INFORMATION TO USERS

The most advanced technology has been used to photograph and reproduce this manuscript from the microfilm master. UMI films the text directly from the original or copy submitted. Thus, some thesis and dissertation copies are in typewriter face, while others may be from any type of computer printer.

The quality of this reproduction is dependent upon the quality of the copy submitted. Broken or indistinct print, colored or poor quality illustrations and photographs, print bleedthrough, substandard margins, and improper alignment can adversely affect reproduction.

In the unlikely event that the author did not send UMI a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyright material had to be removed, a note will indicate the deletion.

Oversize materials (e.g., maps, drawings, charts) are reproduced by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps. Each original is also photographed in one exposure and is included in reduced form at the back of the book.

Photographs included in the original manuscript have been reproduced xerographically in this copy. Higher quality 6" x 9" black and white photographic prints are available for any photographs or illustrations appearing in this copy for an additional charge. Contact UMI directly to order.

U·M·I

University Microfilms International
A Bell & Howell Information Company
300 North Zeeb Road Ann Arbor, MI 48106-1346 USA
313 761-4700 800 521-0600

Order Number 9105202

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

Villegas, Fernando Rodriguez, Ph.D.

The Ohio State University, 1990

U·M·I
300 N. Zeeb Rd.
Ann Arbor, MI 48106

ON THE SQUARE ROOT OF SPECIAL VALUES OF CERTAIN L-SERIES

DISSERTATION

Presented in Partial Fulfillment of the Requirements for

the Degree Doctor of Philosophy in the Graduate

School of the Ohio State University

by

Fernando Rodriguez Villegas

* * * * *

The Ohio State University

1990

Dissertation Committee:

Prof. W. Sinnott.

Prof. J. Hsia.

Prof. R. Gold.

Approved by

Advisor

Department of Mathematics

"... je me resigne, Monsieur, à interroger les formules elliptiques des diverses catégories, en demandant à chacune son secret arithmétique, et à recueillir les réponses utiles ou inutiles avec patience et persévérance; *plus laboris quam artis.*"

Letter of Hermite to Stieltjes, March 12 1884.

"I had opportunity of seeing a Phenomenon. I had never before seen a lunar rainbow, which appeared about 10 o'clock, very faint and almost or quite without colour, so that it could be traced by little else than appearence, which looked like shade on a cloud."

Entry of October 16, 1768. The Endeavour Journal of Sir Joseph Banks.

To Adriana

ACKNOWLEDGEMENTS

I want to express my sincere gratitude to my advisor, Warren Sinnott, for his infinite patience, his encouragment and support during these years.

Thanks to Karl Rubin for suggesting the calculations that were the starting point of this work and for helpful discussions since, to Eduardo Dubuc of the University of Buenos Aires for his enthusiasm and perseverance in the verification of the numerical results, to Y. Kida for sharing with the public his useful programming language Ubasic, and to Barry Spieler for the careful reading of this manuscript, which resulted in its considerable improvement.

I would also like to thank my friends for their affection and especially my wife, Adriana, for her constant support, love, and faith in me.

VITA

June 20, 1959	Born in Buenos Aires, Argentina.
1985	Licenciatura en Matematicas. Facultad de Ciencias Exactas, Universidad de Buenos Aires.
1984-1986	Teaching Assistant, Facultad de Ciencias Exactas, Universidad de Buenos Aires.
1986-89	Teaching Assistant, Department of Mathematics, The Ohio State University, Columbus, Ohio.

FIELDS OF STUDY

MAJOR FIELD: Mathematics

Table of Contents

CHAPTER I

Introduction

1.1 Introduction

In his thesis (see [3]), B.Gross defined an elliptic curve $A(p)$, which has complex multiplication by $K = \mathbf{Q}(\sqrt{-p})$, for every prime number p. It is defined over the Hilbert class field of K. We give a brief description of this curve in section 3.1 using notation established in section 1.2.

Among many other things, Gross proves that $A(p)$ has rank zero when $p \equiv 7 \bmod 8$. In this case the conjectures of Birch and Swinnerton-Dyer predict that the value of the L-series of $A(p)$ at $s = 1$, when divided by an appropriate factor (call this quotient $\mathcal{S}(p)$), must be the order of the Tate-Shafarevich group of $A(p)$. It is known that, when finite, the order of this group is a square. So, in particular, the conjectures imply that $\mathcal{S}(p)$ must be the square of a nonzero integer. In this paper we give a proof of this last statement. In fact, we obtain in section 3.2 an explicit formula for a square root of $\mathcal{S}(p)$, which includes an intriguing choice of sign.

This is acomplished by first giving an explicit formula for the square root of the value at $s = 1$ of certain L-series of Hecke characters of K (see Theorem 2.4.2 (ii)). Our starting point is a formula of Hecke (Theorem 1.2.6), which involves values of theta series of binary quadratic forms. These values can be factored as values of the classical Jacobi theta function θ_{10} (notation as in Weber's book [12]). This is our crucial Factorization Lemma 2.1.1. It was only after much of this work was finished that we found that this factorization is actually a consequence of a somewhat neglected result of Kronecker (see [7, vol. IV, pp. 354-357]). We expect this more general result to provide some insight as to how to extend our work to quadratic twists of $A(p)$.

Roughly speaking, the factorization exhibits the value 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. A precise formulation is given in section 2.4.

Finally, we use the Shimura reciprocity law to get algebraic and Galois properties of the terms in the new formula. This is established in sections 2.2 and 2.3 using the formulation in Deuring, Lang, and Stark. ([2],[8], and [11]). These properties allow us to show that $S(p)$ is a nonzero rational square. A further argument shows that a possible denominator of 4^{h-1} actually divides the numerator, proving it to be an integer. This is done in section 3.2.

Our original intention was to calculate $S(p)$ for various p to investigate their

nature. We found the above mentioned formula after trying to simplify the calculations involved. The formula does provide a very effective way of computing $S(p)$. We have programmed it in Kida's language Ubasic, which allows fast arbitrary precision calculations for PC's. It compares very favorably to the method used in [1] based on Manin's formula (see [9, Th. 9.3]). Manin's formula is a consequence of the functional equations satisfied by the L-series, and as such is more general than ours since it also covers quadratic twists of $A(p)$. In order to check our calculations we programmed this method as well.

1.2 Notation, Basic Lemmas and Hecke's Formula

We let $K = \mathbf{Q}(\sqrt{-d})$, $d > 3$ be an imaginary quadratic field with $d \equiv 3 \bmod 4$ and we fix an embedding of K into the complex numbers. For any number field L, $\mathcal{O}_L$ will denote its ring of integers and for any ring R, R^* will denote its group of units. Note that $\mathcal{O}_K^* = \{\pm 1\}$ and $d = \mathrm{disc}(K)$. 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 C. We will use $\mathcal{H}$ for the upper-half plane, $Cl(K)$ for the class group of K, and if $\mathcal{A}$ is an ideal, $[\mathcal{A}]$ for its class.

We give now a brief overview of the Hecke character of K related to the elliptic

curves $A(p)$. For more details we refer the reader to Gross [3] or to section 3.1 where we summarize what we need about these curves.

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

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

Composing its inverse with the Jacobi symbol $(\frac{}{d})$ 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

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

We now define a Hecke character ψ by the following conditions:

(i) If $\mathcal{A}$ is an ideal of $\mathcal{O}_K$ prime to d, then

$$\psi(\mathcal{A}) = \beta$$

where $\mathcal{A}^h = (\alpha)$, $\varepsilon(\alpha) = +1$, and β is a complex number such that $\beta^h = \alpha$. Here h is the class number of K.

(ii) If α is an integer prime to d, then

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

(iii) If $\mathcal{A}$ is not prime to d, then $\psi(\mathcal{A}) = 0$.

There are h such characters, and any two ψ, ψ' satisfy

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

where, with some abuse of notation, $Cl(K)^*$ is the dual group of $Cl(K)$. We will fix one such ψ once and for all. It takes values in an extension T/K of degree h, with a fixed embedding in the complex numbers. Note that $\overline{\psi(\mathcal{A})} = \psi(\bar{\mathcal{A}})$.

As usual, we define the L-series associated to ψ by

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

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

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

We clearly have

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

and

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

for every $\varphi \in Cl(K)^*$. Also, it is easy to see that if $\mathcal{A} \in C^{-1}$ is an ideal prime to d, then

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

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 1.2.6). As opposed to Manin's approach using the functional equations (see [9, Th. 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 [10].

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

Definition 1.2.1 *For any ideal $\mathcal{F}$ we let*

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

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

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

Lemma 1.2.2 *If $\mathcal{A} \in \mathcal{R}$, then $\bar{\mathcal{A}} \in \mathcal{R}$, and we can write*

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

and

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

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

$$b^2 \equiv -d \mod 4a.$$

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

Lemma 1.2.3 *Assume $\bar{\mathcal{F}} = \mathcal{F}$. If $\mathcal{A}_1, \bar{\mathcal{A}}_2 \in \mathcal{R}_{\mathcal{F}}$ are relatively prime, then $\mathcal{A}_1\mathcal{A}_2 \in \mathcal{R}_{\mathcal{F}}$. In particular, if $\mathcal{A} \in \mathcal{R}_{\mathcal{F}}$ and $(\sqrt{-d})$ divides $\mathcal{F}$, then $\mathcal{A}^n \in \mathcal{R}_{\mathcal{F}}$ for every positive integer n.*

Furthermore, if

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

then

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

with $a = a_1a_2$ and some $b \equiv b_i \bmod 2a_i$, $i = 1, 2$.

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

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

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

where $\mathcal{A}' \in C'^{-1}$ and $a' = \mathrm{N}\mathcal{A}'$. 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 $(\frac{-}{d})$ (see [6, pp. 442-447], for example).

In the next definition we will not indicate the dependence on the character ψ, which remains fixed.

Definition 1.2.4 *Given classes $C, C' \in Cl(K)$ we take an ideal $\mathcal{A} \in \mathcal{R}_d \cap C^{-1}$ and we define*

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

where

$$(\sqrt{-d})\mathcal{A} = [ad, \frac{bd + \sqrt{-d}}{2}]$$

for some integer b *(by Lemmas 1.2.2 and 1.2.3), and*

$$\tau = \frac{-bd + \sqrt{-d}}{2ad}.$$

Lemma 1.2.5 $\theta_{C'}(C)$ *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 $\mathcal{A}, \mathcal{A}' \in \mathcal{R}_d$ that satisfy

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

for some $\mu \in \bar{\mathcal{A}}$. We let $\tau = \frac{-bd+\sqrt{-d}}{2ad}$. It is not hard to see that $\mu/a = \gamma\tau + \delta$, for some integers γ and δ, with d dividing γ. By Lemma 1.2.3, γ and δ must be relatively prime. Also,

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

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

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

where $a' = \mathbf{N}\mathcal{A}'$ and b' is such that

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

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

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

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

Theorem 1.2.6 (Hecke's formula). *For any* $C \in Cl(K)$,

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

Proof: See Hecke [6, pages 450-455]. □

CHAPTER II

Square root of special values

2.1 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 $C_1, C_2 \in Cl(K)$. We choose ideals $\mathcal{A}_i \in \mathcal{R}_{2d} \cap C_i^{-1}$ for $i = 1, 2$ such that their norms $a_i = \mathbf{N}\mathcal{A}_i$ are relatively prime. It is not hard to see that this is always possible. We let $a = a_1 a_2$. By Lemmas 1.2.2 and 1.2.3 we can find odd integers b, b^* and $\check{b}$ such that:

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

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

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

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

where

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

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

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

Finally, recall that we defined

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

and further let

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

one of the classical Jacobi theta functions (in Weber's notation, see [12]).

Lemma 2.1.1 (Factorization Lemma)

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

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

$$\zeta = e_{16}(ab)e_{16}(ab^*)(\frac{2b}{a_2})(\frac{-a_2}{a_1})\epsilon_a \epsilon_{a_1}$$

where

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

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

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

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

Therefore

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

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

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

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 mod 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 2.1.2 *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

$$\sum_{k \equiv bm \bmod a_1} e_{2a}(-\bar{b}(k^2+dm^2))e^{-\pi\frac{k^2+dm^2}{a}}\tfrac{1}{\sqrt{d}}$$

$$= \sum_{k \equiv bm \bmod a_1} e_a(-\bar{b}(k^2+dm^2)2^t)(-1)^{k+m}e^{-\pi\frac{k^2+dm^2}{a}}\tfrac{1}{\sqrt{d}}$$

by Lemma 2.1.2. 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

$$A_j = \sum_k e_{a_1}(jk)e_a(-\bar{b}k^2 2^t)(-1)^k e^{-\pi\frac{k^2}{a}}\tfrac{1}{\sqrt{d}}$$

and

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

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

$$\sum_k f(k)(-1)^k e^{-\pi\frac{k^2}{N}t} = t^{-1/2}\sum_{k \text{ odd}} \hat{f}(k\,2^t)e^{-\pi\frac{k^2}{tN}\frac{1}{t}},$$

where

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

is the Fourier transform mod N.

In our case we have

$$f(k) = e_a(ja_2k - \bar{b}\, 2^t k^2)$$

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

$$\hat{f}(k) = (\frac{2b}{a}) \epsilon_a e_a(-2^t b(a_2 j + k)^2).$$

Using Lemma 2.1.3 and interchanging sums, we get, after some calculation,

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

where, again using the known values of Gauss sums,

$$C = \frac{\sqrt[4]{d}}{\sqrt{a_1}} (\frac{2b}{a_2}) (\frac{-a_2}{a_1}) \epsilon_a \epsilon_{a_1}.$$

Now we do a change of variables via

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

This establishes a bijection

$$\{m, k \in \mathbf{Z} : m \text{ even}, k \text{ odd}\} \longleftrightarrow \{u, v \in \mathbf{Z} : uv \equiv 1 \bmod 4\}$$

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

Hence our series can be written as

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

(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

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

and

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

Notice that

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

since by definition

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

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

Therefore,

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

Now, by Lemma 2.1.2,

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

and similarly

$$e_a(-16^t bv^2) = e_{16a}(-bv^2)e_{16}(a^t bv^2).$$

We leave to the reader to check the following simple lemma.

Lemma 2.1.4 *For any odd integer n we have*

$$e_{16}(n^t) = e_{16}(n)(\frac{2}{n}),$$

and

$$e_{16}(n^2) = e_{16}(1)(\frac{2}{n}).$$

By means of this last lemma and the fact that $u, v \equiv 1 \mod 4$, we find

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

and

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

Finally, using the identity

$$\sum_{n \text{ odd}} e^{\pi i \frac{n^2}{4}\tau} = 2 \sum_{n \equiv 1 \mod 4} e^{\pi i \frac{n^2}{4}\tau},$$

we arrive at

$$\frac{1}{2}\frac{\sqrt[4]{d}}{\sqrt{a_1}}(\frac{2b}{a})(\frac{-2a_2 b}{a_1})e_{16}(ab^*)\theta_{10}(\frac{-b^* + \sqrt{-d}}{2a})e_{16}(ab)\theta_{10}(\frac{-b + \sqrt{-d}}{2a}).$$

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 $(\frac{2}{d})$. This finishes the proof of the Factorization Lemma. □

Corollary 2.1.5 *For $d \equiv 3 \bmod 8$ we have*

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

and consequently, for every $\varphi \in Cl(K)^*$,

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

Proof: It follows immediately from the Factorization Lemma just proved and Hecke's formula (Theorem 1.2.6). □

Remark: At least when d is a prime p, the last statement also follows easily from the fact, proved by Gross in [3, Th. 19.1.1], that the sign in the functional equation for $L(s;\varphi\psi)$ is $(\frac{2}{p})$.

2.2 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 $s(C)$ and $t(C)$ for each class $C \in Cl(K)$, 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 2.1.1). We will not make their dependence on the Hecke character ψ explicit, since ψ is fixed throughout. Some important properties of these numbers are given in the next section.

Definition 2.2.1 *Given a class $C \in Cl(K)$ we take an ideal $\mathcal{A} \in \mathcal{R}_{6d} \cap C^{-1}$, and we define*

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

and

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

where

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

for some integer $\tilde{b}$ (by Lemmas 1.2.2 and 1.2.3),

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

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

and

$$\theta_{10}(\tau) = \sum_{n \text{ odd}} e^{\frac{\pi i n^2}{4}\tau}, \quad \tau \in \mathcal{H}.$$

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 2.2.2 *$s(C)$ and $t(C)$ are well defined.*

Proof: As in the proof of Lemma 1.2.5, we will show later that it suffices to prove that the definition agrees on relatively prime ideals $\mathcal{A}, \mathcal{A}' \in \mathcal{R}_{6d}$ that satisfy

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

for some $\mu \in \bar{\mathcal{A}}$. 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 τ and τ', corresponding to $\mathcal{A}$ and $\mathcal{A}'$ respectively, are related by an element of $Sl_2(\mathbf{Z})$ 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 $\mathcal{A}$ have weight zero: η and θ_{10} have weight one-half, $\mathcal{A}$ 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 $(\frac{7}{\delta})$ (see below), which we will do in detail; we leave other computations to the reader.

Let $a = \mathbf{N}\mathcal{A}$ and $a' = \mathbf{N}\mathcal{A}'$. By Lemmas 1.2.2 and 1.2.3, $(\mu) \in \mathcal{R}_{6d}$ and

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

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 $\mu \in \bar{\mathcal{A}}$, 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 1.2.3 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

$$\begin{cases} \gamma = (2an - mb)m \\ \delta = n^2 + 2rnm - m^2(br + c)/a. \end{cases} \tag{2.1}$$

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 1.2.3, (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 $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in Sl_2(\mathbf{Z})$, 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

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

and

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

where

$$\begin{cases} \tilde{c} = (\tilde{b}^2 + d)/4a^2 \\ a'^2 = \gamma^2\tilde{c} - \tilde{b}\gamma\delta + a^2\delta^2 \\ \tilde{b}' = (1 + 2\beta\gamma)\tilde{b} - 2(\alpha\gamma\tilde{c} + \beta\delta a^2). \end{cases} \tag{2.2}$$

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 2.2.3 *Let* $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in Sl_2(\mathbf{Z})$ *with* γ *even,* δ *positive (and odd), and* $\tau \in \mathcal{H}$. *Then*

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

and

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

where

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

and

$$\rho = (2\alpha + 1)(1 - \delta) + \delta\beta + (\delta^2 - 1)\gamma\alpha.$$

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

Proof: See [12, 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

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

and

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

Combining this with properties of ψ we see that

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

and

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

Recall that ε is the quadratic character on $\mathcal{O}_K$ defined in section 1.2. 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

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

For this, let $m = 2^l m'$ with m' odd. Then by (2.1),

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

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

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

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

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

It follows from (2.1), 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

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

and therefore

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

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

Similarly,

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

and we are done.

It remains to reduce the general case to the one just proved. Let then, $\mathcal{A}, \mathcal{A}' \in \mathcal{R}_{2d} \cap C^{-1}$. We can choose a third ideal $\mathcal{B} \in \mathcal{R}_{2d} \cap C^{-1}$ prime to the norm of $\mathcal{A}\mathcal{A}'$ and now apply the above case to the pairs $\mathcal{A}, \mathcal{B}$ and $\mathcal{A}', \mathcal{B}$. This completes the proof of the proposition. □

2.3 Properties of s and t

In this section we assume that d is a prime $p \equiv 7 \bmod 8$. Recall that in section 1.2 we defined a Hecke character of K which takes values in an extension T/K of degree h. We have fixed one of the h possible characters; in other words, we have fixed an embedding of T/K in the complex numbers. Consider also a fixed embedding of H, the Hilbert class field of K, in $\mathbf{C}$.

We let $M = TH$. The above choices fix an embedding of $M/\mathbf{Q}$ in $\mathbf{C}$. We let $M^+ = M \cap \mathbf{R}$. It is not hard to see that $T \cap H = K$ (see [1]). We may therefore identify $Cl(K)^*$ with the embeddings of M/H in $\mathbf{C}$, the trivial character corresponding to our fixed embedding. We will use the same letter φ to denote the embedding corresponding to $\varphi \in Cl(K)^*$. Also, we may identify $Gal(M/T)$ with $Cl(K)$ via the Artin map. For a class $C \in Cl(K)$ 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 2.3.1 *(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 2.3.2 *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 2.3.3 *(i) u_C is a unit in M.*

(ii) For any C, C' and φ,

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

(iii) Consider $\xi = 2 - \sigma_D$ and $\bar{\xi} = 2 - \sigma_{D^{-1}}$ in the group ring $\mathbf{Z}[\mathrm{Gal}(M/T)]$, 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

$$\begin{array}{ccc} Cl(K) & \longrightarrow & (\mathcal{O}_M/2\mathcal{O}_M)^* \\ C & \mapsto & v_C \end{array}$$

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 [11]. We will also need some facts from Lang's book [8]. We first set up some notation that we will use throughout this proof. As in section 2.2, for any ideal $\mathcal{A} \in \mathcal{R}_{6p}$ we write

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

We define

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

and

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

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

$$u_{[\mathcal{A}]} = U(\mathcal{A})/\psi(\mathcal{A}) \tag{2.3}$$

and

$$v_{[\mathcal{A}]} = V(\mathcal{A})/\psi(\mathcal{A}). \tag{2.4}$$

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

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

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

and

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

Here $l = \mathbf{N}\mathcal{L}$ and $\mathcal{Q}$ 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

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

It follows from [2, p. 14] and [8, ch. 12-13] that $g \in \mathcal{F}_{a^2}$ (notation as in [8]), is fixed by upper triangular matrices, 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], $U(\mathcal{A}) \in \mathcal{O}_H$ and $(U(\mathcal{A})) = \mathcal{A}\mathcal{O}_H$. Also, $\psi(\mathcal{A}) \in \mathcal{O}_T$ and $(\psi(\mathcal{A})) = \mathcal{A}\mathcal{O}_T$. Therefore, by (2.3), u_C is a unit in M, proving (i).

The first two properties in (ii) are easy. For the third, we apply [11, Th. 3] twice, using

$$\mathcal{LA}^2 = [la^2, \frac{\tilde{b} + \sqrt{-p}}{2}]$$

and

$$\mathcal{L}^2\mathcal{A}^2 = [l^2a^2, \frac{\tilde{b} + \sqrt{-p}}{2}]$$

to get

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

Therefore,

$$U(\mathcal{A})^{\sigma_{\mathcal{C}\mathcal{L}}} = U(\mathcal{AL})/U(\mathcal{L}).$$

Our claim now follows from (2.3).

To prove (iii) we recall the classical formulas (see [12, 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

$$\theta_{10}(\tau) = 2e_{24}(1)\eta(\tau)^5\eta(\tau/2)^{-2}\eta((\tau+1)/2)^{-2}. \tag{2.5}$$

Again by [11, Th. 3], if $\tau = (-\tilde{b} + \sqrt{-p})/2$ then

$$g(\tau/2) = U(\mathcal{A})^{\sigma_D}, \tag{2.6}$$

and also, after some calculation,

$$g((\tau + a^2)/2) = U(\mathcal{A})^{\sigma_D - 1}. \tag{2.7}$$

Now notice that

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

and so by (2.5), (2.6), and (2.7),

$$V(\mathcal{A}) = U(\mathcal{A})^{\xi\bar{\xi}}. \tag{2.8}$$

Our claim now follows from (2.3) and (2.4).

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

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

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

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

$$\alpha^{\xi} \equiv 1 \bmod \mathcal{Q}\mathcal{O}_H, \tag{2.9}$$

and

$$\alpha^{\bar{\xi}} \equiv 1 \bmod \bar{\mathcal{Q}}\mathcal{O}_H \tag{2.10}$$

(recall that H/K is abelian).

So now (v) follows from (2.8) by taking $\alpha = U(\mathcal{A})^{\bar{\xi}}$ and $\alpha = U(\mathcal{A})^{\xi}$ in (2.9) and (2.10), respectively. (It is not hard to see that these numbers generate $\mathcal{A}$ and, in particular, they are prime to 2). This completes the proof of the theorem. □

2.4 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 $Cl(K)$.

Proposition 2.4.1 *For any classes $C, C' \in Cl(K)$ we have*

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

Proof: It follows from the Factorization Lemma (Lemma 2.1.1) applied to squares of ideals, Lemma 2.1.4, and the definition of t. We leave the details to the reader. □

We can now combine this with Hecke's formula (Theorem 1.2.6).

Theorem 2.4.2 *For every class $C \in Cl(K)$ and every $\varphi \in Cl(K)^*$,*

(i)

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

(ii)

$$L(1; \varphi\psi) = \frac{\pi}{\sqrt[4]{p}} \left(\sum_{C \in Cl(K)} \varphi(C)t(C) \right)^2,$$

and

(iii)

$$\sum_{\varphi} L(1; \varphi\psi) = \frac{h\pi}{\sqrt[4]{p}} \sum_{C} |t(C)|^2.$$

Proof: Recall that every class is a square. Part (i) follows directly from Proposition 2.4.1 and Hecke's formula (Theorem 1.2.6). 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 2.4.3 *For $\varphi \in Cl(K)^*$, let*

$$L(\varphi) = \frac{\sqrt{p}}{\pi} \frac{L(1;\varphi\psi)}{t(C_0)^2}$$

and

$$l(\varphi) = \sum_C \varphi(C) v_C.$$

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

(i)

$$L(\varphi)^{\sigma_C} = v_C^{-1} L(\varphi),$$

(ii)

$$L(\varphi)^{\varphi'} = L(\varphi'\varphi),$$

and

(iii)

$$L(\varphi) = l(\varphi)^2.$$

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

$$L(1;\varphi\psi) > 0.$$

Remark: That $L(1;\varphi\psi)$ is positive was first proved by Rohrlich in a different way (see [10]). Regarding the integrality of $L(\varphi)$, compare [5, cor. 3.2].

Proof: Parts (i) and (ii) follow easily from the properties of t given in Theorem 2.3.3. The first 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 2.3.3 that $t(C)$ is never zero). On the other hand, by part (ii) of this corollary, if one of the summands is zero, they all are. We conclude that $L(1;\varphi\psi)$ 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 $|v_C| \geq 1$ 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.

CHAPTER III

Applications

3.1 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 Gross' work in [1], [3], and [4].

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

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

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

where m and n are in F and satisfy

$$m^3 = j,$$

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

and

$$\text{sign}(n) = (\frac{2}{p}).$$

We let $\omega = \frac{dx}{2y}$ be the differential associated to this model; it is straightforward to check that $\Delta(\omega) = -p^3$.

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

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

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 $v = \mathcal{P}_0$, $m_v = 2$, and (ii) for $v = \mathcal{P}_i$ $(i = 1, 2, \ldots, h')$, $m_v = 4$.

We note in passing that from the above factorization of p and the fact that no other prime ramifies in $H/\mathbf{Q}$, it follows easily that the discriminant of $F/\mathbf{Q}$ 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 $\psi \circ \mathbf{N}_{H/K}$, with ψ being the Hecke character defined in section 1.2. It follows that the L-series of $A(p)$ over F factors as

$$L(s; A(p)/F) = \prod_{\varphi \in Cl(K)^*} L(s; \varphi\psi). \tag{3.1}$$

3.2 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 2.4.2) 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 [9, sec. 8]). In section 3.1 we already have most of the terms: we know the order of the torsion, the discriminant of $F/\mathbf{Q}$, 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

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

obtained by combining Theorem 2.4.2 (ii) with (3.1). It remains to compute m_v for the archimedean primes of F.

As in section 2.3, we identify the Galois group of H/K with the class group $Cl(K)$ via the Artin map. We pick representatives $\mathcal{A}_i \in \mathcal{R}$ for $i = 0, 1, \ldots, h'$ (here, as before, $h' = (h-1)/2$) such that

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

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

By Lemma 1.2.2 we can write

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

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

Corresponding to $\mathcal{A}_i$ 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 section 3.1. 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 [9] 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 3.2.1 *With the notation as above, we have the identity*

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

Proof: This follows from Theorem 2.3.3. We leave it to the reader. □

Theorem 3.2.2 *We denote by $S(p)$ the order of the Tate-Shafarevich group of $A(p)$ over F as predicted by the Birch-Swinnerton Dyer conjecture. We have the formula*

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

Remark: We should understand the right hand side as giving a specific choice of sign for the square root. This sign remains the same if we replace t by $-t$.

Proof: It amounts to putting together all the terms calculated above into the Birch-Swinnerton Dyer conjecture, as given for example by Manin (see [9, sec. 8]). We leave this to the reader. □

Corollary 3.2.3 *The number $S(p)$ is the square of a nonzero rational integer.*

Proof: That $S(p)$ is nonzero follows from Corollary 2.4.3 (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

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

where $v_C = t(C)/t(C_0)$ are the units defined in section 2.3. This already shows that $\mathcal{S}(p)$ is an algebraic number with at most powers of two in the denominator. We need to prove: (i) $\sqrt{\mathcal{S}(p)}$ is a rational number, and (ii) 2^{h-1} divides the numerator.

(i) To show $\sqrt{\mathcal{S}(p)}$ is a rational number, we check its behaviour under the action of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$. For this we use the various properties of t described in Theorem 2.3.3.

(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 $C \in Cl(K)$, the numerator changes by a factor of $v_C^{-h} \prod_\varphi \varphi^{-1}(C)$, and the denominator by v_C^{-h}. Since $Cl(K)^*$ is of odd order, it follows that $\sqrt{\mathcal{S}(p)}$ remains fixed.

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

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

(ii) To show that 2^{h-1} divides the numerator in the formula for $\sqrt{\mathcal{S}(p)}$, let $M' = M(\zeta_h)$, where ζ_h is a primitive hth root of unity. Let $\mathcal{Q}$ be any prime of M' above 2. It follows from Theorem 2.3.3 (v) that the map

$$\begin{array}{ccc} Cl(K) & \longrightarrow & (\mathcal{O}_{M'}/\mathcal{Q})^* \\ C & \mapsto & v_C \end{array}$$

is a homomorphism. Therefore, $h-1$ of the factors in the numerator are divisible

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

Bibliography

[1] Joe P. Buhler and B. H. Gross. Arithmetic on Elliptic Curves with Complex Multiplication II. Inventiones Mathematicae **79**, 11-29 (1985)

[2] M. Deuring. Die Klassenkörper der Komplexen Multiplication. Ency. der Math. Wiss. Band I, 2. Teil, Heft 10, Teil II (1958)

[3] B. H. Gross. Arithmetic on Elliptic Curves with Complex Multiplication. Springer Lecture Notes **776** (1980)

[4] B. H. Gross. Minimal Models for Elliptic Curves with Complex Multiplication. Compositio Mathematica **45**, 155-164 (1982)

[5] C. Goldstein and N. Schappacher. Series d'Eisenstein et fonctions L de courbes elliptiques a multiplication complexe. Crelle J. **327**, 184-218 (1981)

[6] E. Hecke. Mathematische Werke. Vandenhoeck and Ruprecht, Götingen, 1959

[7] L. Kronecker. Leopold Kronecker's Werke. B.G. Teubner, Leipzig und Berlin, 1929

[8] S. Lang. Elliptic Functions. Reading: Addison-Wesley (1973)

[9] Y. I. Manin. Cyclotomic fields and Modular Curves. Russian Math. Surveys **26**, (No. 6), 7-78 (1971)

[10] D. Rohrlich. The non-vanishing of certain Hecke L-functions at the center of the critical strip. Duke Math. J. **47**, No 1, 223-232 (1980)

[11] H. Stark. L-series at s=1 IV. Adv. in Math. **35**, 197-235 (1980)

[12] H. Weber. Lehrbuch der Algebra. Vol. 3, Chelsea, New York, 1961