On the square root of special values of certain L-series.

Rodriguez Villegas, Fernando

pp. 549 - 574

Invent. math. 106, 549–573 (1991)

Inventiones mathematicae

On the square root of special values of certain L-series*

Fernando Rodriguez Villegas
Institute for Advanced Study Princeton, NJ 08540, USA

Oblatum 6-XI-1990

1 Introduction

Our main goal is to prove an explicit formula for the square root of the value at $s = 1$ of L-series associated to particular Hecke characters of an imaginary quadratic field K. In this paper we will prove the formula when the discriminant of K is a prime $p \equiv 7 \bmod 8$; the case of general discriminant, as well as quadratic twists, will be treated in a subsequent paper.

We will then apply this result to study the value at $s = 1$ of the L-series of the elliptic curve $A(p)$, studied by Gross in [4], when $p \equiv 7 \bmod 8$. In this case $A(p)$ has rank zero and so by the Birch-Swinnerton Dyer conjectures the L-series at $s = 1$ divided by appropriate factors should equal the order of the Tate-Shafarevich group of the curve. We will call this conjectural order the predicted order of the Tate-Shafarevich group. Using our main formula we obtain an explicit nonzero rational integer $\mathcal{S}(p)$ whose square is the predicted order of the Tate-Shafarevich group of $A(p)$.

The formula for $\mathcal{S}(p)$ provides an effective way of computing this predicted order. It also includes an intriguing choice of sign. We should recall that if the order of the Tate-Shafarevich group is finite it is known to be a square.

There are two key ingredients in the proof of the main formula. First, a formula of Hecke expressing the partial L-series at $s = 1$ as a sum of values of binary theta functions. This, in fact, is a consequence of Kronecker's limit formulas. Second, a factorization lemma which shows that for certain points in the upper-half plane, the values of the binary theta functions factor, essentially, as the product of values of Jacobi theta functions. Roughly speaking, this factorization exhibits the L-series at $s = 1$ as a sum of h^2 terms (here h is the class number of K), each a product of two factors out of a set of h. This then equals the square of the sum of the h factors.

For the application to $A(p)$ we use the Shimura reciprocity law to get algebraic and Galois properties of the terms involved. A further argument is needed to show

* Partial support for the writing of this paper was provided by NSF grant DMS-8610730

that a possible denominator of 2^{h-1} actually divides the numerator, proving integrality.

Hecke's formula is given in Sect. 2 and the factorization lemma in Sect. 3. We obtain the algebraic and Galois properties mentioned above in Sects. 4 and 5 and the main formula in Sect. 6. Finally, we apply all this to the curve $A(p)$ in Sects. 7 and 8. In Sect. 9 we give the values of $\mathscr{S}(p)$ for primes $p \equiv 7 \bmod 8$ less than 3000.

We should stress that results of the type presented here also follow from the work of J.P. Waldspurger; see [18] and [19]. We should also point out that the factorization lemma mentioned above follows, in a special case, from a somewhat neglected result of Kronecker (see [8, vol. IV, pp. 354–357]). That the Tate-Shafarevich group is finite is now known for a family of elliptic curves; see [7] and [12].

We have programmed our formula in Kida's language Ubasic, which allows fast arbitrary precision calculation for PC's. It compares very favorably to the method used in [1], which we also programmed to check our calculations.

2 Notation, Basic lemmas and Hecke's formula

We let $K = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic field with $d > 3$, squarefree, and $d \equiv 3 \bmod 4$, viewed as a subfield of the complex numbers. We understand by $\sqrt{-d}$ the root with positive imaginary part. Throughout the paper square roots and fourth roots of positive numbers will be chosen positive. For any number field L, $\mathcal{O}_L$ will denote its ring of integers and for any ring R, $R^\times$ will denote its group of units. Note that $\mathcal{O}_K^\times = \{\pm 1\}$ and $-d = \operatorname{disc}(K)$. By ideals we will always understand integral ideals.

For integers $N > 1$ and n we let

$$e_N(n) = e^{2\pi i \frac{n}{N}} .$$

For complex numbers w_1 and w_2, $[w_1, w_2]$ will denote their integral span in $\mathbb{C}$. We will use $\mathscr{H}$ for the upper-half plane, $\mathrm{Cl}(K)$ for the class group of K, and if $\mathscr{A}$ is an ideal, $[\mathscr{A}]$ for its class.

We give now a brief overview of the Hecke characters that we will consider. For more details we refer the reader to [3, 13, 14] and [15]. Although we only prove our final results in the case that d is a prime $p \equiv 7 \bmod 8$, we will carry on with a general d as long as possible. We will indicate at the beginning of each section what generality we assume in it.

The natural ring inclusion $\mathbb{Z} \hookrightarrow \mathcal{O}_K$ defines an isomorphism

$$\mathbb{Z}/d\mathbb{Z} \xrightarrow{\sim} \mathcal{O}_K/\sqrt{-d}\,\mathcal{O}_K .$$

Composing its inverse with the Jacobi symbol $(\bar{\mathrm{d}})$ defines a quadratic character on $\mathcal{O}_K$, which we will denote by ε. Explicitly, we can write any $\mu \in \mathcal{O}_K$ as $\mu = (n + m\sqrt{-d})/2$, with n, m of the same parity, and then

$$\varepsilon(\mu) = \left(\frac{2n}{d}\right) .$$

We now look at the set Ψ of Hecke characters ψ of K, of conductor $(\sqrt{-d})$, that satisfy

$$\psi((\alpha)) = \varepsilon(\alpha)\alpha\ ,$$

for $\alpha \in \mathcal{O}_K$ prime to d. It is not hard to see that the cardinality of Ψ equals h, the class number of K, and that any two ψ, $\psi' \in \Psi$ satisfy

$$\psi/\psi' = \varphi \in \mathrm{Cl}(K)^*$$

where, with some abuse of notation, $\mathrm{Cl}(K)^*$ is the dual group of $\mathrm{Cl}(K)$. We extend ψ to all ideals by setting $\psi(\mathscr{A}) = 0$ if $\mathscr{A}$ is not prime to d. It follows that $\overline{\psi(\mathscr{A})} = \psi(\bar{\mathscr{A}})$ for every $\mathscr{A}$. Each $\psi \in \Psi$ takes values in an extension T_ψ/K of degree h inside the complex numbers.

As usual, we define the L-series associated to $\psi \in \Psi$ by

$$L(s; \psi) = \sum_{\mathscr{A}} \frac{\psi(\mathscr{A})}{\mathbf{N}\mathscr{A}^s}\ ,$$

which converges for $\Re s > \frac{3}{2}$. For any ideal class $C \in \mathrm{Cl}(K)$ we define the partial L-series to be

$$L(s; \psi, C) = \sum_{\mathscr{A} \in C} \frac{\psi(\mathscr{A})}{\mathbf{N}\mathscr{A}^s}\ .$$

We clearly have

$$L(s; \psi) = \sum_{C \in \mathrm{Cl(K)}} L(s; \psi, C)\ .$$

Also, it is easy to see that if $\mathscr{A} \in C^{-1}$ is an ideal prime to d, then

$$L(s; \psi, C) = \frac{\mathbf{N}\mathscr{A}^s}{2\psi(\mathscr{A})} \sum_{\gamma \in \mathscr{A}} \frac{\varepsilon(\gamma)\gamma}{\mathbf{N}\gamma^s}\ .$$

These partial L-series can be analytically continued to the whole s-plane, and satisfy a functional equation. Our main interest is in their value at $s = 1$. The starting point will be the formula due to Hecke given below (Theorem 2.6). As opposed to Manin's approach using the functional equations (see [10, Theorem 9.3]), following Hecke, we get values of weight one theta series rather than integrals of weight two theta series. This was also the approach taken by Rohrlich in [11].

Before stating this formula, let us give two lemmas which we will use often; we omit their (simple) proofs.

Definition 2.1 For any ideal $\mathscr{F}$ we let

$$\mathscr{R}_{\mathscr{F}} = \{\text{primitive ideals prime to } \mathscr{F}\}$$

(Primitive means not divisible by rational integers > 1).

When $\mathscr{F} = \mathcal{O}_K$ we will just write $\mathscr{R}$, which then corresponds to the set of all primitive ideals.

Lemma 2.2 *If $\mathscr{A} \in \mathscr{R}$, then $\bar{\mathscr{A}} \in \mathscr{R}$, and we can write*

$$\mathscr{A} = \left[a, \frac{b + \sqrt{-d}}{2}\right]$$

and

$$\bar{\mathscr{A}} = \left[a, \frac{-b + \sqrt{-d}}{2}\right],$$

where $a = \mathbf{N}\mathscr{A} = \mathbf{N}\bar{\mathscr{A}}$ and b is an integer (determined $\bmod 2a$*) which satisfies*

$$b^2 \equiv -d \bmod 4a\,.$$

Conversely, given a solution b to this congruence and defining $\mathscr{A}$ by the above formula we get an ideal in $\mathscr{R}$ with norm a.

Lemma 2.3 *Assume $\bar{\mathscr{F}} = \mathscr{F}$. If $\mathscr{A}_1$, $\mathscr{A}_2 \in \mathscr{R}_{\mathscr{F}}$ are relatively prime, then $\mathscr{A}_1\mathscr{A}_2 \in \mathscr{R}_{\mathscr{F}}$. In particular, if $\mathscr{A} \in \mathscr{R}_{\mathscr{F}}$ and $(\sqrt{-d})$ divides $\mathscr{F}$, then $\mathscr{A}^n \in \mathscr{R}_{\mathscr{F}}$ for every positive integer n.*

Furthermore, if

$$\mathscr{A}_i = \left[a_i, \frac{b_i + \sqrt{-d}}{2}\right], \quad i = 1, 2\,,$$

then

$$\mathscr{A}_1\mathscr{A}_2 = \left[a, \frac{b + \sqrt{-d}}{2}\right],$$

with $a = a_1 a_2$ and some $b \equiv b_i \bmod 2a_i$, $i = 1, 2$.

Let us also note that for any ideal $\mathscr{F}$ and any class $C \in \mathrm{Cl}(K)$, $\mathscr{R}_{\mathscr{F}} \cap C$ is nonempty.

For any class $C' \in \mathrm{Cl}(K)$, we let

$$\theta_{C'}(\tau) = \sum_{\mu \in \mathscr{A}'} q^{\mathbf{N}\mu/a'}, \quad q = e^{2\pi i \tau}\,,$$

where $\mathscr{A}' \in C'^{-1}$ and $a' = \mathbf{N}\mathscr{A}'$. It is easy to see that this definition is independent of the choice of ideal. It is known that this theta series is a modular form of weight one, level d and character $(\bar{\mathrm{d}})$ (see [6, pp. 442–447], for example).

Definition 2.4 Given classes $C, C' \in \mathrm{Cl}(K)$ and $\psi \in \Psi$ we take an ideal $\mathscr{A} \in \mathscr{R}_d \cap C^{-1}$ and we define

$$\theta_{C'}(\psi, C) = \theta_{C'}(\tau)/\psi(\mathscr{A})\,,$$

where

$$(\sqrt{-d})\mathscr{A} = \left[ad, \frac{\check{b}d + \sqrt{-d}}{2}\right]$$

for some integer $\check{b}$ (by Lemmas 2.2 and 2.3), and

$$\tau = \frac{-\check{b}d + \sqrt{-d}}{2ad}\,.$$

Lemma 2.5 $\theta_{C'}(\psi, C)$ *is well defined.*

Proof. The proof hinges on the modular property of $\theta_{C'}$; in fact, the corresponding result is true for any such modular form. We will prove it first for relatively prime ideals $\mathscr{A}$, $\mathscr{A}' \in \mathscr{R}_d$ that satisfy

$$\mathscr{A}'\bar{\mathscr{A}} = (\mu)$$

for some $\mu \in \bar{\mathscr{A}}$. We let $\tau = \dfrac{-\check{b}d + \sqrt{-d}}{2ad}$. It is not hard to see that $\mu/a = \gamma\tau + \delta$, for some nonzero integers γ and δ, with d dividing γ. By Lemma 2.3, γ and δ must be relatively prime. Also,

$$\varepsilon(\mu) = \left(\frac{\delta}{d}\right).$$

Choose integers α and β such that $\alpha\delta - \beta\gamma = 1$ and let $\tau' = \dfrac{\alpha\tau + \beta}{\gamma\tau + \delta}$. It is straightforward to check that

$$\tau' = \frac{-\check{b}'d + \sqrt{-d}}{2a'd}\,,$$

where $a' = \mathrm{N}\mathscr{A}'$ and $\check{b}'$ is such that

$$(\sqrt{-d})\mathscr{A}' = \left[a'd, \frac{\check{b}'d + \sqrt{-d}}{2}\right].$$

The claim now follows from the modularity of $\theta_{C'}$.

To prove the general case, given $\mathscr{A}, \mathscr{A}' \in \mathscr{R}_d \cap C^{-1}$ choose a third ideal $\mathscr{B} \in \mathscr{R}_d \cap C^{-1}$, prime to the norm of $\mathscr{A}\mathscr{A}'$, and apply the previous case to the pairs $\mathscr{A}$, $\mathscr{B}$ and $\mathscr{A}'$, $\mathscr{B}$. This proves the lemma. □

Now we can state the promised formula for the value of the L-series at $s = 1$.

Theorem 2.6 (Hecke's formula) *For any* $C \in \mathrm{Cl}(K)$ *and any* $\psi \in \Psi$,

$$L(1; \psi, C) = \left(\frac{2}{d}\right)\frac{\pi}{\sqrt{d}} \sum_{C' \in \mathrm{Cl}(K)} \theta_{C'}(\psi, C)\,.$$

Proof. See Hecke [6, pp. 450–455]. □

3 Factorization lemma

In this section we prove a crucial factorization of the value of the weight one theta series in Hecke's formula, as the product of two values of weight one-half theta series and a constant.

We set up the notation for the lemma as follows: Let $C_1, C_2 \in \mathrm{Cl}(K)$. We choose ideals $\mathscr{A}_i \in \mathscr{R}_{2d} \cap C_i^{-1}$ for $i = 1, 2$ such that their norms $a_i = \mathrm{N}\mathscr{A}_i$ are relatively prime. It is not hard to see that this is always possible. We let $a = a_1 a_2$. By Lemmas 2.2 and 2.3 we can find odd integers b, b^* and $\check{b}$ such that

$$\mathscr{A}_i = \left[a_i, \frac{b + \sqrt{-d}}{2}\right], \quad i = 1, 2$$

$$\mathscr{A}_1 \mathscr{A}_2 = \left[a, \frac{b + \sqrt{-d}}{2}\right]$$

$$\bar{\mathscr{A}}_1 \mathscr{A}_2 = \left[a, \frac{b^* + \sqrt{-d}}{2}\right]$$

$$(\sqrt{-d})\mathscr{A}_2 = \left[a_2 d, \frac{\check{b}d + \sqrt{-d}}{2}\right],$$

where

$$b^* \equiv -b \bmod 2a_1$$

$$b^* \equiv b \bmod 2a_2$$

$$\check{b}b \equiv -1 \bmod 2a\,.$$

Finally, recall that we defined

$$\theta_{C_1}(\tau) = \sum_{\mu \in \mathscr{A}_1} q^{\mathrm{N}\mu/a_1}, \quad q = e^{2\pi i \tau},$$

and further let

$$\theta_{10}(\tau) = \sum_{k\,\mathrm{odd}} e^{(\pi i k^2/4)\tau},$$

one of the classical Jacobi theta functions (in Weber's notation, see [20]).

Lemma 3.1 (Factorization lemma)

$$\theta_{C_1}\left(\frac{-\check{b}d + \sqrt{-d}}{2a_2 d}\right) = \frac{1}{2}\left(1 + \left(\frac{2}{d}\right)\right)\frac{\sqrt[4]{-d}}{\sqrt{a_1}}\zeta \cdot \theta_{10}\left(\frac{-b^* + \sqrt{-d}}{2a}\right) \cdot \theta_{10}\left(\frac{-b + \sqrt{-d}}{2a}\right).$$

Here ζ is a 16th root of unity given explicitly by

$$\zeta = e_{16}(ab) e_{16}(ab^*) \left(\frac{2ba_1}{a_2}\right) \varepsilon_{a_2}$$

where

$$\varepsilon_n = \begin{cases} 1 & \textit{if } n \equiv 1 \bmod 4 \\ i & \text{if } n \equiv 3 \bmod 4. \end{cases}$$

Remark. Note that ζ is actually an 8th root of unity.

Proof. We let $k = 2a_1 n + bm$; this gives a bijection

$$\{m, n \in \mathbb{Z}\} \leftrightarrow \{k, m \in \mathbb{Z} : k \equiv bm \bmod 2a_1\} .$$

Therefore

$$\theta_{C_1}(\tau) = \sum_{k \equiv bm \bmod 2a_1} e^{2\pi i(k^2 + dm^2/4a_1)\tau} .$$

Now let $\tau = (-\check{b}d + \sqrt{-d})/2a_2 d$. Then

$$\theta_{C_1}\left(\frac{-\check{b}d + \sqrt{-d}}{2a_2 d}\right) = \sum_{k \equiv bm \bmod 2a_1} e_{2a}\left(-\check{b}\left(\frac{k^2 + dm^2}{4}\right)\right) e^{-\pi(k^2 + dm^2/4a)\, 1/\sqrt{d}} .$$

We will break the sum in two, according to the parity of k and m (recall that b is odd so k and m have the same parity). We will give the details only in the case in which they are even; the other case is entirely analogous.

It will be convenient to introduce the following notation. For relatively prime integers M, N we let M' be an integer (determined $\bmod N$) such that $M'M \equiv 1 \bmod N$. We will only use M' as an argument in various functions of period N, and therefore we will not need to indicate its dependence on N. It is easy now to verify the next lemma.

Lemma 3.2 *For relatively prime integers M, N*

$$e_N(M'n)\, e_M(N'n) = e_{MN}(n)$$

for every integer n.

Assume then that k and m are even. Writing k, m for $k/2$, $m/2$ we get

$$\sum_{k \equiv bm \bmod a_1} e_{2a}(-\check{b}(k^2 + dm^2)) e^{-\pi(k^2 + dm^2/a)\, 1/\sqrt{d}} =$$

$$\sum_{k \equiv bm \bmod a_1} e_a(-\check{b}(k^2 + dm^2)2')(-1)^{k+m} e^{-\pi(k^2 + dm^2/a)\, 1/\sqrt{d}}$$

by Lemma 3.2. We now replace the congruence condition on k and m by the sum

$$\frac{1}{a_1} \sum_{j \bmod a_1} e_{a_1}(jk)\, e_{a_1}(-bjm) ,$$

and factor the k and m terms for each j to obtain

$$\frac{1}{a_1} \sum_{j \bmod a_1} A_j B_j ,$$

where

$$A_j = \sum_k e_{a_1}(jk)\, e_a(-\check{b}k^2 2')(-1)^k e^{-\pi(k^2/a)\, 1/\sqrt{d}}$$

and

$$B_j = \sum_m e_{a_1}(-bjm)e_a(-bm^2 2')(-1)^m e^{-\pi(m^2/a)\sqrt{d}} .$$

Here we have used the fact that $b^2 \equiv -d \bmod a$. We now apply the following lemma, a direct consequence of the Poisson summation formula, to A_j.

Lemma 3.3 *Let $f:\mathbb{Z} \to \mathbb{C}$ be periodic with period $N > 1$, N odd; i.e., $f(n+N) = f(n)$, for all $n \in \mathbb{Z}$. Then for $t > 0$ we have*

$$\sum_k f(k)(-1)^k e^{-\pi(k^2/N)t} = t^{-1/2} \sum_{k\,\mathrm{odd}} \hat{f}(k2')e^{-\pi(k^2/4N)\,1/t} ,$$

where

$$\hat{f}(k) = \frac{1}{\sqrt{N}} \sum_{j \bmod N} f(j)e_N(jk)$$

is the Fourier transform $\bmod N$.

In our case we have

$$f(k) = e_a(ja_2k - \check{b}2'k^2)$$

and $N = a$. Using the known values of Gauss sums we get

$$\hat{f}(k) = \left(\frac{2b}{a}\right)\varepsilon_a e_a(-2'b(a_2j + k)^2) .$$

Using Lemma 3.3 and interchanging sums, we get, after some calculation,

$$C \cdot \sum_{k\,\mathrm{odd},\, m\,\mathrm{even}} e_{a_1}((8a_2)'b(k+m)^2)e_a(-8'b(m^2+k^2))(-1)^{m/2} e^{-\pi(k^2+m^2/4a)\sqrt{d}}$$

where, again using the known values of Gauss sums,

$$C = \frac{\sqrt[4]{d}}{\sqrt{a_1}}\left(\frac{2b}{a_2}\right)\left(\frac{-a_2}{a_1}\right)\varepsilon_a\varepsilon_{a_1} .$$

Now we do a change of variables via

$$\begin{cases} m = \dfrac{u-v}{2} \\ k = \dfrac{u+v}{2} . \end{cases}$$

This establishes a bijection

$$\{m, k \in \mathbb{Z} : m \text{ even, } k \text{ odd}\} \leftrightarrow \{u, v \in \mathbb{Z} : uv = 1 \bmod 4\}$$

with $k + m = u$, and $m^2 + k^2 = \dfrac{u^2 + v^2}{2}$.

Hence our series can be written as

$$2C\cdot \sum_{u,v\,\equiv\,1 \bmod 4} e_{a_1}((8a_2)' bu^2)e_a(-16'b(u^2+v^2))(-1)^{u-v/4}e^{-\pi(u^2+v^2/8a)\sqrt{d}}$$

(noting that the sum over $u, v \equiv -1 \bmod 4$ gives the same value). Next, we factor the series again to get $2C\cdot A\cdot B$, with

$$A = \sum_{u\,\equiv\,1 \bmod 4} e_{a_1}((8a_2)' bu^2)e_a(-16'bu^2)e_8(u)e^{-\pi(u^2/8a)\sqrt{d}}$$

and

$$B = \sum_{v\,\equiv\,1 \bmod 4} e_a(-16'bv^2)e_8(-v)e^{-\pi(v^2/8a)\sqrt{d}}\,.$$

Notice that

$$e_{a_1}((8a_2)'bu^2)e_a(-16'bu^2) = e_a(-16'b^*u^2)\,,$$

since by definition

$$b^* \equiv -b \bmod 2a_1$$

$$b^* \equiv b \bmod 2a_2\,.$$

Therefore,

$$A = \sum_{u\,\equiv\,1 \bmod 4} e_a(-16'b^*u^2)e_8(u)e^{-\pi(v^2/8a)\sqrt{d}}\,.$$

Now, by Lemma 3.2,

$$e_a(-16'b^*u^2) = e_{16a}(-b^*u^2)e_{16}(a'b^*u^2)\,,$$

and similarly

$$e_a(-16'bv^2) = e_{16a}(-bv^2)e_{16}(a'bv^2)\,.$$

Using the known expression for the symbol $\left(\frac{2}{a}\right)$ we get

$$e_{16}(-a'b^*u^2)e_8(u) = e_{16}(ab^*)e_8(1)\left(\frac{2}{a}\right)$$

and

$$e_{16}(-a'bv^2)e_8(-v) = e_{16}(ab)e_8(-1)\left(\frac{2}{a}\right).$$

Finally, using the identity

$$\sum_{n\ \mathrm{odd}} e^{\pi i(n^2/4)\tau} = 2\sum_{n\,\equiv\,1 \bmod 4} e^{\pi i(n^2/4)\tau}\,,$$

we arrive at

$$\frac{1}{2}\frac{\sqrt[4]{d}}{\sqrt{a_1}}\zeta\cdot\theta_{10}\left(\frac{-b^*+\sqrt{-d}}{2a}\right)\theta_{10}\left(\frac{-b+\sqrt{-d}}{2a}\right).$$

This completes the case where k, m are even. As we mentioned above, the calculations for k, m odd are similar, yielding the same term times $\left(\frac{2}{m}\right)$. This finishes the proof of the factorization lemma. □

Corollary 3.4 *For $d \equiv 3 \bmod 8$ and any $\psi \in \Psi$ we have*

$$L(1; \psi, C) = 0,$$

and consequently

$$L(1; \psi) = 0\,.$$

Proof. It follows immediately from the factorization lemma just proved and Hecke's formula (Theorem 2.6). □

Remark. The last statement also follows easily from the fact, proved by Gross in [3, Theorem 19.1.1], that the sign in the functional equation for $L(s; \psi)$ is $\left(\frac{2}{d}\right)$.

4 Definition of the invariants *s* and *t*

In this section we assume that $d \equiv 7 \bmod 8$ and $d \not\equiv 0 \bmod 3$. We will define complex numbers $s(\psi, C)$ and $t(\psi, C)$, for each $C \in \mathrm{Cl}(K)$ and $\psi \in \Psi$, using values of Dedekind's eta function and the classical Jacobi theta function θ_{10}, respectively. They will be related to the right hand side of the factorization lemma (Lemma 3.1). Some important properties of these numbers are given in the next section.

Definition 4.1 Given a class $C \in \mathrm{Cl}(K)$ we take an ideal $\mathscr{A} \in \mathscr{R}_{6d} \cap C^{-1}$, and we define

$$s(\psi, C) = e_{48}(\tilde{b})\eta(\tilde{\tau})/\psi(\mathscr{A})$$

and

$$t(\psi, C) = e_{16}(\tilde{b})\theta_{10}(\tilde{\tau})/\psi(\mathscr{A})\,,$$

where

$$\mathscr{A}^2 = \left[a^2, \frac{\tilde{b}+\sqrt{-d}}{2}\right]$$

for some integer $\tilde{b}$ (by Lemmas 2.2 and 2.3),

$$\tilde{\tau} = \frac{-\tilde{b}+\sqrt{-d}}{2a^2}\,,$$

$$\eta(\tau) = e^{(\pi i/12)\tau}\prod_{n \geqq 1}(1-q^n), \quad q = e^{2\pi i\tau}\,,$$

and

$$\theta_{10}(\tau) = \sum_{n\,\mathrm{odd}} e^{(\pi i n^2/4)\tau}, \quad \tau \in \mathscr{H} ,$$

Note that the definitions do not depend on the choice of $\tilde{b}$ since

$$\eta(\tau + 1) = e_{24}(1)\eta(\tau) ,$$

and

$$\theta_{10}(\tau + 1) = e_8(1)\theta_{10}(\tau) .$$

We will spend the rest of this section proving that the roots of unity by which η and θ_{10} change (8th and 24th roots of unity, respectively) are under control.

Proposition 4.2 *$s(\psi, C)$ and $t(\psi, C)$ are well defined.*

Proof. As in the proof of Lemma 2.5, we will show later that it suffices to prove that the definition agrees on relatively prime ideals $\mathscr{A}, \mathscr{A}' \in \mathscr{R}_{6d}$ that satisfy

$$\mathscr{A}'\bar{\mathscr{A}} = (\mu)$$

for some $\mu \in \bar{\mathscr{A}}$. In that case we choose μ so that $\Re\mu > 0$; this is possible because μ is prime to $\sqrt{-d}$.

The idea of the proof is that $\tilde{\tau}$ and $\tilde{\tau}'$, corresponding to $\mathscr{A}$ and $\mathscr{A}'$ respectively, are related by an element of $\mathrm{Sl}_2(\mathbb{Z})$ with controlled behaviour modulo 24. We can then apply the transformation formulas for η and θ_{10} to relate their corresponding values. Roughly speaking, s and t as functions of $\mathscr{A}$ have weight zero: η and θ_{10} have weight one-half, $\mathscr{A}$ appears squared, so the total weight of the numerator is one, and ψ also has weight one. The crucial point is the computation of the quadratic symbol $\left(\frac{\gamma}{\delta}\right)$ (see below), which we will do in detail; we leave other computations to the reader.

Fix C and ψ. Let $a = \mathrm{N}\mathscr{A}$ and $a' = \mathrm{N}\mathscr{A}'$. By Lemmas 2.2 and 2.3, $(\mu) \in \mathscr{R}_{6d}$ and

$$\mathscr{A} = \left[a, \frac{b + \sqrt{-d}}{2}\right]$$

for some integer b. Note that $d \equiv 3 \bmod 4$ implies that b must be odd; also, a is relatively prime to $2d$. Since $\mu \in \bar{\mathscr{A}}$, we get that $\mu = m\frac{1}{2}(-b + \sqrt{-d}) + na$ for some integers m and n, which must be relatively prime because (μ) is primitive. Let $c = (b^2 + d)/4a$. It follows from $d \equiv 7 \bmod 8$ that c is even, m is even and n is odd.

Also note that a, b are relatively prime since a is relatively prime to d and $b^2 - 4ac = d$. It follows from Lemma 2.3 that $\tilde{b} = b + 2ar$ for some integer r, with $br \equiv -c \bmod a$. It is now a straightforward, if tedious, calculation to show that

$$\mu^2 = a^2(\gamma\tilde{\tau} + \delta)$$

where

$$\begin{cases} \gamma = (2an - mb)m \\ \delta = n^2 + 2rnm - m^2(br + c)/a \end{cases} \qquad (1)$$

We can clearly choose b and r so that $\tilde{b} \equiv 0 \bmod 3$ and $\delta > 0$. We fix one such choice for the rest of this proof; it will simplify matters when using the transformation formulas.

By Lemma 2.3, (μ^2) is primitive so γ and δ must be relatively prime. Observe that $(\gamma, \delta) \equiv (0, 1) \bmod 8$. It is not hard to verify that modulo 3 there are two possibilities: (i) $\mu^2 \equiv \pm 1 \bmod 3$ or (ii) $\mu^2 \equiv \pm\sqrt{-d} \bmod 3$. (Recall that we assumed $d \not\equiv 0 \bmod 3$.) It follows that: (i) $(\gamma, \delta) \equiv (0, \pm 1) \bmod 3$ or (ii) $(\gamma, \delta) \equiv (\pm 1, 0) \bmod 3$.

We can therefore find integers α and β such that $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{Sl}_2(\mathbb{Z})$, with $M \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod 8$, and either $M \equiv \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix} \bmod 3$ in case (i) or $M \equiv \begin{pmatrix} 0 & \mp 1 \\ \pm 1 & 0 \end{pmatrix} \bmod 3$ in case (ii). Finally, let

$$\tilde{\tau}' = \frac{\alpha\tilde{\tau} + \beta}{\gamma\tilde{\tau} + \delta}.$$

We leave to the reader to verify that

$$\mathscr{A}'^2 = \left[a'^2, \frac{-\tilde{b}' + \sqrt{-d}}{2}\right]$$

and

$$\tilde{\tau}' = \frac{-\tilde{b}' + \sqrt{-d}}{2a'^2},$$

where

$$\begin{cases} \tilde{c} = (\tilde{b}^2 + d)/4a^2 \\ a'^2 = \tilde{c}\gamma^2 - \tilde{b}\gamma\delta + a^2\delta^2 \\ \tilde{b}' = (1 + 2\beta\gamma)\tilde{b} - 2(\alpha\gamma\tilde{c} + \beta\delta a^2) \ . \end{cases} \tag{2}$$

Notice that $\tilde{b}' \equiv \tilde{b} \bmod 16$ and also $\tilde{b}' \equiv 0 \bmod 3$ in both cases (i) and (ii).

We are now ready to use the transformation formulas.

Theorem 4.3 *Let* $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{Sl}_2(\mathbb{Z})$ *with* γ *even,* δ *positive (and odd), and* $\tau \in \mathscr{H}$. *Then*

$$\eta\left(\frac{\alpha\tau + \beta}{\gamma\tau + \delta}\right) = \left(\frac{\gamma}{\delta}\right) e_{24}(\kappa)\sqrt{\gamma\tau + \delta}\,\eta(\tau)$$

and

$$\theta_{10}\left(\frac{\alpha\tau + \beta}{\gamma\tau + \delta}\right) = \left(\frac{\gamma}{\delta}\right) e_8(\rho)\sqrt{\gamma\tau + \delta}\,\theta_{10}(\tau),$$

where

$$\kappa = 3(\delta - 1) + \delta(\beta - \gamma) - (\delta^2 - 1)\gamma\alpha$$

and

$$\rho = \delta - 1 + \delta\beta .$$

Here the square root is the usual branch with non-negative real part, and $\left(\frac{\gamma}{\delta}\right)$ is the usual Jacobi symbol, where it is understood that $(\frac{0}{1}) = +1$.

Proof. See [20, pp. 126, 131]. We have modified the notation slightly. □

Applying this theorem to our situation, we see that $\rho \equiv 0 \bmod 8$ and $\kappa \equiv 0 \bmod 24$ in every case. Also $\sqrt{\gamma\tilde{\tau} + \delta} = \mu/a$ because we have chosen $\Re\mu > 0$. We then have

$$ae_{48}(\tilde{b}')\eta(\tilde{\tau}') = \left(\frac{\gamma}{\delta}\right)\mu e_{48}(\tilde{b})\eta(\tilde{\tau})$$

and

$$ae_{16}(\tilde{b}')\theta_{10}(\tilde{\tau}') = \left(\frac{\gamma}{\delta}\right)\mu e_{16}(\tilde{b})\theta_{10}(\tilde{\tau}) .$$

Combining this with properties of ψ we see that

$$e_{48}(\tilde{b})\eta(\tilde{\tau})/\psi(\mathscr{A}) = \left(\frac{\gamma}{\delta}\right)\varepsilon(\mu)e_{48}(\tilde{b}')\eta(\tilde{\tau}')/\psi(\mathscr{A}')$$

and

$$e_{16}(\tilde{b})\theta_{10}(\tilde{\tau})/\psi(\mathscr{A}) = \left(\frac{\gamma}{\delta}\right)\varepsilon(\mu)e_{16}(\tilde{b}')\theta_{10}(\tilde{\tau}')/\psi(\mathscr{A}') .$$

Recall that ε is the quadratic character on $\mathcal{O}_K$ defined in Sect. 2. It satisfies $\psi((\mu)) = \varepsilon(\mu)\mu$.

As we said above, this is now the crucial point: we must prove that both signs cancel out. That is, we have to prove the identity

$$\varepsilon(\mu) = \left(\frac{\gamma}{\delta}\right) .$$

For this, let $m = 2^l m'$ with m' odd. Then by (1),

$$\left(\frac{\gamma}{\delta}\right) = \left(\frac{2an - mb}{\delta}\right)\left(\frac{2}{\delta}\right)^l\left(\frac{m'}{\delta}\right) .$$

Now $\left(\frac{2}{\delta}\right)^l = +1$ since $\delta \equiv 1 \bmod 8$. Also $\delta \equiv n^2 \bmod m'$; so by the quadratic reciprocity law $\left(\frac{m'}{\delta}\right) = +1$. Notice that $2\Re\mu = 2an - mb$, and therefore

$$\varepsilon(\mu) = \left(\frac{2an - mb}{d}\right)$$

$\left(\text{recall that } d \equiv 7 \bmod 8, \text{ so } \left(\frac{2}{d}\right) = +1\right)$. Hence, it remains to prove that

$$\left(\frac{2an - mb}{\delta}\right) = \left(\frac{2an - mb}{d}\right).$$

It follows from (1), after a short calculation, that

$$4a^2\delta = -dm^2 + (2an - mb)(4arm + 2an + mb).$$

Again, write $2an - mb = 2^l k$, where k is odd (and positive because of our choice of μ). By the quadratic reciprocity law we obtain

$$\left(\frac{2an - mb}{\delta}\right) = \left(\frac{\delta}{k}\right),$$

and therefore

$$\left(\frac{\delta}{k}\right) = \left(\frac{4a^2\delta}{k}\right) = \left(\frac{-d}{k}\right)$$

(notice that $2a$ is relatively prime to k).

Similarly,

$$\left(\frac{2an - mb}{d}\right) = \left(\frac{-d}{k}\right)$$

and we are done.

It remains to reduce the general case to the one just proved. Let then, $\mathscr{A}$, $\mathscr{A}' \in \mathscr{R}_{6d} \cap C^{-1}$. We can choose a third ideal $\mathscr{B} \in \mathscr{R}_{6d} \cap C^{-1}$ prime to the norm of $\mathscr{A}\mathscr{A}'$ and now apply the above case to the pairs $\mathscr{A}$, $\mathscr{B}$ and $\mathscr{A}'$, $\mathscr{B}$. This completes the proof of the proposition. □

5 Properties of s and t

In this section we assume that d is a prime $p \equiv 7 \bmod 8$. To simplify our notation we chose a character $\psi_0 \in \Psi$, which we keep fixed for the rest of the paper, and we drop the dependence on ψ from our notations, as follows.

$$\theta_{C'}(C) = \theta_{C'}(\psi_0, C)$$

$$s(C) = s(\psi_0, C)$$

$$t(C) = t(\psi_0, C).$$

Notice that $\Psi = \{\varphi\psi_0 : \varphi \in \mathrm{Cl}(K)^*\}$ and that for $\psi = \varphi\psi_0$ we have

$$\theta_{C'}(\psi, C) = \varphi(C)\theta_{C'}(C)$$

$$s(\psi, C) = \varphi(C)s(C)$$

$$t(\psi, C) = \varphi(C)t(C).$$

We also write

$$L(\varphi, C) = L(1; \varphi\psi_0, C)$$

and

$$L(\varphi) = L(1; \varphi\psi_0) .$$

Note that

$$L(\varphi'\varphi, C) = \varphi'(C) L(\varphi, C) .$$

Finally let $T = T_{\psi_0}$ be the extension of K in the complex numbers generated by the values of ψ_0.

Let now $j = j((1 + \sqrt{-p})/2)$ where $j(\tau)$ is the classical modular function. It is easy to check that j is real. Let $F = \mathbb{Q}(j)$. We have then that $F/\mathbb{Q}$ is an extension of degree h with a fixed embedding in the real numbers, and $H = FK$ is the Hilbert class field of K (see [9]).

Let $M = TH$. The above choices fix an embedding of $M/\mathbb{Q}$ in $\mathbb{C}$. We let $M^+ = M \cap \mathbb{R}$. It is not hard to see that $T \cap H = K$ (see [1]). We may therefore identify $\mathrm{Cl}(K)^*$ with the embeddings of M/H in $\mathbb{C}$, the trivial character corresponding to our fixed embedding. We will use the same letter φ to denote the embedding corresponding to $\varphi \in \mathrm{Cl}(K)^*$. Also, we may identify $\mathrm{Gal}(M/T)$ with $\mathrm{Cl}(K)$ via the Artin map. For a class $C \in \mathrm{Cl}(K)$ we denote the corresponding automorphism by σ_C.

We now summarize all the properties of the invariants s and t that we will need.

Proposition 5.1 (i) *$s(C)$ and $t(C)$ are nonzero for every class C.*
(ii) *$\overline{s(C)} = s(C^{-1})$ and $\overline{t(C)} = t(C^{-1})$.*

Proof. Part (i) follows from the fact that neither η nor θ_{10} vanish on the upper-half plane. Part (ii) is an easy consequence of the definitions. □

Definition 5.2 Let C_0 denote the principal class. For every class C we define

$$u_C = s(C)/s(C_0)$$

and

$$v_C = t(C)/t(C_0) .$$

Note that by the above Proposition u_C and v_C are well defined.

Theorem 5.3 (i) *u_C is a unit in M.*

(ii) *For any C, C' and φ,*

$$\begin{cases} \overline{u_C} = u_{C^{-1}} \\ u_C^{\varphi} = \varphi(C) u_C \\ u_C u_{C'}^{\sigma_C {}^2} = u_{CC'} \ . \end{cases}$$

(iii) *Consider the elements $\xi = 1 - 2\sigma_D$ and $\bar{\xi} = 1 - 2\sigma_{D^{-1}}$ of the group ring $\mathbb{Z}[\mathrm{Gal}(M/T)]$, where $D = [\mathcal{Q}]$ and $\mathcal{Q} = [2, (1 + \sqrt{-p})/2]$ is one of the primes of K above 2. Then for every class C*

$$v_C = u_C^{\xi\bar{\xi}} .$$

(iv) *Properties* (i) *and* (ii) *also hold for* v_C.

(v) *The map*

$$\mathrm{Cl}(K) \to (\mathcal{O}_M/2\mathcal{O}_M)^\times$$
$$C \mapsto v_C$$

is a homomorphism.

Remark. The units u_C and v_C are a slight generalization of elliptic units and are similar to the ones in [1] and [4] (but there is a clash of notation!).

Proof. Our claims are consequences of the Shimura reciprocity law. We will not need its full strength and hence we will use its more classical formulation. For this we will follow Deuring [2] and Stark [17]. We will also need some facts from Lang's book [9]. We first set up some notation that we will use throughout this proof. As in Sect. 4, for any ideal $\mathscr{A} \in \mathscr{R}_{6p}$ we write

$$\mathscr{A}^2 = \left[a^2, \frac{\tilde{b} + \sqrt{-p}}{2}\right].$$

We define

$$U(\mathscr{A}) = e_{48}(\tilde{b} - 1)\eta\left(\frac{-\tilde{b} + \sqrt{-p}}{2a^2}\right)\Big/\eta\left(\frac{-1 + \sqrt{-p}}{2}\right)$$

and

$$V(\mathscr{A}) = e_{16}(\tilde{b} - 1)\theta_{10}\left(\frac{-\tilde{b} + \sqrt{-p}}{2a^2}\right)\Big/\theta_{10}\left(\frac{-1 + \sqrt{-p}}{2}\right).$$

These are well defined because the right hand sides are independent of $\tilde{b}$. It is easy to see that

$$u_{[\mathscr{A}]} = U(\mathscr{A})/\psi_0(\mathscr{A}) \tag{3}$$

and

$$v_{[\mathscr{A}]} = V(\mathscr{A})/\psi_0(\mathscr{A}). \tag{4}$$

We now pick an ideal $\mathscr{A} \in \mathscr{R}_{6p} \cap C'^{-1}$ and let $a = \mathrm{N}\mathscr{A}$. By the Chebotarev density theorem there exists a prime ideal of degree one, $\mathscr{L}$ say, in $\mathscr{R}_{6ap} \cap C^{-1}$. As before, we choose an odd integer $\tilde{b}$ so that

$$\mathscr{A}^2 = \left[a^2, \frac{\tilde{b} + \sqrt{-p}}{2}\right],$$

$$\mathscr{L}^2 = \left[l^2, \frac{\tilde{b} + \sqrt{-p}}{2}\right],$$

and

$$\mathscr{Q} = \left[2, \frac{\tilde{b} + \sqrt{-p}}{2}\right].$$

Here $l = \mathrm{N}\mathscr{L}$ and $\mathscr{Q}$ is the prime above 2 chosen in (iii).

We define a function on the upper-half plane by

$$g(\tau) = \frac{\eta(\tau/a^2)}{\eta(\tau)}\,.$$

It is an easy matter to verify that

$$U(\mathscr{A}) = g\left(\frac{-\tilde{b}+\sqrt{-p}}{2}\right).$$

It follows from [2, p. 14] and [9, Chap. 12–13] that $g \in \mathscr{F}_{a^2}$ (notation as in [9]), has no poles (or zeros) in the upper-half plane, and has integral coefficients in its q-expansion at every cusp.

We can now start with the proof. By [2, p. 41], $U(\mathscr{A}) \in \mathcal{O}_H$ and $(U(\mathscr{A})) = \mathscr{A}\mathcal{O}_H$. Also, $\psi_0(\mathscr{A}) \in \mathcal{O}_T$ and $(\psi_0(\mathscr{A})) = \mathscr{A}\mathcal{O}_T$. Therefore, by (3), u_C is a unit in M, proving (i).

The first two properties in (ii) are easy. For the third, we apply [17, Theorem 3] twice, using

$$\mathscr{L} = \left[l, \frac{\tilde{b}+\sqrt{-p}}{2}\right]$$

and

$$\mathscr{L}^2 = \left[l^2, \frac{\tilde{b}+\sqrt{-p}}{2}\right]$$

to get

$$U(\mathscr{A})^{\sigma_{C^{-2}}} = \eta\left(\frac{-\tilde{b}+\sqrt{-p}}{2a^2l^2}\right)\bigg/\eta\left(\frac{-\tilde{b}+\sqrt{-p}}{2l^2}\right).$$

Therefore,

$$U(\mathscr{A})^{\sigma_{C^{-2}}} = U(\mathscr{A}\mathscr{L})/U(\mathscr{L})\,.$$

Our claim now follows from (3).

To prove (iii) we recall the classical formulas (see [20, p. 114])

$$\theta_{10}(\tau) = 2\eta(2\tau)^2/\eta(\tau)$$

and

$$e_{48}(1)\eta(\tau)^3 = \eta(2\tau)\eta(\tau/2)\eta((\tau+1)/2)\,.$$

Combining these, we obtain

$$\theta_{10}(\tau) = 2e_{24}(1)\eta(\tau)^5\eta(\tau/2)^{-2}\eta((\tau+1)/2)^{-2}\,. \tag{5}$$

Again by [17, Theorem 3], if $\tau = (-\tilde{b}+\sqrt{-p})/2$ then

$$g(\tau/2) = U(\mathscr{A})^{\sigma_{D^{-1}}}\,, \tag{6}$$

and also

$$g((\tau + a^2)/2) = U(\mathscr{A})^{\sigma_D} . \tag{7}$$

Now notice that

$$\xi\bar{\xi} = 5 - 2\sigma_D - 2\sigma_{D^{-1}} ,$$

and so by (5), (6), and (7),

$$V(\mathscr{A}) = U(\mathscr{A})^{\xi\bar{\xi}} . \tag{8}$$

Our claim now follows from (3) and (4).

Part (iv) is a direct consequence of (iii), (ii) and (i).

Finally, we prove (v). It will be enough to show that

$$V(\mathscr{A}) \equiv 1 \bmod 2\mathcal{O}_H .$$

By the fundamental property of the Artin map, for any integer $\alpha \in \mathcal{O}_H$ prime to 2, we have

$$\alpha^{\xi} \equiv 1 \bmod \mathscr{Q}\mathcal{O}_H , \tag{9}$$

and

$$\alpha^{\bar{\xi}} \equiv 1 \bmod \bar{\mathscr{Q}}\mathcal{O}_H \tag{10}$$

(recall that H/K is abelian).

So now (v) follows from (8) by taking $\alpha = U(\mathscr{A})^{\bar{\xi}}$ and $\alpha = U(\mathscr{A})^{\xi}$ in (9) and (10), respectively. (It is not hard to see that these numbers generate $\mathscr{A}$ and, in particular, they are prime to 2). This completes the proof of the theorem. □

6 Formula for the L-series at $s = 1$

In this section we continue to assume that d is a prime $p \equiv 7 \bmod 8$. Recall that h is odd when d is prime and hence every class is a square in $\mathrm{Cl}(K)$.

Proposition 6.1 *For any classes C, $C' \in \mathrm{Cl}(K)$ we have*

$$\theta_{C'^2}(C^2) = \sqrt[4]{p}\,t(CC')t(CC'^{-1}) .$$

Proof. It follows from the factorization lemma (Lemma 3.1) applied to squares of ideals, and the definition of t. We leave the details to the reader. □

We can now combine this with Hecke's formula (Theorem 2.6).

Theorem 6.2 *For every class $C \in \mathrm{Cl}(K)$ and every $\varphi \in \mathrm{Cl}(K)^*$,*

(i) $$L(\varphi, C^2) = \varphi(C^2)\frac{\pi}{\sqrt[4]{p}} \sum_{C' \in \mathrm{Cl}(K)} t(CC')t(CC'^{-1}) ,$$

(ii) $$L(\varphi) = \frac{\pi}{\sqrt[4]{p}}\left(\sum_{C \in \mathrm{Cl}(K)} \varphi(C)t(C)\right)^2 ,$$

and

(iii)
$$\sum_{\varphi} L(\varphi) = \frac{h\pi}{\sqrt[4]{p}} \sum_{C} |t(C)|^2 \, .$$

Proof. Recall that every class is a square. Part (i) follows directly from Proposition 6.1 and Hecke's formula (Theorem 2.6). Part (ii) follows from (i) after a change of indices in the sum. Part (iii) follows from (ii) by expanding the right hand side and summing over φ. □

Corollary 6.3 *For* $\varphi \in \mathrm{Cl}(K)^*$, *let*

$$l(\varphi) = \sum_{C} \varphi(C) v_C \, .$$

Then for every $C \in \mathrm{Cl}(K)$ *and* φ, $\varphi' \in \mathrm{Cl}(K)^*$, *we have*

(i)
$$l(\varphi)^{\sigma_{C^2}} = v_C^{-1} l(\varphi) \, ,$$

(ii)
$$l(\varphi)^{\varphi'} = l(\varphi' \varphi) \, ,$$

and

(iii)
$$L(\varphi) = \frac{\pi}{\sqrt[4]{p}} t(C_0)^2 l(\varphi)^2 \, .$$

Moreover, $l(\varphi)$ *is a nonzero integer in* $(M^+)^{\varphi}$; *in particular*

$$L(\varphi) > 0 \, .$$

Remark. That $L(\varphi)$ is positive was first proved by Rohrlich in a different way (see [11]). Regarding the integrality of $\frac{\sqrt[4]{p}}{\pi} t(C_0)^{-2} L(\varphi)$, compare [5, Corollary 3.2].

Proof. Parts (i) and (ii) follow easily from the properties of t given in Theorem 5.3. The identity in (iii) follows from part (ii) of the theorem. It is clear that $l(\varphi)$ is an integer in M fixed by complex conjugation. It is also clear that each $L(\varphi)$ is a non-negative real number. To see that it is actually positive, observe that by part (iii) of the theorem, $\sum_{\varphi} L(\varphi)$ is positive (we have shown in Theorem 5.3 that $t(C)$ is never zero). On the other hand, by parts (ii) and (iii) of this corollary, if one of the summands is zero, they all are. We conclude that $L(\varphi)$ is positive for all φ. □

Remark. Let us note that v_C, and therefore $l(\varphi)$, remains unchanged if we replace t by $-t$. In particular the sign of $l(\varphi)$ is uniquely determined. Interestingly, not all of these signs can be the same. To see this, note that

$$\sum_{\varphi} l(\varphi) = h$$

and

$$\sum_{\varphi} l(\varphi)^2 = h \sum_{C} |v_C|^2 \, .$$

Therefore

$$\frac{1}{h}\sum_{\varphi\neq\varphi'} l(\varphi)l(\varphi') = h - \sum_{C} |v_C|^2 .$$

A crude estimate using the definitions (left to the reader) shows that $|v_C| \geqq 1$ for every class C. Hence, the right hand side is negative and, in particular, not all of the $l(\varphi)$ can have the same sign.

7 The curve $A(p)$

Throughout this section we assume that d is a prime $p \equiv 3 \bmod 4$. Following Gross we consider the elliptic curve $A(p)$ and state some of its properties. For details and proofs we refer the reader to [1, 3, 4, 13, 14], and [15]. Recall the notation introduced at the beginning of section 5: $j = j((1+\sqrt{-p})/2)$ where j is the classical modular function, $F = \mathbb{Q}(j)$, and $H = FK$ is the Hilbert class field of K.

We define the elliptic curve $A(p)$ by the Weierstrass equation

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

where m and n are the unique, a priori, real numbers such that

$$m^3 = j ,$$

$$-n^2 p = j - 1728 ,$$

and

$$\operatorname{sign}(n) = \left(\frac{2}{p}\right) .$$

Actually m and n lie in F and so the curve $A(p)$ is defined over F. We let $\omega = \dfrac{dx}{2y}$ be the differential associated to this model; it is straightforward to check that $\Delta(\omega) = -p^3$ and that j is the j-invariant of $A(p)$.

The only primes of bad reduction for $A(p)$ are the primes dividing p. In F we have

$$(p) = \mathscr{P}_0\mathscr{P}_1^2 \dots \mathscr{P}_{h'}^2$$

where $h' = (h-1)/2$. The type of reduction for each of these primes is given explicitly by Gross in [3, 14.1]. For our purposes it is enough to know the value of m_v, the number of connected components of the Neron model of $A(p)$ at v that are rational over the residue class field. These are as follows:

(i) for $v = \mathscr{P}_0$, $m_v = 2$, and

(ii) for $v = \mathscr{P}_i$ $(i = 1, 2, \dots, h')$, $m_v = 4$.

We note in passing that from the above factorization of p and the fact that no other prime ramifies in $H/\mathbb{Q}$, it follows easily that the discriminant of $F/\mathbb{Q}$ is $p^{h'}$.

The torsion subgroup of $A(p)$ over F is of order 2 and $A(p)(F)$ has rank zero when $p \equiv 7 \bmod 8$.

The curve $A(p)$ over H has complex multiplication by $\mathcal{O}_K$ and its associated Hecke character is $\psi \circ \mathbf{N}_{H/K}$, for any $\psi \in \Psi$. It follows that the L-series of $A(p)$ over F factors as

$$L(s; A(p)/F) = \prod_{\psi \in \Psi} L(s; \psi) . \tag{11}$$

8 Formula for the square root of the predicted order of the Tate-Shafarevich group

In this section we assume that d is a prime $p \equiv 7 \bmod 8$. We will put our formula for the L-series at $s = 1$ (Theorem 6.2) together with the calculation of all the factors involved in the Birch-Swinnerton Dyer conjecture to obtain a formula for the square root of the predicted order of the Tate Shafarevich group of $A(p)$ over F. We will be able to show that this number is in fact an integer. Our formula gives a specific choice of sign for this square root, which seems very interesting.

For the setting up of the Birch-Swinnerton Dyer conjecture we follow Manin (see [10, Sect. 8]). In Sect. 7 we already have most of the terms: we know the order of the torsion, the discriminant of $F/\mathbb{Q}$, and the m_v's corresponding to primes of bad reduction. We also have a formula for the value of the L-series of $A(p)$ at $s = 1$; namely

$$L(1; A(p)/F) = \left(\frac{\pi}{\sqrt[4]{p}}\right)^h \left(\prod_{\varphi \in \mathrm{Cl}(K)^*} \sum_{C \in \mathrm{Cl}(K)} \varphi(C) t(C)\right)^2 ,$$

obtained by combining Theorem 6.2 (ii) with (11). It remains to compute m_v for the archimedean primes of F.

As in Sect. 5, we identify the Galois group of H/K with the class group $\mathrm{Cl}(K)$ via the Artin map. We pick representatives $\mathscr{A}_i \in \mathscr{R}$ for $i = 0, 1, \ldots, h'$ (here, as before, $h' = (h-1)/2$) such that

$$\mathrm{Cl}(K) = \{[\mathscr{A}_0], [\mathscr{A}_1], \ldots, [\mathscr{A}_{h'}], [\mathscr{A}_1]^{-1}, \ldots, [\mathscr{A}_{h'}]^{-1}\} ,$$

where $[\mathscr{A}]$ denotes the class of $\mathscr{A}$ in $\mathrm{Cl}(K)$. We choose $\mathscr{A}_0 = \mathcal{O}_K$.

By Lemma 2.2 we can write

$$\mathscr{A}_i = \left[a_i, \frac{b_i + \sqrt{-p}}{2}\right]$$

for $i = 0, \ldots, h'$, where $a_i = \mathbf{N}\mathscr{A}_i$. We let $\tau_i = \dfrac{-b_i + \sqrt{-p}}{2a_i}$.

Corresponding to $\mathscr{A}_i$ we have an embedding of F in the complex numbers which we will denote by σ_i. For $i = 0$ we have our chosen real embedding of F, and for $i = 1, \ldots, h'$ we have pairwise nonconjugate complex embeddings.

Recall that ω is the differential form on $A(p)$ defined in Sect. 7. It is not hard to see that the lattice of periods of ω^{σ_i} is $\Omega_i[1, \tau_i]$, for some Ω_i, which is real for $i = 0$, and complex for $i = 1, \ldots, h'$. Since $\Delta(\omega^{\sigma_i}) = -p^3$ for every $i = 0, 1, \ldots, h'$, we obtain

$$|\Omega_i| = \frac{2\pi}{\sqrt[4]{p}} |\eta(\tau_i)|^2 ,$$

where η is Dedekind's eta function.

Using now the formulas in [10] it is not hard to verify that:

(i) for $v = \sigma_0$,

$$m_v = \frac{2\pi}{\sqrt[4]{p}}|\eta(\tau_0)|^2 ,$$

(ii) for $v = \sigma_i$ and $i = 1, \ldots, h'$,

$$m_v = \frac{\sqrt{p}}{2a_i}\left(\frac{2\pi}{\sqrt[4]{p}}|\eta(\tau_i)|^2\right)^2 .$$

We need one more fact.

Lemma 8.1 *With the notation as above, we have the identity*

$$|\eta(\tau_0)| \prod_{i=1}^{h'} \frac{|\eta(\tau_i)|^2}{\sqrt{a_i}} = \prod_{C \in \mathrm{Cl}(K)} t(C) .$$

Proof. This follows from Theorem 5.3. We leave it to the reader. □

Remark. The product $\prod_v m_v$ can also be given in terms of values of the classical gamma function. This is the Chowla-Selberg formula. See [4] for example.

Theorem 8.2 *Let*

$$\mathscr{S}(p) = \frac{1}{2^{h-1}} \frac{\prod_{\varphi \in \mathrm{Cl}(K)^*} \sum_{C \in \mathrm{Cl}(K)} \varphi(C)t(C)}{\prod_{C \in \mathrm{Cl}(K)} t(K)} .$$

(i) *The number $\mathscr{S}(p)$ is a nonzero rational integer.*

(ii) *The predicted order of the Tate-Shafarevich group of $A(p)$ over F equals $\mathscr{S}(p)^2$.*

Proof. The proof of (ii) amounts to putting together all the terms calculated above into the Birch-Swinnerton Dyer conjecture, as given for example by Manin (see [10, Sect. 8]). We leave this to the reader. We now prove (i). That $\mathscr{S}(p)$ is nonzero follows from Corollary 6.3 (iii). By dividing numerator and denominator by $t(C_0)^h$ (here again, C_0 denotes the trivial class) we can rewrite the formula as

$$\mathscr{S}(p) = \frac{1}{2^{h-1}} \frac{\prod_\varphi \sum_C \varphi(C)v_C}{\prod_C v_C} ,$$

where $v_C = t(C)/t(C_0)$ are the units defined in Sect. 5. This already shows that $\mathscr{S}(p)$ is an algebraic number with at most powers of two in the denominator. We need to prove: (i) $\mathscr{S}(p)$ is a rational number, and (ii) 2^{h-1} divides the numerator.

(i) To show $\mathscr{S}(p)$ is a rational number, we check its behaviour under the action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. For this we use the various properties of t described in Theorem 5.3.

(a) Both numerator and denominator are fixed by complex conjugation since we have $\overline{\varphi(C)} = \varphi(C^{-1})$ and $\overline{t(C)} = t(C^{-1})$.

(b) Under the action of σ_{C^2}, for any class $C \in \mathrm{Cl}(K)$, the numerator changes by a factor of $v_C^{-h} \prod_\varphi \varphi^{-1}(C)$, and the denominator by v_C^{-h}. Since $\mathrm{Cl}(K)^*$ is of odd order, it follows that $\mathscr{S}(p)$ remains fixed.

(c) Under the action of φ, for any $\varphi \in \mathrm{Cl}(K)^*$, the numerator remains fixed and the denominator changes by a factor of $\prod_C \varphi^{-1}(C)$. Again, since $\mathrm{Cl}(K)$ is of odd order, $\mathscr{S}(p)$ remains fixed.

This shows that $\mathscr{S}(p)$ is a rational number.

(ii) To show that 2^{h-1} divides the numerator in the formula for $\mathscr{S}(p)$, let $M' = M(\zeta_h)$, where ζ_h is a primitive hth root of unity. Let $\mathscr{Q}$ be any prime of M' above 2. It follows from Theorem 5.3 (v) that the map

$$\mathrm{Cl}(K) \to (\mathcal{O}_{M'}/\mathscr{Q})^\times$$

$$C \mapsto v_C$$

is a homomorphism. Therefore, $h - 1$ of the factors in the numerator are divisible by $\mathscr{Q}$, the remaining factor being congruent to h mod $\mathscr{Q}$. This is enough for our purposes, but note that h is odd so that exactly $h - 1$ of the factors are divisible by $\mathscr{Q}$. We conclude that 2^{h-1} divides the numerator, since 2 is unramified in $M'/\mathbb{Q}$. This completes the proof of the Corollary. □

9 Table

In this section we include a table of the values of $\mathscr{S}(p)$ for primes $p \equiv 7 \bmod 8$ less than 3000. We may make a few remarks. First, very few of these numbers are even; this is probably related to fact that the 2-part of the Tate-Shafarevich group fixed by Galois is trivial (see [4]). In all examples where $\mathscr{S}(p)$ is even it is also divisible by 4. Second, the numbers $\mathscr{S}(p)$ grow very rapidly with p and seems natural to expect them to tend to infinity; in fact, the h-th root of $\mathscr{S}(p)$ seems to be a slowly essentially increasing function of p. The calculations also seem to indicate that $p = 487$ is the last prime with $\mathscr{S}(p) = \pm 1$.

p	h	$\mathscr{S}(p)$
7	1	1
23	3	− 1
31	3	1
47	5	1
71	7	3
79	5	− 3
103	5	1
127	5	3
151	7	− 9
167	11	− 115
191	13	− 131
199	9	− 43
223	7	− 47
239	15	357
263	13	− 21
271	11	29
311	19	− 7185
359	19	− 30529
367	9	171
383	17	3321
431	21	− 29976
439	15	11311
463	7	73
479	25	− 802369
487	7	1
503	21	− 151
599	25	19597793
607	13	3723
631	13	− 8199
647	23	− 233639
719	31	− 1667632553
727	13	9393
743	21	553649
751	15	− 30436
823	9	− 2885
839	33	− 136363465939
863	21	43265419
887	29	− 799319015
911	31	101669719469
919	19	− 6983195
967	11	105013
983	27	4475472187
991	17	325251
1031	35	1881259442341

p	h	$\mathscr{S}(p)$	p	h	$\mathscr{S}(p)$
1039	23	− 44931457	1951	33	35824844471641
1063	19	− 2492169	1999	27	− 17038555487
1087	9	− 7493	2039	45	− 612976093531479229
1103	23	− 13010521	2063	45	53534416007696889040
1151	41	− 8422760498003	2087	35	− 385471050781
1223	35	268182807825	2111	49	− 3238384256630627126675
1231	27	167342437	2143	13	821595
1279	23	− 85163285	2207	39	− 42907145154487223
1303	11	5355	2239	35	14478184446851
1319	45	− 139647575106523413	2287	29	526738119443
1327	15	− 15371	2311	29	− 39291761934983
1367	25	319059600	2351	63	3259496183640400896670687
1399	27	− 613369452	2383	29	32238586919
1423	9	240388	2399	59	26866771242856003982690113
1439	39	4571993303375	2423	33	27679998882827
1447	23	4394787	2447	37	− 779681288967987
1471	23	− 436269935	2503	21	1378792179
1487	37	178107280559	2543	35	− 1770945783765240
1511	49	9341609604469929	2551	41	1666137270760191923
1543	19	64763035	2591	57	− 26816260710910034928973
1559	51	103388761720463677	2647	15	66784929
1567	15	− 12369639	2663	43	− 162124593439144934039
1583	33	89427244881719	2671	23	71684499
1607	27	524286640211	2687	51	6242332599034307618716
1663	17	− 4742751	2711	53	− 152998708643518444621
1759	27	− 1331737066655	2719	41	− 91921478549620405
1783	17	8140797	2767	21	− 399869556
1823	45	49747212133304799488	2791	39	8044448046795653
1831	19	− 213575585	2879	57	6245912690491342295948609
1847	43	− 11783606010669817	2887	25	− 23296822398697
1871	45	328894316393842365831	2903	59	4481256203885731006684319085
1879	27	105352698996	2927	31	1152748492348591

References

1. Buhler, J.P., Gross, B.H.: Arithmetic on Elliptic Curves with Complex Multiplication II. Invent. Math. **79**, 11–29 (1985)
2. Deuring, M.: Die Klassenkörper der komplexen Multiplikation. (Enzy. der Math. Wiss. Band I, 2. Teil, Heft 10, Teil II) Stuttgart: Teubner 1958
3. Gross, B.H.: Arithmetic on Elliptic Curves with Complex Multiplication. (Lect. Notes Math., vol. 776) Berlin Heidelberg New York: Springer 1980
4. Gross, B.H.: Minimal Models for Elliptic Curves with Complex Multiplication. Compos. Math. **45**, 155–164 (1982)
5. Goldstein, C., Schappacher, N.: Series d'Eisenstein et fonctions L de courbes elliptiques a multiplication complexe. J. Reine Angew. Math. **327**, 184–218 (1981)
6. Hecke, E.: Mathematische Werke. Göttingen: Vandenhoeck and Ruprecht 1959
7. Kolyvagin, V.A.: Finiteness of $E(\mathbf{Q})$ and the Tate-Shafarevich group of E over $\mathbf{Q}$ for a subclass of Weil curves. Math. USSR, Izv. **32**, No 3, 523–541 (1989)
8. Kronecker, L.: Leopold Kronecker's Werke. Leipzig Berlin: Teubner 1929
9. Lang, S.: Elliptic Functions. Reading: Addison-Wesley 1973
10. Manin, Y.I.: Cyclotomic fields and Modular Curves. Russ. Math. Surv. **26**, No. 6, 7–78 (1971)
11. Rohrlich, D.: The non-vanishing of certain Hecke L-functions at the center of the critical strip. Duke Math. J. **47**, No 1, 223–232 (1980)
12. Rubin, K.: Tate-Shafarevich groups and L-functions of elliptic curves with complex multiplition. Invent. Math. **89**, 527–560 (1987)

13. Shimura, G.: On elliptic curves with complex multiplication as factors of the Jacobian of modular function fields. Nagoya Math. J. **43**, 199–208 (1971)
14. Shimura, G.: On the zeta-function of an abelian variety with complex multiplication. Ann. Math. **94**, 504–533 (1971)
15. Shimura, G.: On the factors of the Jacobian variety of a mod ular function field. J. Math. Soc. Japan **25**, 523–544 (1973)
16. Shimura, G.: Introduction to the arithmetic theory of automorphic functions. Publ. Math. Soc. Japan **11** (1971)
17. Stark, H.: L-series at $s = 1$ IV. Adv. Math. **35**, 197–235 (1980)
18. Waldspurger, J.P.: Correspondance de Shimura. J. Math. Pures Appl. **59**, 1–132 (1980)
19. Waldspurger, J.P.: Sur les coefficients de Fourier des formes modulaires de poids demi-entier. J. Math. Pures Appl. **60**, 375–484 (1981)
20. Weber, H.: Lehrbuch der Algebra, vol. 3. New York: Chelsea 1961