T}_{\mathfrak{P}} \to F^* \otimes \mathbb{Z}_p/n\mathbb{Z}_p, \tag{13.3}$$

and the following result will be useful in the study of the Heegner divisors.

Lemma 13.4 *Assume that e is a point of $J(F)$ with $\delta_p(e) \neq 0$. Then $e \neq 0$ in $J(F) \otimes_{\mathbb{T}} \mathbb{T}_{\mathfrak{P}}$. If e is not $\mathfrak{P}$-primary torsion, its projection $e^{(p)}$ to $J^{(p)}(F)$ has infinite order.*

Proof The first statement is clear. Let $k_{\mathfrak{P}} = \mathbb{T}_{\mathfrak{P}} \otimes \mathbb{Q}_p$; this is a product of local fields, and projection induces an isomorphism: $J(F) \otimes_{\mathbb{T}} k_{\mathfrak{P}} \simeq J^{(p)}(F) \otimes_{\mathbb{T}} k_{\mathfrak{P}}$. If e is not $\mathfrak{P}$-primary torsion, then $e \otimes 1 \neq 0$ in $J(F) \otimes_{\mathbb{T}} k_{\mathfrak{P}}$, so its projection has infinite order on $J^{(p)}$.

14. We now treat the case $\chi = 1$, for which there is some precedent [11]. Let K be an imaginary quadratic field in which the prime $(N) = \mathfrak{n} \cdot \mathfrak{n}^{\tau}$ is split. Let $x = (\mathcal{O}_K, \mathfrak{n}, [\mathcal{O}_K])$ and let y_χ denote the class of the divisor $\sum_G x^{\sigma} - h \cdot (\infty)$ in $J(K)$.

This divisor class has some cuspidal support, which makes it awkward to study using the map δ. To avoid this minor nuisance, we let

$$e = y_\chi - y_\chi^{\tau} = \left(\sum_G x^{\sigma} - \sum_G x^{\sigma\tau} \right).$$

This lies in the minus space for the action of complex conjugation on $J(K)$; on $J^{(p)}(K)$ we find the identity $e^{(p)} = 2y_\chi^{(p)}$ using (5.2).

Let $A = \mathcal{O}_K[N^{-1}]$ and let h_A denote the order of $\mathrm{Pic}(A)$. Then $h_K = h_A \cdot O(\mathfrak{n})$, where $O(\mathfrak{n})$ is the order of $[\mathfrak{n}]$ in $\mathrm{Pic}(\mathcal{O}_K)$.

Proposition 14.1 *Assume that p is odd and $(p, w_K) = 1$. Then $\delta_p(e) \neq 0$ if and only if $\mathrm{ord}_p(h_A) < \mathrm{ord}_p(n)$. In this case, $y_\chi^{(p)}$ has infinite order in $J^{(p)}(K)$.*

Proof From the definition of δ, we find that

$$\delta_p(e) \equiv \left\{ \prod_{\mathrm{Pic}(\mathcal{O})} \frac{\Delta(\mathfrak{a})}{\Delta(\mathfrak{n}\mathfrak{a})} \cdot \frac{\Delta(\mathfrak{n}^{\tau}\mathfrak{a}^{\tau})}{\Delta(\mathfrak{a}^{\tau})} \right\}^{1/m} \qquad (\mathrm{mod}\ K^{*n}).$$

It is well known that $\Delta(\mathfrak{a})/\Delta(\mathfrak{n}\mathfrak{a})$ is an integer of H which generates the ideal $\mathfrak{n}^{12}$ of K. Hence $\delta_p(e)$ is congruent to an element of K^* which generates the ideal $(\mathfrak{n}/\mathfrak{n}^{\tau})^{12h_K/m}$ and is in the minus space for complex conjugation. Thus $\delta_p(e) \equiv \zeta \cdot \alpha^{12h_A/m}$, where ζ is a root of unity in K^* and α is a generator of the principal ideal $(\mathfrak{n}/\mathfrak{n}^{\tau})^{O(\mathfrak{n})}$. Since $[\mathfrak{n}^{\tau}] = [\mathfrak{n}]^{-1}$ and $p \neq 2$, α is *not* a pth-power in K^*.

If $p>3$, then ζ is a pth-power, so that $\delta_p(e)$ is a p^k-power if and only if $h_A \equiv 0 \pmod{p^k}$. If $p=3$ divides n, then $3\,\|\, m$ and $\mathrm{ord}_3(12h_A/m)=\mathrm{ord}_3(h_A)$. Since ζ is a cube by the assumption $(3, w_K)=1$, we see that the same argument applies. Hence $\delta_p(e)\neq 0$ if and only if $\mathrm{ord}_p(h_A)<\mathrm{ord}_p(n)$.

Finally we must show that e is not $\mathfrak{P}$-primary torsion. If it were, we could find a non-trivial element $p^k e$ in $J(K)_{\mathfrak{P}}^{\varepsilon=-1}$. This is impossible by Mazur's determination of the group scheme $J_{\mathfrak{P}}=\mathbb{Z}/p\oplus\mu_p$ [10].

15. We now turn to the case where χ is quadratic, retaining the assumption that N is prime. Let K be an imaginary quadratic field in which N has a factor of degree 1, let χ be a quadratic ring class character of K of conductor c, let $\mathcal{O}$ be the order of index c in $\mathcal{O}_K$ and $\mathfrak{n}$ an ideal of $\mathcal{O}$ with $\mathcal{O}/\mathfrak{n}\simeq\mathbb{Z}/N$. We further assume that $\chi([\mathfrak{n}])=-1$.

Recall that χ corresponds to a pair (k,k') of quadratic fields and has class-field $L=Kk=Kk'$. Let y_χ denote the Heegner class in $J(L)^\chi$.

Proposition 15.1 *Assume that p is odd. Then $\delta_p(y_\chi)\neq 0$ if and only if $\mathrm{ord}_p(hh')<\mathrm{ord}_p(n)$. In this case, $y_\chi^{(p)}$ has infinite order in $J^{(p)}(L)^\chi$.*

Proof In this case, we have $\delta_p(y_\chi)\equiv E_\chi \pmod{L^{*n}}$, where E_χ is the elliptic unit

$$E_\chi=\left\{\prod_{\mathrm{Pic}(\mathcal{O})}\left(\frac{\Delta(\mathfrak{a})}{\Delta(\mathfrak{n}\mathfrak{a})}\right)^{\chi(\mathfrak{a})}\right\}^{1/m}. \tag{15.1}$$

Since $\chi(\mathfrak{n})=-1$, Kronecker's first limit formula yields [14]

$$\log|E_\chi|=\frac{-24}{m}L'(\chi,0), \tag{15.2}$$

where $L(\chi,s)$ is the abelian L-function of the character χ.

This L-function factors as a product $L(\chi,s)=L(\psi,s)L(\psi',s)$, and we have the formulae

$$L'(\psi,0)=-h\log u,\qquad L(\psi',0)=2h'/w'. \tag{15.3}$$

Combining (15.2) and (15.3) gives the relation $\log|E_\chi|=(48hh'/mw')\log u$.

But E_χ and u are both units in L^*, where the rank of the unit group is 1. Hence $E_\chi=\zeta\cdot u^{48hh'/mw'}$, where ζ is a root of unity in $(L^*)^\chi$. Since L is biquadratic, $\zeta^{24}=1$. Also u is *not* a pth-power in L^* for any odd prime p.

If $p>3$, ζ is a pth-power and $\delta_p(e)$ is a p^k-power if and only if $hh'\equiv$

$0 \pmod{p^k}$). If $p=3$ divides N then $3 \| m$ and $N \equiv 1 \pmod 9$. Since N is inert or ramified in k' – by the hypothesis $\chi(n) = -1$ – we have $(3, w') = 1$. Thus ζ is a cube and $\mathrm{ord}_3(48hh'/mw') = \mathrm{ord}_3(hh')$. The argument then proceeds as above.

Again, there is no $\mathfrak{P}$-torsion in $J(L)^\chi$ by Mazur's result: $J_{\mathfrak{P}} \simeq \mathbb{Z}/p \oplus \mu_p$. This, combined with Lemma 13.4, completes the proof.

16. Let us restate the results of the last two sections in a common way, which will generalize to composite N. The integer n is the order of the cuspidal group C of $J_0(N)$. The integers h_A and hh' are, up to powers of 2, the orders of the eigenspaces D^χ, where D is the class group of the Dedekind domain $\mathcal{O}_L[N^{-1}]$. Both C and D^χ are finite $\mathbb{Z}_p$-modules, and we have shown that for odd primes p

$$\delta_p(y_\chi) \neq 0 \quad \text{if and only if} \quad \mathrm{length}_{\mathbb{Z}_p} D^\chi < \mathrm{length}_{\mathbb{Z}_p} C. \tag{16.1}$$

We note that certain parts of the proof can also be made to work for $p=2$. If 2 divides n then $m \equiv 4 \pmod 8$ and $N \equiv 1 \pmod 8$. Since N is ramified or inert in k' when $\chi \neq 1$, $w' \equiv 2 \pmod 4$. Hence

$$\mathrm{ord}_2(12h_A/m) = \mathrm{ord}_2(h_A), \qquad \mathrm{ord}_2(48hh'/mw') = \mathrm{ord}_2(2hh').$$

In particular, $\delta_2(e) \neq 0$ whenever $\mathrm{ord}_2(2h_A) < \mathrm{ord}_2(n)$, and $\delta_2(y_\chi) \neq 0$ for $\chi \neq 1$ whenever $\mathrm{ord}_2(4hh') < \mathrm{ord}_2(n)$. If we know that u is not a square in L^*, the last condition may be relaxed to $\mathrm{ord}_2(2hh') < \mathrm{ord}_2(n)$. The first condition can also be improved, if we work with the original divisor y_χ and not the modified class e.

The above results can be combined with a first p-descent on $J^{(p)}$ to give evidence for conjecture (11.2) We will treat this in greater detail elsewhere; here we merely state the result.

Proposition 16.2 *Let p be an odd prime with $p \| n$, and assume that $D_p^\chi = 0$. Then the rank of $J^{(p)}(L)^\chi$ is equal to the dimension of $J^{(p)}$. Furthermore $Ш(J^{(p)}/L)_{\mathfrak{P}}^\chi = 0$ and the point $y_\chi^{(p)}$ is not divisible by $\mathfrak{P}$ in $J^{(p)}(L)^\chi$.*

For a discussion of this descent in the first non-trivial case, where $N = 11$ and $p = 5$, see [5].

17. We now treat the case where $N = m^2$, with $m > 1$. The method is similar, but the cuspidal group of $X_0(N)$ is no longer rational over $\mathbb{Q}$, and we have an Eisenstein series and an Eisenstein ideal for each Galois eigenspace. We will only study the primitive components; this explains our restriction to $N = m^2$ or N a prime. We shall also restrict our attention in this section to primes $p > 3$; the primes $p = 2, 3$ can be similarly treated, but this requires more care.

We let R denote the ring of integers in an unramified extension of $\mathbb{Q}_p$, and $\alpha : (\mathbb{Z}/m)^* \to R^*$ be a primitive Dirichlet character. Let M denote the cyclic extension of $\mathbb{Q}$ corresponding to α by class field theory. The degree of M is then prime to p; if A is an abelian group on which $\mathrm{Gal}(M/\mathbb{Q})$ acts, we will write $A(\alpha)$ for the eigenspace $(A \otimes R)^{\alpha}$.

Let a and b be integers relatively prime to m, and define the Siegel unit $\phi(a/m, b/m, z)$ as in Stark [14]. This is a modular function in the function field of $X(12N)$ over $\mathbb{Q}(\mu_m)$. The product

$$f(z) = \prod_{a=1}^{m} \prod_{b=1}^{m} \phi(a/m, b/m, mz)^{12\alpha^{-1}(ab)}, \tag{17.1}$$

then lies in $\mathscr{F}(\alpha)$, where $\mathscr{F}$ is the function field of $X = X_0(N)$ over M, *provided that* $\alpha \neq \omega$ the Teichmuller character. We will assume this in all that follows.

The divisor of f is supported at the cusps $[c/m]$ of X with $(c, m) = 1$. In fact, one has the formula

$$\mathrm{div}(f) = n \cdot \sum_{c=1}^{m} \alpha^{-1}(c)[c/m] \tag{17.2}$$

with

$$n = m \sum_{a=1}^{m} \sum_{b=1}^{m} \alpha^{-1}(ab) \mathbb{B}_2\left(\frac{a+b}{m}\right) \quad \text{in} \quad R - 0.$$

The cuspidal group $C(\alpha)$ in $J(M)(\alpha)$ is isomorphic to the cyclic R-module R/nR; we will assume $n \equiv 0 \pmod{p}$, so that $C(\alpha)$ is non-trivial. For a determination of the p-adic valuation of n, we refer readers to a forthcoming paper by G. Stevens.

Let D_0' denote the divisors of degree 0 on X over the field F which are relatively prime to $\mathrm{div}(f)$. Define a homomorphism $\delta: D_0' \to (FM)^*(\alpha)$ by the formula $\delta(\sum a_i(x_i)) = \prod f(x_i)^{a_i}$. By arguments similar to those in §13, this induces a homomorphism of points in the Jacobian

$$\delta: J(F) \to (FM)^* \otimes R/nR(\alpha). \tag{17.3}$$

Let $I = I(\alpha)$ be the ideal of $\mathbb{T} \otimes R$ which annihilates the class of the divisor $\sum_{c=1}^{m} \alpha^{-1}(c)[c/m]$ in $J(M) \otimes R$. This ideal contains the elements $T_l - l/\alpha(l) - \alpha(l)$ for $(l, m) = 1$ and $w_N - \alpha(-1)$, and has quotient $\mathbb{T} \otimes R/I \simeq C(\alpha) \simeq R/nR$. Let $\mathfrak{P} = (p, I)$ be the corresponding Eisenstein prime, and let $\mathbb{T}_{\mathfrak{P}}$ be the completion of $\mathbb{T} \otimes R$ at $\mathfrak{P}$. Then δ induces a homomorphism of $\mathbb{T}_{\mathfrak{P}}$-modules:

$$\delta_p: J(F) \otimes_{\mathbb{T}} \mathbb{T}_{\mathfrak{P}}/I\mathbb{T}_{\mathfrak{P}} \to (FM)^* \otimes R/nR(\alpha). \tag{17.4}$$

18. Let K be an imaginary quadratic field in which all primes dividing m are split and let $\chi = \chi^{-1}$ be a ring class character of K of conductor c prime to m. Then χ corresponds to a pair (ψ, ψ') of Dirichlet characters; we order these so that $\alpha\psi$ is even.

The class field L of χ is abelian over $\mathbb{Q}$ and disjoint from M. Let $N = LM$, and let D and U denote the class group and unit group of the abelian field N:

$$\begin{tikzcd}
 & N \arrow[dl, dash] \arrow[dr, dash] & \\
L \arrow[d, dash, "(\psi,\psi')\sim\chi"'] & & M \arrow[ddl, dash, "\alpha"] \\
K \arrow[dr, dash] & & \\
 & \mathbb{Q} &
\end{tikzcd}$$

Let $\mathcal{O}$ be the order of K of conductor c, and let $\mathfrak{n}$ be an ideal with $\mathfrak{n}\cdot\mathfrak{n}^\tau = N$ and $(\mathfrak{n}, \mathfrak{n}^\tau) = 1$. Let y_χ be the corresponding Heegner divisor in $J(L)^\chi$, so $\delta_p(y_\chi)$ lies in the eigenspace $N^* \otimes R/nR\,(\chi\alpha)$.

Proposition 18.1 $\delta_p(y_\chi) \neq 0$ *if and only if* $\mathrm{length}_R D(\chi\alpha) < \mathrm{ord}_p(n) = \mathrm{length}_R C(\alpha)$.

Proof By Kronecker's second limit formula [14], we have the relation $\log|\delta(y_\chi)| = \pm 24 L'(\overline{\chi\alpha}, 0)$. This abelian L-series factors as the product $L(\overline{\chi\alpha}, s) = L(\overline{\psi'\alpha}, s)L(\overline{\psi'\alpha}, s)$, and we have

$$L'(\overline{\psi\alpha}, 0) = -\tfrac{1}{2}\log|c|, \qquad L(\overline{\psi'\alpha}, 0) = B_{1,\overline{\psi'\alpha}},$$

where $c = \sum_{a=1}^{m} \overline{\psi\alpha}(a) \otimes (1 - \zeta^a)$ is a circular unit in $U(\chi\alpha) = U(\psi\alpha)$. Since this unit space has rank 1 over R and no p-torsion, we have $\delta_p(y_\chi) \neq 0$ if and only if $B_{1,\overline{\psi'\alpha}} \cdot c$ lies in the subspace $nU(\psi\alpha)$.

But by Gras's conjecture (now a corollary of some work of Greenberg, Mazur, and Wiles [4], [12]) we have the equality

$$\mathrm{length}_R\, U(\psi\alpha)/cU(\psi\alpha) = \mathrm{length}_R\, D(\psi\alpha).$$

Similarly, one has $\mathrm{ord}_p(B_{1,\overline{\psi'\alpha}} = \mathrm{length}_R D(\psi'\alpha)$. The proposition then follows from the direct sum decomposition $D(\psi\alpha) \otimes D(\psi'\alpha) = D(\chi\alpha)$.

If the conditions of (25.1) are met, and y_χ is not $\mathfrak{P}$-primary torsion in $J(L)^\chi$, its projection to the (p, α)-Eisenstein factor has infinite order. Of course, the points y_χ can be $\mathfrak{P}$-torsion for at most a finite number of characters χ. They are *never* $\mathfrak{P}$-torsion if the Eisenstein ideal $I\mathbb{T}_\mathfrak{P}$ is principal in $\mathbb{T}_\mathfrak{P}$.

As in §16, we can combine the results on Heegner points with a first p-descent on the (p, α)-Eisenstein factor to obtain interesting results. I will treat this matter in a forthcoming paper with J. Lubin.

III. THE L-SERIES OF MODULAR FORMS

19. We retain the notation of Section I. Thus $f = \sum_{n \geq 1} a_n q^n$ is a normalized newform of weight 2 for $\Gamma_0(N)$ and χ is a ring class character of K of conductor c prime to N. The two-dimensional representation $\mathrm{Ind}_K^{\mathbb{Q}}\chi$ has conductor $D = d_K \cdot c^2$, and the equation $D = B^2\text{-}4NC$ can be solved in integers with $\gcd(N, B, C) = 1$.

By Hecke's theory, the L-series of Ind χ is equal to the L-series of a modular form $g_\chi = \sum_{n \geqslant 0} b_n q^n$ of weight 1 for $\Gamma_1(D)$. For every prime p dividing gcd(N, D) we have the further condition: $a_p b_p = -1$.

The form g_χ is actually a modular form for $\Gamma_0(D)$ with odd character $\varepsilon = \det(\operatorname{Ind}\chi)$. This character is just the quadratic character associated to the extension $K/\mathbb{Q}$: since χ is a ring class character, $\mathrm{Ver}_K^{\mathbb{Q}}\chi = 1$. We remark that g_χ vanishes at ∞ if and only if $\chi \neq 1$, and that g_χ is a cusp form if and only if $\chi^2 \neq 1$. It is always an eigenform for the entire Hecke algebra, and has level equal to D.

The Dirichlet series for f and g_χ both have Euler products:

$$\left.\begin{aligned} L(f,s) &= \sum_{n \geqslant 1} a_n n^{-s} = \prod_p (1-\alpha_p p^{-s})(1-\alpha'_p p^{-s})^{-1}, \\ L(g_\chi,s) &= \sum_{n \geqslant 1} b_n n^{-s} = \prod_p (1-\beta_p p^{-s})(1-\beta'_p p^{-s})^{-1}. \end{aligned}\right\} \tag{19.1}$$

We have $\alpha_p\alpha'_p\beta_p\beta'_p = p\cdot\varepsilon(p)$ if p does not divide ND; otherwise this product is equal to zero.

20. The modular forms f and g_χ each correspond to infinite-dimensional representations of the adèlic group GL$(2, \mathbb{A}_{\mathbb{Q}})$. Define the L-series for the 'tensor product representation' $f \otimes g_\chi$ of PGL(2) × GL(2) by the formula

$$\begin{aligned} L(f\otimes g_\chi, s) = \prod_p &(1-\alpha_p\beta_p p^{-s})(1-\alpha'_p\beta_p p^{-s}) \\ &\times (1-\alpha_p\beta'_p p^{-s})(1-\alpha'_p\beta'_p p^{-s})^{-1}. \end{aligned} \tag{20.1}$$

This Euler product converges, and is non-zero, in the half-plane $\mathrm{Re}(s) > \frac{3}{2}$.

By the assumptions made on N and D, the naive Euler factors in (20.1) actually equal the local L-factors for the representation $f \otimes g_\chi$. The degree of each factor is equal to 0, 1, 2, or 4; it is equal to 4 if and only if p does not divide ND. When p divides ND, we have the following situation:

$$\left.\begin{array}{lll} p \mid c \text{ or } p^2 \mid N, & L_p(s) = 1, & \text{degree } 0; \\ p \,\|\, N \text{ and } p \nmid d, & L_p(s) = (1-a_p p^{-s})^{-2}, & \text{degree } 2; \\ p \mid d \text{ and } p \nmid Nc, & L_p(s) = (1-a_p b_p p^{-s} + p^{1-2s})^{-1}, & \text{degree } 2; \\ p \mid \gcd(D,N), & L_p(s) = (1-a_p b_p p^{-s})^{-1} & \\ & = (1+p^{-s})^{-1}, & \text{degree } 1. \end{array}\right\} \tag{20.2}$$

The conductor A of the representation $f \otimes g_\chi$ is equal to $N^2D^2/\gcd(N, D)$. Notice that the assumption that $(N, c) = 1$ implies that the local representations associated to f and g_χ are not simultaneous supercuspidal. This seems a natural one in view of the computations of the next section.

21. The infinite Euler factor associated to the representation $f \otimes g_\chi$ is given by $L_\infty(f\otimes g_\chi, s) = \Gamma_{\mathbb{C}}(s)^2 = 4(2\pi)^{-2s}\Gamma(s)^2$. Put

$$\Lambda(f\otimes g_\chi, s) = A^{s/2} L_\infty(f\otimes g_\chi, s) L(f\otimes g_\chi, s). \tag{21.1}$$

This function is defined in the half-plane $\mathrm{Re}(s) > 3/2$; Rankin's method, suitably modified by Jacquet, can be used to show

Proposition 21.2 *$\Lambda(f\otimes g_\chi, s)$ has an analytic continuation to the entire complex plane, and satisfies the functional equation*

$$\Lambda(f\otimes g_\chi, 2-s) = -\Lambda(f\otimes g_\chi, s). \tag{21.2}$$

The proof of (21.2) is fairly standard. It reduces to showing that $\Lambda(\bar{f}\otimes \bar{g}_\chi, s) = \Lambda(f\otimes g_\chi, s)$, and that the global root number $w(f\otimes g_\chi)$ in the functional equation is equal to -1. The first statement can be checked directly, using the identity $\chi(\bar{\mathfrak{p}}) = \bar{\chi}(\mathfrak{p})$. In fact, $\mathrm{Ind}\,\chi$ is an orthogonal Galois representation. The root number will be computed in the next paragraph.

An immediate corollary to (21.2) is the following:

Corollary 21.3 *The order of $L(f\otimes g_\chi, s)$ at $s=1$ is non-negative and odd. In particular, $L(f\otimes g_\chi, 1) = 0$.*

Similar results were obtained by Kurčanov [9].

22. We begin with a computation of local root numbers. Let v denote a place of $\mathbb{Q}$; the automorphic representations f and $g = g_\chi$ of $\mathrm{GL}(2, \mathbb{Q}_v)$ correspond to two-dimensional representations σ_f and σ_g of the Weil–Deligne group of $\mathbb{Q}_v$, and we have the formulas

$$w_v(f) = w_v(\sigma_f), \quad w_v(g) = w_v(\sigma_g), \quad w_v(f\otimes g) = w_v(\sigma_f \otimes \sigma_g). \tag{22.1}$$

The last is due to Jacquet [8], and permits the calculation of $w_v(f\otimes g)$ from the two quantities $w_v(f)$ and $w_v(g)$.

Since f is on $\Gamma_0(N)$, we have $w_v(f)^2 = 1$. Since σ_g is an orthogonal Galois representation with determinant ε, we have $w_v(g)^2 = \varepsilon_v(-1)$. Thus $w_v(f)^2 w_v(g)^2 = \varepsilon_v(-1)$ for all v; we shall prove

Proposition 22.2 *$w_\infty(f\otimes g) = 1$, $w_p(f\otimes g) = \varepsilon_p(-1)$ for all finite p, and $w(f\otimes g) = \varepsilon(-1) = -1$.*

Proof At the infinite place $\sigma_f \otimes \sigma_g \simeq \mathrm{Ind}_{\mathbb{C}}^{\mathbb{R}} z^{-1} \otimes \mathrm{Ind}_{\mathbb{C}}^{\mathbb{R}} 1 \simeq 2\,\mathrm{Ind}_{\mathbb{C}}^{\mathbb{R}} z^{-1}$ This has sign $(-1)^2 = 1$.

At finite primes p not dividing ND, we have $w_p(f\otimes g) = \varepsilon_p(-1) = 1$, as the representation is unramified at p. If p divides N but not D, we have

$$w_p(f\otimes g) = w_p(f)^2 w_p(g)^2 \varepsilon_p(N) = \varepsilon_p(-1)\varepsilon_p(N).$$

But $\varepsilon_p(-1) = \varepsilon_p(N) = 1$, as every prime p dividing N but not D is split in K. Similarly, if p divides D but not N, we have the formula $w_p(f \otimes g) = w_p(f)^2 w_p(g)^2$ as f has trivial determinant.

If p divides $\gcd(N, D)$ then $p \| N$ and f corresponds to a twisted form of the special representation. A short calculation yields the formula $w_p(f \otimes g) = w_p(f)^2 w_p(g)^2(-a_p b_p)$. But $a_p b_p = -1$, by assumption.

The formula $w(f \otimes g)$ follows from the decomposition [8]

$$w(f \otimes g) = \prod_v w_v(f \otimes g)$$

and our local formulas.

23. Let $M = H^1(X) = H^1(J)$ be the 1-motive of rank $2g$ over $\mathbb{Q}$ associated to the cohomology of the curve $X = X_0(N)$. The theorems of Eichler and Deligne can be combined with the Artin formalism to yield the identity

$$L(M/H, s) = \prod_{f, \chi} L(f \otimes g_\chi, s) \quad \text{for} \quad \mathrm{Re}(s) > 3/2. \tag{23.1}$$

Here the product is taken over all characters f of the Hecke algebra on the cotangent space W and over all characters χ of $G = \mathrm{Gal}(H/K)$.

By Rankin's method (21.2), this function has an analytic continuation to the entire complex plane, and satisfies a suitable functional equation when s is replaced by $2 - s$.

Recall that $V = J(H) \otimes \mathbb{C}$, and that $V^{\chi, f}$ is the subspace where G acts via the primitive character χ and $\mathbb{T}$ acts via the newform f. The equality $\dim V = \mathrm{ord}_{s=1} L(M/H, s)$ is predicted by the conjecture of Birch and Swinnerton-Dyer. A natural refinement of that conjecture, in the light of (23.1), is the following:

Conjecture 23.2 $\dim V^{\chi, f} = \mathrm{ord}_{s=1} L(f \otimes g_\chi, s)$

By (21.3), this conjecture would imply that the dimension of $V^{\chi, f}$ is *odd*. In particular, I would always expect that $V^{\chi, f}$ is non-trivial.

24. The conjectures (11.2) and (23.2) seem difficult to me, as they make reference to the entire subspace $V^{\chi, f}$ (about which one knows nothing ...). But they can be combined into a statement which refers *only* to the Heegner divisor $v_{\chi, f}$ and the relevant L-series.

Theorem 24.1 [6] *Assume that D is a fundamental discriminant which is relatively prime to N, and let $2u = |\mathcal{O}^*|$. Then*

$$L'(f \otimes g_\chi, 1) = \frac{(\omega_f, \omega_f)}{u^2 |D|^{1/2}} 2\langle v_{f,\chi}, v_{f,\chi} \rangle \tag{24.1}$$

In particular, $L'(f \otimes g_\chi, 1) = 0$ if and only if $v_{f,\chi} = 0$ in $J(H) \otimes \mathbb{C}$.

In the proof that Zagier and I found for (24.1), the left-hand side is calculated by using a variant of Rankin's method, and the right-hand side by using Néron's theory of local heights. This method should yield an analogous formula for arbitrary D; however, in the general case the right-hand side should be divided by 2^r, where r is the number of primes dividing $\gcd(N, D)$.

IV. THE DERIVATIVES OF AUTOMORPHIC L-FUNCTIONS AND THE ARITHMETIC OF MODULAR CURVES

25. The approach to Heegner points via the L-series of a representation for $\mathrm{PGL}(2) \times \mathrm{GL}(2)$ which was developed in Section III suggests the following generalization.

Let k be a global field, and let $\pi = \otimes \pi_v$ be an irreducible representation of $\mathrm{PGL}(2, \mathbb{A}_k)$ which occurs in the space of cusp forms. If v is an archimedean place of k, we will assume π_v is square-integrable when $k_v = \mathbb{R}$, or a base change lifting of a square-integrable representation of $\mathrm{PGL}(2, \mathbb{R})$ when $k_v \simeq \mathbb{C}$. Let $c(\pi)$ denote the conductor of π, which is an effective divisor of k.

Let K be a separable quadratic extension of k, and let $\chi: \mathbb{A}_K^*/K^* \to \mathbb{C}^*$ be an idèle class character of finite order. We will assume that the restriction of χ to $\mathbb{A}_k^*$ is trivial, and that the conductor $c(\chi)$ of χ is prime to $c(\pi)$. Let ρ be the Weil representation of $\mathrm{GL}(2, \mathbb{A}_k)$ which corresponds to χ; this has central character α, the quadratic character associated to the extension K/k. The corresponding Galois representation $\mathrm{Ind}(\chi)$ is orthogonal, of determinant α.

By Rankin's method, the L-series of the representation $\pi \otimes \rho$ of $\mathrm{PGL}(2) \times \mathrm{GL}(2)$ extends to an entire function on the complex plane, and can be normalized to satisfy the functional equation: $L(\pi \otimes \rho, s) = \varepsilon(\pi \otimes \rho, s) L(\pi \otimes \rho, 2 - s)$. Furthermore, the global root number $w(\pi \otimes \rho) = \varepsilon(\pi \otimes \rho, 1)$ admits a product decomposition: $w(\pi \otimes \rho) = \prod_v w_v(\pi \otimes \rho)$ with all local terms $w_v(\pi \otimes \rho) = \pm 1$. Define

$$\Sigma = \Sigma(\pi \otimes \rho) = \{v : w_v(\pi \otimes \rho) \neq \alpha_v(-1)\}. \tag{25.1}$$

This is a finite set of places of k; if v is contained in Σ then the representation π_v in square-integrable and the algebra $K \otimes k_v = K_v$ is a field. Write $c(\pi) = N_\Sigma \cdot N$, where N_Σ is divisible by the non-archimedean places in Σ, and N is prime to N_Σ.

If $w(\pi \otimes \rho) = 1$, the set Σ has even cardinality. Let B be the quaternion algebra over k which is ramified at Σ, and G the algebraic group over k which represents the functor on k-algebras: $k' \to (k' \otimes B)^*/k'^*$. Since K embeds as a subfield of B, the group $T = K^*/k^*$ gives a maximal torus in G. For $\chi = 1$, Waldspurger [15] has studied the value $L(\pi \otimes \rho, 1) = L(\pi, 1) L(\pi \otimes \alpha, 1)$ using the integrals of arithmetic automorphic forms for G over the torus T.

Now assume that $w(\pi\otimes\rho) = -1$, so $L(\pi\otimes\rho, 1) = 0$. We wish to study $L'(\pi\otimes\rho, 1)$ using the height of special points on modular curves. To do this, we must assume that

$$\Sigma \text{ contains all archimedean places of } k. \tag{25.2}$$

Since $w_v(\pi\otimes\rho) = 1$ for all archimedean v, this means that whenever k is a number field, it is totally real and K is a totally complex quadratic extension of it.

Let A denote the ring of Σ-integers of k. Since Σ is non-empty and contains all archimedean places of k, A is a Dedekind domain. Every non-zero ideal $m \subseteq A$ has finite index; let $\hat{A} = \varprojlim A/m$ denote the profinite completion of A. Let k' denote the class field of k with norm group $k^*\prod_{v\in\Sigma}k^*_{v,+}\prod_{v\notin\Sigma}A^*_v\,\mathbb{A}^{*2}_k/k^*$ in $\mathbb{A}^*_k/k^*$, where $k^*_{v,+}$ is the set of positive real numbers when v is archimedean and $k^*_{v,+} = k^*_v$ if v is non-archimedean. Let $n = [k':k]$; this is the order of the narrow class group of A modulo squares.

The data (Σ, N) determines a curve X over k, which is projective and non-singular. The n components of X over $\bar{k}$ are rational over k', and, for each place $v\in\Sigma$, there is an analytic description of the set of K_v-valued points on X. Namely, let $\Omega_v = K_v - k_v$; then Ω_v is a rigid analytic space of dimension 1 over K_v which admits a left action of $\mathrm{PGL}(2, k_v)$ by fractional linear transformations. Let B be the quaternion algebra over k which is ramified at $\Sigma - \{v\}$ and let R be an Eichler A-order of level N in B. Let G be the group functor on A-algebras: $A' \to (A'\otimes R)^*/A'^*$. Then $X(K_v)$ contains the double coset space

$$X(K_v) = G(k)\backslash\Omega_v \times G(\hat{A}\otimes k)/G(\hat{A}) \tag{25.3}$$

as a dense open subset. We note that $G(\hat{A}\otimes k) \simeq \mathrm{PGL}(2, \hat{A}\otimes k)$ and that

$$G(\hat{A}) \simeq \left\{\begin{pmatrix} a & b \\ c & d\end{pmatrix} \in \mathrm{PGL}(2, \hat{A}) : c \equiv 0 \pmod{N\hat{A}}\right\}.$$

Let J denote the Jacobian of X over k, representing divisor classes of degree zero. If $k = \mathbb{Q}$ and $\Sigma = \{\infty\}$, X is the curve $X_0(N)$ studied in Section I, and $J = J_0(N)$.

Let $\mathcal{O}_K$ denote the integral closure of A in K, and $\mathcal{O} = A + c\mathcal{O}_K$ the unique order of conductor $c = c(\chi)$ in $\mathcal{O}_K$ which contains A. We now assume the following:

$$\text{If } \mathrm{ord}_v(N) \geqslant 2, \text{ then } v \text{ splits in } K. \tag{25.4}$$

Then $\mathcal{O}$ admits optimal embeddings into any Eichler order R of level N in B. This situation gives rise to a collection of Heegner points x on X, which are rational over the class field H of K, with norm group $K^*\prod_{v\in\Sigma}K^*_v\prod_{v\notin\Sigma}\mathcal{O}^*_v\,\mathbb{A}^*_K/K^*$. Since χ may be viewed as a character of $\mathrm{Gal}(H/K)$

by class field theory, we may form the divisors $\Sigma\chi^{-1}(\sigma)x^{\sigma}$ in $\mathrm{Div}(X/H)^{\chi}$. Using certain canonical classes in $\mathrm{Pic}(X)\otimes\mathbb{Q}$ of degree $=\deg(x)$ we may obtain classes $y_{\chi}\in(J(H)\otimes\mathbb{C})^{\chi}$ as in §8.

For simplicity, we shall finally assume that

$$\left.\begin{array}{l}\pi_v \text{ is isomorphic to the special (or Steinberg) representation of}\\ \mathrm{PGL}(2,k_v) \text{ on the non-constant functions on } \mathbb{P}^1(k_v), \text{ for all } v\in\Sigma.\end{array}\right\} \tag{25.5}$$

If k is a number field, this implies that π corresponds to a holomorphic Hilbert modular form f of weight $(2,2,\ldots,2)$ with Fourier coefficients $a_v=1$ for all $v\mid N_{\Sigma}$. In general, (25.5) implies that the eigenvalues of a new vector f for π occur in the regular representation of the Hecke algebra of X in $\mathrm{End}_k(J)$. Hence we may form the class $v_{\chi,f}$ in $J(H)\otimes\mathbb{C}$ as in §10. (To treat the general case, where π_v is square-integrable for all $v\in\Sigma$, one must introduce certain sheaves $\mathscr{F}$ on X corresponding to representations of the compact group $\Pi_{v\in\Sigma}D_v^*/k_v^*$, where D_v is the quaternion division algebra over k_v.)

In analogy with (24.1), it is reasonable to conjecture that $L'(\pi\otimes\rho,1)$ is given by an explicit formula of the shape $\prod_{v\in\Sigma}p_v(\pi)\cdot\langle v_{f,\chi},v_{f,\chi}\rangle$, where $p_v(\pi)$ is a positive constant which arises from a period integral on $X(K_v)$. Zagier and I are confident that the methods used in treating (24.1) will extend to handle the general case. The cases when $k=\mathbb{Q}$ or k is a function field are easier to work with, as X represents a simple moduli problem. But perhaps the case when k is a number field of degree greater than one is more interesting: here the analogous limit formulae for GL(1) have not yet been found.

REFERENCES

[1] Birch, B. J., Elliptic curves and modular functions., *Symp. Math. Inst. Alta Math.*, 4 (1970), 27–32.

[2] Birch, B. J., Heegner points of elliptic curves, *Symp. Math. Inst. Alta Math.* **15** (1975), 441–445.

[3] Birch, B. J., and Stephens, N. M., Computations of Heegner points; in this volume, pp. 13–41.

[4] Greenberg, R., On p-adic L-functions and cyclotomic fields, II, *Nagoya Math J.* 67 (1977), 139–158.

[5] Gross, B. H., Heegner points on $X_0(11)$, in *Séminaire de la théorie des nombres de Bordeaux* 1981–1982, pp. 34.01–34.05.

[6] Gross, B. H., and Zagier, D., Points de Heegner et dérivées de fonctions L, *C. R. Acad. Sci. Paris*, **297** (1983), 85–87.

[7] Heegner, K., Diophantische Analysis und Modulfunktionen, *Math. Z.*, **56** (1952), 227–253.

[8] Jacquet, H., *Automorphic Forms on* GL(2), *II*, Lecture Notes in Mathematics No. 278, Springer, Berlin, 1972.

[9] Kurčanov, P. K., The zeta-function of elliptic curves over certain abelian extensions of imaginary quadratic fields, *Math. Sb.* (N. S.), **102** (144) (1977), 56–70.

[10] Mazur, B., Modular curves and the Eisenstein ideal, *Publ. Math. IHES* 47 (1978), 33–186.

[11] Mazur, B., On the arithmetic of special values of L-functions, *Invent Math.* **55** (1979), 207–240.

[12] Mazur, B. and Wiles, A., Class fields of abelian extensions of $\mathbb{Q}$; *Invent. Math.*, **76** (1984), 179–330.

[13] Serre, J.-P., Complex multiplication, in *Algebraic Number Theory*, Academic Press, New York, 1967, pp. 292–296.

[14] Stark, H., L-functions at $s = 1$, IV, *Advanc. Math.* **35**, (1980), 197–235.

[15] Waldspurger, J. L., Correspondances de Shimura et quaternions, Preprint.