Mathematical Research Letters **5**, 637–655 (1998)

ON THE TATE-SHAFAREVICH GROUP OF CERTAIN ELLIPTIC CURVES

Farshid Hajir and Fernando Rodriguez Villegas

Let $K \subset \mathbb{C}$ be an imaginary quadratic field with prime discriminant $-p < -3$, ring of integers $\mathcal{O}_K = \mathcal{O}$ and class group Cl_K of (odd) order $h_K = h$. The j-invariant $j(\mathcal{O})$ generates a field $F/\mathbb{Q}$ of degree h such that $H = FK$ is the Hilbert class field of K. Suppose A/F is a $\mathbb{Q}$-curve with j-invariant $j(\mathcal{O})$; thus, A is an elliptic curve which, over H, is isogenous to each of its Galois conjugates, and has complex multiplication by $\mathcal{O}$. We let $B = \mathrm{Res}_{F/\mathbb{Q}}A$ be the h-dimensional abelian variety over $\mathbb{Q}$ obtained from A by restriction of scalars. Any two such A (and any two such B) are quadratic twists of one another: letting $A(p)$ denote the canonical curve of discriminant ideal $(-p^3)$, with restriction $B(p)$, we have $A = A(p)^D$ (and $B = B(p)^D$) for some quadratic discriminant D. We refer the reader to Gross [Gr1] for general facts about CM $\mathbb{Q}$-curves. Much progress has been made recently on proving the conjecture of Birch and Swinnerton-Dyer for these curves. For instance, if $L(1, A/F) \neq 0$, and $h = 1$, Rubin [Ru2] has proved that the Birch-Swinnerton–Dyer conjecture for A/F holds up to a power of 2. Note that the ring $\mathcal{R}^+$ of $\mathbb{Q}$-endomorphisms of B (or $B(p)$) is an order in $T^+ = \mathcal{R}^+ \otimes \mathbb{Q}$, a totally real field of degree h over $\mathbb{Q}$. The Tate-Shafarevich group $Ш_{B/\mathbb{Q}}$ is a finite module over $\mathcal{R}^+$; our main goal in this paper is to gain insight into the structure of this module via L-series in some special cases.

Namely, suppose $p \equiv 3 \bmod 8$ and $A = A(p)^{-3}$. Also, assume that $\mathcal{R}^+$ is integrally closed. Let ψ be a Hecke character of K such that $\psi \circ \mathbb{N}_{H/K}$ is the Hecke character attached to A/H. This choice of ψ gives rise to an embedding of T^+ in $\mathbb{R}$ (see section 2). We define an algebraic integer $s \neq 0$ in FT^+ as a sum of certain modified elliptic units first introduced by Gross [Gr3] and show that there is a (unique) integral ideal $\mathfrak{f}$ of $\mathcal{R}^+$ whose lift to FT^+ is generated by s. Our starting point is a formula (Theorem 2) expressing $L(1, \psi)$ as a period times s^2, showing, in particular, that this central critical value does not vanish. Writing $L(s, A/F)$ as a product of Hecke L-series, calculating the local factors in the Birch-Swinnerton–Dyer conjecture, and applying our formula together with results of Coates, Wiles, Arthaud, and Rubin [CW], [Ar], [Ru1], we obtain

Main Theorem(Theorem 5) *With the above assumptions and notation, $A(F) = B(\mathbb{Q})$ is finite. If the Birch-Swinnerton–Dyer conjecture holds for A/F (or for*

Received September 19, 1997, revision received May 4, 1998.

The first author was supported in part by a Mathematical Sciences Postdoctoral Research Fellowship from the NSF. The second author was supported in part by a grant from the NSF and by a fellowship from the John Simon Guggenheim Memorial Foundation.

$B/\mathbb{Q}$), then the order of its Tate-Shafarevich group is $\mathbb{N}_{T^+/\mathbb{Q}}(\mathfrak{f})^2$, where $\mathfrak{f}$ is the integral $\mathcal{R}^+$-ideal defined in section 2.

Following Buhler-Gross [BG], we conjecture that the order ideal $\mathfrak{s}_B$ of the $\mathcal{R}^+$-module $\text{Ш}_{B/\mathbb{Q}}$ is in fact $\mathfrak{f}^2$; note that, by our theorem, this is compatible with the Birch-Swinnerton–Dyer conjecture, and is a refinement of it. Our results shore up the Buhler-Gross conjecture in several ways: namely, our predicted order ideal $\mathfrak{f}^2$ is known to be the *square* of an *integral* ideal of $\mathcal{R}^+$. Previously, Buhler and Gross verified these properties numerically in hundreds of cases.

Our formula gives an effective means of computing the (predicted) order ideal of the Tate-Shafarevich group for these curves, and is similar to the formula one of us [RV] found for the cardinality of $\text{Ш}_{A(p)/F}$ for $p \equiv 7 \bmod 8$; see also [H]. We implemented this procedure on a computer (some tables of our data appear at the end of the paper). This allowed us to make a conjectural numerical study of the $\mathcal{R}^+$-module $\text{Ш}_{B/\mathbb{Q}}$. We were particularly interested in the question of whether this module can be "non-trivial," in the sense that its order ideal $\mathfrak{s}_B$ is not trivial in the class group of $\mathcal{R}^+$. We succeeded in finding three examples where the (predicted) order ideal $\mathfrak{f}^2$ is not principal, not an entirely trivial task. Using some results from [H], this answers, at the same time, a question of Gross concerning the triviality of a certain 1-cocycle induced by the units used to define $\mathfrak{f}$. We should remark that there are order ideals attached to the torsion of $B/\mathbb{Q}$ and to its local factors at infinity and at the places of bad reduction (see Gross [Gr2]), and that a suitable product of all these ideals with the order ideal of the Tate-Shafarevich group is expected to be principal (generated by the algebraic part of the critical L-value), but that these ideals need not be principal in $\mathcal{R}^+$ individually, as demonstrated here.

We should explain that the restriction to the rather special case of twisting by -3 is made in order to keep the technicalities in the calculation of $L(1,\psi)$ (in section 5) to a minimum. The general factorization formula we prove in that section (Proposition 8) should yield a similar formula for $L(1,\psi)$ for more general twists, but in the case of twisting by -3, the various Jacobi theta functions with characteristics reduce down to the relatively simple eta function; moreover, in the calculation of the local factors in the Birch-Swinnerton–Dyer conjecture, various dyadic primes just cancel in the case of twist by -3, giving the clean formula for the predicted order ideal presented here. Also, see the recent paper by Rodriguez Villegas and Yang [RVY].

The organization of the sections is as follows. We set up the notation and make various definitions in section 1. In section 2, we define the algebraic quantities s and $\mathfrak{f}$; the action of Galois on them is determined easily using the results of [HRV]. In section 3, we introduce the elliptic curves A of interest, and obtain a formula for $L(1, A/F)$, assuming the formula for $L(1,\psi)$ (whose proof, being somewhat technical, we defer to section 5). A calculation of the various factors in the Birch-Swinnerton–Dyer conjecture then yields the main theorem. In section 4, we recall the question of Gross, first posed in [Gr3] and further investigated in [H], and present calculations carried out using the package GP-

PARI, illustrating three examples where the class of the (predicted) order ideal of the Tate-Shafarevich group is non-trivial, answering Questions 2.9, 2.10 and 2.13 of [H]. As in [RV], the two main ingredients for expressing $L(1,\psi)$ as a period times s^2 are, first a formula, following Hecke, expressing $L(1,\psi)$ in terms of binary theta series (section 5.1), and a "factorization formula" expressing values of these theta series at CM points as a product of values of two half-integral-weight theta series at related CM points (section 5.2). We conclude with a table of predicted orders of the Tate-Shafarevich group of $A(p)^{-3}$, as well as a table of the ideals $\mathfrak{f}$ for small p.

1. Preliminaries

Suppose $K \subset \mathbb{C}$ is an imaginary quadratic field with discriminant $-d$ relatively prime to 6 and class number h. With the exception of sections 1 and 5, we will in fact assume $d = p$ is a prime $\equiv 3 \bmod 8$. (At the top of each section, we indicate our assumptions regarding d). We write $\mathcal{O} = \mathcal{O}_K$ for the ring of integers of K. Let ϵ be the Dirichlet character associated to K, extended to K via the natural isomorphism $\mathcal{O}/(\sqrt{-d}) \cong \mathbb{Z}/d\mathbb{Z}$; concretely,

$$\epsilon(\alpha) = \left(\frac{2(\alpha+\overline{\alpha})}{d}\right) \qquad (\alpha \in \mathcal{O}_K).$$

Here and throughout the paper, we use the notation $\left(\frac{\cdot}{\cdot}\right)$ for the Kronecker symbol. We write $\left(\frac{2}{d}\right) = (-1)^{\delta}$ with $\delta = 0, 1$. Also, define

$$\kappa = \frac{3-\epsilon(3)}{2} = \begin{cases} 1 & d \equiv 2 \bmod 3, \\ 2 & d \equiv 1 \bmod 3. \end{cases} \tag{1}$$

Consider the set Φ of Hecke characters ϕ of K such that

$$\phi((\alpha)) = \epsilon(\alpha)\alpha, \qquad \alpha \in \mathcal{O}_K, \qquad (\alpha, d) = 1.$$

There are exactly h such characters, they all have conductor $(\sqrt{-d})$, the ratio of any two being a character of Cl_K. Let χ be the quadratic Dirichlet character associated to $\mathbb{Q}(\sqrt{-3})$,i.e. $\chi(a) = \left(\frac{-3}{a}\right) = \left(\frac{a}{3}\right)$ for integers a prime to 3 and $\chi(a) = 0$ otherwise. Consider the set Ψ of twists $\psi = \phi \cdot \chi \circ \mathbb{N}_{K/\mathbb{Q}}$ with $\phi \in \Phi$. If $\mathfrak{a}$ is not relatively prime to $3d$, $\psi(\mathfrak{a}) = 0$, and, for all $\mathfrak{a}$, $\psi(\overline{\mathfrak{a}}) = \overline{\psi(\mathfrak{a})}$. Also,

$$\overline{\psi}(\mathfrak{a})\psi(\mathfrak{a}) = \mathbb{N}\mathfrak{a}. \tag{2}$$

For the remainder of the paper, fix a base point $\phi_0 \in \Phi$ and its χ-twist $\psi_0 \in \Psi$; their unramified twists $\phi_0\varphi$, $\psi_0\varphi$ – with $\varphi \in \widehat{\mathrm{Cl}_K}$ – span Φ, Ψ, respectively.

We will need two kinds of CM-points attached to an ideal $\mathfrak{a}$ of $\mathcal{O}$: one, denoted $\tau_{\mathfrak{a}}$, at which we will evaluate integral-weight modular forms (of level d) , and another, denoted $z_{\mathfrak{a}}$, for half-integral-weight modular forms (of level a power of 2). For a primitive $\mathcal{O}$-ideal $\mathfrak{a}$ of norm a prime to $6d$, we may always choose a basis

$\mathfrak{a} = a\mathbb{Z} + \frac{b+\sqrt{-d}}{2}\mathbb{Z}$ with $b \in \mathbb{Z}$ determined modulo $2a$ satisfying $b^2 \equiv -d \bmod 4a$. In particular, we may choose $b \in 3d\mathbb{Z}$, and put

$$\tau_{\mathfrak{a}} = \frac{b+\sqrt{-d}}{2ad} \in \mathcal{H} \qquad \left(\mathfrak{a} = \left[a, \frac{b+\sqrt{-d}}{2}\right], \qquad b \equiv 0 \bmod 3d\right),$$

which is well-defined modulo $3\mathbb{Z}$ and whose image in $\mathcal{H}/\Gamma_0(d)$ depends only the class $[\mathfrak{a}]$. Similarly, we may always choose $b \equiv 1 \bmod 16$ and then set

$$z_{\mathfrak{a}} = \frac{b+\sqrt{-d}}{2a} \in \mathcal{H} \qquad \left(\mathfrak{a} = \left[a, \frac{b+\sqrt{-d}}{2}\right], \qquad b \equiv 1 \bmod 16\right),$$

well-defined modulo $8\mathbb{Z}$.

2. The units u_C and the ideal $\mathfrak{f}$

In this section, we assume that $d = p > 3$ is a prime satisfying $p \equiv 3 \bmod 8$, so $\delta = 1$ and h is odd. Let $j = j(\mathcal{O}) \in \mathbb{R}$ where $j(L)$ is the classical modular invariant of a lattice $L \subset \mathbb{C}$. Let $F = H^+ = \mathbb{Q}(j) \subset \mathbb{R}$; this is a number field of degree h whose remaining embeddings are complex. Recall that $H = H^+K$ is the Hilbert class field of K.

Let $T = T_{\phi_0}$ be the subfield of $\mathbb{C}$ generated by the values of ϕ_0, and put $T^+ = T \cap \mathbb{R}$. Then T^+ is totally real of degree h over $\mathbb{Q}$ and T/T^+ is a CM extension. Let $M^+ = T^+H^+$, $M = M^+K$. Then $T \cap H = K$, and we may identify $\widehat{\mathrm{Cl}_K}$ with the embeddings of M/H in $\mathbb{C}$, the trivial character corresponding to our fixed embedding T_{ϕ_0}. For instance, for $x \in H$, $\varphi \in \widehat{\mathrm{Cl}_K}$, and $\mathfrak{a} \subseteq \mathcal{O}$, we have $(\phi_0(\mathfrak{a})x)^{\varphi} = (\varphi\phi_0)(\mathfrak{a})x$. Also, we may identify Cl_K with $\mathrm{Gal}(M/T)$ via the Artin map $C \mapsto \sigma_C$. For more detailed explanations of these facts, we refer the reader to Gross [Gr1].

Recall that the Dedekind eta function defined for $z \in \mathcal{H}$ by

$$\eta(z) = e^{\pi i z/12} \prod_{n \geq 1} (1 - e^{2\pi i z n})$$

has the series expansion

$$\eta(z) = \sum_{m \geq 1} \left(\frac{12}{m}\right) e^{\pi i m^2 z/12}, \tag{3}$$

which converges quickly, when $\Im(z)$ is bounded below by a positive constant.

Definition 1. *For each ideal class C, choose a primitive ideal $\mathfrak{a}$ prime to $6d$ such that $[\mathfrak{a}^2] = C^{-1}$ and put*

$$u_C = \left(\frac{-4}{\mathbb{N}\mathfrak{a}}\right) \overline{\phi_0}(\mathfrak{a})^{-1} \eta(z_{\mathfrak{a}^2})/\eta(z_{\mathcal{O}}).$$

Remark. That u_C is well-defined may be checked directly; it also follows easily from Corollary 10 which we will establish in section 5. For $d \equiv 7 \bmod 8$, the units u_C were introduced already in [RV]; the definition in the two cases differs only by the factor $(\frac{-4}{\mathbb{N}\mathfrak{a}})^\delta$. In the proof of [H, Theorem 3.1], the presence of this symbol should have been mentioned.

To see the algebraic properties of u_C, we note that, in the notation of [HRV],

$$\frac{\eta(z_{\mathfrak{a}^2})}{\eta(z_{\mathcal{O}})} = \frac{\eta(\overline{\mathfrak{a}}^2)}{\eta(\mathcal{O})},$$

hence by [HRV, Prop. 10] $\eta(z_{\mathfrak{a}^2})/\eta(z_{\mathcal{O}}) \in \mathcal{O}_H$ and generates $\overline{\mathfrak{a}}\mathcal{O}_H$. Since $\overline{\phi_0}(\mathfrak{a}) \in \mathcal{O}_T$ and generates $\overline{\mathfrak{a}}\mathcal{O}_T$, u_C is a unit in M. Moreover, by [HRV, Prop. 10],

$$\overline{u}_C = u_{C^{-1}}, \qquad u_C^{\sigma_{C'}} = u_{CC'}/u_{C'} \qquad (C, C' \in \mathrm{Cl}_K).$$

We see that these units give rise to a 1-cocycle with values in $E_M = \mathcal{O}_M^\times$. In order to maintain consistency with the notation in [H], let us write for $\sigma = \sigma_C \in \mathrm{Gal}(M/T)$, $w_\sigma = u_C$. The assignment

$$\sigma_- \mapsto 1, \sigma \mapsto w_\sigma,$$

(where σ_- is a generator of $\mathrm{Gal}(M/M^+)$ and $\sigma \in \mathrm{Gal}(M/T)$) defines a 1-cocycle w on $\mathrm{Gal}(M/T^+)$ with values in E_M.

We let $s = \sum_{C\in \mathrm{Cl}_K} u_C \in \mathcal{O}_M$. It is easily verified that $\mathrm{Tr}_{M/H}(s) = h$, and that $\overline{s^\varphi} = s^\varphi$ for each $\varphi \in \widehat{\mathrm{Cl}_K}$; hence, s^φ is a non-zero real number. Furthermore,

$$s^{\sigma_C} = s u_C^{-1}, \qquad (C \in \mathrm{Cl}_K).$$

In particular, the integral ideal $s\mathcal{O}_M$ is fixed by $\mathrm{Gal}(M/T)$. Since M/T is unramified, and since $\overline{s} = s$, there is a unique ideal $\mathfrak{f}$ of $\mathcal{O}_{T^+}$ such that $\mathfrak{f}\mathcal{O}_M = s\mathcal{O}_M$. Note that $\mathfrak{f}^h$ is principal, generated by $s\prod_C u_C \in \mathcal{O}_{T^+}$; we will be interested in whether $\mathfrak{f}$ itself is principal in $\mathcal{O}_{T^+}$. We note that in [H], s and $\mathfrak{f}$ were called s_w and $\mathfrak{f}_w$, respectively.

Section 5 will be devoted to the proof of

Theorem 2. *For any unramified character $\varphi \in \widehat{\mathrm{Cl}_K}$,*

$$L(1, \psi_0\varphi) = \frac{4\pi\kappa|\eta(z_{\mathcal{O}})|^2}{3^{1/2}p^{1/4}}(s^\varphi)^2.$$

3. The $\mathbb{Q}$-curve $A(p)^{-3}$

In this section, we continue to assume that $d = p > 3$ is a prime satisfying $p \equiv 3 \bmod 8$. There is an elliptic curve $A(p)$ of invariant $j = j(\mathcal{O})$ with global minimal equation of discriminant $(-p^3)$ over H^+

$$y^2 = x^3 + \frac{mp}{2^4 3}x - \frac{np^2}{2^5 3^3},$$

where m, n are the unique real numbers defined by

$$m^3 = j, \qquad -n^2 p = j - 1728, \qquad n < 0.$$

Using the classical theory of complex multiplication, one shows that m, n are actually elements of H^+; see, for example, [HRV, Theorem 17]. Over H, $A(p)$ acquires complex multiplication by $\mathcal{O}_K$, and is isogenous to all of its Galois conjugates.

Consider the elliptic curve $A = A(p)^\chi = A(p)^{-3}$, the twist of $A(p)$ by $\mathbb{Q}(\sqrt{-3})$. The CM elliptic curve A has associated Hecke character $\psi_0 \circ \mathbb{N}_{H/K}$. By Shimura [Sh], we have the factorization

$$L(s, A/H^+) = \prod_{\varphi \in \widehat{\mathrm{Cl}_K}} L(s, \psi_0 \varphi). \tag{4}$$

Recall that $B = \mathrm{Res}_{H^+/\mathbb{Q}} A$ is the abelian variety over $\mathbb{Q}$ obtained from A via restriction of scalars. It is an h-dimensional quotient of the Jacobian $J_0(9p^2)$ of the modular curve $X_0(9p^2)$. The L-series of A/H^+ and $B/\mathbb{Q}$ coincide; the Birch-Swinnerton–Dyer conjecture holds for one if and only if it holds for the other, and $Ш_{A/H^+}$ and $Ш_{B/\mathbb{Q}}$ are isomorphic, see Milne [Mi, Theorem 1]. The $\mathbb{Q}$-endomorphism ring $\mathcal{R}^+ = \mathrm{End}_{\mathbb{Q}} B$ is an order in $T^+ = \mathcal{R}^+ \otimes \mathbb{Q}$ with a simple description: it is the ring generated over $\mathbb{Z}$ by the values $\phi_0(\mathfrak{a}) + \phi_0(\overline{\mathfrak{a}})$ as $\mathfrak{a}$ runs over integral ideals of $\mathcal{O}_K$. For simplicity, let us assume $\mathcal{R}^+ = \mathcal{O}_{T^+}$; our computations indicate that this is often the case, and, in general, $\mathcal{R}^+$ is maximal locally at primes away from h. (We are not aware, however, of a general criterion guaranteeing the maximality of $\mathcal{R}^+$.) This ring acts on $Ш_{B/\mathbb{Q}}$, and we are interested in the order ideal, or characteristic ideal, $\mathfrak{s}_B$, of this $\mathcal{R}^+$-module. Following Buhler-Gross [BG], we have the following conjecture.

Conjecture 3 (Refined Birch-Swinnerton–Dyer Conjecture). *For a prime $p > 3$ satisfying $p \equiv 3 \bmod 8$, and $B = B(p)^{-3}$, $\mathfrak{s}_B = \mathfrak{f}^2$.*

Since the norm of the order ideal is the cardinality of the module, in order to check that this conjecture is consistent with that of Birch and Swinnerton–Dyer, we must verify that the latter predicts the order of $Ш_{B/\mathbb{Q}}$ to be $\mathbb{N}_{T^+/\mathbb{Q}}(\mathfrak{f})^2$. This is our main result (Theorem 5), and is proved below.

We follow Manin's notation and setup for the Birch-Swinnerton–Dyer conjecture [Ma]. For instance, for a place v of H^+, we denote the local factor $|A(H_v^+)/A(H_v^+)^0|$ by m_v. The primes of bad reduction for A/H^+ are the primes above p and those above 3; for all other finite places v, $m_v = 1$.

Lemma 4. *With κ as defined in (1), the local factors m_v (for v a place of H^+) satisfy*

i) $\prod_{v|p} m_v = 2^h$;

ii) $\prod_{v|3} m_v = \kappa^h$;

iii) $\prod_{v|\infty} m_v = 2^{-(h-1)/2} \left(2\pi |\eta(z_{\mathcal{O}})|^2 3^{-1/2} p^{-1/4}\right)^h \prod_{C \in \mathrm{Cl}_K} u_C^2$.

Proof. For *i*) and *iii*), we refer to the calculation of the same quantities for $A(p)$ in [RV, pp. 568–570], as they require little or no modification for $A(p)^{-3}$. For ii), we note that $(\prod_{v|3} m_v)^2 = \prod_{w|3} |B(K_w)/B(K_w)^0|$, where w runs over the primes of K dividing 3 and $B = \mathrm{Res}_{H^+/\mathbb{Q}} A$, then use the formula on p. 232 of Gross [Gr2]. □

Theorem 5. *The group of rational points $A(H^+)$ is trivial. If the conjecture of Birch and Swinnerton-Dyer on the value of $L(1, A/F)$ holds, the cardinality of $\text{Ш}_{A/H^+}$ is $\mathbb{N}_{T^+/\mathbb{Q}}(\mathfrak{f})^2$, where $\mathfrak{f}$ is the integral $\mathcal{R}^+$-ideal defined in section 2.*

Proof. By Theorem 2, and the factorization (4), $L(1, A/H^+) \neq 0$ since $s^\varphi \neq 0$ for all $\varphi \in \widehat{\mathrm{Cl}_K}$. A theorem of Arthaud [Ar] and Rubin [Ru2], extending the Coates-Wiles theorem [CW], implies that A/H^+ has rank 0. By Gross [Gr1], $A(H^+)$ is torsion-free, hence trivial. Our base field H^+ has $r_2(H^+) = (h-1)/2$ many pairs of complex embeddings and discriminant $\mathrm{disc}(H^+/\mathbb{Q}) = p^{(h-1)/2}$. When we combine Theorem 2 with Lemma 4 and compare with the Birch-Swinnerton–Dyer conjecture

$$L(1, A/F) \stackrel{?}{=} \frac{|\text{Ш}_{A/F}|}{|A(F)_{\mathrm{tor}}|^2} \frac{2^{r_2(F)}}{|\mathrm{disc}(F/\mathbb{Q})|^{1/2}} \prod_v m_v,$$

we find that the predicted order of $\text{Ш}_{A/H^+}$ is S^2 where

$$S = \prod_{\varphi \in \widehat{\mathrm{Cl}_K}} s^\varphi \prod_{C \in \mathrm{Cl}_K} u_C^{-1}. \tag{5}$$

Using $\mathbb{N}_{T^+/\mathbb{Q}}(\mathfrak{f})^h = \pm\mathbb{N}_{M^+/\mathbb{Q}}(s)$, it is easily shown ([H, Lemma 2.7.v]) that S is a generator of the $\mathbb{Z}$-ideal $\prod_{\sigma \in \mathrm{Cl}_K} \mathfrak{f}^\sigma$, i.e. $S = \pm\mathbb{N}_{T^+/\mathbb{Q}}(\mathfrak{f}) \in \mathbb{Z}$, completing the proof. □

4. The class of the order ideal, and a question of Gross

We continue to assume that $d = p > 3$ is a prime satisfying $p \equiv 3 \bmod 8$. Let us return to the cocycle w defined in section 3. It is easily seen that the cohomology class $[w]^h$ is trivial, split by $\prod_\sigma w_\sigma^{-1}$, and it is natural to ask whether $[w]$ itself is trivial in $H^1(\mathrm{Gal}(M/T^+), E_M)$. Indeed, Gross [Gr3] constructed units (called u_σ in [H]) which are essentially the squares of w_σ and asked the same question about their cohomology class $[u]$. The classes $[u]$ and $[w]$ in fact are either both trivial or both non-trivial; for more details, see [H], especially Theorem 3.4 and Questions 2.9, 2.10, 2.13.

Question 2.10 was answered in the negative in [H] by calculating some examples; here we will do the same for Questions 2.9 and 2.13 of [H]. Before doing so, we recall ([H, Theorem 2.12]) that the cohomology class of w is trivial if and only if the ideal class of $\mathfrak{f}$ in Cl_{T^+} is trivial. Hence, assuming the above refined Birch-Swinnerton–Dyer conjecture, Gross' original question boils down to whether the ideal class of the Tate-Shafarevich order ideal of $B/\mathbb{Q}$ is trivial in the class group of $\mathcal{R}^+$. The difficulty in finding non-trivial examples is that the class number of T^+ is seldom greater than 1 and very seldom has a non-trivial factor in common with h, which is what we need since $[\mathfrak{f}]$ is killed by h. In one case previously investigated where h_{T^+} and h have a factor in common, namely $p = 4027$, it turned out that $\mathfrak{f}$ was principal [H]. Here we present three examples where the predicted order ideal of $Ш_{B/\mathbb{Q}}$, i.e. $\mathfrak{f}^2$, is *not* principal in $\mathcal{R}^+$, though of course it capitulates in M^+. Let us write $|Ш|_?$ for the order of $Ш_{B/\mathbb{Q}}$ as predicted by Birch–Swinnerton-Dyer, namely S^2 where S is given by (5).

Example 1. $p = 571$, $h = 5$, $|Ш|_? = 4^2$, $\mathfrak{f} = \mathfrak{p}_2^2$, where $\mathfrak{p}_2$ is the unique prime of degree 1 above 2. Here, $\mathfrak{p}_2$ generates the ideal class group of $\mathcal{R}^+ = \mathcal{O}_{T^+}$ (it has order 5), hence $\mathfrak{f}$ and $\mathfrak{f}^2$ are not principal. A defining polynomial for T^+ is $x^5 - 24x^3 + 125x - 58$.

Example 2. $p = 1523$, $h = 7$, $|Ш|_? = 2485^2$, $\mathfrak{f} = \mathfrak{p}_5\mathfrak{p}_7\mathfrak{p}_{71}$; as before, $\mathfrak{p}_r$ is the unique prime of degree 1 above r. The class group of $\mathcal{R}^+ = \mathcal{O}_{T^+}$ has order 7 and $\mathfrak{f}$ generates it. We have $\mathcal{R}^+ \cong \mathbb{Z}[\theta]$ where θ is a root of $x^7 - 21x^5 + 126x^3 - 189x + 85$.

Example 3. $p = 3019$, $h = 7$, $|Ш|_? = 15373^2$. The prime 15373 splits into 7 prime ideals in $\mathcal{R}^+ = \mathcal{O}_{T^+}$, one of which is $\mathfrak{f}$. All seven of these primes give rise to the same non-trivial class in the class group of $\mathcal{R}^+$, which has order 7. If the predicted order is in fact correct, then $Ш \cong (\mathcal{R}^+/\mathfrak{f})^2$ as $\mathcal{R}^+$-modules. A defining polynomial for T^+ is $x^7 - 35x^5 + 350x^3 - 875x + 514$.

Remarks. 1) These calculations were carried out in GP/Pari [B] on a Power Computing Power 100. We double-checked the calculation of $L(1, A/H^+)$ by using the standard algorithm [BG] as well.

2) In examples 1 and 3, the class of the different in $\mathcal{R}^+$ is not principal, so there is no power basis for $\mathcal{R}^+/\mathbb{Z}$. According to de Smit [dS], the non-triviality of the class of the different implies that, as $\mathbb{Z}$-algebra, $\mathcal{R}^+$ is not a complete intersection. Note that $\mathcal{R}^+$ is a *quotient* of the Hecke algebra $\mathbb{T} \subset \mathrm{End}(J_0(9p^2))$.

5. Calculating $L(1, \psi)$

We now give a proof of Theorem 2. We divide this section into three parts. In the first two subsections, we relax the condition on the discriminant $-d$, requiring only that it be prime to 6. In the third subsection, we return to the case where $d = p > 3$ is a prime $\equiv 3 \bmod 8$, and complete the proof of Theorem 2.

5.1. Eisenstein series of weight 1. For an ideal $\mathfrak{a}$ of $\mathcal{O}_K$ prime to $6d$, define a partial Hecke series

$$Z(s, \mathfrak{a}) = \frac{1}{2} \sum_{\lambda \in \mathfrak{a}}{}' \frac{\epsilon(\lambda)\chi(|\lambda|^2)\overline{\lambda}}{|\lambda|^{2s}}, \qquad (\Re(s) > 3/2)\,.$$

As usual, the prime indicates that the sum is over the non-zero elements of $\mathfrak{a}$. Via a standard argument, one expresses the Hecke L-series $L(s, \psi) =$

$\sum_{\mathfrak{b}\subseteq\mathcal{O}_K}\psi(\mathfrak{b})\mathbb{N}\mathfrak{b}^{-s}$ in terms of the $Z(s,\mathfrak{a})$:

$$L(s,\psi)=\sum_{[\mathfrak{a}]\in\mathrm{Cl}_K}\frac{\psi(\mathfrak{a})}{\mathbb{N}\mathfrak{a}^{1-s}}Z(s,\mathfrak{a}). \tag{6}$$

Recall the Eisenstein series (of weight 1 and character ϵ on $\Gamma_0(d)$)

$$G_{1,\epsilon}(z)=\frac{1}{2}\sum_{m,n\in\mathbb{Z}}{}'\frac{\epsilon(n)}{mdz+n}\qquad(z\in\mathcal{H}),$$

which is not an absolutely convergent series, but is summed by the Hecke trick

$$G_{1,\epsilon}(z)=\frac{1}{2}\sum_{m,n}{}'\frac{\epsilon(n)}{mdz+n}\frac{1}{|mdz+n|^{2s}}\Bigg|_{s=0}. \tag{7}$$

Its Fourier expansion is given by Hecke [He, *Werke* p. 454]

$$G_{1,\epsilon}(z)=L(1,\epsilon)+\frac{2\pi}{\sqrt{d}}\sum_{n\geq 1}r_ne^{2\pi inz}, \tag{8}$$

where $r_n=\sum_{m|n}\epsilon(m)$ is the number of ideals of norm n in $\mathcal{O}_K$. For an ideal $\mathfrak{a}$ of $\mathcal{O}_K$, the associated binary theta series

$$\Theta_{\mathfrak{a}}(z)\;=\;\frac{1}{2}\sum_{\mathfrak{b}\subseteq\mathcal{O}_K,[\mathfrak{b}]=[\mathfrak{a}]}e^{2\pi iz\mathbb{N}\mathfrak{b}}\qquad(z\in\mathcal{H}),$$

is a weight-one modular form (on $\Gamma_0(d)$ with character ϵ) which depends only on the class $[\mathfrak{a}]\in\mathrm{Cl}_K$. By (8) and Dirichlet's class number formula ($L(1,\epsilon)=\pi h/\sqrt{d}$), the h binary series of discriminant $-d$ add up to a constant times $G_{1,\epsilon}$:

$$G_{1,\epsilon}(z)=\frac{2\pi}{\sqrt{d}}\sum_{[\mathfrak{a}]\in\mathrm{Cl}_K}\Theta_{\mathfrak{a}}(z). \tag{9}$$

In [RVZ], $L(1,\phi)$ was expressed as a sum of values of $G_{1,\epsilon}$ at CM-points. Here we do the same for $L(1,\psi)$, but the expression is, at least initially, more complicated as we must pass through an intermediary twisted Eisenstein series

$$G_{1,\epsilon,\chi}(z)=\frac{1}{2}\sum_{m,n}{}'\frac{\epsilon(n)\chi(m^2d+n^2)}{mdz+n},$$

again summed via Hecke's trick. One way to calculate the Fourier expansion of $G_{1,\epsilon,\chi}$ is to relate it to $G_{1,\epsilon}$.

Lemma 6. *For all* $z\in\mathcal{H}$, $G_{1,\epsilon,\chi}(z)=\kappa(G_{1,\epsilon}(3z)-\frac{1}{3}G_{1,\epsilon}(z/3))$.

Proof. We can break up the sum (7) according to congruence classes modulo 3, and verify:

$$\frac{1}{2}\sum_{\substack{m\in 3\mathbb{Z}\\ n\notin 3\mathbb{Z}}} \frac{\epsilon(n)}{mdz+n}\,\frac{1}{|mdz+n|^{2s}}\bigg|_{s=0} = G_{1,\epsilon}(3z)-\tfrac{\epsilon(3)}{3}G_{1,\epsilon}(z),$$

$$\chi(d)\frac{1}{2}\sum_{\substack{m\notin 3\mathbb{Z}\\ n\in 3\mathbb{Z}}} \frac{\epsilon(n)}{mdz+n}\,\frac{1}{|mdz+n|^{2s}}\bigg|_{s=0} = \chi(d)\tfrac{\epsilon(3)}{3}\big(G_{1,\epsilon}(\tfrac{z}{3})-G_{1,\epsilon}(z)\big),$$

$$\chi(d+1)\frac{1}{2}\sum_{\substack{m\notin 3\mathbb{Z}\\ n\notin 3\mathbb{Z}}} \frac{\epsilon(n)}{mdz+n}\,\frac{1}{|mdz+n|^{2s}}\bigg|_{s=0} = \chi(d+1)\left[\left(1+\frac{\epsilon(3)}{3}\right)G_{1,\epsilon}(z)-G_{1,\epsilon}(3z)-\tfrac{\epsilon(3)}{3}G_{1,\epsilon}(\tfrac{z}{3})\right].$$

Adding these together, and taking note of the identities $\chi(d)=-\epsilon(3),\chi(d+1)=(\epsilon(3)-1)/2$, we get the desired formula. □

We are now ready to express the critical value $L(1,\psi)$ in terms of binary theta series evaluated at CM points.

Lemma 7. *With κ as in* (1)*, we have*

$$L(1,\psi)=\frac{2\pi\kappa}{\sqrt{d}}\sum_{[\mathfrak{a}],[\mathfrak{a}_1]\in\mathrm{Cl}_K}\overline{\psi}(\mathfrak{a})^{-1}\left(\Theta_{\mathfrak{a}\mathfrak{a}_1}(3\tau_{\mathfrak{a}})-\frac{1}{3}\Theta_{\mathfrak{a}\mathfrak{a}_1}\left(\frac{\tau_{\mathfrak{a}}}{3}\right)\right).$$

Proof. Suppose $\mathfrak{a}$ is primitive and has norm a prime to $6d$. Elements $\lambda\in\mathfrak{a}$ correspond to integer pairs m,n via $\lambda=a(md\tau_{\mathfrak{a}}+n)$; for this λ, one easily checks that $\epsilon(\lambda)=\epsilon(n),\chi(|\lambda|^2)=\chi(m^2d+n^2)$. Hence

$$Z(s,\mathfrak{a})=\frac{a^{1-2s}}{2}\sum_{m,n}{}'\,\frac{\epsilon(n)\chi(m^2d+n^2)(\overline{md\tau_{\mathfrak{a}}+n})}{|md\tau_{\mathfrak{a}}+n|^{2s}},\qquad(\Re(s)>3/2).$$

In particular,

$$Z(1,\mathfrak{a})=a^{-1}G_{1,\epsilon,\chi}(\tau_{\mathfrak{a}}).\tag{10}$$

Combining (10) with (2) and (6), and using Lemma 6 together with (9), we arrive at the desired formula. □

5.2. A factorization formula. Our goal in this subsection is to express each term in the sum appearing in Lemma 7 as a product of two η-values times simple constants. We derive this from a suitable generalization of the factorization formula of Rodriguez Villegas and Zagier [RVZ], which reads

$$(11)\qquad \sum_{m,n\in\mathbb{Z}} e^{2\pi i(m\nu+n\mu)} e^{\pi(imn-Q_z(m,n))/a} = \sqrt{2ay}\, \theta\begin{bmatrix} a\mu \\ \nu \end{bmatrix}(z/a)\, \theta\begin{bmatrix} \mu \\ -a\nu \end{bmatrix}(-a\overline{z}),$$

where a is a positive integer, $z = x + iy \in \mathcal{H}$, $Q_z(m,n) = |mz-n|^2/2y$ is a quadratic form of discriminant -1, and the theta function $\theta\begin{bmatrix} \mu \\ \nu \end{bmatrix}$ with arbitrary characteristics $\mu, \nu \in \mathbb{Q}$ is defined by

$$\theta\begin{bmatrix} \mu \\ \nu \end{bmatrix}(z) = \sum_{n\in\mathbb{Z}} e^{\pi i(n+\mu)^2 z + 2\pi i\nu(n+\mu)}.$$

More generally, for any function f on $\mathbb{Z}$, we put

$$\theta_f\begin{bmatrix} \mu \\ \nu \end{bmatrix}(z) = \sum_{n\in\mathbb{Z}} f(n) e^{\pi i(n+\mu)^2 z + 2\pi i\nu(n+\mu)}.$$

For later reference, we note the identities

$$(12)\ \theta\begin{bmatrix} \mu+r \\ \nu \end{bmatrix}(z) = \theta\begin{bmatrix} \mu \\ \nu \end{bmatrix}(z), \qquad \theta\begin{bmatrix} \mu \\ \nu+r \end{bmatrix}(z) = e^{2\pi i\mu r}\theta\begin{bmatrix} \mu \\ \nu \end{bmatrix}(z), \qquad (r\in\mathbb{Z}).$$

For a positive integer N, and a function g modulo N, recall that the (finite) *Fourier Transform* $\hat{g}$ of g is defined by

$$\hat{g}(s) = \sum_{r \bmod N} g(r) e_N(-rs),$$

where $e_N(x) = e^{2\pi ix/N}$. For an integer a relatively prime to N, and functions f, g modulo N, we introduce the (finite) *Wigner Transform* $W_{f,g}^{(a)}$ defined (as a function of pairs of integers modulo N) by

$$W_{f,g}^{(a)}(m,n) = \sum_{r,s \bmod N} f(r)\hat{g}(s) e_N(ars) e_N(ms+nr).$$

(For the classical Wigner transform, see Folland [Fo]). A simple change of variables yields the expression

$$(13)\qquad W_{f,g}^{(a)}(m,n) = N \sum_{r \bmod N} f(r) g(ar+m) e_N(rn).$$

We are now ready to state the promised factorization formula.

Proposition 8. *Suppose a, N are relatively prime positive odd integers, and μ, ν are rational numbers; assume that the denominator of μ is relatively prime to N. For functions f, g modulo N, and $z = x + iy$ in the upper half-plane, we have*

$$\sum_{m,n\in\mathbb{Z}} e^{2\pi i(m\nu+n\mu)} W^{(a)}_{f,g}(m,n) e^{\pi(imn-Q_z(m,n))/aN} =$$
$$N\sqrt{2yaN}\,\theta_g\begin{bmatrix} aN\mu \\ \nu \end{bmatrix}(z/aN)\ \theta_f\begin{bmatrix} N\mu \\ -a\nu \end{bmatrix}(-a\overline{z}/N)\,.$$

Proof. Suppose r, s are integers and that $s\mu \in \mathbb{Z}$. We consider the factorization formula (11) with new parameters $\mu + r/N, \nu + s/N, aN$ in place of μ, ν, a, and multiply both sides by $f(r)\hat{g}(s)e_N(ars)$, then add over r, s modulo N to get

$$\sum_{m,n\in\mathbb{Z}} e^{2\pi i(m\nu+n\mu)} W^{(a)}_{f,g}(m,n) e^{\pi(imn-Q_z(m,n))/aN} =$$
$$\sqrt{2yaN}\sum_{s \bmod N}\hat{g}(s)\ \theta\begin{bmatrix} aN\mu \\ \nu + s/N \end{bmatrix}(z/aN) \sum_{r \bmod N} f(r)\theta\begin{bmatrix} \mu + r/N \\ -aN\nu \end{bmatrix}(-aN\overline{z}).$$

In the first sum on the right hand side of the above equation, we may choose representatives s mod N with $s\mu \in \mathbb{Z}$ since N is prime to the denominator of μ. It remains to simplify the two sums of theta series. First, the sum over s:

$$\begin{aligned}
\sum_{s \bmod N}\hat{g}(s)\theta\begin{bmatrix} aN\mu \\ \nu + s/N \end{bmatrix}(z/aN) &= \sum_{m\in\mathbb{Z}+aN\mu}\ \sum_{s \bmod N}\hat{g}(s)e_N(sm)e^{2\pi i\nu m}e^{\frac{2\pi i m^2 z}{aN}}, \\
&= \sum_{n\in\mathbb{Z}} Ng(n)e^{2\pi i\nu(n+aN\mu)}e^{\frac{\pi i(n+aN\mu)^2 z}{aN}}, \\
&= N\theta_g\begin{bmatrix} aN\mu \\ \nu \end{bmatrix}(z/aN).
\end{aligned}$$

For the sum over r, we write:

$$\sum_{r \bmod N} f(r)\theta\begin{bmatrix} \mu + r/N \\ -aN\nu \end{bmatrix}(-aN\overline{z}) = \sum_{m\in\mathbb{Z}+\mu+r/N} f(r)e^{-2\pi i maN\nu}e^{-\pi i m^2 aN\overline{z}},$$

then make a change of variables

$$m = \mu + n/N, \qquad n \in \mathbb{Z}, n \equiv r \bmod N, \qquad m^2 = \frac{(n+N\mu)^2}{N^2},$$

to get

$$\begin{aligned}
&= \sum_{r \bmod N}\ \sum_{n\equiv r \bmod N} f(n)e^{2\pi i(-a\nu)(n+N\mu)}e^{\pi i(n+N\mu)^2(-a\overline{z}/N)} \\
&= \theta_f\begin{bmatrix} N\mu \\ -a\nu \end{bmatrix}(-a\overline{z}/N).
\end{aligned}$$

This completes the proof. ∎

Proposition 9. *For ideals $\mathfrak{a}, \overline{\mathfrak{a}}_1$ of $\mathcal{O}_K$ relatively prime to $6d$ and to each other,*

$$\Theta_{\mathfrak{a}\mathfrak{a}_1}(3\tau_{\mathfrak{a}}) - \frac{1}{3}\Theta_{\mathfrak{a}\mathfrak{a}_1}(\tau_{\mathfrak{a}}/3) = \frac{2\delta d^{1/4}}{\sqrt{3a_1}}\left(\frac{3}{a}\right)\eta(z_{\mathfrak{a}^2\mathfrak{a}_1})\overline{\eta(z_{\mathfrak{a}_1})}.$$

Proof. We first plug in $\mu = 1/2, \nu = \delta/2,\ f = g = \chi$ into the factorization formula and use the identity

$$\theta_\chi\begin{bmatrix}3r/2\\ s/2\end{bmatrix}(z/3) = 2\delta e^{3\pi i rs/4}\left(\frac{-4}{r}\right)\eta(z), \qquad (r \equiv 1 \bmod 2, s \equiv \delta \bmod 2, z \in \mathcal{H}),$$

which is easily verified using (3), to obtain

$$(16)\qquad \sum_{m,n\in\mathbb{Z}} (-1)^{m\delta+n} W^{(a)}_{\chi,\chi}(m,n)e^{\pi(imn - Q_z(m,n))/3a} = 12\delta\sqrt{6ya}\left(\frac{-4}{a}\right)\eta(z/a)\overline{\eta(az)}.$$

Recall that for $z = x+iy$, $Q_z(m,n) = |mz-n|^2/2y$. We may choose a basis

$$\mathfrak{a}^2\mathfrak{a}_1 = [a^2a_1, (b+\sqrt{-d})/2], \qquad b \in 3d\mathbb{Z}, \qquad b \equiv 1 \bmod 16,$$

and put

$$z = \frac{b+\sqrt{-d}}{2aa_1},$$

so that $a_1 z/d = \tau_{\mathfrak{a}}$, $z/a = z_{\mathfrak{a}^2\mathfrak{a}_1}$, and $az = z_{\mathfrak{a}_1}$. The integer $c = (b^2+d)/4aa_1$ is odd and divisible by a. To simplify the notation, let

$$Q(m,n) = Q_z(m,n)/\sqrt{d} = cm^2 - bmn + aa_1n^2$$

be a quadratic form associated to $\mathfrak{a}\mathfrak{a}_1 = aa_1[1,z]$. Substituting the congruence

$$\pi(imn - Q_z(m,n))/3a \equiv 2\pi i(Q(m,n)\tau_{\mathfrak{a}}/3 + \frac{m\delta+n}{2} - amn/3) \bmod 2\pi i\mathbb{Z}$$

into (16), we find

$$\sum_{m,n\in\mathbb{Z}} W^{(a)}_{\chi,\chi}(m,n)e_3(-amn)e^{2\pi i Q(m,n)\tau_{\mathfrak{a}}/3} = 12\delta d^{1/4}\sqrt{\frac{3}{a_1}}\left(\frac{-4}{a}\right)\eta(z_{\mathfrak{a}^2\mathfrak{a}_1})\overline{\eta(z_{\mathfrak{a}_1})}.$$

It is easy (using (13), say) to verify that

$$\frac{1}{3}W^{(a)}_{\chi,\chi}(m,n)e_3(-amn) = \begin{cases}2\chi(a) & \text{if } m \equiv n \equiv 0 \bmod 3,\\ -\chi(a) & \text{otherwise.}\end{cases}$$

Plugging this into the previous equation yields the result since

$$\Theta_{\mathfrak{a}\mathfrak{a}_1}(3\tau_{\mathfrak{a}}) = \frac{1}{2}\sum_{m,n\in 3\mathbb{Z}} e^{2\pi i Q(m,n)\tau_{\mathfrak{a}}/3}.$$

□

From the transformation properties of the modular form $\Theta_{\mathfrak{a}}(z)$ under homotheties of $\mathfrak{a}$ and under the $\Gamma_0(d)$-action on z, we deduce the following:

Corollary 10. *Suppose* $\mathfrak{a}, \overline{\mathfrak{a}}_1$ *are as in the Proposition, and that* $d \equiv 3 \bmod 8$. *Then,*

$$\left(\frac{-4}{\mathbb{N}\mathfrak{a}}\right)\overline{\phi}(\mathfrak{a})^{-1}\eta(z_{\mathfrak{a}^2\mathfrak{a}_1})$$

depends only the Hecke character ϕ*, the ideal* $\mathfrak{a}_1$ *and the ideal class* $[\mathfrak{a}]$ *of* $\mathfrak{a}$.

When $d \equiv 7 \pmod 8$, i.e. $\delta = 0$, we see from Proposition 9, together with (10) and (9), that each $Z(1, \mathfrak{a})$ vanishes, in particular $L(1, \psi) = 0$. Of course, the latter also follows easily from the calculation of the sign in the functional equation of $L(s, \psi)$ [Gr1, Theorem 19.1.1].

5.3. Proof of Theorem 2. Suppose $d = p > 3$ is $\equiv 3 \bmod 8$. We are finally ready to write $L(1, \psi)$ as a period times the square of a non-zero algebraic integer in M^+.

Proof of Theorem 2. Combining Proposition 9 and Lemma 7, we have

$$L(1, \psi_0\varphi) = \frac{4\pi\kappa}{3^{1/2}p^{1/4}} \sum_{[\mathfrak{a}],[\mathfrak{a}_1]} \frac{(\overline{\varphi\psi_0})(\mathfrak{a})^{-1}}{\sqrt{a_1}} \left(\frac{3}{a}\right) \eta(z_{\mathfrak{a}^2\mathfrak{a}_1})\overline{\eta(z_{\mathfrak{a}_1})}.$$

Since h is odd, every ideal class is representable by a square ideal. Now we change variables twice, first replacing $\mathfrak{a}_1$ by $\mathfrak{a}_1^2$, then replacing $\mathfrak{a}$ by $\mathfrak{a}\mathfrak{a}_1^{-1}$ to get

$$\begin{aligned} L(1, \psi_0\varphi) &= \frac{4\pi\kappa}{3^{1/2}p^{1/4}} \sum_{[\mathfrak{a}],[\mathfrak{a}_1]} (\overline{\varphi\psi_0})(\mathfrak{a})^{-1} \left(\frac{3}{a}\right) \eta(z_{\mathfrak{a}^2}) \frac{(\overline{\varphi\psi_0})(\mathfrak{a}_1)}{a_1} \left(\frac{3}{a_1}\right) \overline{\eta(z_{\mathfrak{a}_1^2})} \\ &= \frac{4\pi\kappa}{3^{1/2}p^{1/4}} \left| \sum_{[\mathfrak{a}]} (\overline{\varphi\psi_0})(\mathfrak{a})^{-1} \left(\frac{-4}{\mathbb{N}\mathfrak{a}}\right) \eta(z_{\mathfrak{a}^2}) \right|^2 \\ &= \frac{4\pi\kappa|\eta(z_{\mathcal{O}})|^2}{3^{1/2}p^{1/4}} \left| \sum_{C\in \mathrm{Cl}_K} u_C^{\varphi} \right|^2. \end{aligned}$$

This completes the proof, since s^{φ} is real. □

Corollary 11. *For* $\psi \in \Psi$, $L(1, \psi) > 0$.

□

6. Tables

In this section, we present the results of numerical calculations in the form of a few tables. In the first table, for primes $3 < p < 3000$, congruent to 3 modulo 8, we list p, h, and $S = \pm\mathbb{N}_{T^+/\mathbb{Q}}(\mathfrak{f})$ (computed via (5)), the square root of the predicted order of $\text{Ш}_{B/\mathbb{Q}}$. Since u_C is a unit, it is immediate from our formula that $A(p)^{-3}$ has trivial predicted Tate-Shafarevich group for the class number one discriminants $-p = -11, -19, -43, -67, -163$. Of the 108 cases listed in table 1, 44 have even S, 39 have S divisible by 3, and 20 have S divisible by 5. None has S divisible by p.

In the second, third and fourth tables, for primes $p \equiv 3 \bmod 8$ such that $\mathbb{Q}(\sqrt{-p})$ has class number $h = 3, 5$, or 7, and such that $\mathcal{R}^+$ is the maximal order $\mathcal{O}_{T^+}$, we list p and $\mathfrak{f}$, the ideal whose square is conjecturally the order ideal of the Tate-Shafarevich group of $B/\mathbb{Q}$. In all cases other than the three detailed in section 4, the $\mathcal{R}^+$-ideal $\mathfrak{f}$ is principal. The notation for these tables is as follows: $\mathfrak{p}_r$ denotes a prime of degree one over the rational prime r, and and $\mathfrak{q}_{r,f}$ denotes a prime of degree $f > 1$ over r. When there is more than one prime of degree 1, respectively of degree $f > 1$, in $\mathcal{R}^+$, we write instead $\mathfrak{p}'_r, \mathfrak{p}''_r, \ldots$, respectively $\mathfrak{q}'_{r,f}, \mathfrak{q}''_{r,f}, \ldots$. In the latter cases, we have not specified exactly which ideals occur in $\mathfrak{f}$, in order to keep the notation from becoming even more cumbersome. Note that primes of degree one are much more prevalent.

Finally, we take this opportunity to make a few remarks on a table (for the curve $A(p)$, $p \equiv 7 \bmod 8$), which appears in [RV]; it was noted in that paper that within the range of calculations ($p < 3000$) the number $\mathcal{S}(p)$ (whose square is the predicted order of $\text{Ш}_{A(p)/F}$) was rarely even, and never divisible exactly by 2. The latter part of this observation is easily explained: it was shown by Gross [Gr1] that $\mathrm{Gal}(H/K)$, a group of odd order, acts non-trivially (indeed without fixed points) on the 2-part of $\text{Ш}_{A(p)/F}$, and this action commutes with the Cassels-Tate pairing. It follows (e.g. from Iwasawa [Iw]) that the 2-rank of $\text{Ш}_{A(p)/F}$, if non-zero, is at least $2f$ where f is the minimum, over prime divisors q of h, of the order of 2 in $(\mathbb{Z}/q\mathbb{Z})^*$. As for the rarity of $\text{Ш}_{A(p)/F}$ of even order, Gross has pointed out that there is heuristic evidence (and we have verified numerically) that the 2-part of this group is trivial if and only if the 2-part of the class group of F is trivial. The Cohen-Lenstra heuristic suggests that the latter should often be the case (again sustained by numerical data [Ha]) since the class group of F is non-cyclic whenever it is not trivial.

p	h	S	$\lvert S\rvert$	p	h	S	$\lvert S\rvert$	p	h	S	$\lvert S\rvert$
11	1	1	1	131	5	-6	$2\cdot 3$	283	3	-11	11
19	1	1	1	139	3	-1	1	307	3	-8	2^3
43	1	1	1	163	1	1	1	331	3	-7	7
59	3	-3	3	179	5	20	$2^2\cdot 5$	347	5	-36	$2^2\cdot 3^2$
67	1	1	1	211	3	3	3	379	3	-13	13
83	3	-5	5	227	5	8	2^3	419	9	2143	2143
107	3	-1	1	251	7	358	$2\cdot 179$	443	5	100	$2^2\cdot 5^2$

p	h	S	$\|S\|$
467	7	44	$2^2 \cdot 11$
491	9	-105	$3 \cdot 5 \cdot 7$
499	3	-9	3^2
523	5	11	11
547	3	12	$2^2 \cdot 3$
563	9	381	$3 \cdot 127$
571	5	-4	2^2
587	7	90	$2 \cdot 3^2 \cdot 5$
619	5	15	$3 \cdot 5$
643	3	13	13
659	11	473	$11 \cdot 43$
683	5	-31	31
691	5	19	19
739	5	4	2^2
787	5	-15	$3 \cdot 5$
811	7	246	$2 \cdot 3 \cdot 41$
827	7	-152	$2^3 \cdot 19$
859	7	289	17^2
883	3	7	7
907	3	25	5^2
947	5	-15	$3 \cdot 5$
971	15	702121	$7^3 \cdot 23 \cdot 89$
1019	13	-176	$2^4 \cdot 11$
1051	5	89	89
1091	17	311264513	$7^2 \cdot 67 \cdot 94811$
1123	5	144	$2^4 \cdot 3^2$
1163	7	166	$2 \cdot 83$
1171	7	-23	23
1187	9	-9354	$2 \cdot 3 \cdot 1559$
1259	15	34101824	$2^6 \cdot 23 \cdot 23167$
1283	11	-207248	$2^4 \cdot 12953$
1291	9	-187	$11 \cdot 17$
1307	11	1739184	$2^4 \cdot 3 \cdot 19 \cdot 1907$
1427	15	-26904385	$5 \cdot 71 \cdot 75787$
1451	13	761379	$3 \cdot 17 \cdot 14929$
1459	11	-74928	$2^4 \cdot 3 \cdot 7 \cdot 223$
1483	7	8	2^3
1499	13	45498	$2 \cdot 3 \cdot 7583$
1523	7	2485	$5 \cdot 7 \cdot 71$
1531	11	-22720	$2^6 \cdot 5 \cdot 71$
1571	17	242697813	$3 \cdot 199 \cdot 223 \cdot 1823$
1579	9	7611	$3 \cdot 43 \cdot 59$
1619	15	-88275739	$29 \cdot 401 \cdot 7591$

p	h	S	$\|S\|$
1627	7	747	$3^2 \cdot 83$
1667	13	9626039	9626039
1699	11	−33342	$2 \cdot 3 \cdot 5557$
1723	5	−175	$5^2 \cdot 7$
1747	5	−190	$2 \cdot 5 \cdot 19$
1787	7	−1942	$2 \cdot 971$
1811	23	−27172020350	$2 \cdot 5^2 \cdot 43 \cdot 12638149$
1867	5	−609	$3 \cdot 7 \cdot 29$
1907	13	303885	$3^3 \cdot 5 \cdot 2251$
1931	21	−119115284992	$2^9 \cdot 11 \cdot 21149731$
1979	23	640380659636	$2^2 \cdot 19 \cdot 491 \cdot 17161021$
1987	7	2307	$3 \cdot 769$
2003	9	−229719	$3 \cdot 7 \cdot 10939$
2011	7	54	$2 \cdot 3^3$
2027	11	144642	$2 \cdot 3 \cdot 24107$
2083	7	−13409	$11 \cdot 23 \cdot 53$
2099	19	39574291187	$83 \cdot 476798689$
2131	13	−4031	$29 \cdot 139$
2179	7	−108	$2^2 \cdot 3^3$
2203	5	−286	$2 \cdot 11 \cdot 13$
2243	15	−12460096	$2^6 \cdot 11^2 \cdot 1609$
2251	7	1008	$2^4 \cdot 3^2 \cdot 7$
2267	11	1598897	1598897
2339	19	−27980957102	$2 \cdot 7 \cdot 523 \cdot 3821491$
2347	5	635	$5 \cdot 127$
2371	13	90441	$3^2 \cdot 13 \cdot 773$
2411	23	−237374573222	$2 \cdot 37 \cdot 1163 \cdot 2758181$
2459	19	96436584	$2^3 \cdot 3^2 \cdot 67 \cdot 19991$
2467	7	72713	$19 \cdot 43 \cdot 89$
2531	17	20814832370	$2 \cdot 5 \cdot 73 \cdot 547 \cdot 52127$
2539	11	24685	$5 \cdot 4937$
2579	21	−6427649341	6427649341
2659	13	371447	371447
2683	5	15	$3 \cdot 5$
2699	15	1378519456	$2^5 \cdot 43 \cdot 1001831$
2707	7	−4901	$13^2 \cdot 29$
2731	11	−1092	$2^2 \cdot 3 \cdot 7 \cdot 13$
2803	9	29181	$3 \cdot 71 \cdot 137$
2819	21	−5427534418429	$23 \cdot 37 \cdot 6377831279$
2843	15	4551355173	$3 \cdot 1517118391$
2851	11	−25563	$3 \cdot 8521$
2939	29	1677457225439091	$3^4 \cdot 31 \cdot 151 \cdot 33937 \cdot 130363$
2963	13	−96843276	$2^2 \cdot 3^6 \cdot 33211$
2971	11	95873	95873

p	$\mathfrak{f}$
59	$\mathfrak{p}_3$
83	$\mathfrak{p}'_5$
139	(1)
211	$\mathfrak{p}_3$
283	$\mathfrak{p}_{11}$
307	$\mathfrak{p}_2'^2 \cdot \mathfrak{p}''_2$
379	$\mathfrak{p}_{13}$
499	$\mathfrak{p}_3^2$
547	$\mathfrak{p}'_2 \cdot \mathfrak{p}''_2 \cdot \mathfrak{p}_3$
883	$\mathfrak{p}_7$
907	$\mathfrak{p}_5'^2$
	$h = 3$

p	$\mathfrak{f}$
131	$\mathfrak{p}_2 \cdot \mathfrak{p}_3$
179	$\mathfrak{p}_2^2 \cdot \mathfrak{p}_5$
227	$\mathfrak{p}_2^3$
523	$\mathfrak{p}'_{11}$
571	$\mathfrak{p}_2^2$
619	$\mathfrak{p}_3 \cdot \mathfrak{p}_5$
683	$\mathfrak{p}_{31}$
691	$\mathfrak{p}'_{19}$
787	$\mathfrak{p}_3 \cdot \mathfrak{p}_5$
947	$\mathfrak{p}_3 \cdot \mathfrak{p}_5$
1747	$\mathfrak{p}_2 \cdot \mathfrak{p}_5 \cdot \mathfrak{p}_{19}$
1867	$\mathfrak{p}_3 \cdot \mathfrak{p}_7 \cdot \mathfrak{p}'_{29}$
2203	$\mathfrak{p}_2 \cdot \mathfrak{p}_{11} \cdot \mathfrak{p}_{13}$
2347	$\mathfrak{p}_5 \cdot \mathfrak{p}_{127}$
2683	$\mathfrak{p}_3 \cdot \mathfrak{p}_5$
	$h = 5$

p	$\mathfrak{f}$
251	$\mathfrak{p}_2 \cdot \mathfrak{p}_{179}$
467	$\mathfrak{p}_2^2 \cdot \mathfrak{p}_{11}$
587	$\mathfrak{p}_2 \cdot \mathfrak{p}_3^2 \cdot \mathfrak{p}_5$
811	$\mathfrak{p}_2 \cdot \mathfrak{p}_3 \cdot \mathfrak{p}_{41}$
827	$\mathfrak{p}_2^3 \cdot \mathfrak{p}_{19}$
859	$\mathfrak{p}_{17}^2$
1171	$\mathfrak{p}_{23}$
1483	$\mathfrak{p}_2^3$
1523	$\mathfrak{p}_5 \cdot \mathfrak{p}_7 \cdot \mathfrak{p}_{71}$
1627	$\mathfrak{p}_3^2 \cdot \mathfrak{p}_{83}$
1787	$\mathfrak{p}_2 \cdot \mathfrak{p}_{971}$
1987	$\mathfrak{p}_3 \cdot \mathfrak{p}_{769}$
2011	$\mathfrak{p}_2 \cdot \mathfrak{q}'_{3,3}$
2083	$\mathfrak{p}_{11} \cdot \mathfrak{p}_{23} \cdot \mathfrak{p}_{53}$
2179	$\mathfrak{p}_2^2 \cdot \mathfrak{p}_3^3$
2251	$\mathfrak{p}_2^4 \cdot \mathfrak{p}_3^2 \cdot \mathfrak{p}_7$
2467	$\mathfrak{p}_{19} \cdot \mathfrak{p}_{43} \cdot \mathfrak{p}_{89}$
3019	$\mathfrak{p}_{15373}$
3067	$\mathfrak{p}_2^4 \cdot \mathfrak{p}_{5683}$
3187	$\mathfrak{p}_2 \cdot \mathfrak{p}_3$
3907	$\mathfrak{p}_2^8 \cdot \mathfrak{p}_3 \cdot \mathfrak{p}_5^2$
4603	$\mathfrak{p}_3^2 \cdot \mathfrak{p}'_{83}$
5107	$\mathfrak{p}_2 \cdot \mathfrak{p}_7^2 \cdot \mathfrak{p}_{673}$
5923	$\mathfrak{p}_{11} \cdot \mathfrak{p}_{14879}$
	$h = 7$

References

[Ar] N. Arthaud, Thesis, Stanford University, 1987.

[B] C. Batut, D. Bernardi, H. Cohen, M. Olivier, GP/PARI Calculator, `ftp://megrez.math.u-bordeaux.fr`.

[BG] J. Buhler and B.H. Gross, *Arithmetic on elliptic curves with complex multiplication II*, Invent. Math. **79** (1985), 11–29.

[CW] J. Coates and A. Wiles, *On the conjecture of Birch and Swinnerton–Dyer*, Invent. Math. **39** (1977), 223–251.

[Fo] G. Folland, *Harmonic analysis in phase space*, Annals of Math Studies **122**, Princeton University Press, Princeton, NJ, 1989.

[Gr1] B.H. Gross, *Arithmetic on elliptic curves with complex multiplication*, Lecture Notes in Mathematics **776**, Springer-Verlag, Berlin-Heidelberg-New York, 1979.

[Gr2] B.H. Gross, *On the conjecture of Birch and Swinnerton–Dyer for elliptic curves with complex multiplication in "Conference on Fermat's Last Theorem"* pp. 219–236, Birkhauser, Boston, 1982.

[Gr3] B.H. Gross, *Minimal models for elliptic curves with complex multiplication*, Compositio Math. **45** (1982), 155–164.

[Ha] F. Hajir, *On the class number of Hilbert class fields*, Pacific J. Math. **181** (1997), 177–189.

[H] F. Hajir, *On units related to the arithmetic of elliptic curves with complex multiplication*, Arch. Math. (Basel) **66** (1995), 280–291.

[HRV] F. Hajir and F. Rodriguez Villegas, *Explicit elliptic units I*, Duke Math. J. **90** (1997), 256–271.

[He] E. Hecke, *Zur Theorie der elliptischen Modulfunktionen*, Math. Ann. **97** (1926), 210–242; also in *Mathematische Werke*, Vandenhoeck & Ruprecht, Göttingen, 1970, §23.

[Iw] K. Iwasawa, *A note on ideal class groups*, Nagoya Math. J. **27** (1966), 239–47.

[Ma] Y. I. Manin, *Cyclotomic fields and modular curves*, Russian Math. Surveys **26** (1971), 7–78.

[Mi] J. S. Milne, *On the arithmetic of abelian varieties*, Invent. Math. **17** (1972), 177–190.

[RV] F. Rodriguez Villegas, *On the square root of special values of certain L-series*, Invent. Math. **106** (1991), 549–573.

[RVY] F. Rodriguez Villegas and T. Yang, *Central values of Hecke L-functions of CM number fields*, preprint.

[RVZ] F. Rodriguez Villegas and D. Zagier, *Square roots of central values of Hecke L-series*, *Advances in Number Theory (Kingston, ON, 1991)*, pp. 81–99, Oxford Sci. Publ., Oxford University Press, New York, 1993.

[Ru1] K. Rubin, *Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton–Dyer*, Invent. Math. **64** (1981), pp. 455–470.

[Ru2] K. Rubin, *The "main conjectures" of Iwasawa theory for imaginary quadratic fields*, Invent. Math. **103** (1991), 25–68.

[Sh] G. Shimura, *On the zeta-function of an abelian variety with complex multiplication*, Ann. of Math. **94** (1971), 504–533.

[dS] B. de Smit, *A differential criterion for complete intersections*, Journées Arithmétiques, Barcelona, 1995, Collect. Math. **48** (1997), 85–96.

Dept. of Mathematics, UCLA, Los Angeles, CA 90095
E-mail address: fhajir@math.ucla.edu

Dept. of Mathematics, California State University, San Marcos, San Marcos, CA 92096
E-mail address: fhajir@csusm.edu

Dept. of Mathematics, Princeton University, Princeton, NJ 08544
E-mail address: villegas@math.princeton.edu

Dept. of Mathematics, University of Texas, Austin, TX 78712
E-mail address: villegas@math.utexas.edu