The Birch and Swinnerton-Dyer formula for modular abelian varieties of analytic rank zero

by

Amod Sadanand Agashe

B. Tech. (Indian Institute of Technology, Bombay) 1991
M. S. (Stanford University) 1993

A dissertation submitted in partial satisfaction of the
requirements for the degree of
Doctor of Philosophy

in

Mathematics

in the

GRADUATE DIVISION
of the
UNIVERSITY of CALIFORNIA at BERKELEY

Committee in charge:

Professor Kenneth A. Ribet, Chair
Professor Hendrik W. Lenstra
Professor David A. Forsyth

Spring 2000

The dissertation of Amod Sadanand Agashe is approved:

Chair Date

Date

Date

University of California at Berkeley

Spring 2000

The Birch and Swinnerton-Dyer formula for modular abelian varieties of analytic rank zero

Abstract

The Birch and Swinnerton-Dyer formula for modular abelian varieties of analytic rank zero

by

Amod Sadanand Agashe
Doctor of Philosophy in Mathematics

University of California at Berkeley

Professor Kenneth A. Ribet, Chair

Let N be a positive integer and let A be an optimal quotient of $J_0(N)$ such that its special L-value, $L_A(1)$, is non-zero. Let Ω_A be the volume of $A(\mathbf{R})$ calculated using a set of generators of the group of invariant differentials on the Néron model of A. Denote the Shafarevich-Tate group of A by $Ш_A$ and the dual abelian variety of A by $\widehat{A}$. Let $c_p(A)$ be the order of the arithmetic component group of A at the prime p. Then the Birch and Swinnerton-Dyer (BSD) conjecture (as generalized by Tate and Gross) asserts the formula:

$$\frac{L_A(1)}{\Omega_A} = \frac{|Ш_A| \cdot \prod_{p|N} c_p(A)}{|A(\mathbf{Q})| \cdot |\widehat{A}(\mathbf{Q})|}.$$

We express the ratio $L_A(1)/\Omega_A$ as a rational number when A is the quotient associated to a newform of weight 2 for $\Gamma_0(N)$, and also, in the case of prime level, when A is the winding quotient of $J_0(N)$. One would like to compare our expression for $L_A(1)/\Omega_A$ to the right-hand side of the BSD formula above. We present partial results in that direction and also outline a program to approach the problem. We compute $L_A(1)/\Omega_A$, up to a bounded factor, using modular symbols. Assuming the BSD formula, when $N = 1091$ and A is the winding quotient, we find that there are elements of $Ш_A$ that are visible neither in $J_0(N)$ nor in $J_1(N)$.

There are three numbers associated to a strong modular elliptic curve: the modular degree, the congruence number and the Manin constant. We prove a result about primes whose squares do not divide the conductor of the elliptic curve: if such a prime divides either the Manin constant or the congruence number, then it divides the modular degree as well. We also generalize the Manin constant to higher dimensional quotients of $J_0(N)$ and prove some results about our generalization.

Professor Kenneth A. Ribet
Dissertation Committee Chair

Contents

Acknowledgements

I started my graduate research with Prof. L. Merel, and most of the work in this thesis was done under his guidance. In particular, Chapter 3, Section 4.2, and Section 5.3 owe a lot to him. I would like to express my heartfelt gratitude to him for patiently spending a lot of time in discussions with me and for giving me direction during my graduate research. I am also deeply grateful to Prof. K. Ribet for acting as my official advisor, for his constant support, and for his mathematical input at various points in this thesis. Special thanks go to William Stein for the great collaboration that shaped the latter part of my graduate research. Finally, I am grateful to Prof. B. Mazur for answering several mathematical questions.

There are a lot of other people to whom I am indebted for several mathematical discussions and general advice during my graduate research. They are too many to name here, and also I am afraid I might miss out someone, so I hope they excuse me for not mentioning their names; my gratitude to them is no less than to anyone else: their help will never be forgotten. In any case, I would like to at least thank Ahmed Abbes, Matt Baker, Jim Borger, Kevin Buzzard, Bas Edixhoven, Hendrik Lenstra, Martin Olsson, Bjorn Poonen, Bernd Sturmfels and Richard Taylor who provided direct mathematical input at certain points in this thesis.

I am very grateful to the Department of Mathematics at the University of California, Berkeley for supporting me financially with teaching assistantships and fellowships, including the Raymond H. Sciobereti fellowship. Also, I would like to thank the Department of Mathematics at the Université de Paris 6 for their excellent hospitality during my stay there. Part of the research on this thesis was supported by NSF grant #DMS 99 70593, for which I am very grateful.

A guide to this thesis

There are three different themes in this thesis:

1) The ratio of the special L-value to the real volume: As mentioned in the abstract, if A is an abelian variety over $\mathbf{Q}$, then the Birch and Swinnerton-Dyer (BSD) formula gives a conjectural formula for the ratio of the special L-value of A, denoted $L_A(1)$, to the real volume of A, denoted Ω_A. We first describe the conjectural formula in Chapter 1. In Chapter 3, we give a formula that expresses the ratio mentioned above as a rational number when A is the winding quotient of prime level. In Chapter 4, we give a similar formula for this ratio for some other quotients of $J_0(N)$, including the quotient associated to a newform by Shimura. Such formulas were known for strong modular elliptic curves, but not for any higher dimensional quotients. Chapters 3 and 4 depend on Chapter 1, but otherwise can be read fairly independently of the rest of the thesis.

2) The generalized Manin constant, congruence primes and the modular degree: In Chapter 2, we obtain new results on the Manin constant, state a generalization of its definition, and give some new relations between congruence primes and the modular degree. This chapter can be read independently of the rest of the thesis.

3) Invisible elements of the Shafarevich-Tate group: Mazur introduced the notion of visible elements of the Shafarevich-Tate group of optimal modular elliptic curves. In Chapter 5, we generalize some of his results to higher dimensional abelian varieties. This chapter can be read fairly independently of the rest of the thesis.

At the beginning of each of Chapters 2, 3, and 5, and the beginnings of the sections of Chapter 4, we summarize the contents of those particular parts of the thesis. So the reader can read those summaries for a more detailed outline. Also, Chapter 1 serves as an introduction and motivation for the entire thesis.

We have tried to write this thesis so that it can be easily used as a reference. Even though the chapters appear in a sequence demanded by logical progression, they need not be read in a linear order. At the beginning of each chapter (or section), we mention the prerequisites for that chapter and its relation to the rest of the thesis. Also, in each chapter we try to recall the notation from before that will be used, or give cross-references for the notation. Moreover, there is a list of symbols and an index of definitions at the end of the thesis. So the readers can safely jump directly into any chapter they are interested in.

The Theorems, Lemmas, Remarks, etc., are numbered consecutively and by section. Thus Theorem 2.1.6 is the 6th result in Section 1 of Chapter 2. The equations are labeled consecutively and by chapter, but independent of the Theorems, Lemmas, etc.; however, the

equations are usually only referred to within the proof or the section that they appear in.

The two main new ideas in this thesis are: the trick used to cancel the "discriminant" from the numerator and the denominator of $L_A(1)/\Omega_A$ that allows us to express this ratio as a rational number (see the Claim in the proof of Theorem 3.2.2 on p. 21), and the idea of using a "conjugate" isogeny to obtain some new information about the Manin constant and about the relation between congruence primes and the modular degree (see the latter half of the proof of Proposition 2.3.5 on p. 13).

Chapter 1

Introduction: The Birch and Swinnerton-Dyer conjecture

1.1 The conjecture for abelian varieties

Now that the Shimura-Taniyama-Weil conjecture has been proved, one of the main outstanding problems in number theory is the Birch and Swinnerton-Dyer (BSD) conjecture. This conjecture was made more than thirty years ago by Birch and Swinnerton-Dyer [BSD63] [BSD65] for elliptic curves; it was then extended to abelian varieties by Tate [Tat95], and to motives by Deligne, Beilinson, Bloch and Kato [BK90]. As Cassels remarks [Cas63], a fundamental problem of number theory is: given a set of polynomial equations with rational coefficients, find all of its rational solutions and investigate their structure. In many cases, the BSD conjecture predicts the existence of such solutions and describes their structure without actually finding the solutions. Thus the BSD conjecture addresses some basic questions in number theory. It also gives a relation among several fundamental invariants of an abelian variety defined over a number field. In particular, it proposes a formula for the order of the Shafarevich-Tate group of the abelian variety, a mysterious invariant that arises in the calculation of the Mordell-Weil group using descent, and elsewhere. A lot of progress has been made on the BSD conjecture by the works of Coates, Wiles, Gross, Zagier, Rubin, Kolyvagin, Kato, et al.; but a large part of the conjecture is still not proved (for a summary of results and references, see [IR90, Chap. 20, §5], [Dar97, §4], and [Rub98, Thm. 8.6, Cor. 8.9]).

We now describe the conjecture briefly. Let A be an abelian variety defined over $\mathbf{Q}$. Attached to A is a complex-valued function $L_A(s)$, defined on the part of the complex plane where $\mathrm{Re}(s)$ is sufficiently large. It is called the *L-function* of A and is obtained by packaging information about the number of points of A over finite fields (see [Lan91, § III.5, p. 95] for the precise definition). Suppose, as conjectured, that the function $L_A(s)$ extends to an analytic function on the entire complex plane. Let r denote the rank of the finitely generated abelian group $A(\mathbf{Q})$.

The first part of the Birch and Swinnerton-Dyer conjecture says:

Conjecture 1.1.1. *$L_A(s)$ has a zero of order r at $s = 1$.*

Let W denote the $\mathbf{Z}$-module of invariant differentials on the Néron model of A. Then $\mathrm{rank}(W) = d$, where $d = \dim(A)$, and $\wedge^d W$ is a free $\mathbf{Z}$-module of rank 1 contained in $H^0(A, \Omega^d_{A/\mathbf{Q}})$. Let D be a generator of $\wedge^d W$. Let $\{\omega_1, \ldots, \omega_d\}$ be a basis of $H^0(A, \Omega_{A/\mathbf{Q}})$ over $\mathbf{Q}$. Then $D = c \cdot \wedge_j \omega_j$ for some $c \in \mathbf{Q}^*$. If G is a group with an action of complex conjugation, then we denote the subgroup of elements of G invariant under this action by G^+. Let $\{\gamma_1, \ldots, \gamma_d\}$ be a basis of $H_1(A, \mathbf{Z})^+$ and let $c_\infty(A)$ denote the number of connected components of $A(\mathbf{R})$. Then the quantity $|c_\infty(A) \cdot c \cdot \det(\int_{\gamma_i} \omega_j)|$ depends only on A; we call it the *real volume* of A, and denote it by Ω_A.

Let $\widehat{A}$ denote the dual abelian variety of A. We define the *regulator* of A, denoted R_A, by $R_A = |\det(h(P_i, P'_j))|$, where $\{P_1, \ldots, P_r\}$ is a basis of $A(\mathbf{Q})/A(\mathbf{Q})_{\mathrm{tor}}$, $\{P'_1, \ldots, P'_r\}$ is a basis of $\widehat{A}(\mathbf{Q})/\widehat{A}(\mathbf{Q})_{\mathrm{tor}}$, and h denotes the Néron pairing (see [Lan91, III.1.7]).

The Shafarevich-Tate group of A, denoted $Ш_A$, consists of equivalence classes of principal homogeneous spaces of A that are locally trivial everywhere; it is conjectured to be finite. Let $\mathcal{A}$ denote the Néron model of A over $\mathbf{Z}$ and let $\mathcal{A}^0$ denote the largest open subgroup scheme of $\mathcal{A}$ in which all the fibers are connected. If p is a prime number, then let $c_p(A) = [\mathcal{A}_{\mathbf{F}_p}(\mathbf{F}_p) : \mathcal{A}^0_{\mathbf{F}_p}(\mathbf{F}_p)]$.

If G is a finite group, then $|G|$ denotes its order. Assume that the Shafarevich-Tate group is finite, and that the first part of the BSD conjecture is true. Then the second part of the BSD conjecture, as generalized by Tate, and reformulated by Gross (e.g., see [Lan91, III.5]) gives the formula:

Conjecture 1.1.2.

$$\frac{1}{r!}\frac{L_A^{(r)}(1)}{\Omega_A} \stackrel{?}{=} \frac{|Ш_A| \cdot R_A \cdot \prod_p c_p(A)}{|A(\mathbf{Q})_{\mathrm{tor}}| \cdot |\widehat{A}(\mathbf{Q})_{\mathrm{tor}}|},$$

where $L_A^{(r)}(s)$ denotes the rth derivative of $L_A(s)$, and the rest of the terms are as defined above.

Here, and in the future, the symbol $\stackrel{?}{=}$ denotes an equality that is conjectured but not proved. The formula above shall be called the *BSD formula*.

Note that the formula says that the ratio $L_A^{(r)}(1)/\Omega_A$, which a priori is a complex number, is in fact rational; moreover, the formula expresses this rational number in terms of certain arithmetic invariants of A.

1.2 The conjectural formula for modular abelian varieties

In this thesis, we will consider the BSD formula only for a certain class of abelian varieties that we define now. In this section, we also gather some results and notation that will be used in Chapters 3 and 4. We continue to us the notation of the previous section.

Let N be a positive integer and let $X_0(N)$ be the modular curve over $\mathbf{Q}$ associated with the problem of parametrizing elliptic curves with a cyclic subgroup of order N. Let $J_0(N)$ denote the Jacobian of $X_0(N)$; it is an abelian variety defined over $\mathbf{Q}$. The integer N will be referred to as the *level*. The *Hecke algebra*, denoted by $\mathbf{T}$, is the subring of endomorphisms of $J_0(N)$ generated by the Hecke operators T_ℓ for $\ell \nmid N$ and U_p for $p \mid N$. See, for example, [DDT94, §1.3, §1.5] for detailed definitions of all of the above. Let I be an ideal of

the Hecke algebra such that $\mathbf{T}/I$ is torsion-free, and let A be the quotient abelian variety $J_0(N)/IJ_0(N)$, defined over $\mathbf{Q}$. We call such abelian varieties *modular abelian varieties*. Then the L-function of A, $L_A(s)$, has analytic continuation to the entire complex plane (by [Shi94, Thm. 7.14], completed by [Car86]). The order of vanishing of $L_A(s)$ at $s = 1$ is called the *analytic rank* of A. This definition is motivated by Conjecture 1.1.1. In this thesis, we consider only modular abelian varieties A whose analytic rank is zero, i.e., for which $L_A(1)$ is non-zero. We call $L_A(1)$ the *special L-value* of A. So assume that A has analytic rank zero. Then, by [KL89] (which uses [GZ86], and was completed independently in [BFH90] and [MM91]), the Mordell-Weil group, $A(\mathbf{Q})$, and the Shafarevich-Tate group, $Ш_A$, are finite. In particular, the first part of the BSD conjecture (Conjecture 1.1.1) is true in this case, and also the regulator, R_A, is equal to 1. Since $\widehat{A}$, the dual abelian variety of A, is isogenous to A, the Mordell-Weil group $\widehat{A}(\mathbf{Q})$ is also finite.

The BSD formula becomes

Conjecture 1.2.1.

$$\frac{L_A(1)}{\Omega_A} \stackrel{?}{=} \frac{|Ш_A| \cdot \prod_{p|N} c_p(A)}{|A(\mathbf{Q})| \cdot |\widehat{A}(\mathbf{Q})|}.$$

It is known that $L_A(1)/\Omega_A$ is a rational number [Shi77] and when A is an elliptic curve, there are formulas to calculate this rational number as well as all the invariants in the BSD formula except $|Ш_A|$ (e.g., see [Cre97]). Also, one can use Euler systems to bound the order of $Ш_A$ from above in terms of the order given by Conjecture 1.2.1 (staying away from certain primes), as in the work of Kolyvagin and of Kato (e.g., see [Rub98, Thm. 8.6]). However, as Swinnerton-Dyer remarked in [SD67], there was no known formula for calculating $L_A(1)/\Omega_A$ when A is not an elliptic curve. In this thesis, we give such formulas for certain quotients of $J_0(N)$ that need not be elliptic curves (see Sections 3.2, 4.1.1, and 4.2.1); the first such formula appeared in [Aga99] (although it was not stated explicitly there).

Now we discuss the left-hand side of the BSD formula in Conjecture 1.2.1 in more detail. Let $S_2(\Gamma_0(N), \mathbf{C})$ denote the space of cusp forms of weight 2 for $\Gamma_0(N)$. By the *Fourier expansion* of a cusp form, we mean its Fourier expansion at the cusp ∞ (e.g., see [DDT94, §1.2]); the coefficients of this expansion are called the *Fourier coefficients* of the cusp form. Let $S_2(\Gamma_0(N), \mathbf{Z})$ be the subgroup of cusp forms with integral Fourier coefficients. If R is a ring, let $S_2(\Gamma_0(N), R) = S_2(\Gamma_0(N), \mathbf{Z}) \otimes R$. The Hecke algebra $\mathbf{T}$ acts on $S_2(\Gamma_0(N), R)$ (see, e.g., [DDT94, §1.3, §1.5] for details). If M is a $\mathbf{T}$-module, then $M[I]$ denotes the submodule of elements of M that are killed by every element of I. The map

$$S_2(\Gamma_0(N), \mathbf{C}) \to H^0(X_0(N), \Omega_{X_0(N)/\mathbf{C}}),$$

given by $f \mapsto \omega_f = 2\pi i f(z)dz$ induces a canonical isomorphism

$$S_2(\Gamma_0(N), \mathbf{Q}) \stackrel{\cong}{\longrightarrow} H^0(X_0(N), \Omega_{X_0(N)/\mathbf{Q}})$$

(for example, by [DDT94, Thm. 1.33]). We have the standard immersion $X_0(N) \to J_0(N)$ obtained by sending the cusp ∞ to 0; pulling back differentials along this map gives us an isomorphism (e.g., see [Mil86c, Prop. 2.2])

$$H^0(J_0(N), \Omega_{J_0(N)/\mathbf{Q}}) \cong H^0(X_0(N), \Omega_{X_0(N)/\mathbf{Q}}).$$

Using the two isomorphisms above, we get an isomorphism:

$$S_2(\Gamma_0(N), \mathbf{Q}) \xrightarrow{\cong} H^0(J_0(N), \Omega_{J_0(N)/\mathbf{Q}}). \tag{1.1}$$

Let $d = \dim(A)$. A $\mathbf{Q}$-basis for $H^0(A, \Omega_{A/\mathbf{Q}})$ is given by the differentials corresponding to a set of generators of the $\mathbf{Z}$-module $S_A = S_2(\Gamma_0(N), \mathbf{Z})[I]$ under the isomorphism (1.1); denote this basis by $\{\omega_1, \ldots, \omega_d\}$. As in Section 1.1, let D be a generator of $\wedge^d H^0(\mathcal{A}, \Omega^d_{\mathcal{A}/\mathbf{Z}})$, where again $\mathcal{A}$ is the Néron model of A over $\mathbf{Z}$. Then $D = c \cdot \wedge_j \omega_j$ for some $c \in \mathbf{Q}^*$. The absolute value of c is depends only on A; denote this absolute value by c_A. We call the constant c_A the generalized Manin constant and study it in Chapter 2. The generalized Manin constant is an integer (Theorem 2.2.2) and the only primes that can divide it are the prime 2 and the primes whose squares divide N (Theorem 2.2.3).

If $\langle\ ,\ \rangle : M \times M' \to \mathbf{C}$, is a pairing between two $\mathbf{Z}$-modules M and M', each of the same rank m, and $\{\alpha_1, \ldots, \alpha_m\}$ and $\{\beta_1, \ldots, \beta_m\}$ are some bases of M and M' (respectively), then the *discriminant of the pairing* $\langle\ ,\ \rangle$ is defined as the absolute value of $\det(\langle \alpha_i, \beta_j \rangle)$, and denoted by $\mathrm{disc}(M \times M' \to \mathbf{C})$. We have a pairing

$$\langle\ ,\ \rangle : (H_1(X_0(N), \mathbf{Z})^+ \otimes \mathbf{C}) \times S_2(\Gamma_0(N), \mathbf{C}) \to \mathbf{C}$$

given by $(\gamma, f) \mapsto \langle \gamma, f \rangle = \int_\gamma \omega_f$. This induces a pairing $H_1(A, \mathbf{Z})^+ \times S_A \to \mathbf{C}$.

From the definition of Ω_A in Section 1.1 and the discussion above, we get

$$\Omega_A = c_A \cdot c_\infty(A) \cdot \mathrm{disc}(H_1(A, \mathbf{Z})^+ \times S_A \to \mathbf{C}).$$

In this thesis, we shall study only the left-hand side of the BSD formula in Conjecture 1.2.1 (except in Section 3.4, where we discuss the right-hand side briefly). We may rewrite the left-hand side as

$$\frac{1}{c_A} \cdot \frac{L_A(1)}{c_\infty(A) \cdot \mathrm{disc}(H_1(A, \mathbf{Z})^+ \times S_A \to \mathbf{C})}\ . \tag{1.2}$$

Now we are in a position to describe in more detail how the various chapters are related to the BSD formula. In Chapter 2, we study the constant c_A in (1.2) above. We prove formulas expressing the term

$$\frac{L_A(1)}{c_\infty(A) \cdot \mathrm{disc}(H_1(A, \mathbf{Z})^+ \times S_A \to \mathbf{C})}$$

appearing in (1.2) as a rational number when A is the winding quotient of prime level (in Chapter 3) and for certain other quotients (in Chapter 4). The only relation of the BSD formula to Chapter 5 is that we use it to get some information on $|Ш_A|$ (assuming the conjectural formula) by using the formula for (1.2) that we derive in Chapter 3.

Chapter 2

A generalization of the Manin constant and the relation between congruence primes and the modular degree

We extend the techniques of a paper of Abbes and Ullmo [AU96] to show that if E is a strong modular elliptic curve and if p is a prime such that p does not divide the modular degree of E, and p^2 does not divide the conductor of E, then p does not divide the Manin constant of E either. We also show that except for primes whose squares divide the conductor, the congruence primes associated to the newform corresponding to E divide the modular degree of E. Finally we generalize the notion of the Manin constant to arbitrary quotients of $J_0(N)$ under the action of ideals of the Hecke algebra and mention the corresponding results and a conjecture for it. This chapter may be read independently of the rest of the thesis. Only Theorem 2.2.3 and Conjecture 2.2.8 from this section will be referred to later.

2.1 Introduction and results

We recall the definition of the Manin constant and what is known about it. Let N be a positive integer and recall that $X_0(N)$ is the modular curve over $\mathbf{Q}$ that classifies elliptic curves with a given cyclic subgroup of order N. Let $J_0(N)$ be the Jacobian of $X_0(N)$ and let f be a newform of weight 2 for $\Gamma_0(N)$ with integral Fourier coefficients. Recall that the Hecke algebra, denoted $\mathbf{T}$, is the sub-ring of endomorphisms of $J_0(N)$ generated by the Hecke-operators T_ℓ for primes $\ell \nmid N$ and by U_p for $p \mid N$. Let I_f be the annihilator of f under the action of $\mathbf{T}$, and let $E = J_0(N)/I_f J_0(N)$ be the indicated quotient, an elliptic curve over $\mathbf{Q}$. We call such an elliptic curve the *strong modular elliptic curve* associated to f. Composing the quotient map $J_0(N) \to E$ with the standard immersion $X_0(N) \to J_0(N)$

obtained by sending the cusp ∞ to 0, we get a surjective map of curves

$$\phi_E : X_0(N) \to E.$$

The degree of the map ϕ_E, denoted $\deg\phi_E$, is called *the modular degree* of E.

Let $E_{\mathbf{Z}}$ be the Néron model of E. Then the $\mathbf{Z}$-module of invariant differentials on $E_{\mathbf{Z}}$ is free of rank one; let ω be one of its two generators. Pulling it back to $X_0(N)$, we get a differential form $\phi_E^*\omega$ on $X_0(N)$. Now the newform f gives another differential $2\pi i f(z)dz$ on $X_0(N)$. By the multiplicity one theorem, we have $\phi_E^*\omega = c \cdot 2\pi i f(z)dz$ for some $c \in \mathbf{Q}^*$. The absolute value of c depends only on E; we denote this absolute value by c_E. It is called the *Manin constant* of E. The Manin constant is of interest because it plays a role in the BSD conjecture (see Sections 1.2 and 2.2.1).

Conjecture 2.1.1 (Manin). $c_E = 1$.

The following results are known towards this conjecture:

Theorem 2.1.2 (Edixhoven [Edi91, Prop. 2]). $c_E \in \mathbf{Z}$.

Theorem 2.1.3 (Mazur [Maz78, Cor. 4.1]). *If p is a prime such that $p \mid c_E$, then $p^2 \mid N$ or $p = 2$.*

Theorem 2.1.4 (Raynaud [AU96, Prop. 3.1]). *If $2^2 \nmid N$, then $2^2 \nmid c_E$.*

Theorem 2.1.5 (Abbes-Ullmo [AU96, Thm. A]). *If p is a prime such that $p \mid c_E$, then $p \mid N$.*

Also B. Edixhoven has unpublished results (see [Edi89]) which say that the only primes that can possibly divide c_E are $2, 3, 5, 7$; he also gives bounds on the valuation of c_E (independent of E) with respect to these primes. Thus, from what is known so far, if a prime p divides c_E, then either $p = 2$ and $2 \mid N$, or $p = 3, 5,$ or 7 and $p^2 \mid N$; moreover, there are bounds (independent of E) on the powers of these primes that can divide c_E.

To this, we add the following theorem, whose proof builds on the techniques of [AU96].

Theorem 2.1.6. *If p is a prime such that $p \mid c_E$, then $p^2 \mid N$ or $p \mid \deg\phi_E$.*

In view of what was known before, the only new information is that if $2 \mid N$, but $2^2 \nmid N$ and $2 \nmid \deg\phi_E$, then $2 \nmid c_E$. For example, for the elliptic curve $E = 46\text{A}1$ of [Cre97, Table 1], earlier one could only conclude that c_E is 1 or 2. But, from [Cre97, Table 5], we find that the modular degree of E is 5, and so by Theorem 2.1.6, $c_E = 1$.

Let r_E be the largest integer such that there exists a modular form g that has integral Fourier coefficients, that is orthogonal to f with respect to the Petersson inner product, and that satisfies $g \equiv f \bmod r_E$. It is called the *congruence number* of E and primes dividing it are called the *congruence primes* of E.

Theorem 2.1.7 (Ribet [Zag85, Thm. 3], [AU96, Lem 3.3]). $\deg\phi_E \mid r_E$; *moreover, if N is prime, then $r_E = \deg\phi_E$.*

The congruence number and the modular degree are quantities of great interest: congruence primes have been studied by Hida and Ribet, among others, and played a role in Wiles' proof of Fermat's last theorem, and the modular degree plays a role in a reformulation of the *abc*-conjecture, among other things.

K. Ribet pointed out to us that results regarding the relationship between congruence primes and the modular degree can be obtained from the techniques in the proofs of multiplicity one theorems as in [Maz77, II.9] and [Wil95, §2.1]. Using these techniques, one can show that if p is a prime such that $p \mid \frac{r_E}{\deg\phi_E}$, then $p \mid N$ (see [AS99a] for details). This result also follows independently from [AU96, Prop. 3.3 and Prop. 3.4].

Frey and Muller [FM99] raised the question whether $r_E = \deg\phi_E$. The answer, however, is no. For example, consider the elliptic curve 54B1 of [Cre97]; call it F. By [Cre97, Table 5]), $\deg\phi_F = 2$; calculations of W. Stein show that $r_F = 6$. Thus $r_F \neq \deg\phi_F$, and $3 \mid \frac{r_F}{\deg\phi_F}$. The problem, of course, is that 3^2 divides the level, which is 54. In all the examples where W. Stein found that $r_E \neq \deg\phi_E$, it is always the case that if p is a prime such that $p \mid \frac{r_E}{\deg\phi_E}$, then $p^2 \mid N$. So one can reformulate the question of Frey and Muller as:

Question 2.1.8. If p is a prime such that $p^2 \nmid N$, then is it true that $p \nmid \frac{r_E}{\deg\phi_E}$?

As an outcome of the proof of Theorem 2.1.6, we get the result:

Theorem 2.1.9. *Let p be a prime such that $p^2 \nmid N$. If $p \mid \frac{r_E}{\deg\phi_E}$ then $p \mid \deg\phi_E$; in particular, if $p \mid r_E$, then $p \mid \deg\phi_E$ also.*

Thus if N is squarefree, then the congruence primes divide the modular degree. For example, from [Cre97, Table 3] (and using [Stu87]), we find that the eigenform corresponding to the elliptic curve 26A shares a 2-congruence with the form corresponding to the elliptic curve 26B; also we have $2^2 \nmid 26$. So we conclude that 2 divides the modular degrees of the elliptic curves 26A and 26B. Indeed, on looking up [Cre97, Table 5], we find that the modular degrees of 26A and 26B are in fact equal to 2.

In Section 2.2, we generalize the notion of the Manin constant to quotients of $J_0(N)$ of arbitrary dimension associated to ideals of the Hecke algebra, and indicate which of the above results apply in the general situation. Finally, in Section 2.3, we prove all the new theorems mentioned in Sections 2.1 and 2.2.

2.2 A generalization of the Manin constant

Again let N be a positive integer. For simplicity of notation, we will often denote the Jacobian of $X_0(N)$, usually denoted $J_0(N)$, by just J. Let I be an ideal of $\mathbf{T}$ such that $\mathbf{T}/I$ is torsion-free and let A be the quotient abelian variety J/IJ defined over $\mathbf{Q}$. If R is a Dedekind domain with field of fractions $\mathbf{Q}$, and B is an abelian variety over $\mathbf{Q}$, then let B_R denote its Néron model over R. If R is a subring of $\mathbf{C}$, let $S_2(R)$ denote the subgroup of $S_2(\Gamma_0(N), \mathbf{C})$ consisting of modular forms whose Fourier expansions (at the cusp ∞) have coefficients in R (this is the same as the definition of $S_2(\Gamma_0(N), R)$ in Section 1.2: for a proof, see [DDT94, §1.5]).

2.2.1 Motivation and definition

In the Birch and Swinnerton-Dyer conjecture for A, one considers the ratio of a certain L-value to the real volume of A (see Section 1.1). This real volume is calculated by using a set of generators for $H^0(A_{\mathbf{Z}}, \Omega^1_{A/\mathbf{Z}})$, which is the group of global differentials on the Néron model of A. But in calculations (see [AS99b]), or while proving formulas regarding the BSD conjecture (see Sections 3.2, 4.1.1, and 4.2.1), it is easier to work with the volume obtained by using a set of generators of $S_2(\mathbf{Z})[I]$, which is the group of cusp forms with integral Fourier expansion annihilated by I.

We recall the definition of the generalized Manin constant from Section 1.2. Let $d = \dim(A)$. A $\mathbf{Q}$-basis for $H^0(A, \Omega_{A/\mathbf{Q}})$ is given by the differentials corresponding to a set of generators of the $\mathbf{Z}$-module $S_2(\mathbf{Z})[I]$; denote this basis by $\{\omega_1, \ldots, \omega_d\}$. If D is a generator of $\wedge^d H^0(A_{\mathbf{Z}}, \Omega^1_{A/\mathbf{Z}})$, then there exists $c \in \mathbf{Q}^*$ such that $D = c \cdot \wedge_j \omega_j$ in $H^0(A_{\mathbf{Q}}, \Omega^1_{A/\mathbf{Q}})$. The absolute value of c depends only on A.

Definition 2.2.1. *The* generalized Manin constant c_A *is the absolute value of the constant c defined above.*

If the abelian variety A is an elliptic curve, then c_A is the usual Manin constant. In calculations or formulas regarding the Birch and Swinnerton-Dyer conjecture, one finds the real volume with respect to $S_2(\mathbf{Z})[I]$ and corrects it by c_A (see Section 1.2) . Note that the generalized Manin constant in this form was considered by Gross [Gro82, (2.5) on p. 222] and Lang [Lan91, III.5, p.95].

2.2.2 A finer definition

We essentially follow the ideas in [Edi91, Prop. 2]. Let $M_0(N)$ denote the compactified coarse moduli scheme $\overline{M}([\Gamma_0(N)])$ (see [KM85, 8.6]) and let $M_0(N)^0$ be the open part of $M_0(N)$ where the projection to Spec$\mathbf{Z}$ is smooth. By the Néron property, we get maps

$$M_0(N)^0 \to J_{\mathbf{Z}} \to A_{\mathbf{Z}}.$$

Call the composite map ϕ_A (we are abusing notation slightly here; however this map ϕ_A induces the map ϕ_E from Section 2.1 when A is an elliptic curve E). It follows from [KM85, Thm. 8.11.10] that the formal completion of $M_0(N)$ along the (unramified) cusp ∞ is Spf($\mathbf{Z}[[q]]$). Thus we have a map

$$H^0(M_0(N)^0, \Omega^1_{M_0(N)^0/\mathbf{Z}}) \to \mathbf{Z}[[q]].$$

which we denote by q-exp. Its image is contained in $S_2(\mathbf{Z})$, which is considered as a subgroup of $\mathbf{Z}[[q]]$ by taking the Fourier expansion of cusp forms (see [DDT94, Thm. 1.33], for example). We have the series of maps:

$$H^0(A_{\mathbf{Z}}, \Omega^1_{A_{\mathbf{Z}}/\mathbf{Z}}) \xrightarrow{\phi_A^*} H^0(M_0(N)^0, \Omega^1_{M_0(N)^0/\mathbf{Z}}) \xrightarrow{q\text{-exp}} \mathbf{Z}[[q]].$$

The image of $H^0(A_{\mathbf{Z}}, \Omega^1_{A_{\mathbf{Z}}/\mathbf{Z}})$ under the composite is contained in $S_2(\mathbf{Z})[I] \subseteq \mathbf{Z}[[q]]$. Let

$$C_A = \frac{S_2(\mathbf{Z})[I]}{q\text{-exp}(\phi_A^*(H^0(A_{\mathbf{Z}}, \Omega^1_{A_{\mathbf{Z}}/\mathbf{Z}})))}$$

be the finite quotient group. It is in fact a module over $\mathbf{T}$, and c_A is just the order of C_A. In particular, the above argument gives:

Theorem 2.2.2 (generalization of Thm. 2.1.2 of Edixhoven). $c_A \in \mathbf{Z}$.

2.2.3 Results and a conjecture

At first, one might think that the generalized Manin constant should also be 1. But, when $A = J_0(N)$, the constant c_A is just the order of the cokernel of the map

$$H^0(M_0(N)^0, \Omega^1_{M_0(N)^0/\mathbf{Z}}) \stackrel{q\text{-exp}}{\longrightarrow} S_2(\mathbf{Z}), \tag{2.1}$$

and this map is not surjective in general. The order of the cokernel can be calculated using methods in [DR73]. For example, B. Edixhoven informed us that for $N = 33$ the cokernel has order 3, and thus $c_{J_0(33)} = 3$. So the generalized Manin constant is not 1 in general.

B. Edixhoven informed us that if N is square-free, then the map (2.1) is surjective if and only if there are no old-spaces in $S_2(\Gamma_0(N), \mathbf{C})$. In the formula for the ratio of the special L-value to the real volume for winding quotients of level a product of two distinct primes (see Theorem 4.2.1), primes dividing the level appear in the numerator, and if the BSD formula is true, then it is reasonable to expect that they cancel the Manin constant that appears in the denominator (this was found to be the case in an explicit example). However, in the corresponding formula for the winding quotient of prime level (see Theorem 3.2.2), there is no reason to expect that the prime level divides any factor in the numerator. All this led us to suspect that c_A might be 1 for quotients of J^{new}, where $J^{\text{new}} = J/J_{\text{old}}$, where, in turn, J_{old} is the subvariety of $J = J_0(N)$ generated by the images of the degeneracy maps from $J_0(M)$ to $J_0(N)$ for all M such that $M \,|\, N$, but $M \neq N$.

We have the following results in that direction:

Theorem 2.2.3 (Stein [AS99a], generalization of Thm. 2.1.3 of Mazur). *If A is a quotient of J^{new} and if p is a prime such that $p \,|\, c_A$, then $p^2 \,|\, N$ or $p = 2$.*

Also, it is easy to see that [AU96, Prop. 3.1] generalizes to give:

Theorem 2.2.4 (Raynaud). *If A is a quotient of J^{new} and $2^2 \nmid N$, then $2^{(\dim A+1)} \nmid c_A$.*

Let A be a quotient of J^{new} and let ϕ_2 denote the quotient map $J \to A$. There is a canonical isomorphism $J \cong \widehat{J}$ (see [Mil86c, Thm. 6.6]) and we shall use this to implicitly identify $\widehat{J}$ with J. Dualizing the map ϕ_2, we get the map $\phi_1 : \widehat{A} \to J$; recall that $\widehat{A}$ denotes the dual abelian variety of A. Then, by [Maz98, Prop. 8], the composite

$$\widehat{A} \stackrel{\phi_1}{\longrightarrow} J \stackrel{\phi_2}{\longrightarrow} A \tag{2.2}$$

is an isogeny. If G is a finite group, then by the *exponent* of G, we mean the smallest integer n such that multiplication by n kills every element of G.

Definition 2.2.5. *The* modular exponent *of A, denoted n_A, is the exponent of the kernel of the isogeny (2.2).*

We have the following theorem, which we prove in the next section:

Theorem 2.2.6. *If A is a quotient of J^{new} and if p is a prime such that $p^2 \nmid N$, but $p \mid c_A$, then $p \mid n_A$.*

Question 2.2.7. Is the direct generalization of Theorem 2.1.5 of Abbes and Ullmo true, i.e., if A is a quotient of J^{new} and p is a prime that divides c_A, then does p divide N?

The theorems above give good reasons why the generalized Manin constant may be 1 when the level is square-free. But what if the level is not square-free? Computations of [FpS+99] involving Jacobians of genus 2 curves that were quotients of J^{new} found $c_A = 1$ in 28 cases, including cases with quotients at the following non-square-free levels:
$3^2 \cdot 7, \quad 3^2 \cdot 13, \quad 5^3, \quad 3^3 \cdot 5, \quad 3 \cdot 7^2, \quad 5^2 \cdot 7, \quad 2^2 \cdot 47, \quad 3^3 \cdot 7.$

All the above facts have led the author and W. Stein [AS99a] to make the following conjecture.

Conjecture 2.2.8. *If A is a quotient of J^{new}, then $c_A = 1$.*

Note that strong modular elliptic curves are quotients of J^{new} and so this conjecture is a generalization of the conjecture of Manin (Conjecture 2.1.1). The hard part is to settle the question whether primes whose squares divide N can divide the generalized Manin constant. One approach to this problem is to construct good models for $X_0(N)$ when N is not necessarily square free; for example, this has been done in certain cases in [Edi89].

2.3 Proofs of Theorems 2.1.6, 2.1.9 and 2.2.6

We continue to us the notation introduced so far. In particular, A is the quotient of $J = J_0(N)$ under the action of an ideal I of the Hecke algebra. Also we will use notation similar to the one in [AU96] since we will follow their techniques closely. If G is a finite group, then in this section, we denote its order by $\#G$. Recall that we had the maps $\widehat{A} \xrightarrow{\phi_1} J \xrightarrow{\phi_2} A$.

Pulling back differentials along ϕ_2 and ϕ_1, we get the maps:

$$H^0(A_{\mathbf{C}}, \Omega^1_{A/\mathbf{C}}) \xrightarrow{\phi_2^*} H^0(J_{\mathbf{C}}, \Omega^1_{J/\mathbf{C}}) \xrightarrow{\phi_1^*} H^0(\widehat{A}_{\mathbf{C}}, \Omega^1_{\widehat{A}/\mathbf{C}}).$$

Let m denote the largest square that divides the level N and let $S = \mathrm{Spec}(\mathbf{Z}[\frac{1}{m}])$. Then $M_0(N)_S$ is smooth and semistable over S. Let Ω be the relative dualizing sheaf of $M_0(N)_S$ over S. As in [AU96, § 2.1], we have an injection

$$q\text{-exp} : H^0(M_0(N)_S, \Omega) \hookrightarrow S_2(\mathbf{Z}[\tfrac{1}{m}]) \ ;$$

this is not an isomorphism in general, but it induces an isomorphism

$$q\text{-exp} : H^0(M_0(N)_{\mathbf{F}_p}, \Omega) \xrightarrow{\cong} S_2(\mathbf{F}_p) \tag{2.3}$$

for each prime p that does not divide N (we are abusing notation slightly by calling different maps q-exp; however it will be clear from the context which map we are using). We have

$$H^0(M_0(N)_S, \Omega) \hookrightarrow S_2(\mathbf{Z}[\tfrac{1}{m}]) \hookrightarrow S_2(\mathbf{C}) \cong H^0(J_{\mathbf{C}}, \Omega^1_{J/\mathbf{C}}).$$

Applying ϕ_1^* to the first two groups, we get an injection

$$\phi_1^*(H^0(M_0(N)_S, \Omega)) \hookrightarrow \phi_1^*(S_2(\mathbf{Z}[\tfrac{1}{m}])).$$

Denote the cokernel by C. It is a finite group and, by (2.3), the only primes that can divide its order are the primes that divide N. An easy generalization of [AU96, Prop. 3.2] gives

$$\phi_1^*(H^0(M_0(N)_S, \Omega)) \cong H^0(\widehat{A}_S, \Omega^1_{\widehat{A}/S}).$$

So we have an exact sequence

$$0 \to H^0(\widehat{A}_S, \Omega^1_{\widehat{A}/S}) \to \phi_1^*(S_2(\mathbf{Z}[\tfrac{1}{m}])) \to C \to 0.$$

Taking the quotient by the pullback of $H^0(A_S, \Omega^1_{A/S})$ under $\phi_2 \circ \phi_1$, we get

$$0 \to \frac{H^0(\widehat{A}_S, \Omega^1_{\widehat{A}/S})}{\phi_1^*\phi_2^* H^0(A_S, \Omega^1_{A/S})} \to \frac{\phi_1^*(S_2(\mathbf{Z}[\frac{1}{m}]))}{\phi_1^*\phi_2^* H^0(A_S, \Omega^1_{A/S})} \to C \to 0. \tag{2.4}$$

Now

$$\#\left(\frac{\phi_1^*(S_2(\mathbf{Z}[\frac{1}{m}]))}{\phi_1^*\phi_2^* H^0(A_S, \Omega^1_{A/S})}\right) = (c_A)_m \cdot \#\left(\frac{\phi_1^*(S_2(\mathbf{Z}[\frac{1}{m}]))}{\phi_1^*(S_2(\mathbf{Z})[I] \otimes \mathbf{Z}[\frac{1}{m}])}\right), \tag{2.5}$$

where, if i is an integer, then i_m denotes the largest divisor of i prime to m.

Let $W(I)$ denote the orthogonal complement of $S_2(\mathbf{Z})[I]$ in $S_2(\mathbf{C})$ with respect to the Petersson inner product.

Definition 2.3.1. *Consider the group*

$$\left(\frac{S_2(\mathbf{Z})}{S_2(\mathbf{Z})[I] \oplus (W(I) \cap S_2(\mathbf{Z}))}\right).$$

Its order is called the congruence number *of A, denoted r_A, and its exponent is called the* congruence exponent *of A, denoted m_A.*

Note that this definition of the congruence number coincides with the definition in Section 2.1 when A is an elliptic curve. Theorem 2.1.7 generalizes (e.g., generalizing the proof of [AU96, Lem 3.3]) to gives us:

Theorem 2.3.2. *$n_A \,|\, m_A$; moreover, if N is prime, then $n_A = m_A$. In particular, $n_A \,|\, r_A$.*

As in the proof of [AU96, Prop. 3.3], we have the isomorphisms

$$\begin{aligned}\left(\frac{S_2(\mathbf{Z})}{S_2(\mathbf{Z})[I] \oplus (W(I) \cap S_2(\mathbf{Z}))}\right) \otimes \mathbf{Z}[\tfrac{1}{m}] &\xrightarrow{\cong} \frac{S_2(\mathbf{Z}[\frac{1}{m}])}{(S_2(\mathbf{Z})[I] \otimes \mathbf{Z}[\frac{1}{m}]) \oplus (W(I) \cap S_2(\mathbf{Z}[\frac{1}{m}]))} \\ &\xrightarrow{\cong} \frac{\phi_1^*(S_2(\mathbf{Z}[\frac{1}{m}])))}{\phi_1^*(S_2(\mathbf{Z})[I] \otimes \mathbf{Z}[\frac{1}{m}])}.\end{aligned}$$

Thus

$$\#\left(\frac{\phi_1^*(S_2(\mathbf{Z}[\frac{1}{m}]))}{\phi_1^*(S_2(\mathbf{Z})[I]\otimes\mathbf{Z}[\frac{1}{m}])}\right)=(r_A)_m.$$

Putting this in (2.5) and then using (2.4), we get

$$(c_A)_m(r_A)_m=\#\left(\frac{H^0(\widehat{A}_S,\Omega^1_{\widehat{A}/S})}{\phi_1^*\phi_2^*H^0(A_S,\Omega^1_{A/S})}\right)\ \#C. \tag{2.6}$$

Recall (Definition 2.2.5) that n_A was the smallest integer that annihilates the kernel of the composite isogeny

$$\widehat{A}\xrightarrow{\phi_1}J\xrightarrow{\phi_2}A. \tag{2.7}$$

If B and B' are abelian varieties with an isogeny $f:B\to B'$, and if n is an integer that kills $\ker f$, then using the fact that $\ker f\subseteq\ker n_B$, where n_B denotes the multiplication by n map on B, we find that n_B factors as $n_B=g_n\circ f$ with g_n an isogeny $B'\to B$ (see [Mil86a, §8]).

Definition 2.3.3. *If B and B' are abelian varieties with an isogeny $f:B\to B'$, then a conjugate isogeny to f (or an isogeny conjugate to f) is an isogeny $g:B'\to B$ such that $g\circ f$ is multiplication by the exponent of* $\ker f$ *on B. By the discussion above, given any isogeny, there always exists an isogeny conjugate to it.*

Let ϕ' be an isogeny conjugate to the isogeny (2.7). So the composite

$$\widehat{A}\xrightarrow{\phi_1}J\xrightarrow{\phi_2}A\xrightarrow{\phi'}\widehat{A}$$

is multiplication by n_A. Using this, we see that some power of n_A kills $\left(\frac{H^0(\widehat{A}_S,\Omega^1_{\widehat{A}/S})}{\phi_1^*\phi_2^*H^0(A_S,\Omega^1_{A/S})}\right)$. Thus we have

Lemma 2.3.4. *If p is a prime such that p divides $\#\left(\frac{H^0(\widehat{A}_S,\Omega^1_{\widehat{A}/S})}{\phi_1^*\phi_2^*H^0(A_S,\Omega^1_{A/S})}\right)$, then $p\,|\,n_A$.*

We already remarked that a prime can divide $\#C$ only if it divides N. The main addition to the techniques of [AU96] is the following result that further controls the primes that can divide $\#C$:

Proposition 2.3.5. *If A is a quotient of J^{new} and p is a prime such that $p^2\nmid N$, but $p\,|\,\#C$, then $p\,|\,n_A$.*

We will prove this shortly, but let us first use this to prove the theorems from Sections 2.1 and 2.2.

Proofs of Theorems 2.2.6, 2.1.6 and 2.1.9. Theorem 2.2.6 follows easily, since if p satisfies the hypothesis of the theorem, then $p\mid(c_A)_m$; so by equation (2.6), Lemma 2.3.4 and

Proposition 2.3.5, it divides n_A. Also if $A = E$ is an elliptic curve, as in Section 2.1, then (e.g., see [AU96]):

$$n_E = \deg\phi_E = \# \left(\frac{H^0(\widehat{E}_S, \Omega^1_{\widehat{E}/S})}{\phi_2^* \phi_1^* H^0(E_S, \Omega^1_{E/S})} \right).$$

Equation (2.6) becomes

$$(c_E)_m (r_E)_m = (\deg\phi_E)_m \# C,$$

and, since $\deg\phi_E \,|\, r_E$, we get

$$(c_E)_m (r_E/\deg\phi_E)_m = \# C.$$

Using Proposition 2.3.5, we again easily get theorems 2.1.6 and 2.1.9. □

Also note that by equation (2.6), Lemma 2.3.4 and Proposition 2.3.5, we get the following generalization of Theorem 2.1.9:

Theorem 2.3.6. *Let p be a prime such that $p^2 \nmid N$. If $p \,|\, r_A$, then $p \,|\, n_A$.*

It remains to give:

Proof of Proposition 2.3.5. We have the exact sequence

$$0 \to \phi_1^*(H^0(M_0(N)_S, \Omega)) \to \phi_1^*(S_2(\mathbf{Z}[\tfrac{1}{m}])) \to C \to 0. \tag{2.8}$$

We want to show that certain primes do not divide $\#C$. We already know that the only primes that can divide $\#C$ are those that divide N. So let p be a prime that divides N. Then considering the multiplication by p map applied to each term of the sequence of maps (2.8) and using the snake lemma, we get:

$$0 \to C[p] \to \phi_1^*(H^0(M_0(N)_S, \Omega)) \otimes \mathbf{F}_p \to \phi_1^*(S_2(\mathbf{Z}[\tfrac{1}{m}])) \otimes \mathbf{F}_p \to C \otimes \mathbf{F}_p \to 0.$$

Suppose $p \nmid n_A$. Then to show that $p \nmid \#C$, i.e., that $C[p]$ is trivial, all we have to show is that the map

$$\begin{array}{c} \phi_1^*(H^0(M_0(N)_S, \Omega)) \otimes \mathbf{F}_p \\ \downarrow q\text{-exp} \\ \phi_1^*(S_2(\mathbf{Z}[\tfrac{1}{m}])) \otimes \mathbf{F}_p \end{array} \tag{2.9}$$

is injective.

The key idea is to use the conjugate isogeny ϕ' (defined just after Definition 2.3.3). Let $\phi'' = \phi' \circ \phi_2$. Then we have maps $\widehat{A} \xrightarrow{\phi_1} J \xrightarrow{\phi''} \widehat{A}$ such that the composite is multiplication by n_A. Pulling back differentials, we get the maps

$$H^0(\widehat{A}_{\mathbf{C}}, \Omega^1_{\widehat{A}/\mathbf{C}}) \xrightarrow{\phi''^*} H^0(J_{\mathbf{C}}, \Omega^1_{J/\mathbf{C}}) \xrightarrow{\phi_1^*} H^0(\widehat{A}_{\mathbf{C}}, \Omega^1_{\widehat{A}/\mathbf{C}}),$$

where the composite is again multiplication by n_A. Note that these maps extend to the Néron models over S and preserve the $\mathbf{Z}[\frac{1}{m}]$-integral structure. Hence, applying these maps to (2.9), we get:

$$\begin{array}{ccccc} \phi_1^*(H^0(M_0(N)_S,\Omega))\otimes\mathbf{F}_p & \stackrel{\phi''^*}{\longrightarrow} & H^0(M_0(N)_S,\Omega)\otimes\mathbf{F}_p & \stackrel{\phi_1^*}{\longrightarrow} & \phi_1^*(H^0(M_0(N)_S,\Omega))\otimes\mathbf{F}_p \\ \downarrow q\text{-exp} & & \downarrow q\text{-exp} & & \downarrow q\text{-exp} \\ \phi_1^*(S_2(\mathbf{Z}[\frac{1}{m}]))\otimes\mathbf{F}_p & \stackrel{\phi''^*}{\longrightarrow} & S_2(\mathbf{Z}[\frac{1}{m}])\otimes\mathbf{F}_p & \stackrel{\phi_1^*}{\longrightarrow} & \phi_1^*(S_2(\mathbf{Z}[\frac{1}{m}]))\otimes\mathbf{F}_p \end{array}$$

Suppose x is an element of the group $\phi_1^*(H^0(M_0(N)_S,\Omega))\otimes\mathbf{F}_p$ in the top left corner of the diagram above that is in the kernel of the map in (2.9), i.e., the left-most q-exp map above. Then its image $y=(\phi''^*)(x)$ in the group $H^0(M_0(N)_S,\Omega)\otimes\mathbf{F}_p$ above maps to 0 in $S_2(\mathbf{Z}[\frac{1}{m}])\otimes\mathbf{F}_p$ under the middle q-exp map (by commutativity of the first square). But we have $H^0(M_0(N)_S,\Omega)\otimes\mathbf{F}_p\cong H^0(M_0(N)_{\mathbf{F}_p},\Omega)$. Suppose $p^2\nmid N$. Then $M_0(N)_{\mathbf{F}_p}$ consists of two irreducible components. Now $q\text{-exp}(y)=0$ means that $y\in H^0(M_0(N)_{\mathbf{F}_p},\Omega)$ is zero on the component that contains the cusp ∞. Since A is a quotient of J^{new}, the element x is an eigenvector for the Atkin-Lehner involution W_N, and hence so is y. But W_N is an involution that swaps the two components of $M_0(N)_{\mathbf{F}_p}$. Hence y is zero on all of $M_0(N)_{\mathbf{F}_p}$; i.e., $y=0$. Looking at the top line in the diagram above, we find that x maps to 0 under the composite. But its image under this composite is n_Ax; so $n_Ax=0$. Since $p\nmid n_A$, this means that $x=0$, i.e., the map (2.9) is injective, which is what was left to prove. $\square$

Chapter 3

The Birch and Swinnerton-Dyer conjecture for the winding quotient of prime level

We first define the winding quotient of $J_0(N)$ in Section 3.1. Then, in Section 3.2, we give a formula that expresses the ratio of the L-value to the real volume for the winding quotient of prime level as a rational number that can be computed. In Section 3.3 we present some calculations using the formula just mentioned. Finally, in Section 3.4, we outline a program to prove the BSD formula for the winding quotient. This chapter depends on Chapter 1.

3.1 Definition of the winding quotient

Let N be a positive integer and again let $X_0(N)$ denote the usual modular curve of level N. Let $\mathcal{H}$ denote the complex upper half plane, and let $\{0, i\infty\}$ denote the projection of the geodesic path from 0 to $i\infty$ in $\mathcal{H} \cup \mathbf{P}^1(\mathbf{Q})$ to $X_0(N)(\mathbf{C})$. We have an isomorphism

$$H_1(X_0(N), \mathbf{Z}) \otimes \mathbf{R} \xrightarrow{\cong} \mathrm{Hom}_{\mathbf{C}}(H^0(X_0(N), \Omega^1), \mathbf{C}),$$

obtained by integrating differentials along cycles (see [Lan95, § IV.1]). Let e be the element of $H_1(X_0(N), \mathbf{Z}) \otimes \mathbf{R}$ that corresponds to the map $\omega \mapsto -\int_{\{0,i\infty\}} \omega$ under this isomorphism. It is called the *winding element* and was introduced by Mazur [Maz77, §II.18]. Let $\mathbf{T}$ denote the Hecke algebra (as in Section 1.2); it acts on $H_1(X_0(N), \mathbf{Z}) \otimes \mathbf{R}$. Let I_e be the annihilator of e with respect to this action. The quotient abelian variety $J_e(N) = J_0(N)/I_e J_0(N)$ is called the *winding quotient of level N*. It was introduced by L. Merel in his proof of the uniform boundedness conjecture [Mer96a].

In this chapter, we take N to be a prime number p and denote $J_e(p)$ by J_e for simplicity of notation. Also, we use notation from Chapter 1.

3.2 A formula for the ratio of the special L-value to the real volume

One can easily check that $L_{J_e}(1)$ is non-zero and hence, by the work of Kolyvagin and Logachev, $J_e(\mathbf{Q})$ is finite; so the first part of the Birch and Swinnerton-Dyer conjecture is valid in this case. Also, the order of the Shafarevich-Tate group, $Ш_{J_e}$, is known to be finite. See [Mer96a, Prop. 1] and [KL89] for details of all of the above.

The Birch and Swinnerton-Dyer formula (Conjecture 1.2.1) becomes:

Conjecture 3.2.1.

$$\frac{L_{J_e}(1)}{\Omega_{J_e}} \stackrel{?}{=} \frac{|Ш_{J_e}| \cdot c_p(J_e)}{|J_e(\mathbf{Q})| \cdot |\widehat{J}_e(\mathbf{Q})|}.$$

Let $H = H_1(X_0(p), \mathbf{Z})$, $H_e = H[I_e]$, $\widehat{I}_e = \mathrm{Ann}_{\mathbf{T}} I_e$, $\widehat{H_e} = H[\widehat{I}_e]$, $n = \mathrm{num}((p-1)/12)$, and again let c_{J_e} denote the generalized Manin constant of J_e. Let $\Im$ denote the annihilator of the divisor $(0) - (\infty)$, considered as an element of $J_0(N)(\mathbf{C})$, under the action of $\mathbf{T}$; it is called the Eisenstein ideal and was introduced by Mazur ([Maz77, §II.9]). It follows from [Maz77, II.18.6] that $\Im e \subseteq H_e^+$. We will show presently that the groups $H^+/(\widehat{H_e}^+ + H_e^+)$ and $H_e^+/\Im e$ are finite. The main result of this section is the following formula, which expresses the left-hand side of the formula in Conjecture 3.2.1 as a rational number:

Theorem 3.2.2. *With notation as above,*

$$\frac{L_{J_e}(1)}{\Omega_{J_e}} = \frac{1}{c_{J_e}} \cdot \frac{\left|\frac{H^+}{\widehat{H_e}^+ + H_e^+}\right| \cdot \left|\frac{H_e^+}{\Im e}\right|}{n}.$$

It was L. Merel's idea that a formula like the one above should hold. Before stating the proof of this proposition, we state some preparatory results.

First, we give some information on certain subgroups and quotients of H. If f is a newform of weight 2 for $\Gamma_0(p)$, then let $[f]$ denote its orbit under the action of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. Let $S_{[f]}$ be the $\mathbf{Q}$-subspace consisting of forms in $\oplus_{g \in [f]} \mathbf{C} g$ that have rational Fourier coefficients. The space $S_{[f]}$ is stable under the action of $\mathbf{T} \otimes \mathbf{Q}$; let $\mathbf{T}_{[f]}$ denote the image of $\mathbf{T} \otimes \mathbf{Q}$ acting on $S_{[f]}$.

Lemma 3.2.3. *The natural projection map $\phi : \mathbf{T} \otimes \mathbf{Q} \to \oplus_{[f]} \mathbf{T}_{[f]}$ is an isomorphism of rings. The image of $I_e \otimes \mathbf{Q}$ under ϕ is $\oplus_{[f]:\langle e, f\rangle = 0} \mathbf{T}_{[f]}$ and the image of $\widehat{I}_e \otimes \mathbf{Q}$ under ϕ is $\oplus_{[f]:\langle e, f\rangle \neq 0} \mathbf{T}_{[f]}$*

Proof. The fact that the map $\mathbf{T} \otimes \mathbf{Q} \to \oplus_{[f]} \mathbf{T}_{[f]}$ is an isomorphism is well known (e.g., see [DDT94, §1.6]). The statement about the image of $\widehat{I}_e \otimes \mathbf{Q}$ under ϕ follows from the other statements and the fact that $\mathbf{T}$ has no nilpotents. So we only have to prove that the image of $I_e \otimes \mathbf{Q}$ under ϕ is $\oplus_{[f]:\langle e, f\rangle = 0} \mathbf{T}_{[f]}$. Suppose $t \in I_e \otimes \mathbf{Q}$. Then $te = 0$. Let f be a newform, and let its eigenvalue for t be λ. Then $\langle te, f\rangle = 0$, hence $\lambda \langle e, f\rangle = 0$. If $\langle e, f\rangle \neq 0$, then this means $\lambda = 0$, i.e. $tf = 0$. This shows that the image of $I_e \otimes \mathbf{Q}$ is contained in $\oplus_{[f]:\langle e, f\rangle = 0} \mathbf{T}_{[f]}$. All we have to do is show the reverse containment. So suppose t is an

element of $\mathbf{T}$ such that $\phi(t) \in \oplus_{[f]:\langle e,f\rangle=0}\mathbf{T}_{[f]}$. If f is a newform such that $\langle e, f\rangle \neq 0$ and $g \in S_{[f]}$, then by definition $tg = 0$, so $\langle te, g\rangle = 0$. If f is a newform such that $\langle e, f\rangle = 0$, and $g \in S_{[f]}$, then $\langle te, g\rangle = \langle e, tg\rangle = 0$ (because tg can be written as the linear combination of the action of tf_i, where f_i are the the Galois conjugates of f, each of which pair to 0 with e). So te pairs to 0 with every element of $S_{[f]}$ for all newforms f. Since the $S_{[f]}$'s constitute the entire space of cusp forms, and the de Rham pairing is non-degenerate, we have $te = 0$, i.e., $t \in I_e \otimes \mathbf{Q}$. This finishes the proof. □

Corollary 3.2.4. $\dim_{\mathbf{Q}} \mathbf{T} \otimes \mathbf{Q} = \dim_{\mathbf{Q}}(\mathbf{T} \otimes \mathbf{Q})[I_e] + \dim_{\mathbf{Q}}(\mathbf{T} \otimes \mathbf{Q})[\widehat{I_e}]$.

Proof. Immediate from Lemma 3.2.3 and the fact that $\mathbf{T} \otimes \mathbf{Q}$ has no nilpotents. □

Corollary 3.2.5. *The natural map* $(I_e \otimes \mathbf{Q}) \oplus (\widehat{I_e} \otimes \mathbf{Q}) \to \mathbf{T} \otimes \mathbf{Q}$ *given by* $(a, b) \mapsto a + b$ *is an isomorphism.*

Proof. Immediate from Lemma 3.2.3, using the isomorphism ϕ. □

Remark 3.2.6.
1) $S_2(\Gamma_0(N), \mathbf{Q})$ is a free $\mathbf{T} \otimes \mathbf{Q}$-module of rank 1 (e.g., see [DI95, Prop. 12.4.14]).
2) $H \otimes \mathbf{Q}$ is a free $\mathbf{T} \otimes \mathbf{Q}$-module of rank 2 (e.g. see [DDT94, Lemma 1.37]).
3) $H^+ \otimes \mathbf{Q}$ is a free $\mathbf{T} \otimes \mathbf{Q}$-module of rank 1 (e.g., see the proof of Lemma 1.37 in [DDT94]).

Let π denote the quotient map $J_0(p) \to J_e$; since its kernel is connected, it induces a sujection $\pi_* : H \to H_1(J_e, \mathbf{Z})$.

Lemma 3.2.7. *The kernel of the surjection* $H \xrightarrow{\pi_*} H_1(J_e, \mathbf{Z})$ *is* $\widehat{H_e}$.

Proof. Let K denote the kernel of π_*.

Claim 1: $\widehat{H_e} \subseteq K$.

Proof of the claim. Since $J_e = J_0(p)/I_e J_0(p)$, all we have to show is that $\widehat{H_e}$ pairs to zero with every cusp form killed by I_e under the de Rham pairing (which is a perfect pairing). Suppose $h \in \widehat{H_e}$, considered as an element of $H \otimes \mathbf{Q}$. By Corollary 3.2.5, there are elements $\widehat{i_e} \in \widehat{I_e} \otimes \mathbf{Q}$ and $i_e \in I_e \otimes \mathbf{Q}$ such that $\widehat{i_e} + i_e = 1$ in $\mathbf{T} \otimes \mathbf{Q}$. Thus $h = (\widehat{i_e} + i_e)h = i_e h$. Since the de Rham pairing is equivariant under the action of $\mathbf{T}$, this shows that h pairs to 0 with every cusp form killed by I_e. □

Claim 2: $\dim_{\mathbf{Q}} \widehat{H_e} \otimes \mathbf{Q} = \dim_{\mathbf{Q}} K \otimes \mathbf{Q}$.

Proof of the claim. We have

$$\dim J_e = \dim_{\mathbf{Q}} H^0(J_e, \Omega_{J_e/\mathbf{Q}}) = \dim_{\mathbf{Q}} S_2(\Gamma_0(N), \mathbf{Q})[I_e] = \dim_{\mathbf{Q}}(\mathbf{T} \otimes \mathbf{Q})[I_e],$$

where the last equality follows by Part 1 of Remark 3.2.6. Hence

$$\dim_{\mathbf{Q}} K \otimes \mathbf{Q} = 2(\dim J_0(p) - \dim J_e) = 2(\dim_{\mathbf{Q}} \mathbf{T} \otimes \mathbf{Q} - \dim_{\mathbf{Q}}(\mathbf{T} \otimes \mathbf{Q})[I_e]).$$

Next, $\dim_{\mathbf{Q}} \widehat{H_e} \otimes \mathbf{Q} = 2 \cdot \dim_{\mathbf{Q}}(\mathbf{T} \otimes \mathbf{Q})[\widehat{I_e}]$, by Part 2 of Remark 3.2.6. The claim now follows from Corollary 3.2.4. □

Lemma 3.2.7 follows from Claims 1 and 2 above. □

If A be an abelian variety over $\mathbf{R}$, then let c denote the action of complex conjugation on $A(\mathbf{C})$ as well as the induced action on $H_1(A(\mathbf{C}), \mathbf{Z})$. The following result is probably well known, but we could not find a suitable reference; the proof given below was provided by H. Lenstra.

Proposition 3.2.8. *If A is an abelian variety over $\mathbf{R}$, then the group of connected components of $A(\mathbf{R})$ is canonically isomorphic to $H^1(\mathrm{Gal}(\mathbf{C}/\mathbf{R}), H_1(A, \mathbf{Z}))$ and its order is equal to the order of the 2-group $H_1(A, \mathbf{Z})^+/(1+c)H_1(A, \mathbf{Z})$.*

Proof. Denote $H_1(A, \mathbf{Z})$ by L and let $V = L \otimes \mathbf{R}$ (so $V = H_1(A, \mathbf{R})$). Now consider the exact sequence

$$0 \to L \to V \to A(\mathbf{C}) \to 0$$

of $\langle c \rangle$-modules, and take its Tate cohomology sequence. The group V is uniquely divisible, hence multiplication by any integer is an isomorphism on V, and so it is an isomorphism on the Tate cohomology groups of V as well. At the same time, by [AW67, §6, Cor. 2], these cohomology groups are finite, hence are killed by multiplication by the order. Thus V has trivial cohomology. So the long exact sequence gives us:

$$0 \to \widehat{H}^0(\langle c \rangle, A(\mathbf{C})) \to H^1(\langle c \rangle, L) \to 0.$$

But $\widehat{H}^0(\langle c \rangle, A(\mathbf{C}))$ is, by definition, equal to $A(\mathbf{C})^+/(1+c)A(\mathbf{C})$, and $A(\mathbf{C})^+ = A(\mathbf{R})$. So we get an isomorphism $A(\mathbf{R})/(1+c)A(\mathbf{C}) \xrightarrow{\cong} H^1(\langle c \rangle, L)$. Now $A(\mathbf{C})$ is compact and connected, so its continuous image $(1+c)A(\mathbf{C})$ is compact (hence closed) and connected as well. Since $(1+c)A(\mathbf{C})$ is closed, $A(\mathbf{R})/(1+c)A(\mathbf{C})$ is an Hausdorff group (for example, using [Bou66, Prop. 18 of § III.2.6]); and since $(1+c)A(\mathbf{C})$ is connected, $A(\mathbf{R})/(1+c)A(\mathbf{C})$ has the same group of components as $A(\mathbf{R})$ itself. But the group $A(\mathbf{R})/(1+c)A(\mathbf{C})$ is also finite, since $H^1(\langle c \rangle, L)$ is finite (using [AW67, §6, Cor. 2]). So $A(\mathbf{R})/(1+c)A(\mathbf{C})$, being Hausdorff and finite, is discrete and equal to its own component group. Thus, the group of components of $A(\mathbf{R})$ is canonically isomorphic to $H^1(\langle c \rangle, L)$.

So all we have to show is that the order of $H^1(\langle c \rangle, L)$ is equal to the order of $L^+/(1+c)L$. Observe that the latter group is $\widehat{H}^0(\langle c \rangle, L)$, so it suffices to prove that the Herbrand quotient of L is equal to 1. Now, by the semilinearity of the action of c on V (with respect to the complex structure on V), it follows that c has equally many eigenvalues $+1$ as -1 on V. Now use [AW67, §8, Prop. 12] and the fact that $L \otimes \mathbf{Q} \cong \mathbf{Z}\langle c \rangle^{\dim A} \otimes \mathbf{Q}$ as $\langle c \rangle$-representation spaces (which can be checked by looking at traces), to conclude that the Herbrand quotient of L is the same as that of $\mathbf{Z}\langle c \rangle^{\dim A}$. But $\mathbf{Z}\langle c \rangle^{\dim A}$ has Herbrand quotient 1. Hence so does L, and that finishes the proof. □

Corollary 3.2.9. *$J_0(p)(\mathbf{R})$ is connected.*

Proof. By [Mer96b, Prop. 5], $H_1(J_0(p), \mathbf{Z})^+ = (1+c)H_1(J_0(p), \mathbf{Z})$. Then by Proposition 3.2.8, $J_0(p)(\mathbf{R})$ has only one connected component. □

Lemma 3.2.10.

$$\left| \frac{(H/\widehat{H_e})^+}{H^+/\widehat{H_e}^+} \right| = c_\infty(J_e).$$

Proof. Since the level is prime, by [Mer96b, Prop. 5], we have $H^+ = (1+c)H$. Now, by Lemma 3.2.7, $H_1(J_e, \mathbf{Z}) \cong H/\widehat{H}_e$, and so

$$(1+c)H_1(J_e, \mathbf{Z}) \cong \frac{(1+c)H}{(1+c)\widehat{H}_e} \cong \frac{H^+}{\widehat{H}_e{}^+}.$$

Thus

$$\left|\frac{(H/\widehat{H}_e)^+}{H^+/\widehat{H}_e{}^+}\right| = \left|\frac{H_1(J_e, \mathbf{Z})^+}{(1+c)H_1(J_e, \mathbf{Z})}\right| = c_\infty(J_e),$$

by Proposition 3.2.8. □

As mentioned earlier, $\Im e$ is a subgroup of H_e^+.

Lemma 3.2.11. *The group $H_e^+/\Im e$ is finite.*

Proof. All we have to show is that $\dim_{\mathbf{Q}} \Im e \otimes \mathbf{Q} = \dim_{\mathbf{Q}} H_e^+ \otimes \mathbf{Q}$. By [Maz77, Prop. 9.7], $T/\Im \cong \mathbf{Z}/n\mathbf{Z}$; so $\dim_{\mathbf{Q}} \Im e \otimes \mathbf{Q} = \dim_{\mathbf{Q}} \mathbf{T}e \otimes \mathbf{Q} = \dim_{\mathbf{Q}} \mathbf{T}/I_e \otimes \mathbf{Q} = \dim_{\mathbf{Q}} \mathbf{T} \otimes \mathbf{Q} - \dim_{\mathbf{Q}} I_e \otimes \mathbf{Q}$, and $\dim_{\mathbf{Q}} H_e^+ \otimes \mathbf{Q} = \dim_{\mathbf{Q}} (\mathbf{T} \otimes \mathbf{Q})[I_e]$. The lemma now follows from Lemma 3.2.3 and Corollary 3.2.4. □

Also, note that using Corollary 3.2.4 and Part 3 of Remark 3.2.6, we find that the group $H^+/(\widehat{H}_e{}^+ + H_e^+)$ is finite.

Let $S_e = S_2(\Gamma_0(p), \mathbf{Z})[I_e]$. We have a perfect pairing

$$\mathbf{T} \times S_2(\Gamma_0(p), \mathbf{Z}) \to \mathbf{Z} \tag{3.1}$$

which associates to (T, f) the first Fourier coefficient $a_1(f \mid T)$ of the modular form $f \mid T$ (see [Rib83, (2.2)]); this induces a pairing

$$\psi : \mathbf{T}/I_e \times S_e \to \mathbf{Z}.$$

Lemma 3.2.12. *The pairing ψ above is a perfect pairing.*

Proof. Both $\mathbf{T}/I_e$ and S_e are free $\mathbf{Z}$-modules; moreover by Lemma 3.2.3 and Part 1 of Remark 3.2.6, they have the same rank. So it suffices to prove that the induced maps $S_e \to \mathrm{Hom}(\mathbf{T}/I_e, \mathbf{Z})$ and $\mathbf{T}/I_e \to \mathrm{Hom}(S_e, \mathbf{Z})$ are injective. The injectivity of the first map follows from the perfectness of the pairing (3.1). Suppose the image of $T \in \mathbf{T}$ in $\mathbf{T}/I_e$ maps to the trivial element of $\mathrm{Hom}(S_e, \mathbf{Z})$. Then $a_1(f \mid T) = 0 \ \forall f \in S_e$. Now if f is in S_e, then so is $f \mid T_n$ for any Hecke operator T_n (including U_p). But then $a_n(f \mid T) = a_1((f \mid T_n) \mid T) = 0 \ \forall n$. Thus $f = 0$. Hence $f \mid T = 0 \ \forall f \in S_e$. By Lemma 3.2.3, this shows that $\mathbf{T} \in I_e$. Thus the map $\mathbf{T}/I_e \to \mathrm{Hom}(S_e, \mathbf{Z})$ is injective and we are done. □

Finally, we are ready to give:

Proof of Theorem 3.2.2. Recall that we have the pairing $\langle\ ,\ \rangle : (H^+ \otimes \mathbf{C}) \times S_2(\Gamma_0(p), \mathbf{C}) \to \mathbf{C}$ given by $(\gamma, f) \mapsto \langle \gamma, f \rangle = \int_\gamma 2\pi i f(z) dz$. In the rest of this proof, at various points, we will consider pairings between two $\mathbf{Z}$-modules; unless otherwise stated, each such pairing is obtained in a natural way from this pairing.

For simplicity of notation, we denote $c_\infty(J_e)$ simply by c_∞ in this proof. Using Lemma 3.2.7 and the discussion in Section 1.2, we get

$$\Omega_{J_e} = c_{J_e} \cdot c_\infty \cdot \mathrm{disc}((H/\widehat{H_e})^+ \times S_e \to \mathbf{C}).$$

Next, by [Shi94, Thm. 7.14] (completed by [Car86]), we have $L_{J_e}(1) = \prod\langle e, f\rangle$, where, in this proof, the product symbol denotes the product over all elements f belonging to the normalized eigenform basis for the $\mathbf{C}$-vector space $S_2(\Gamma_0(p), \mathbf{C})[I_e]$.

Using all this, we get

$$\frac{L_{J_e}(1)}{\Omega_{J_e}} = \frac{1}{c_{J_e}} \cdot \frac{\prod\langle e, f\rangle}{c_\infty \cdot \mathrm{disc}((H/\widehat{H_e})^+ \times S_e \to \mathbf{C})}. \tag{3.2}$$

We are going to replace $(H/\widehat{H_e})^+$ by another lattice. We need some preparation before doing this. From Corollary 3.2.5, $\mathbf{T} \otimes \mathbf{Q} \cong (I_e \otimes \mathbf{Q}) \oplus (\widehat{I_e} \otimes \mathbf{Q})$. Thus if an element of H is killed by both I_e and $\widehat{I_e}$, then it is killed by $\mathbf{T}$, and then by Part 2 of Remark 3.2.6, it is the trivial element. Thus $H_e \cap \widehat{H_e} = \phi$. So the the homomorphism $H_e^+ \to (H/\widehat{H_e})^+$ is an injection. The homomorphism

$$H^+ \to (H/\widehat{H_e})^+/H_e^+ \tag{3.3}$$

has kernel $(\widehat{H_e}^+ + H_e^+)$. But the map (3.3) is not surjective; consider the following map to its cokernel:

$$(H/\widehat{H_e})^+ \to \frac{(H/\widehat{H_e})^+/H_e^+}{H^+/(\widehat{H_e}^+ + H_e^+)}.$$

It is surjective and has kernel $H^+/\widehat{H_e}^+$. Hence

$$\frac{(H/\widehat{H_e})^+}{H^+/\widehat{H_e}^+} \cong \frac{\frac{(H/\widehat{H_e})^+}{H_e^+}}{\left(\frac{H^+}{\widehat{H_e}^+ + H_e^+}\right)} \tag{3.4}$$

Now we are ready to perform some change of lattices:

$$\begin{aligned}
\frac{\prod\langle e, f\rangle}{\mathrm{disc}((H/\widehat{H_e})^+ \times S_e \to \mathbf{C})} &= \frac{\prod\langle e, f\rangle}{\mathrm{disc}(H_e^+ \times S_e \to \mathbf{C})} \cdot \left|\frac{(H/\widehat{H_e})^+}{H^+/\widehat{H_e}^+}\right| \cdot \left|\frac{H^+}{\widehat{H_e}^+ + H_e^+}\right| \\
&= \frac{\prod\langle e, f\rangle}{\mathrm{disc}(\Im e \times S_e \to \mathbf{C})} \cdot c_\infty \cdot \left|\frac{H^+}{\widehat{H_e}^+ + H_e^+}\right| \cdot \left|\frac{H_e^+}{\Im e}\right| \\
&= \frac{\prod\langle e, f\rangle}{\mathrm{disc}(\mathbf{T}e \times S_e \to \mathbf{C})} \cdot c_\infty \cdot \frac{\left|\frac{H^+}{\widehat{H_e}^+ + H_e^+}\right| \cdot \left|\frac{H_e^+}{\Im e}\right|}{\left|\frac{\mathbf{T}e}{\Im e}\right|},
\end{aligned} \tag{3.5}$$

where we got the first equality using (3.4) and the second equality by Lemma 3.2.10. Note that

$$\left|\frac{\mathbf{T}e}{\Im e}\right| = \left|\frac{\mathbf{T}}{\Im}\right| = n, \tag{3.6}$$

where the latter equality is from [Maz77, II.9.7].

The following claim is the key step of the proof.

Claim:

$$\frac{\prod\langle e, f\rangle}{\mathrm{disc}(\mathbf{T}e \times S_e \to \mathbf{C})} = 1. \tag{3.7}$$

Proof of the claim. The perfect pairing ψ of Lemma 3.2.12 defines $t_e \in \mathbf{T}/I_e \otimes \mathbf{C}$ characterized by $\langle e, f\rangle = a_1(t_e f)\ \forall f \in S_e$. On the one hand,

$$\prod\langle e, f\rangle = \prod a_1(t_e f) = (\det_{S_e \otimes \mathbf{C}} t_e) \prod a_1(f) = \det_{\mathbf{T}/I_e \otimes \mathbf{C}} t_e.$$

On the other hand, by the perfectness of the pairing ψ and the canonical isomorphism $\mathbf{T}e \cong \mathbf{T}/I_e$, the discriminant of the pairing $\mathbf{T}e \times S_e \to \mathbf{C}$ that associates to (te, f) the complex number $\langle te, f\rangle$ coincides with the discriminant of the pairing $\mathbf{T}/I_e \times \mathrm{Hom}(\mathbf{T}/I_e, \mathbf{Z}) \to \mathbf{C}$ that associates to (t, ψ) the complex number $\psi(t_e t)$, obtained by extending ψ by $\mathbf{C}$-linearity. The latter discriminant is also equal to $\det_{\mathbf{T}/I_e \otimes \mathbf{C}} t_e$. □

Putting (3.7) and (3.6) in (3.5) and then using (3.2), we get

$$\frac{L_{J_e}(1)}{\Omega_{J_e}} = \frac{1}{c_{J_e}} \cdot \frac{\left|\frac{H^+}{\widehat{H_e}^+ + H_e^+}\right| \cdot \left|\frac{H_e^+}{\Im e}\right|}{n}.$$

That proves Theorem 3.2.2. □

3.3 Calculations of certain factors from Section 3.2

We continue using notation from Sections 3.1 and 3.2. With the idea of studying the conjectural Birch and Swinnerton-Dyer formula, we did computations (with the help of a computer) to calculate the terms $\left|\frac{H^+}{\widehat{H_e}^+ + H_e^+}\right|$ and $\left|\frac{H_e^+}{\Im e}\right|$ appearing in Theorem 3.2.2, for various primes p. For the former, we did calculations up to $p = 397$, and for the latter, up to $p = 1447$. The computations were done using the theory of modular symbols; we describe this theory in §3.3.1. In §3.3.2, we describe algorithms to calculate $\left|\frac{H^+}{\widehat{H_e}^+ + H_e^+}\right|$ and $\left|\frac{H_e^+}{\Im e}\right|$. The results of the calculations are mentioned in §3.3.3. These were used in [Aga99], and will be used in Section 3.4 and Proposition 5.3.3. Only §3.3.3 will be referred to later, so the reader primarily interested in the rest of the thesis can safely skip this section (Section 3.3). In this section, we assume that the prime p under consideration is greater than 3 (if $p \leq 3$, the calculations are vacuous anyway).

3.3.1 Algorithms using modular symbols

Let N be any positive integer. The theory of modular symbols gives a presentation of the group $H_1(X_0(N), \mathbf{Z})$ together with a description of the action of Hecke operators on

the set of generators. The real vector spaces $S_2(\Gamma_0(N), \mathbf{R})$ and $H_1(X_0(N), \mathbf{R})$ are dual in a way that make the Hecke operators self dual; hence we can use modular symbols to obtain information about $S_2(\Gamma_0(N), \mathbf{R})$ as a $\mathbf{T}$-module (see [Cre97, §2.1.2]). Thus they are of vital use in computations involving modular forms. We mention only the part of the theory that we need for our calculations; in particular, we will take N to be a prime number. For details, see [Ste00] and the references therein.

Let $\mathcal{H}$ denote the complex upper half plane. If $\alpha, \beta \in \mathbf{P}^1(\mathbf{Q})$, then let $\{\alpha, \beta\}$ denote the class in $H_1(X_0(p), \text{cusps}; \mathbf{Z})$ of the image in $X_0(p)(\mathbf{C})$ of the geodesic path from α to β in $\mathcal{H} \cup \mathbf{P}^1(\mathbf{Q})$. It is called a *modular symbol*. This generalizes the definition of $\{0, i\infty\}$ in Section 3.1. Following [Man72], we have a map

$$\Gamma_0(p) \setminus \mathrm{SL}_2(\mathbf{Z}) \to H_1(X_0(p), \text{cusps}; \mathbf{Z})$$

given by $g \mapsto \{g0, g\infty\}$. The image of this map generates $H_1(X_0(p), \text{cusps}; \mathbf{Z})$ as a $\mathbf{Z}$-module. Next we have a bijection

$$\Gamma_0(p) \setminus \mathrm{SL}_2(\mathbf{Z}) \xrightarrow{\cong} \mathbf{P}^1(\mathbf{Z}/p\mathbf{Z})$$

given by

$$\Gamma_0(p) \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto (c : d).$$

So we have a map

$$\mathbf{P}^1(\mathbf{Z}/p\mathbf{Z}) \to H_1(X_0(p), \text{cusps}; \mathbf{Z}). \tag{3.8}$$

The image of $\mathbf{F}_p^\times \setminus \{-1, 1\}$ under this map is contained in $H_1(X_0(p); \mathbf{Z})$, which sits inside $H_1(X_0(p), \text{cusps}; \mathbf{Z})$ canonically; this image generates $H_1(X_0(p); \mathbf{Z})$ as a $\mathbf{Z}$-module. If $x \in \mathbf{F}_p$, then let $[x]$ denote the image of x in $H_1(X_0(p); \mathbf{Z})$ under (3.8). The symbol $[x]$ is called a *Manin symbol*.

We obtain the following presentation of the group $H_1(X_0(p); \mathbf{Z})$ (see [Mer96b, §1.3], or [Cre97, §2.2]):

generators: $[x]$ for $x \in \mathbf{F}_p^\times \setminus \{-1, 1\}$, where $[x]$ is just a symbol
relations: $[x] + [-1/x] = 0 \quad \forall x : x \not\equiv (-1/x) \bmod p$
$[x] = 0 \quad \forall x : x \equiv (-1/x) \bmod p$
$[x] + [-1 - 1/x] + [-1/(1+x)] = 0 \quad \forall x : x \not\equiv (-1 - 1/x) \bmod p$
$[x] = 0 \quad \forall x : x \equiv (-1 - 1/x) \bmod p$
$[-2] + [-1/2] = 0$
where all the calculations in the brackets are done modulo p

We can express the winding element in terms of the Manin symbols using the formula (see [Mer96b, Prop. 11 and Lem. 3]):

$$(p-1)e = -\sum_{x=2}^{p-2} F(x)[x], \tag{3.9}$$

where

$$F(x) = (p-1)/2 - 2\sum_{q=1}^{(p-1)/2} \left(\left\lfloor \frac{q(x+1)}{p} \right\rfloor - \left\lfloor \frac{q(x-1)}{p} \right\rfloor \right),$$

and where $\lfloor y \rfloor$ denotes the integer part of y.

If i is a positive integer, then define $\sigma_1(i) = \sum_{d|i, d>0} d$. There are formulas for the action of the Hecke operators on the Manin symbols. For our purposes, we only need the formula below (see [Mer96a, Lem. 2]):

$$(T_i - \sigma_1(i))e = - \sum_{a,b,c,d \in \mathbf{Z}; a>b\geq 0; d>c>0; ad-bc=i} [c/d]. \tag{3.10}$$

The set over which the sum is taken in (3.10) is finite and there is an algorithm to generate it based on [Mer94, §3.3], which we indicate now (this was communicated to us by L. Merel). First, consider all integers δ such that $\delta \mid i$ and $\delta > 1$. For each δ, consider $k = 1, \ldots, (\delta - 1)$. For each such pair (δ, k), construct matrices

$$\begin{pmatrix} a_q & b_q \\ c_q & d_q \end{pmatrix}$$

inductively as follows. Choose

$$\begin{pmatrix} a_0 & b_0 \\ c_0 & d_0 \end{pmatrix} = \begin{pmatrix} i/\delta & 0 \\ k & \delta \end{pmatrix}.$$

Given the matrix for $q = j$, let t be the smallest integer greater than or equal to d_j/c_j. Then define

$$\begin{pmatrix} a_{j+1} & b_{j+1} \\ c_{j+1} & d_{j+1} \end{pmatrix} = \begin{pmatrix} a_j & b_j \\ c_j & d_j \end{pmatrix} \begin{pmatrix} t & 1 \\ -1 & 0 \end{pmatrix}.$$

At each stage, the value of c_q will decrease. We keep doing the inductive process while $c_q > 0$ (thus the matrix for which $c_q = 0$ is excluded from the set). Now repeat the procedure for every pair (δ, k) as above. The set of all a_q, b_q, c_q, d_q we obtain in the process are the a, b, c, d (respectively) that satisfy the conditions $a, b, c, d \in \mathbf{Z}$; $a > b \geq 0$; $d > c > 0$; $ad - bc = i$ in (3.10) above. For example, for $i = 3$, the matrices we get are

$$\begin{pmatrix} 1 & 0 \\ 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 2 & 3 \end{pmatrix}, \text{ and } \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}.$$

So $(T_3 - \sigma_1(3))e = [1/3] + [2/3] + [1/2]$, where the calculations in the brackets are done modulo p.

To do calculations involving the Hecke algebra or an ideal of the Hecke algebra, we need a finite set of generators for the Hecke algebra as a $\mathbf{Z}$-module. This is achieved in Proposition 3.3.4. Before that, we briefly discuss the generation of the Hecke algebra over certain fields. For Lemma 3.3.1 and Proposition 3.3.2, we take the level to be any positive integer N, not necessarily prime.

Lemma 3.3.1. *Let K denote the field $\mathbf{Q}$ or the field $\mathbf{F}_\ell$ where ℓ is a prime. If r is a positive integer such that $T_1, \ldots, T_r$ do not generate $\mathbf{T} \otimes K$ as a K-vector space, then there exists a non-zero cusp form over K whose first r Fourier coefficients are zero.*

Proof. Recall the definition of $S_2(\Gamma_0(N), K)$ from Section 1.2. We have a perfect pairing $(\mathbf{T} \otimes K) \times S_2(\Gamma_0(N), K) \to K$ given by $(T, f) \mapsto a_1(f \mid T)$ (see [Rib83, (2.2)]). Since $T_1, \ldots, T_r$ do not generate $\mathbf{T} \otimes K$ as a K-vector space, there exists a non-zero cusp form f over K such that f is orthogonal to $T_1, \ldots, T_r$ under this pairing, i.e., such that its first r Fourier coefficients are zero. □

Let g denote the genus of $X_0(N)$. We may assume $g \geq 1$, since otherwise the theory is vacuous.

Proposition 3.3.2. *Let K denote $\mathbf{Q}$ or $\mathbf{F}_\ell$ where $\ell \nmid N$. Then $\mathbf{T} \otimes K$ is generated as a K-vector space by $T_1, \ldots, T_{2g-1}$.*

Proof. Suppose not. Then, by Lemma 3.3.1, there is a cusp form f whose first $(2g-1)$ coefficients vanish. But that gives a differential on $X_0(N)_K$ that vanishes to order at least $(2g-1)$ at ∞, which is forbidden by the Riemann-Roch theorem. □

Let us revert to the assumption that the level N is a prime p. In that case, we can improve on Proposition 3.3.2 to get the following result, communicated to us by M. Baker:

Proposition 3.3.3. $\mathbf{T} \otimes \mathbf{Q}$ *is generated as a $\mathbf{Q}$-vector space by $T_1, \ldots, T_g$.*

Proof. We may assume that $g \geq 2$, since for $g = 1$, the result is already contained in Proposition 3.3.2. Suppose the result is false. Then by Lemma 3.3.1, there is a cusp form f over $\mathbf{Q}$ whose first g coefficients vanish. But that gives a differential on $X_0(p)$ that vanishes to order at least g at ∞. This shows that ∞ is a Weierstrass point [Atk67] on $X_0(p)$. But that cannot happen since the level is a prime, by [Ogg78]. This contradiction proves the lemma. □

Our calculations showed that $T_1, \ldots, T_g$ do not generate $\mathbf{T}$ over $\mathbf{Z}$ in general (e.g., when the level is 53, we found that $T_1, \ldots, T_g$ generate a subgroup of $\mathbf{T}$ of index 3). Let r denote the integer part (or floor) of $(p+1)/6$. A generating set for $\mathbf{T}$ over $\mathbf{Z}$ is provided by the the following result (communicated to us by K. Ribet; for a generalization, see [Ste00]).

Proposition 3.3.4. *The Hecke algebra $\mathbf{T}$ is generated as a $\mathbf{Z}$ module by $T_1, \ldots, T_r$.*

Proof. Suppose not. Let ℓ be a prime that divides the order of the quotient $\mathbf{T}/\langle T_1, \ldots, T_r \rangle$, where $\langle T_1, \ldots, T_r \rangle$ denotes the sub $\mathbf{Z}$-module of $\mathbf{T}$ generated by $T_1, \ldots, T_r$. By a simple group theoretic argument that uses the fact that $\mathbf{T}$ is a finitely generated abelian group, this implies that $\mathbf{T}/\ell\mathbf{T}$ is not generated as a $\mathbf{F}_\ell$-vector space by $T_1 \bmod \ell, \ldots, T_r \bmod \ell$. Then, by Lemma 3.3.1, there exists a non-zero cusp form over $\mathbf{F}_\ell$ whose first r Fourier coefficients are zero. But then, by [Stu87, Thm. 1], $f \equiv 0 \bmod \ell$, i.e., $f = 0$, giving a contradiction. □

It is not clear if $T_1, \ldots, T_{2g-1}$, which generate $\mathbf{T} \otimes \mathbf{Q}$ over $\mathbf{Q}$, generate $\mathbf{T}$ over $\mathbf{Z}$ in general. This might be useful for speeding up calculations since $2g - 1 \leq r$; however $r - (2g-1) \leq 3$.

3.3.2 Algorithms to calculate the factors

We now describe how to compute $\left|\frac{H^+}{\widehat{H_e}^+ + H_e^+}\right|$ and $\left|\frac{H_e^+}{\Im e}\right|$ using modular symbols.

First we describe the calculation of $\left|\frac{H_e^+}{\Im e}\right|$. Note that since H^+/H_e^+ is torsion free, $H_e^+/\Im e$ is just the torsion subgroup of $H^+/\Im e$.

Note that complex conjugation on the $\mathbf{C}$-valued points of $X_0(N)$ (a variety over $\mathbf{Q}$) is the same as the involution on $X_0(N)(\mathbf{C})$ induced by the involution $* : z \mapsto -\overline{z}$ on $\mathcal{H}$, under the quotient map $\mathcal{H} \cup \mathbf{P}^1(\mathbf{Q}) \to X_0(N)(\mathbf{C})$. This is because the rational structure on $X_0(N)$ is given by modular functions that have rational Fourier coefficients, and $*$ acts as complex conjugation on $q(z) = \exp(2\pi i z)$. Using this, one can show that if c denotes complex conjugation on H, then c takes $[x]$ to $[-x]$. Also, in our case (prime level), $H^+ = (1+c)H$ (by [Mer96b, Prop. 5]). Thus H^+ is the subgroup of H generated by $[x]+[-x]$. To find the generators of the subgroup $\Im e$, we use the Lemma below.

Lemma 3.3.5. *The ideal $\Im$ is generated as a $\mathbf{Z}$-module by the set consisting of the element n and the elements $(T_i - \sigma_1(i))$ for $i = 2, \ldots, r$.*

Proof. Let $\Im'$ denote the $\mathbf{Z}$-submodule of $\mathbf{T}$ generated by n and the elements $(T_i - \sigma_1(i))$ for $i = 2, \ldots, r$. Then, by [Maz77, § II.9], $\Im' \subseteq \Im$. Consider the map of $\mathbf{Z}$-modules $\phi : \mathbf{Z} \to \mathbf{T}/\Im'$ given by $1 \mapsto T_1$. Now $T_1, T_2 - \sigma_1(2), \ldots, T_r - \sigma_1(r)$ generate $\mathbf{T}$ as a $\mathbf{Z}$-module and so $\mathbf{T}/\Im'$ is generated as a $\mathbf{Z}$-module by $T_1 = \phi(1)$; thus the map ϕ is surjective. Also, we have $n\mathbf{Z} \subseteq \ker\phi$. Thus we a sequence of surjective maps $\mathbf{Z} \xrightarrow{\phi} \mathbf{T}/\Im' \to \mathbf{T}/\Im$. The kernel of the first map contains $n\mathbf{Z}$, but on the other hand, the kernel of the composite is $n\mathbf{Z}$, by [Maz77, II.9.7]. Hence $\Im' = \Im$. □

So $\Im e$, as a subgroup of H, is generated by the set consisting of the element ne and the elements $(T_i - \sigma_1(i)) \cdot e$ for $i = 1, \ldots, r$. To express these elements in terms of the Manin symbols, we use (3.9) and (3.10) from § 3.3.1. Note that H is a free $\mathbf{Z}$-module and that we can divide out formula (3.9) by $(p-1)/n$ to calculate ne only if we write the right-hand side of (3.9) in terms of a basis for H.

So, to calculate $H^+/\Im e$, we first find a basis for H; then we quotient out by the relation for ne obtained from (3.9), and by the relations (3.10) for $i = 2, \ldots, r$; call the resulting quotient G. Finally, $H^+/\Im e$ is the subgroup of G generated by the images of the elements $[x] + [-x]$ for all x. All this can be done using algorithms for the Smith normal form (for example, see [Coh00, §2.4.4]; these algorithms were pointed out to us by B. Sturmfels). We used Maple and the LiDIA library (in C++) to do the calculations.

In [Aga99, Thm. 1], we used the result that 7 divides $\left|\frac{H_e^+}{\Im e}\right|$ for $p = 1091$, which could not be justified there due to lack of space. To prove this, one can simplify the algorithm using the two facts:
1) We have $H^+ \hookrightarrow H/H_-$ with cokernel of order a power of 2, where H_- is the subgroup generated by $[x] - [-x]$ for all x, and
2) If $\Im''$ is the $\mathbf{Z}$-submodule of $\mathbf{T}$ generated by the set consisting of $(p-1)$ and the elements $(T_i - \sigma_1(i))$ for $i = 2, \ldots, r$, then $\Im'' \subseteq \Im$ with index dividing $(p-1)/n$, and the only primes that can divide $(p-1)/n$ are 2 and 3.

Using this, and some simplifications in the relations, we have that for the prime $p = 1091$, the group given by:

generators: $[x]$ for $x \in \mathbf{F}_p^\times \setminus \{-1, 1\}$, where $[x]$ is just a symbol
relations: $[x] + [-1/x] = 0 \ \ \forall x$
$[x] + [-1 - 1/x] + [-1/(1+x)] = 0 \ \ \forall x$
$[-2] + [-1/2] = 0$
$[x] - [-x] = 0 \ \ \forall x$
$\sum_{x=1}^{p-1} F(x)[x] = 0$
$\sum_{a,b,c,d \in \mathbf{Z}; a>b\geq 0; d>c>0; ad-bc=i} [c/d] = 0$ for $i = 2, \ldots, r$,
where all the calculations in the brackets are done modulo p,

has torsion subgroup that differs from $H_e^+/\Im e$ only by powers of 2 and 3. Hence we can use it to check that 7 divides the factor $\left|\frac{H_e^+}{\Im e}\right|$.

Next, we can calculate $\left|\frac{H^+}{\widehat{H_e}^+ + \Im e}\right|$ as follows. We already know the generators of $\Im e$. Next we find the generators of the kernel of the map $\mathbf{T} \otimes \mathbf{Q} \to H \otimes \mathbf{Q}$ given by $t \mapsto te$. For this, we use the fact that $T_1, T_2 - \sigma_1(2), \ldots, T_g - \sigma_1(g)$ generate $\mathbf{T} \otimes \mathbf{Q}$ (by Proposition 3.3.3) and do calculations using formulas (3.9) and (3.10). Then we clear the denominators of the set of generators of the kernel; call the resulting set S. Let G be the subgroup of H generated by th, where t runs over all elements of S and h runs over the set of generators of H. Now G is a subgroup of $\widehat{H_e}$ with finite index, but not necessarily equal to $\widehat{H_e}$. To remove this problem, use the fact that $H/\widehat{H_e}$ is torsion free: thus $\left|\frac{H^+}{\widehat{H_e}^+ + \Im e}\right|$ is the ratio of the order of the torsion subgroup of $\frac{H^+}{G^+}$ to the order of the torsion subgroup of $\frac{H^+}{G^+ + \Im e}$, both of which can be computed.

Finally, note that we have an exact sequence

$$0 \to \frac{H_e^+}{\Im e} \to \frac{H^+}{\widehat{H_e}^+ + \Im e} \to \frac{H^+}{\widehat{H_e}^+ + H_e^+} \to 0.$$

Hence to get the factor $\left|\frac{H^+}{\widehat{H_e}^+ + H_e^+}\right|$ appearing in Theorem 3.2.2, we only have to divide $\left|\frac{H^+}{\widehat{H_e}^+ + \Im e}\right|$ by $\left|\frac{H_e^+}{\Im e}\right|$.

3.3.3 Tables of calculations

We computed the structure of $H_e^+/\Im e$ for prime levels up to 1447. The results appear in Table 3.1; in that table, a sequence of integers $n_1, \ldots, n_r$ in the second column denotes the abelian group $\mathbf{Z}/n_1\mathbf{Z} \times \cdots \times \mathbf{Z}/n_r\mathbf{Z}$. Only the levels for which the group was found to be non-trivial are reported. Thus, for example, Table 3.1 tells us that the group $H_e^+/\Im e$ is trivial for level 17, and for level 997, it is isomorphic to $\mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/24\mathbf{Z}$.

We calculated $\left|\frac{H^+}{\widehat{H_e}^+ + \Im e}\right|$ for prime levels up to 397. The only level for which an odd prime divided $\left|\frac{H^+}{\widehat{H_e}^+ + \Im e}\right|$ was 389, where 5^2 was a factor. So the odd part of $\left|\frac{H^+}{\widehat{H_e}^+ + H_e^+}\right|$ is $5^2/5 = 5$.

We will interpret the results of our calculations in the next section.

Table 3.1: Nontrivial $H_e^+/\Im e$ for prime levels ≤ 1447.

level	structure
359	$2, 2$
389	10
433	7
563	13
571	12
643	8
709	11
821	4
887	$4, 4$
911	$4, 4, 4$
997	$3, 24$
1061	151
1091	49
1163	4
1171	22
1229	16
1231	$4, 4, 4$
1283	25
1361	$4, 4, 4$
1429	25
1433	$2, 2$

3.4 An approach to the Birch and Swinnerton-Dyer formula

Recall the notation from Sections 3.1 and 3.2. In this section, we outline a program to prove the BSD formula for quotients of $J_0(N)$ whose special L-value is non-zero. Any such quotient is a quotient of $J_e(N)$; so the winding quotient is the first interesting quotient from the point of view of the BSD formula for quotients of analytic rank zero. Hence we focus on the winding quotient $J_e(N)$ and for simplicity assume that N is a prime. The contents of this section are highly speculative and should be taken with a grain of salt!

Let p be a prime and again let $J_e = J_e(p)$. If we compare Theorem 3.2.2 to the BSD formula (Conjecture 3.2.1), then we get:

$$\frac{|Ш_{J_e}| \cdot c_p(J_e)}{|J_e(\mathbf{Q})| \cdot |\widehat{J}_e(\mathbf{Q})|} \stackrel{?}{=} \frac{1}{c_{J_e}} \cdot \frac{\left|\frac{H^+}{\widehat{H_e}^+ + H_e^+}\right| \cdot \left|\frac{H_e^+}{\Im e}\right|}{n}. \tag{3.11}$$

Thus the BSD formula for $J_e(p)$ reduces to formula (3.11) above. In the rest of the section, we describe a plan to prove this formula by examining the terms that appear in it.

- **Mordell-Weil groups:**

Recall that since $J_e(\mathbf{Q})$ is finite, so is $\widehat{J}_e(\mathbf{Q})$. The following result was pointed out to us by L. Merel:

Proposition 3.4.1 (Merel). $|\widehat{J}_e(\mathbf{Q})| = n$.

Proof. We have $\widehat{J}_e(\mathbf{Q}) \subseteq J_0(p)(\mathbf{Q})_{\mathrm{tor}}$. By [Maz77, § II.11 and III.1.2], $J_0(p)(\mathbf{Q})_{\mathrm{tor}}$ is cyclic of order n and is generated by the divisor class of $c = (0) - (\infty)$. So it suffices to show that $c \in \widehat{J}_e(\mathbf{Q})$. Now $J_e = J_0(p)/I_e J_0(p)$. Hence $\widehat{J}_e(\overline{\mathbf{Q}})[n]$ can be seen as the group of elements in $J_0(p)(\overline{\mathbf{Q}})[n]$ which are orthogonal to $(I_e \cdot J_0(p))(\overline{\mathbf{Q}})[n]$ under the Weil pairing. Since the Hecke action is adjoint with respect to the Weil pairing, all we have to show is that $I_e c = 0$; but this follows because I_e annihilates e, and e maps to c under the universal covering map $H \otimes \mathbf{R} \to J_0(p)(\mathbf{C})$ (see [Maz77, § II.18.5]). □

Also, L. Merel communicated to us the following result (see [Oes]):

Proposition 3.4.2 (Merel, Oesterlé). $|J_e(\mathbf{Q})| = n$.

Sketch of the proof. Using [Maz77, II.18.10] (see also a complement given in [Mer96b, §5.1]), we get $I_e \subseteq \cap_{r \geq 1} \Im^r$. Using this condition, one observes that the proof of [Maz77, III.1.4] generalizes to give $J_0(p)(\mathbf{Q})_{\mathrm{tor}} \cong J_e(\mathbf{Q})$. Then the result follows from the fact that $|J_0(p)(\mathbf{Q})_{\mathrm{tor}}| = n$ (again by [Maz77, III.1.2, § II.11]). □

- **Generalized Manin constant:**

We already conjectured (Conjecture 2.2.8) that $c_{J_e} = 1$. The only prime that can divide c_{J_e} is 2 (Theorem 2.2.3). So let us assume $c_{J_e} = 1$ for now; in any case the results will be valid if we stay away from the prime 2.

- **Congruence primes:**

Let $S = S_2(\Gamma_0(p), \mathbf{Z})$. Recall from Definition 2.3.1 that the congruence number of J_e is $r_{J_e} = \#\Big(\frac{S}{S[I_e] \oplus (W(I_e) \cap S)}\Big)$, where $W(I_e)$ is the orthogonal complement of $S[I_e]$ in $S_2(\Gamma_0(p), \mathbf{C})$ with respect to the Petersson inner product. The primes that divide r_{J_e} are called the *congruence primes of* J_e.

Lemma 3.4.3.

$$r_{J_e} = \#\left(\frac{S}{S[I_e] \oplus S[\widehat{I_e}]}\right).$$

Proof. Clearly $S[\widehat{I_e}] \subseteq (W(I_e) \cap S)$. Counting dimensions using Corollary 3.2.4 and the fact that $S \otimes \mathbf{Q}$ is a free $\mathbf{T} \otimes \mathbf{Q}$ module of rank 1 (Part 1 of Remark 3.2.6), we get $S[\widehat{I_e}] = (W(I_e) \cap S)$. The lemma now follows from the definition of r_{J_e}. □

Lemma 3.4.4. *If a prime ℓ is not a congruence prime of J_e, then*

$$\mathbf{T} \otimes \mathbf{Z}_\ell \;\cong\; (I_e \otimes \mathbf{Z}_\ell) \;\oplus\; (\widehat{I_e} \otimes \mathbf{Z}_\ell).$$

Proof. By Corollary 3.2.5, $I_e \cap \widehat{I_e} = \{0\}$. It follows, for example from [Dia89, §2], that

$$\#\left(\frac{S}{S[I_e] \oplus S[\widehat{I_e}]}\right) = \#\left(\frac{\mathbf{T}/I_e \oplus \mathbf{T}/\widehat{I_e}}{\mathbf{T}}\right), \tag{3.12}$$

and that we have a canonical isomorphism

$$\frac{\mathbf{T}}{I_e \oplus \widehat{I_e}} \xrightarrow{=} \frac{\mathbf{T}/I_e \oplus \mathbf{T}/\widehat{I_e}}{\mathbf{T}}, \tag{3.13}$$

induced by the projection maps. The lemma follows from equations (3.12) and (3.13), and Lemma 3.4.3. □

Lemma 3.4.5. *$H^+ \otimes \mathbf{Z}_\ell \cong \mathbf{T} \otimes \mathbf{Z}_\ell$ for every prime $\ell \neq 2$.*

Proof. By [Maz77, II.15.1, II.16.3] (see also [Til97, §3]), $H_1(X_0(p), \mathbf{Z})_{\mathfrak{m}}$ is free of rank 2 over $\mathbf{T}_{\mathfrak{m}}$ for every maximal ideal $\mathfrak{m}$ of $\mathbf{T}$ with residue characteristic unequal to 2. The lemma now follows from the discussion in §II.18 of [Maz77]. □

• **Order of the arithmetic component group:** Recall that if A is an abelian variety over $\mathbf{Q}$ and p is a prime number, then $c_p(A) = [\mathcal{A}_{\mathbf{F}_p}(\mathbf{F}_p) : \mathcal{A}^0_{\mathbf{F}_p}(\mathbf{F}_p)]$, where $\mathcal{A}$ denotes the Néron model of A over $\mathbf{Z}$ and $\mathcal{A}^0$ denotes the largest open subgroup scheme of $\mathcal{A}$ in which all the fibers are connected. The group $\mathcal{A}_{\mathbf{F}_p}/\mathcal{A}^0_{\mathbf{F}_p}$ is called the *component group* of A at p and is denoted by $\Phi_p(A)$. The group of $\mathbf{F}_p$-valued points of $\Phi_p(A)$ is called the *arithmetic component group* of A at p. We have a short exact sequence of group schemes

$$0 \to \mathcal{A}^0_{\mathbf{F}_p} \to \mathcal{A}_{\mathbf{F}_p} \to \Phi_p(A) \to 0,$$

which gives us the long exact sequence of Galois cohomology groups:

$$0 \to \mathcal{A}^0_{\mathbf{F}_p}(\mathbf{F}_p) \to \mathcal{A}_{\mathbf{F}_p}(\mathbf{F}_p) \to \Phi_p(A)(\mathbf{F}_p) \to H^1(\mathrm{Gal}(\overline{\mathbf{F}}_p/\mathbf{F}_p), \mathcal{A}^0_{\mathbf{F}_p}(\overline{\mathbf{F}}_p)).$$

By [Lan56], the group $H^1(\mathrm{Gal}(\overline{\mathbf{F}}_p/\mathbf{F}_p), \mathcal{A}^0_{\mathbf{F}_p}(\overline{\mathbf{F}}_p))$ is trivial. Hence $c_p(A)$ is just the order of the arithmetic component group of A at p.

Recall the discussion around Definition 2.3.3: composing the quotient map $\pi : J_0(p) \to J_e$ with its dual map $\widehat{\pi} : \widehat{J}_e \to J_0(p)$ (where we identify $\widehat{J_0(p)}$ with $J_0(p)$ using the usual canonical isomorphism, e.g., see [Mil86c, Thm. 6.6]), we get maps $\widehat{J}_e \xrightarrow{\widehat{\pi}} J_0(p) \xrightarrow{\pi} J_e$ such that the composite, call it ψ, is an isogeny. Recall that, by definition, n_{J_e} is the exponent of $\ker \psi$. Then using the fact that $\ker \psi \subseteq \ker n_{J_e}$, where n_{J_e} also denotes the multiplication by n_{J_e} map on $\widehat{J}_e$, we find that n_{J_e} factors as $n_{J_e} = \psi' \circ \psi$ with ψ' an isogeny $J_e \to \widehat{J}_e$ (see [Mil86a, §8]). We can easily check by the definition of ψ' that $\psi \circ \psi'$ is the multiplication by n_{J_e} map on J_e. Thus the composite $J_e \xrightarrow{\psi'} \widehat{J}_e \xrightarrow{\widehat{\pi}} J_0(p) \xrightarrow{\pi} J_e$ is multiplication by n_{J_e}. This induces maps $\Phi_p(J_e) \to \Phi_p(J_0(p)) \xrightarrow{\pi} \Phi_p(J_e)$ such that the composite is multiplication by n_{J_e}. Thus multiplication by n_{J_e} kills the cokernel $\Phi_p(J_e)/\pi(\Phi_p(J_0(p)))$. By Theorem 2.3.2, the only primes that can divide n_{J_e} are the congruence primes of J_e. Thus, "away" from the congruence primes of J_e, the map $\Phi_p(J_0(p)) \to \Phi_p(J_e)$ is surjective.

If E is an optimal modular elliptic curve, it is known that the map $\Phi_p(J_0(p)) \to \Phi_p(E)$ is surjective. There are two approaches to this: one strategy is to use Ribet's level-lowering theorem (communication of K. Ribet); another strategy (see [MO89, Cor. 2, p. 183]) is to use explicit formulas for the order of the component group given by Ribet (letter to J.-F. Mestre) (these formulas have been generalized to higher dimensional quotients by W. Stein [Ste00]). Also, calculations of W. Stein always found that the map $\Phi_p(J_0(p)) \to \Phi_p(A_f)$ was surjective, where A_f denotes the quotient of $J_0(p)$ associated to a newform f (see Section 4.1.1). By generalizing the proof for elliptic curves, one hopes to show that the map $\Phi_p(J_0(p)) \xrightarrow{\pi} \Phi_p(J_e)$ is surjective. Since $|\Phi_p(J_0(p))| = n$, where again $n = \mathrm{num}(\frac{p-1}{12})$, this would show that $c_p(J_e)$ divides n. In any case, this is true "away" from the congruence primes of J_e.

For simplicity, assume that $c_p(J_e) = n$ and $c_{J_e} = 1$. Then according to the BSD formula, the order of the Shafarevich-Tate group of J_e is the product of $\left|\frac{H^+}{\widehat{H_e}^+ + H_e^+}\right|$ and $\left|\frac{H_e^+}{\Im e}\right|$. Let us examine the nature of these two factors.

- **The factor $\left|\frac{H^+}{\widehat{H_e}^+ + H_e^+}\right|$:** From Lemmas 3.4.4 and 3.4.5, we find that the only primes that can divide the factor $\left|\frac{H^+}{\widehat{H_e}^+ + H_e^+}\right|$ are the prime 2 and the congruence primes of J_e. For example, the only prime level less than 397 for which our calculations (Section 3.3.3) detected an odd prime that divided $\left|\frac{H^+}{\widehat{H_e}^+ + H_e^+}\right|$ was the level 389, where 5 divided this factor; and in this case, we indeed find that 5 is a congruence prime of J_e (see [AS99b]).

Mazur [Maz98] showed that if E is an elliptic curve such that its Mordell-Weil rank is zero and such that the newform corresponding to E is congruent modulo a prime ℓ to the newform associated to another elliptic curve whose Mordell-Weil rank is non-zero, then, under certain mild hypotheses, ℓ divides $|Ш_E|$. In [AS99b], this result is extended to quotients of higher dimension in certain cases. For example, one finds that 5 divides $|Ш_{J_e(389)}|$; so $\left|\frac{H^+}{\widehat{H_e}^+ + H_e^+}\right|$ divides $|Ш_{J_e}|$ away from the prime 2, for level 389. In view of

this, one hopes to show that the factor $\left|\frac{H^+}{\widehat{H_e}^+ + H_e^+}\right|$ divides $|Ш_{J_e}|$.

- **The factor $\left|\frac{H_e^+}{\Im e}\right|$:** This factor is quite mysterious and deserves further study. In fact, the mystery behind the BSD formula probably lies in this factor. We computed $\left|\frac{H_e^+}{\Im e}\right|$ for several primes p (see Section 3.3.3). We found that for all prime levels up to 1447, except for the levels 1091, 1283 and 1429, whenever a prime divided $\left|\frac{H_e^+}{\Im e}\right|$, it was a congruence prime of J_e. For the level 1091, there was a congruence between the newform corresponding to $J_e(1091)$ and a newform at level $2 \cdot 1091$. Similar calculations for the levels 1283 and 1429 have not been done yet.

  So it is possible that the primes that divide the second factor are either congruence primes of J_e or primes of congruence between a modular form killed by I_e and forms of higher levels (that have L-value equal to zero). Thus, by using the techniques mentioned above for the factor $\left|\frac{H^+}{\widehat{H_e}^+ + H_e^+}\right|$, one may be able to prove that $\left|\frac{H_e^+}{\Im e}\right|$ divides $|Ш_{J_e}|$.

- **Upper and lower bounds on $|Ш_{J_e}|$:** Our strategy above might show that the conjectural order of $Ш_{J_e}$ as predicted by the BSD formula divides the (actual) order of $Ш_{J_e}$. See [AS99b] for some results in this direction. For example, one can show that the odd part of the BSD-conjectured order of $Ш_{J_e(389)}$, which is 25, divides the actual order of $Ш_{J_e(389)}$.

  As mentioned in the introduction, one can use Euler systems to bound the p-primary part of the order of $Ш_{J_e}$ from above in terms of the BSD conjectural order, for almost every prime p (see [Rub98, Cor. 8.9]: the results generalize to abelian varieties; instead of Prop. 8.3 in [Rub98], one has to use the results in [Rib97]).

  So one hopes to show that the BSD conjectural order of $Ш_{J_e}$ bounds the (actual) order of $Ш_{J_e}$ from below as well as from above (in particular cases, for example) and thus prove the BSD formula.

Chapter 4

Formulas for the ratio of the special L-value to the real volume for certain other quotients

In this chapter, we generalize the techniques of Section 3.2 to prove formulas expressing the ratio of the special L-value to the real volume as a rational number for certain other quotients. We do this for the quotient associated to a newform in Section 4.1 and for the winding quotient of level a product of two distinct primes in Section 4.2. In Section 4.3, we indicate other possible extensions. Sections 4.1, 4.2 and 4.3 are independent of each other.

4.1 Quotients associated to newforms

We express as an easily computable rational number the ratio of the L-value to the real volume for the quotient of $J_0(N)$ attached to a newform (by Shimura). This formula is used to do calculations regarding the Birch and Swinnerton-Dyer conjecture in [AS99b], which extend the calculations in [Cre97], for quotients that are elliptic curves, to quotients of higher dimension. This section depends on Section 1.2.

4.1.1 Introduction and results

Let N be a positive integer. Let f be a newform for $\Gamma_0(N)$ and let $a_n(f)$ denote its nth Fourier coefficient. Then the series $\sum_{n=1}^{\infty} \frac{a_n(f)}{n^s}$ converges absolutely in s for $\mathrm{Re}(s) > 3/2$ and can be analytically continued to the entire complex plane [Shi94, Thm. 3.66]. It is called the L-function of f and is denoted $L(f, s)$. Suppose $L(f, 1) \neq 0$. Recall the definition of the Hecke algebra $\mathbf{T}$ from Section 1.2. Let I_f be the annihilator of f under the action of $\mathbf{T}$. Let A_f denote the quotient abelian variety $J_0(N)/I_f J_0(N)$ over $\mathbf{Q}$, which was introduced by Shimura in [Shi94]. We call it the quotient of $J_0(N)$ associated to the newform f . Recall the definition of the special L-value $L_{A_f}(1)$, the Manin constant c_{A_f}, the real volume Ω_{A_f}, and $c_\infty(A_f)$ from Section 1.2. We are interested in giving a formula for $L_{A_f}(1)/\Omega_{A_f}$, which is the left-hand side of the Birch and Swinnerton-Dyer formula (Conjecture 1.2.1).

If V is a finite dimensional vector space over $\mathbf{R}$, then a *lattice* $L \subset V$ is a free abelian group of rank equal to $\dim V$ such that $\mathbf{R}L = V$. If $L, M \subset V$ are lattices, the *lattice index* $[L : M]$ is the absolute value of the determinant of an automorphism of V taking L isomorphically onto M.

Recall the definition of the *winding element* e from Section 3.1. Note that by the Manin-Drinfeld Theorem (see [Lan95, Chap. IV, Thm. 2.1] and [Man72]), $e \in H_1(X_0(N), \mathbf{Z}) \otimes \mathbf{Q}$. Also, since complex conjugation on $H_1(X_0(N), \mathbf{Z})$ is induced by the map $z \mapsto -\overline{z}$ on the complex upper half plane, we see that e is invariant under complex conjugation. Thus $\mathbf{T}e \subseteq H_1(X_0(N), \mathbf{Z})^+ \otimes \mathbf{Q}$. Let $f_1 = f, f_2, \ldots, f_d$ be the Galois conjugates of f (for some integer d) and let Φ denote the map $H_1(X_0(N), \mathbf{Z})^+ \otimes \mathbf{Q} \to \mathbf{C}^d$ given by mapping a cycle γ to $\{\int_\gamma f_1, \ldots, \int_\gamma f_d\}$. Then $\Phi(H_1(X_0(N), \mathbf{Z})^+)$ and $\Phi(\mathbf{T}e)$ are both invariant under complex conjugation, and are lattices in $\mathbf{R}^d \subseteq \mathbf{C}^d$ ($\Phi(\mathbf{T}e)$ is a lattice since $L(f, 1) \neq 0$).

We have the following formula, which was conjectured by W. Stein based on some calculations:

Theorem 4.1.1. *With notation as above,*

$$\frac{L_{A_f}(1)}{\Omega_{A_f}} = \frac{[\Phi(H_1(X_0(N), \mathbf{Z})^+) : \Phi(\mathbf{T}e)]}{c_{A_f} \cdot c_\infty(A_f)}$$

We prove this Theorem in § 4.1.3. The proof is an adaptation of the proof of Theorem 3.2.2. See also [AS99b] for a similar proof. This formula was used for doing computations regarding the Birch and Swinnerton-Dyer conjectural formula in [AS99b].

Let C denote the cuspidal subgroup, i.e., the subgroup of the degree zero divisors on $X_0(N)$ supported on the cusps and let n denote its order (this is consistent with the definition of n in Section 3.2, since when $N = p$ is a prime, the order of the cuspidal subgroup is $\mathrm{num}(\frac{p-1}{12})$). We show:

Proposition 4.1.2. *With notation as above,*

$$n \cdot [\Phi(H_1(X_0(N), \mathbf{Z})^+) : \Phi(\mathbf{T}e)] \in \mathbf{Z}.$$

We prove this in the next section. This result ties in very well with the Birch and Swinnerton-Dyer conjectural formula. See [AS99b] for details and a stronger result which says that the number n above can be replaced by the order of the image in $A_f(\mathbf{Q})$ of the point $(0) - (\infty)$.

4.1.2 Proof of Proposition 4.1.2

Let $\Im$ denote the annihilator of the divisor $(0) - (\infty)$, considered as an element of $J_0(N)(\mathbf{C})$, under the action of $\mathbf{T}$. An easy adaptation of [Maz77, II.18.6] shows that $\Im e \in H_1(X_0(N), \mathbf{Z})^+$. So we have

$$[\Phi(H_1(X_0(N), \mathbf{Z})^+) : \Phi(\mathbf{T}e)] = \frac{[\Phi(H_1(X_0(N), \mathbf{Z})^+) : \Phi(\Im e)]}{[\Phi(\mathbf{T}e) : \Phi(\Im e)]},$$

where both the numerator and the denominator on the right-hand side are the usual indices of subgroups of groups, and hence are integers. So, to prove Proposition 4.1.2, it suffices to prove that $[\Phi(\mathbf{T}e) : \Phi(\Im e)]$ divides n.

We have the surjection $\mathbf{T} \to \Phi(\mathbf{T}e)/\Phi(\Im e)$ given by taking $t \in \mathbf{T}$ to the coset containing $\Phi(te)$. Clearly $\Im$ is in the kernel. Hence we get a surjection $\mathbf{T}/\Im \to \Phi(\mathbf{T}e)/\Phi(\Im e)$. This shows that $[\Phi(\mathbf{T}e) : \Phi(\Im e)]$ divides the order of $\mathbf{T}/\Im$. So it suffices to prove that the order of $\mathbf{T}/\Im$ divides the order of C.

We have the map $\mathbf{T} \to C$, given by taking $t \in \mathbf{T}$ to $t((0) - (\infty))$. By the definition of $\Im$, the kernel of this map is $\Im$. Thus, we have an injection $\mathbf{T}/\Im \to C$, showing that the order of $\mathbf{T}/\Im$ divides the order of C, thus finishing the proof.

4.1.3 Proof of Theorem 4.1.1

We continue to use the notation from § 4.1.1. Theorem 4.1.1 follows immediately from Proposition 4.1.4 and Proposition 4.1.6 below.

We shall first replace the lattice index in Theorem 4.1.1 by another index. Recall that if $f \in S_2(\Gamma_0(N), \mathbf{C})$, then ω_f is the differential on $X_0(N)(\mathbf{C})$ given by $2\pi i f(z)dz$.

Lemma 4.1.3. *The kernel of the composite*

$$\mathbf{T}e \hookrightarrow H_1(X_0(N), \mathbf{Z})^+ \otimes \mathbf{Q} \to (H_1(X_0(N), \mathbf{Z})^+/\ker\Phi) \otimes \mathbf{Q}$$

is $I_f e$, where the second map above is the natural projection map.

Proof. If $t \in I_f$, then $\int_{te} \omega_{f_i} = \int_e \omega_{tf_i} = 0 \ \forall i$, and thus $I_f e$ is in the kernel. Conversely if $t \in \mathbf{T}$ is such that te is in the kernel, then $\int_{te} \omega_f = 0$. Now f is an eigenform for all Hecke operators; let the eigenvalue for t be λ. Then we have $\lambda \int_e \omega_f = 0$, which means that $\lambda = 0$, since $\int_e \omega_f = L(f, 1) \neq 0$. Thus $tf = \lambda f = 0$, i.e., $t \in I_f$, and so the kernel of the map mentioned above is contained in $I_f e$. That proves the lemma. □

Thus we can think of $\mathbf{T}e/I_f e$ as a lattice in $(H_1(X_0(N), \mathbf{Z})^+/\ker\Phi) \otimes \mathbf{R}$. Let π denote the quotient map $J_0(N) \to A_f$. Since its kernel is connected, it induces a surjection $H_1(J_0(N), \mathbf{R}) \to H_1(A_f, \mathbf{R})$. The standard immersion $X_0(N) \to J_0(N)$ obtained by sending the cusp ∞ to 0, gives us an isomorphism $H_1(X_0(N), \mathbf{R}) \cong H_1(J_0(N), \mathbf{R})$. Combining the two maps above, we get a surjection $\pi_* : H_1(X_0(N), \mathbf{R}) \to H_1(A_f, \mathbf{R})$.

Proposition 4.1.4. *The map π_* induces an isomorphism*

$$H_1(X_0(N), \mathbf{Z})^+/\ker\Phi \cong H_1(A_f, \mathbf{Z})^+,$$

and we have

$$[\Phi(H_1(X_0(N), \mathbf{Z})^+) : \Phi(\mathbf{T}e)] = \left[H_1(A_f, \mathbf{Z})^+ : \pi_*(\mathbf{T}e/I_f e)\right],$$

where $H_1(A_f, \mathbf{Z})^+$ and $\pi_*(\mathbf{T}e/I_f e)$ are considered as lattices in $H_1(A_f, \mathbf{R})^+$.

Proof. From Lemma 4.1.3, we have

$$[\Phi(H_1(X_0(N), \mathbf{Z})^+) : \Phi(\mathbf{T}e)] = [H_1(X_0(N), \mathbf{Z})^+/\ker\Phi : \mathbf{T}e/I_f e], \tag{4.1}$$

where the groups on the right-hand side are considered as lattices in the $\mathbf{R}$-vector space $(H_1(X_0(N), \mathbf{Z})^+/\ker\Phi) \otimes \mathbf{R}$.

Let γ be an element of $H_1(X_0(N), \mathbf{Z})$. Then

$$\begin{aligned}\gamma \in \ker \pi_* &\iff \textstyle\int_{\pi_*\gamma} \omega = 0 \quad \forall\, \omega \in H^0(A_f, \Omega_{A_f/\mathbf{C}}) \\ &\iff \textstyle\int_\gamma \pi^*(\omega) = 0 \quad \forall\, \omega \in H^0(A_f, \Omega_{A_f/\mathbf{C}}) \\ &\iff \textstyle\int_\gamma \omega_{f_i} = 0 \quad \forall\, i \\ &\iff \gamma \in \ker\Phi.\end{aligned}$$

Combining this with the fact that π_* is surjective, we see that π_* induces an isomorphism $H_1(X_0(N), \mathbf{Z})^+/\ker\Phi \cong H_1(A_f, \mathbf{Z})^+$.

Applying π_* to the right-hand side of (4.1), we get the proposition. □

Let $S_f = S_2(\Gamma_0(N), \mathbf{Z})[I_f]$. Recall that we have a perfect pairing

$$\mathbf{T} \times S_2(\Gamma_0(p), \mathbf{Z}) \to \mathbf{Z} \tag{4.2}$$

which associates to (T, f) the first Fourier coefficient $a_1(f \mid T)$ of the modular form $f \mid T$ (see [Rib83, (2.2)]); this induces a pairing

$$\psi : \mathbf{T}/I_f \times S_f \to \mathbf{Z}.$$

Lemma 4.1.5. *The pairing ψ above is a perfect pairing.*

Proof. Both $\mathbf{T}/I_f$ and S_f are free $\mathbf{Z}$-modules of the same rank. So it suffices to prove that the induced maps $S_f \to \mathrm{Hom}(\mathbf{T}/I_f, \mathbf{Z})$ and $\mathbf{T}/I_f \to \mathrm{Hom}(S_f, \mathbf{Z})$ are injective. The injectivity of the first map follows from the perfectness of the pairing (4.2). Suppose the image of $T \in \mathbf{T}$ in $\mathbf{T}/I_f$ maps to the trivial element of $\mathrm{Hom}(S_f, \mathbf{Z})$. Then $a_1(f \mid T) = 0$. But f is an eigenform for T; suppose the eigenvalue is λ. Then $0 = a_1(f \mid T) = \lambda a_1(f) = \lambda$. Thus $f \mid T = 0$, i.e., $T \in I_f$. Thus the map $\mathbf{T}/I_f \to \mathrm{Hom}(S_f, \mathbf{Z})$ is injective and we are done. □

Next, we relate the new lattice index in Proposition 4.1.4 to the special L-value:

Proposition 4.1.6.

$$\frac{L_{A_f}(1)}{\Omega_{A_f}} = \frac{[H_1(A_f, \mathbf{Z})^+ : \pi_*(\mathbf{T}e/I_f e)]}{c_{A_f} \cdot c_\infty(A_f)}.$$

Proof. The proof is similar to the proof of Theorem 3.2.2. Recall that we have the pairing $(H_1(X_0(N), \mathbf{Z})^+ \otimes \mathbf{C}) \times S_2(\Gamma_0(N), \mathbf{C}) \to \mathbf{C}$ given by $\langle \gamma, f \rangle = \int_\gamma \omega_f$. In the proof, at various points, we will consider pairings between two $\mathbf{Z}$-modules; unless otherwise stated, each such pairing is obtained in a natural way from this pairing.

Now $L_{A_f}(s) = \prod_i L(f_i, s)$, by [Shi94, Thm. 7.14] and [Car86]. Recall from Section 1.2 that we have $\Omega_{A_f} = c_{A_f} \cdot c_\infty(A_f) \cdot \mathrm{disc}(H_1(A_f, \mathbf{Z})^+ \times S_f \to \mathbf{C}),$. Hence

$$\begin{aligned} c_{A_f} \cdot c_\infty(A_f) \cdot \frac{L_{A_f}(1)}{\Omega_{A_f}} &= \frac{\prod_i \langle e, f_i \rangle}{\mathrm{disc}(H_1(A_f, \mathbf{Z})^+ \times S_f \to \mathbf{C})} \\ &= \frac{\prod_i \langle e, f_i \rangle}{\mathrm{disc}(\mathbf{T}e/I_f e \times S_f \to \mathbf{C})} \left[H_1(A_f, \mathbf{Z})^+ : \pi_*(\mathbf{T}e/I_f e)\right]. \end{aligned}$$

The proposition now follows from:

Claim 1:

$$\frac{\prod_i \langle e, f_i \rangle}{\mathrm{disc}(\mathbf{T}e/I_f e \times S_f \to \mathbf{C})} = 1.$$

Proof of Claim 1. We first make another claim:
Claim 2: The map $\mathbf{T} \to \mathbf{T}e$ given by $t \mapsto te$ induces an isomorphism $\mathbf{T}/I_f \xrightarrow{\cong} \mathbf{T}e/I_f e$.

Proof of Claim 2. It is clear that the map $\mathbf{T} \to \mathbf{T}e/I_f e$ given by $t \mapsto te$ is surjective. All we have to show is that the kernel of this map is I_f. It is clear that the kernel contains I_f. Conversely, if t is in the kernel, then $te \in I_f e$; let $i \in I_f$ be such that $te = ie$. Then $(t-i)e = 0$, and thus $\int_{(t-i)e} \omega_f = 0$, i.e., $\int_e \omega_{(t-i)f} = 0$. If the eigenvalue of f under $(t-i)$ is λ, then this means $\lambda L(f,1) = 0$, i.e., $\lambda = 0$. Thus $(t-i) \in I_f$, i.e., $t \in I_f$. This proves Claim 2. □

In what follows, i, j, k, and ℓ are indices running from 1 to d. Let $\{g_k\}$ be a $\mathbf{Z}$-basis of S_f and let $\{t_j\}$ be the dual basis of $\mathbf{T}/I_f$ under the perfect pairing ψ in Lemma 4.1.5 above. Then by Claim 2, $\{t_j e\}$ is a basis for $\mathbf{T}e/I_f e$. Now $g_k = \sum_k a_{ki} f_i$ for some $\{a_{ki} \in \mathbf{C}\}$. Let A be the matrix having (k,i)-th entry a_{ki}, and let $(a^{-1})_{i\ell}$ denote the (i,ℓ)-th element of the inverse of A. Then

$$\begin{aligned}
\operatorname{disc}(\mathbf{T}e/I_f e \times S_f \to \mathbf{C}) &= \det\{\langle t_j e, g_k\rangle\} = \det\{\langle e, g_k \,|\, t_j\rangle\} = \det\{\langle e, (\textstyle\sum_i a_{ki} f_i) \,|\, t_j\rangle\} \\
&= \det\{\langle e, \textstyle\sum_i a_{ki} a_1(f_i \,|\, t_j) f_i\rangle\} \qquad \text{(since } f_i\text{'s are eigenvectors)} \\
&= \det\{\langle e, \textstyle\sum_i a_{ki} \sum_\ell (a^{-1})_{i\ell} a_1(g_\ell \,|\, t_j) f_i\rangle\} \quad \text{(using } f_i = \textstyle\sum_\ell (a^{-1})_{i\ell} g_\ell\text{)} \\
&= \det\{\langle e, \textstyle\sum_i a_{ki} (a^{-1})_{ij} f_i\rangle\} \qquad \text{(using } a_1(g_\ell \,|\, t_j) = \delta_{\ell j}\text{)} \\
&= \det\{\textstyle\sum_i a_{ki} (a^{-1})_{ij} \langle e, f_i\rangle\} = \det\{\textstyle\sum_i a_{ki} \langle e, f_i\rangle (a^{-1})_{ij}\} \\
&= \det(A \Delta A^{-1}) \qquad \text{(where } \Delta = \operatorname{diag}(\langle e, f_i\rangle)\text{)} \\
&= \det(\Delta) = \textstyle\prod_i \langle e, f_i\rangle.
\end{aligned}$$

This proves Claim 1. □

With that, we are done proving Proposition 4.1.6. □

4.2 The winding quotient of level a product of two distinct primes

Let p and q be two distinct primes and let J_e be the winding quotient at level pq. We give a formula that expresses the ratio of $L_{J_e}(1)$ to the real volume as a rational number and interpret this formula in terms of the Birch and Swinnerton-Dyer conjecture. The proof of this formula uses a generalization of the techniques of Section 3.2. This section depends on Chapter 1 and Section 3.1.

A. Brumer reminded us that if our main interest is to prove the Birch and Swinnerton-Dyer formula for any quotient of $J_0(N)$, then it suffices to prove it for all new quotients (at all levels that divide N). This is because any such a quotient is isogenous to a product of new quotients (at various levels dividing N), and if the BSD formula is true for an abelian variety, then it is true for an isogenous abelian variety (see [Mil86b, Thm. 7.3]). However, since the BSD formula is not known to be true even for new quotients, the results of this section are still of interest. Also, these results led to the investigation of the generalized Manin constant in Chapter 2.

4.2.1 Notations and results

Let p and q be two distinct primes and recall, from Section 3.1, the definitions of the winding element e, the winding ideal I_e and the winding quotient $J_e(N)$ at level $N = pq$. For simplicity of notation, we denote $J_e(pq)$ by just J_e in this section. Also, if f is a modular form, and m is an integer, let $a_m(f)$ denote the mth Fourier coefficient of f. Recall the definitions from Chapter 1, especially the definitions of the special L-value $L_{J_e}(1)$, the Manin constant c_{J_e}, the real volume Ω_{J_e}, and $c_\infty(J_e)$. Let $H = H_1(X_0(pq), \mathbf{Z})$, $H_e = H[I_e]$, $\widehat{I}_e = \mathrm{Ann}_{\mathbf{T}} I_e$, $\widehat{H}_e = H[\widehat{I}_e]$, $\Im = \mathrm{Ann}_{\mathbf{T}}((0) - (\infty))$. If M is a positive integer, then let S_M denote the set of newforms f of level M such that $L(f, 1) \neq 0$. Then we have:

Theorem 4.2.1. *With notation as above,*

$$\frac{L_{J_e}(1)}{\Omega_{J_e}} = \frac{1}{\left|\frac{H^+/\widehat{H_e}^+}{(1+c)(H/\widehat{H_e})}\right|} \cdot \frac{\left|\frac{H^+}{\widehat{H_e}^+ + H_e^+}\right| \cdot \left|\frac{H_e^+}{\Im e}\right|}{\prod_{f \in S_p}(1 + q - a_q(f)) \cdot \prod_{g \in S_q}(1 + p - a_p(g)) \cdot \left|\frac{\mathbf{T}e}{\Im e}\right|} \cdot \frac{q^{\#S_p} \cdot p^{\#S_q}}{c_{J_e}} \cdot$$

Compare this to Theorem 3.2.2. Note that $\left|\frac{H^+/\widehat{H_e}^+}{(1+c)(H/\widehat{H_e})}\right|$ is a power of 2. We will prove the formula above in the next section, but first let us compare it to the Birch and Swinnerton-Dyer formula (Conjecture 1.2.1). We will prove in Section 4.2.2 that $L_{J_e}(1) \neq 0$, and so by [KL89] (which uses [GZ86], and was completed independently in [BFH90] and [MM91]), $J_e(\mathbf{Q})$ and the Shafarevich-Tate group $Ш_{J_e}$ are finite. The BSD formula then says that

$$\frac{L_{J_e}(1)}{\Omega_{J_e}} \stackrel{?}{=} \frac{|Ш_{J_e}| \cdot c_p(J_e) \cdot c_q(J_e)}{|J_e(\mathbf{Q})| \cdot |\widehat{J}_e(\mathbf{Q})|}\,, \tag{4.3}$$

where $c_p(J_e)$ and $c_q(J_e)$ are the orders of the arithmetic component group of J_e at p and q respectively, and $\widehat{J}_e$ is the dual abelian variety of J_e. Compare formula (4.3) to Theorem 4.2.1.

Example 4.2.2. Consider the case when $p = 3$ and $q = 11$. It turns out that $J_0(33)$ has analytic rank zero, so $I_e = 0$ and $J_e = J_0(33)$. There are no newforms of level 3, and there is one newform of level 11, call it g. From [Cre97, Table 3], we find that $a_3(g) = -1$. So $1 + p - a_p(g) = 1 + 3 - (-1) = 5$. Thus, for level 33, Theorem 4.2.1 says that

$$\frac{L_{J_0(33)}(1)}{\Omega_{J_0(33)}} = \frac{\left|\frac{H^+}{\Im e}\right|}{5 \cdot c_\infty(J_0(33)) \cdot \left|\frac{\mathbf{T}e}{\Im e}\right|} \cdot \frac{3}{c_{J_0(33)}}\,. \tag{4.4}$$

Also using [Lig75, Lem. 3.2.15] we find that the order of $(0) - (\infty)$ is 10, so the only primes that can divide $|\mathbf{T}e/\Im e|$ are 2 and 5. Moreover, by an independent calculation (using the fact that $J_0(33)$ is isogenous to a product of elliptic curves), W. Stein found that

$$\frac{L_{J_0(33)}(1)}{\Omega_{J_0(33)}} = \frac{1}{2^2 5^3} \cdot \frac{3}{c_{J_0(33)}}\,, \tag{4.5}$$

which is in accord with the BSD formula (4.4).

Compare formulas (4.4) and (4.5) to what the BSD formula (4.3) predicts. Calculations of W. Stein showed that $c_3 = 2$, $c_{11} = 10$ and $2 \cdot 5 \mid |J_0(33)(\mathbf{Q})| \mid 2^3 5^2$. Now $|Ш_{J_0(33)}|$ is a square; so the only way the number 3 can appear in formulas (4.4) and (4.5) is if 3 divides $c_{J_0(33)}$. This observation actually led to an investigation of the generalized Manin constant for which results are reported in Chapter 2. In fact, as mentioned in Section 2.2.3, we find that $c_{J_0(33)} = 3$.

In view of this example, and looking back at Theorem 4.2.1, we pose the following question:

Question 4.2.3. Is $c_{J_e(pq)} = q^{\#S_p} \cdot p^{\#S_q}$?

4.2.2 Proof of Theorem 4.2.1

The proof is a generalization of the proof of Theorem 3.2.2. Let $S_e = S_2(\Gamma_0(pq), \mathbf{Z})[I_e]$. Just as in that proof, we get

$$\begin{aligned} \frac{L_{J_e}(1)}{\Omega_{J_e}} &= \frac{L_{J_e}(1)}{c_\infty(J_e) \cdot c_{J_e} \cdot \mathrm{disc}(H_1(J_e, \mathbf{Z})^+ \times S_e \to \mathbf{C})} \\ &= \frac{L_{J_e}(1)}{\mathrm{disc}(\mathbf{T}e \times S_e \to \mathbf{C})} \cdot \frac{\left|\frac{(H/\widehat{H_e})^+}{H^+/\widehat{H_e}^+}\right|}{c_\infty(J_e)} \cdot \frac{\left|\frac{H^+}{\widehat{H_e}^+ + H_e^+}\right| \cdot \left|\frac{H_e^+}{\Im e}\right|}{\left|\frac{\mathbf{T}e}{\Im e}\right|} \cdot \frac{1}{c_{J_e}}, \end{aligned} \tag{4.6}$$

where again the pairings above are obtained in a natural way from the pairing

$$\langle\ ,\ \rangle : (H_1(X_0(pq), Z)^+ \otimes \mathbf{C}) \times S_2(\Gamma_0(pq); \mathbf{C}) \to \mathbf{C}$$

given by $(\gamma, f)\langle\gamma, f\rangle = \int_\gamma 2\pi i f(z)dz$; also note that to get the statement of Lemma 3.2.3 in this situation, we use [Par99, Lem. 3.10].

We focus on the factor $\frac{L_{J_e}(1)}{\mathrm{disc}(\mathbf{T}e \times S_e \to \mathbf{C})}$ appearing above. If M is a positive integer, then let T_M denote the set of Galois orbits of newforms f of level M such that $L(f, 1) \neq 0$. If f is a newform of level M, let A_f denote the quotient of $J_0(M)$ associated to f by Shimura (as in Section 4.1.1).

We have the isogeny (see [Par99, §3.8])

$$J_e \sim \prod_{f \in T_p} A_f^2 \cdot \prod_{g \in T_q} A_g^2 \cdot \prod_{h \in T_{pq}} A_h.$$

Hence

$$\begin{aligned} L_{J_e}(1) &= \prod_{f \in T_p} L_{A_f}(1)^2 \cdot \prod_{g \in T_q} L_{A_g}(1)^2 \cdot \prod_{h \in T_{pq}} L_{A_h}(1) \\ &= \prod_{f \in S_p} \langle e, f\rangle^2 \cdot \prod_{g \in S_q} \langle e, g\rangle^2 \cdot \prod_{h \in S_{pq}} \langle e, h\rangle, \end{aligned} \tag{4.7}$$

where the second equality follows from by [Shi94, Thm. 7.14] (completed by [Car86]). Note that in the formula above we should really be taking $\langle e, f\rangle$ "at level p", but it is the same as

taking it "at level pq" by the functoriality of the (de Rham) pairing (ditto for the $\langle e, g\rangle$'s). Hence $L_{J_e}(1) \neq 0$.

Just as in Section 3.2, there is a perfect pairing $\mathbf{T}/I_e \times S_e \to \mathbf{Z}$ which associates to (T, f) the first Fourier coefficient $a_1(f \,|\, T)$ of the modular form $f \,|\, T$. This defines $t_e \in \mathbf{T}/I_e \otimes \mathbf{C}$ characterized by $\langle e, f\rangle = a_1(f \mid t_e) \ \forall f \in S_e$. By the perfectness of this pairing and the canonical isomorphism $\mathbf{T}e \cong \mathbf{T}/I_e$, the discriminant of the pairing $\mathbf{T}e \times S_e \to \mathbf{C}$ that associates to (te, f) the complex number $\langle te, f\rangle$ coincides with the discriminant of the pairing $\mathbf{T}/I_e \times \mathrm{Hom}(\mathbf{T}/I_e, \mathbf{Z}) \to \mathbf{C}$ that associates to (t, ψ) the complex number $\psi(t_e t)$ (obtained by extending ψ by $\mathbf{C}$-linearity). The latter discriminant is equal to $\det\limits_{\mathbf{T}/I_e \otimes \mathbf{C}} t_e = \det\limits_{S_e \otimes \mathbf{C}} t_e$. So we need to find the action of t_e on $S_e \otimes \mathbf{C}$. Note that a basis for $S_e \otimes \mathbf{C}$ is given by $\{h : h \in S_{pq}\} \cup \{f(z), f(qz) : f \in S_p\} \cup \{g(z), g(pz) : g \in S_q\}$. If f is a newform of some level M dividing pq, let V_f denote the space spanned by $f(z)$ and $f((pq/M)z)$. Then $S_e \otimes \mathbf{C} = \oplus_{\{h : h \in S_{pq}\}} V_h \oplus_{\{f : f \in S_p\}} V_f \oplus_{\{g : g \in S_q\}} V_g$. So we have

$$\mathrm{disc}(\mathbf{T}e \times S_e \to \mathbf{C}) = \prod_{h \in S_{pq}} \det_{V_h} t_e \cdot \prod_{f \in S_p} \det_{V_f} t_e \cdot \prod_{g \in S_q} \det_{V_g} t_e. \tag{4.8}$$

From (4.7) and (4.8), we get

$$\frac{L_{J_e}(1)}{\mathrm{disc}(\mathbf{T}e \times S_e \to \mathbf{C})} = \prod_{h \in S_{pq}} \frac{\langle e, h\rangle}{\det\limits_{V_h} t_e} \cdot \prod_{g \in S_q} \frac{\langle e, g\rangle^2}{\det\limits_{V_g} t_e} \cdot \prod_{f \in S_p} \frac{\langle e, f\rangle^2}{\det\limits_{V_f} t_e}. \tag{4.9}$$

If f' is a normalized eigenform for all the Hecke operators (including U_p and U_q), then it is easy to see that $t_e f' = \langle e, f'\rangle f'$ (look at the a_1's of both sides).

If $h \in S_{pq}$, then h is an eigenform for all the Hecke operators. So $\det\limits_{V_h} t_e = \langle e, h\rangle$. Thus if $h \in S_{pq}$, then

$$\frac{\langle e, h\rangle}{\det\limits_{V_h} t_e} = 1. \tag{4.10}$$

But if $g \in S_q$, then $g(z)$ and $g(pz)$ are eigenvectors for all the Hecke operators T_ℓ for $\ell \neq p, q$ and for U_q, but not for U_p. However U_p preserves the subspace V_g. Define $(B_p g)(z) = g(pz)$. Then on Fourier expansions (see [AL70, §3]),

$$\begin{aligned} B_p(\sum_{n \geq 1} a_n q^n) &= \sum_{n \geq 1} a_n q^{np}, \\ U_p(\sum_{n \geq 1} a_n q^n) &= \sum_{n \geq 1} a_{np} q^n, \\ \text{and} \quad T_\ell(\sum_{n \geq 1} a_n q^n) &= \sum_{n \geq 1} a_{np} q^n + \sum_{n \geq 1} a_n q^{np}. \end{aligned}$$

Since g is an eigenform for T_p with eigenvalue $a_p = a_p(g)$, from the above formulas, it is easy to see that $U_p(g) = a_p g - p \cdot B_p g$ and $U_p(B_p g) = g$. Thus the characteristic polynomial of U_p on V_g is $U_p^2 - a_p U_p + p$. By [CE98], the roots of this polynomial are distinct and so the

action of U_p is diagonalizable. If α_1 and α_2 are the eigenvalues, then an easy check shows that $g - \alpha_2 \cdot B_p g$ and $g - \alpha_1 \cdot B_p g$ are eigenvectors with eigenvalues α_1 and α_2 respectively. Thus we can use this eigenbasis to compute $\det t_e$ on V_g. Since $\langle e, B_p g\rangle = \langle e, g\rangle/p$, we get

$$\begin{aligned}\det_{V_g} t_e &= \langle e, g - \alpha_1 B_p g\rangle\langle e, g - \alpha_2 B_p g\rangle = \langle e, g\rangle^2(1 - \alpha_1/p)(1 - \alpha_2/p) \\ &= \langle e, g\rangle^2(1 - (\alpha_1 + \alpha_2)/p + \alpha_1\alpha_2/p^2) = \langle e, g\rangle^2(1 - a_p/p + p/p^2) \\ &= \langle e, g\rangle^2(1 + p - a_p)/p.\end{aligned}$$

So if $g \in S_q$, then

$$\frac{\langle e, g\rangle^2}{\det_{V_g} t_e} = \frac{p}{1 + p - a_p(g)}. \tag{4.11}$$

Similarly, we can show that if $f \in S_p$, then

$$\frac{\langle e, g\rangle^2}{\det_{V_f} t_e} = \frac{q}{1 + q - a_q(f)}. \tag{4.12}$$

Putting (4.10), (4.11), and (4.12) in (4.9), we get

$$\frac{L_{J_e}(1)}{\operatorname{disc}(\mathbf{T}e \times S_e \to \mathbf{C})} = \frac{1}{\prod_{f \in S_p}(1 + q - a_q(f)) \cdot \prod_{g \in S_q}(1 + p - a_p(g))}. \tag{4.13}$$

Finally, from Lemma 3.2.10, we get

$$c_\infty(J_e) = \left| \frac{(H/\widehat{H_e})^+}{(1 + c)(H/\widehat{H_e})} \right|.$$

Putting this and (4.13) in (4.6), we get Theorem 4.2.1.

4.3 Some other extensions

- In Sections 3.2 and 4.1.3 we proved formulas for $L_A(1)/\Omega_A$ for quotients A of the new quotient of $J_0(N)$. In Section 4.2.2, we worked out the formula for the ratio of the special L-value to the real volume for the winding quotient of level a product of two distinct primes (which is not a quotient of the new quotient of $J_0(N)$ in general). An inspection of the proofs shows that our methods will work whenever one can simultaneously diagonalize the action of the Hecke operators. By [CE98], one can do this diagonalization for any quotient of $J_0(N)$ when N is cube-free.
- W. Stein suggested that one can generalize the formula in Theorem 4.1.1 to higher weight modular forms, in which case the abelian varieties get replaced by motives. Thus it may have applications to the conjectures of Deligne, Beilinson, Bloch and Kato (e.g., see [BK90]), which are analogs of the BSD conjecture for motives.
- So far, we considered only those quotients of $J_0(N)$ whose special L-value was non-zero. There is also a BSD formula for quotients that have L-value equal to zero (given in

Conjecture 1.1.2). Our Theorem 4.1.1, together with the ideas in [MT87], suggests a way to find formulas for the left-hand side of the BSD formula in this case.

- Each term in the BSD formula for quotients of $J_0(N)$ is a Hecke module; so there might be a finer version of the formula that gives an equality of Fitting ideals (for example, this has been done for elliptic curves with complex multiplication in [Gro82]).

Chapter 5

Detecting invisible elements of the Shafarevich-Tate group

Mazur [Maz98] introduced the concept of visibility of elements of the Shafarevich-Tate group of optimal modular elliptic curves. We generalize the notion to arbitrary abelian varieties and find, based on calculations that assume the Birch and Swinnerton-Dyer conjecture, that there are elements of the Shafarevich-Tate group of certain abelian subvarieties of $J_0(p)$ and $J_1(p)$ that are not visible in $J_0(p)$ and $J_1(p)$ respectively. This chapter is basically a generalization of the results given in [Maz98] for quotients of $J_0(N)$ that are elliptic curves to quotients of arbitrary dimension. This chapter is fairly independent of the rest of the thesis, except that we refer to the short Section 3.1 for some definitions, and that Proposition 5.3.3 depends on some earlier sections.

5.1 Definitions and the result

Let J be an abelian variety and B be an abelian subvariety of J, both defined over $\mathbf{Q}$. The Galois cohomology group $H^1(\mathbf{Q}, B)$ is isomorphic to the group of principal homogeneous spaces, or torsors, of B [Lan91, III.4.2]. A B-torsor V is said to be *visible* in J if it is isomorphic over $\mathbf{Q}$ to a subvariety of J. The Tate-Shafarevich group of B, denoted $Ш_B$, consists of equivalence classes of principal homogeneous spaces of B that are locally trivial everywhere; it is conjectured to be finite. An element of the Shafarevich-Tate of B is said to be *visible* in J if the corresponding torsor is visible in J. If an element is not visible in J, we say that it is *invisible* (it will be clear from the context what the ambient abelian variety J is).

The notion of visibility arose when Mazur was looking for natural spaces where can one embed the principal homogeneous spaces of an elliptic curve (see [Maz98] for details). Adam Logan, based on Cremona's tables, studied instances of non-trivial Shafarevich-Tate groups for elliptic curves E that were quotients of $J_0(N)$ for N square-free and less than 3000. The order of the elements of the Shafarevich-Tate group of E that are visible in $J_0(N)$ divides the modular degree of E, and thus by comparing the order of the Shafarevich-Tate group (as predicted by the Birch and Swinnerton-Dyer conjecture) with the modular degrees, they

tried to detect elements that are not visible in $J_0(N)$. The only instance of an invisible element they could convincingly detect was for the level $N = 2849$, which was not visible in $J_0(N)$; but they could not test whether this element becomes visible in $J_1(N)$ or not.

As before, if A is an abelian variety, then let $\widehat{A}$ denote the dual abelian variety of A. Recall the definitions of Section 3.1. Let p be a prime and $J_e = J_e(p)$ throughout this chapter. The dual map $\widehat{J_e} \to \widehat{J_0(p)} = J_0(p)$ is an injection (e.g., by [Maz98, Prop. 9]). Thus we can view $\widehat{J_e}$ as a subvariety of $J_0(p)$ and talk about the visibility of its torsors in $J_0(p)$. We have a map $J_0(p) \stackrel{\pi^*}{\to} J_1(p)$ obtained via Picard functoriality from the map $\pi : X_1(p) \to X_0(p)$. Its kernel is finite. Let $\widehat{J_e}'$ denote the image of $\widehat{J_e}$ in $J_1(p)$ under π^*.

Based on calculations concerning the order of $Ш_{J_e}$ as predicted by the Birch and Swinnerton-Dyer conjecture, we find (Theorems 5.3.4 and 5.3.5) that, for $p = 1091$, there is an element of $Ш_{\widehat{J_e}}$ that is not visible in $J_0(p)$ and whose image in $Ш_{\widehat{J_e}'}$ is not visible in $J_1(p)$. This result was mentioned in [Aga99]. After [Maz98] and [Aga99] appeared, other instances of invisibility have been found; e.g., see [CM99] and [AS99b]. The existence of visible elements is closely related to congruences between modular forms of analytic rank zero and modular forms of analytic rank greater than zero (see [AS99b] for details).

5.2 The strategy to detect invisible elements

As in the introduction, let J be an abelian variety and B be an abelian subvariety of J, both defined over $\mathbf{Q}$. The definition of visibility that we gave is one possible extension of the definition given by Mazur. Here is another definition: we say that a B-torsor V is *visible as a torsor* in J, if there is a subvariety V' of J such that the group law of J gives an action of B on V' (both B and V' are contained in J), and there is an isomorphism of B-torsors $\iota : V \stackrel{\cong}{\longrightarrow} V'$ (i.e., an isomorphism of varieties over $\mathbf{Q}$ that respects the B-action).

In [CM99] and [AS99b], the definition used is yet another one: visible elements are defined as the the elements in the kernel of the map $Ш_B \to Ш_J$. We show that this definition is the same as the notion of visibility as a torsor.

Proposition 5.2.1. *Let J be an abelian variety and B be an abelian subvariety of J, both defined over $\mathbf{Q}$. Let V be a B-torsor. Then V is visible as a torsor in J if and only if the cocycle class corresponding to V is in the kernel of the map $H^1(\mathbf{Q}, B) \to H^1(\mathbf{Q}, J)$.*

Proof. It is convenient to use the notion of sheaf torsors (see [Mil80, § III.4]). If B is an abelian variety over $\mathbf{Q}$, let $ST(B)$ denote the equivalence classes of sheaf torsors of B. If V is a sheaf-torsor, pick $P \in V(\overline{\mathbf{Q}})$; then we get a cocycle given by $\sigma \mapsto \sigma(P) - P \in B(\overline{\mathbf{Q}})$, where $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. One can show that this gives an element of $H^1(\mathbf{Q}, B)$ that is independent of the choice of the point P above. Thus we get a canonical map $ST(B) \to H^1(\mathbf{Q}, B)$. By Theorems 1.7, 3.9, 2.10, and 4.6 in Chapter III of [Mil80], this map is an isomorphism.

If V is a B-sheaf torsor, we define the *pushout* $V \times^B J$ as the sheaf whose section over a $\mathbf{Q}$-algebra R of finite type is the set of orbits of $V(R) \times J(R)$ under the action of $B(R)$, where $B(R)$ acts on $V(R)$ in the usual way, but on $J(R)$ the action is by the inverse of the group law on $J(R)$. Also $V(R) \times J(R)$ has an action of $J(R)$ on the second component, which is compatible with the $B(R)$ action, and thus we have an action of $J(R)$ on $(V \times^B J)(R)$. Hence $V \times^B J$ is a J-torsor.

The map $H^1(\mathbf{Q}, B) \to H^1(\mathbf{Q}, J)$ induces a map $ST(B) \to ST(J)$. We first claim that the image of (the sheaf torsor corresponding to) V under this induced map is the pushout $V \times^B J$.

Proof of the claim. Pick $P \in V(\overline{\mathbf{Q}})$. Let $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. Just for this proof, we write the torsor action as composition. The cocycle in $H^1(\mathbf{Q}, B)$ corresponding to V maps σ to a_σ, where a_σ is the unique element of $B(\overline{\mathbf{Q}})$ such that $\sigma(P) = a_\sigma(P)$. Now consider the point $(P, 0)$ in $V(\overline{\mathbf{Q}}) \times J(\overline{\mathbf{Q}})$ and let Q be its image in $(V \times^B J)(\overline{\mathbf{Q}})$. Then an easy check shows that $\sigma(Q) = a_\sigma(Q)$ where, now, a_σ is considered an element of $J(\overline{\mathbf{Q}})$. So the cocycle in $H^1(\mathbf{Q}, J)$ corresponding to $V \times^B J$ maps σ to $a_\sigma \in J(\overline{\mathbf{Q}})$. But this is exactly the image of V under the map $H^1(\mathbf{Q}, B) \to H^1(\mathbf{Q}, J)$. Since σ was an arbitrary element of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, that proves the claim. □

Now we are ready to prove the Proposition. Suppose V is visible as a torsor in J. Let $\iota : V \to J$ be as in the definition of visibility as a torsor in J. Then consider the map of sheaf torsors $j : V \to V \times^B J$ induced by the map on sections $V(R) \to V(R) \times J(R)$ given by $v \mapsto (v, -\iota(v))$. If $v_1, v_2 \in V(R)$, then they are translates by an element of $B(R)$; but then $-\iota(v_1)$ and $-\iota(v_2)$ are also translates by the same element of $B(R)$. Hence the images of v_1 and v_2 under j are the same; i.e., the image of the map $V(R) \to (V \times^B J)(R)$ is a point. This point is also Galois invariant (since the map j is defined over $\mathbf{Q}$). Hence this gives us a point of $V \times^B J$ over $\mathbf{Q}$. But that makes $V \times^B J$ the trivial torsor. Hence by the claim above, the cocycle class corresponding to V in $H^1(\mathbf{Q}, B)$ maps to the trivial element of $H^1(\mathbf{Q}, J)$.

Conversely, suppose the cocycle class corresponding to V is in the kernel of the map $H^1(\mathbf{Q}, B) \to H^1(\mathbf{Q}, J)$. By the claim above, this means that there is an isomorphism $\phi : V \times^B J \xrightarrow{\cong} J$ over $\mathbf{Q}$. Now let R be any $\mathbf{Q}$-algebra of finite type and consider the map $\psi : V(R) \to (V \times^B J)(R)$ induced by the map $V(R) \to V(R) \times J(R)$ given by $v \mapsto (v, 0)$. An easy check shows that the composite $V(R) \xrightarrow{\psi} (V \times^B J)(R) \xrightarrow{\phi} J(R)$ is an injection and that the action of $B(R)$ is preserved. By Yoneda's lemma, we have a monomorphism, i.e., a closed immersion $V \to J$, and the action of B is preserved. This shows that V is visible as a torsor in J. □

If an element is visible as a torsor then it is clear that it is also visible (in the sense we defined it). We do not know if the converse is true. However we have a result which says that the converse is true up to an automorphism of B; we state it next. From now on, whenever we use the term "visible", we mean the definition we gave in Section 5.1.

Recall that J is an abelian variety and B is an abelian subvariety of J, both defined over $\mathbf{Q}$. Consider the following condition on the pair (J, B):

(∗) if $J \sim B \times C$ is an isogeny over $\overline{\mathbf{Q}}$, where C is another abelian variety, then no simple factor (over $\overline{\mathbf{Q}}$) of B is isogenous (over $\overline{\mathbf{Q}}$) to a simple factor (over $\overline{\mathbf{Q}}$) of C.

The following lemma was stated without proof in [Aga99].

Lemma 5.2.2. *Let B be an abelian subvariety of J such that the pair (J, B) satisfies (∗). Let V be a B-torsor that is visible in J; so V can be considered as an element of $H^1(\mathbf{Q}, B)$.*

Consider the natural map $\widetilde{i} : H^1(\mathbf{Q}, B) \to H^1(\mathbf{Q}, J)$ *obtained from the embedding* i *of* B *in* J*. Then there exists an automorphism* ϕ *of* B *(defined over* $\mathbf{Q}$*) such that* V *maps to* 0 *under the composite* $H^1(\mathbf{Q}, B) \xrightarrow{\widetilde{\phi}} H^1(\mathbf{Q}, B) \xrightarrow{\widetilde{i}} H^1(\mathbf{Q}, J)$*, where* $\widetilde{\phi}$ *is the automorphism of* $H^1(\mathbf{Q}, B)$ *induced by* ϕ*.*

Proof. Suppose V is a B-torsor visible in J and let V' be the subvariety of J isomorphic to V over $\mathbf{Q}$ (given by the definition of visibility). Since V is a B-torsor, we have $B \cong V \cong V'$ over $\overline{\mathbf{Q}}$. Consider the composite map $B \xrightarrow{\cong} V' \to J/B$ defined over $\overline{\mathbf{Q}}$. Up to translation, it is a homomorphism of abelian varieties. Its image has to be a point because otherwise $(*)$ would be violated. Hence the image of $V' \to J/B$ is also a point. Thus V' is a translate of B (over $\overline{\mathbf{Q}}$) and hence has an action of B by translation. In the following, let σ denote an arbitrary element of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. As a cocycle in $H^1(\mathbf{Q}, B)$, V' is given by $\sigma \mapsto \sigma(Q) - Q$, where Q is any fixed element of $V'(\overline{\mathbf{Q}})$, and the subtraction is the usual subtraction in J. But then V' maps to 0 in $H^1(\mathbf{Q}, J)$ under $\widetilde{i}$ since $Q \in V'(\overline{\mathbf{Q}}) \subseteq J(\overline{\mathbf{Q}})$. Next, let P be an element of $V(\overline{\mathbf{Q}})$. Then the element of $H^1(\mathbf{Q}, B)$ corresponding to V is the class of the cocycle $\sigma \mapsto \sigma(P) -_V P$, where we use subscripts under the group action symbol to distinguish actions of B on different torsors. Let $\iota : V \to V'$ be the isomorphism between V and V' (over $\mathbf{Q}$). Then the element of $H^1(\mathbf{Q}, B)$ corresponding to V' is given by $\sigma \mapsto \sigma(\iota(P)) -_{V'} \iota(P)$. Consider the map $\phi : B \to B$ given by $a \mapsto \iota(P +_V a) -_{V'} \iota(P)$. The map ϕ is defined over $\mathbf{Q}$ and is a homomorphism of abelian varieties since it takes the identity element of B to itself. It takes the torsor V to V' and thus $\widetilde{i}(\widetilde{\phi}(V)) = \widetilde{i}(V') = 0$. It is an automorphism since it has an inverse given by $a \mapsto \iota^{-1}(\iota(P) +_{V'} a) -_V P$. □

In [CM99], semi-stable elliptic curves were considered, and hence the only possible automorphisms of B were multiplication by ± 1 and so all the definitions of visibility coincided (see [CM99, Remark 2]).

Let J be an abelian variety that is self-dual, i.e., an abelian variety J together with an isomorphism $\widehat{J} \xrightarrow{\cong} J$, using which we implicitly identify $\widehat{J}$ with J. Let A be an optimal quotient of J such that the dual map $\widehat{A} \to J$ is injective. If $(J, \widehat{A})$ satisfy $(*)$, then the composite $\widehat{A} \to J \to A$ is an isogeny; call it f. Define n_A as the exponent of $\ker f$ (this definition is consistent with Definition 2.2.5). In this situation, the following proposition gives a way of detecting invisible elements of $Ш_{\widehat{A}}$.

Proposition 5.2.3. *Let* J *be an abelian variety that is self-dual and let* A *be an optimal quotient such that the dual map* $\widehat{A} \to J$ *is injective, and such that and* $(J, \widehat{A})$ *satisfy* $(*)$*. Then all elements of* $Ш_{\widehat{A}}$ *that are visible in* J *are killed by multiplication by* n_A*.*

Proof. Recall that f was the composite map $\widehat{A} \to J \to A$, which is an isogeny. There is an isogeny $g : A \to \widehat{A}$ such that $g \circ f =$ multiplication by n_A (e.g., see [Mil86a, §8]; we called g an isogeny conjugate to f in Definition 2.3.3). So we have maps

$$\widehat{A} \longrightarrow J \longrightarrow A \xrightarrow{g} \widehat{A}$$

such that the composite is multiplication by n_A. Suppose V is an element of $Ш_{\widehat{A}}$ that is visible in J. Apply Lemma 5.2.2 with $B = \widehat{A}$ and let ϕ be the automorphism of $\widehat{A}$ as given

by the lemma. Consider the maps

$$\widehat{A} \xrightarrow{\phi} \widehat{A} \longrightarrow J \longrightarrow A \longrightarrow \widehat{A} \xrightarrow{\phi^{-1}} \widehat{A}.$$

The composite is again multiplication by n_A. This induces maps

$$Ш_{\widehat{A}} \xrightarrow{\widetilde{\phi}} Ш_{\widehat{A}} \longrightarrow Ш_J \longrightarrow Ш_A \longrightarrow Ш_{\widehat{A}} \xrightarrow{\widetilde{\phi^{-1}}} Ш_{\widehat{A}},$$

where the composite is again multiplication by n_A. Consider V as an element of the first group $Ш_{\widehat{A}}$ in this sequence. Then by Lemma 5.2.2, its image in $Ш_J$ is trivial; hence it is killed under the composite; i.e., it is killed by multiplication by n_A. □

Thus every element of $Ш_{\widehat{A}}$ that has order prime to n_A is not visible in J. We will use this technique in the next section.

5.3 Discovery of invisible elements

We continue to use the notation of Sections 5.1 and 5.2. Let $J_0(p)'$ denote the image of $J_0(p)$ in $J_1(p)$.

Lemma 5.3.1. *Let J denote $J_0(p)$ or $J_1(p)$, and B denote an abelian subvariety of $J_0(p)$ or $J_0(p)'$ respectively. Then the pair (J, B) satisfies $(*)$.*

Proof. First the case of $J = J_0(p)$: this follows because in a decomposition of $J_0(p)$ up to isogeny, no two simple factors can be isogenous over $\mathbf{Q}$ by the multiplicity one theorem and not even over $\overline{\mathbf{Q}}$ because p is squarefree (using [Rib75, Prop. 3.1]). Next the case $J = J_1(p)$: No simple factor of B can be isogenous to another simple factor of $J_0(p)'$ (by the same argument above). Suppose B' is a simple factor of B that is isogenous to a simple factor of $J_1(p)/J_0(p)'$. Now $J_1(p)/J_0(p)'$ has everywhere good reduction over some extension of $\mathbf{Q}$ (this follows from [DR73, §5, Ex. 3.7(i)]), hence so does B'. But $J_0(p)$ has purely multiplicative reduction at p by [DR73, §5, Thm. 6.9], so it cannot have a factor with good reduction even after a base extension. This contradiction finishes the proof of the lemma. □

In what follows, $p = 1091$ and for ease of notation, we frequently denote $J_0(p)$ simply by J_0.

Proposition 5.3.2. *For $p = 1091$, the elements of $Ш_{\widehat{J_e}}$ that are visible in $J_0(p)$ are killed by multiplication by 2.*

Proof. For $p = 1091$, we have $J_e = J_0^-$, where $J_0^- = J_0/(1 + W_p)J_0$ and W_p is the Atkin-Lehner involution (this was checked by a calculation and also follows from [Bru95, §8]). By combining the quotient map $J_0 \to J_e$ and its dual map, and identifying $\widehat{J_0}$ with J_0 using the usual canonical isomorphism (e.g., see [Mil86b, Thm 6.6]), we get the maps $\widehat{J_e} \to J_0 \to J_e$; call the composite f. By [Maz98, Prop. 8], f is an isogeny; let K denote its kernel. The group K is the intersection of $\widehat{J_e}$ and $(1 + W_p)J_0$. On the former group, W_p acts as -1, and on the latter group, W_p acts as $+1$. We conclude that K is killed by multiplication by 2. The proposition now follows from Lemma 5.3.1 (with $J = J_0$ and $B = \widehat{J_e}$) and Proposition 5.2.3. □

Proposition 5.3.3. *Assume the Birch and Swinnerton-Dyer formula (Conjecture 3.2.1) for the prime $p = 1091$. Then for $p = 1091$, there is an element of order 7 in $Ш_{\widehat{J_e}}$.*

Proof. We will use notation from Sections 1.2 and 3.2. Combining the BSD formula (Conjecture 3.2.1) with Theorem 3.2.2, we get

$$|Ш_{J_e}| \cdot c_p(J_e) \cdot c_{J_e} \cdot n = |J_e(\mathbf{Q})_{\mathrm{tor}}| \cdot |\widehat{J}_e(\mathbf{Q})_{\mathrm{tor}}| \cdot \left| \frac{H^+}{\widehat{H_e}^+ + H_e^+} \right| \cdot \left| \frac{H_e^+}{\Im e} \right| \tag{5.1}$$

By a calculation (see Table 3.1) we find that, for $p = 1091$, 7 divides the factor $|H_e^+/\Im e|$ in the equation given above. Thus 7 divides the right-hand side of equation (5.1). We will check that it does not divide any factor of the left-hand side other than $|Ш_{J_e}|$.

First consider $c_p(J_e)$. We apply [BLR90, Prop. 7.5.3] to the exact sequence

$$0 \to (1 + W_p)J_0 \to J_0 \to J_0/(1 + W_p)J_0 \to 0$$

to conclude that a power of 2 kills the cokernel of the map of Néron models $\mathbf{J_0} \to \mathbf{J_e}$. Hence we have that away from 2, $c_p(J_e)$ divides the number of connected components in the special fiber at p of $\mathbf{J_0}$, which is n by [Maz77, Thm. A.1]. But in our case, $n = \mathrm{num}((1091 - 1)/12) = 545$, so 7 does not divide $c_p(J_e)$. Next, by Theorem 2.2.3, the only prime that can divide c_{J_e} is 2, so certainly 7 does not divide c_{J_e}. Finally 7 does not divide $n = 545$.

So looking at equation (5.1), one concludes that 7 divides $|Ш_{J_e}|$. Next, by the Cassels-Tate pairing, $Ш_{\widehat{J_e}}$ is finite, and $|Ш_{\widehat{J_e}}| = |Ш_{J_e}|$. Hence 7 divides $|Ш_{\widehat{J_e}}|$. Thus $Ш_{\widehat{J_e}}$ has a non-trivial element of order 7. □

Theorem 5.3.4. *Assume the Birch and Swinnerton-Dyer formula (Conjecture 1.2.1) for the prime $p = 1091$. Then for $p = 1091$, $Ш_{\widehat{J_e}}$ has an element that is not visible in $J_0(p)$.*

Proof. The element of order 7 of $Ш_{\widehat{J_e}}$ from Proposition 5.3.3 is not visible in $J_0(p)$ by Proposition 5.3.2. □

Theorem 5.3.5. *For $p = 1091$, the image of the element of order 7 of $Ш_{\widehat{J_e}}$ (from Proposition 5.3.3) in $Ш_{\widehat{J_e}'}$ is not visible in $J_1(p)$.*

Proof. Let $J_1 = J_1(p)$. Consider the series of maps

$$J_0 \xrightarrow{\pi^*} J_1 \xrightarrow{\cong} J_1 \xrightarrow{\pi_*} J_0,$$

where the map π_* is obtained from $\pi : X_1(p) \to X_0(p)$ via the Albanese functoriality. The composite is just multiplication by $\deg(\pi) = (p - 1)/2 = 545$. Let ψ denote the quotient map $J_0 \to J_e$ and let $\widehat{\psi}$ denote its dual. Then the composite

$$\widehat{J}_e \xrightarrow{\widehat{\psi}} J_0 \xrightarrow{\pi^*} J_1 \xrightarrow{\cong} J_1 \xrightarrow{\pi_*} J_0 \xrightarrow{\psi} J_e$$

is an isogeny and the only primes that can divide the order of this isogeny are the prime 2 and the primes that divide 545, i.e., 5 and 109. Hence the element of order 7 in $Ш_{\widehat{J_e}}$ does

not get killed in $Ш_{J_1}$ and so there is a nontrivial element of order 7 in $Ш_{\widehat{J_e}'}$. Call it V and suppose it is visible in J_1. Then by Lemma 5.2.2 and Lemma 5.3.1(with $J = J_1$ and $B = \widehat{J_e}'$), there is an automorphism ϕ of $\widehat{J_e}'$ such that V is killed under the composite $Ш_{\widehat{J_e'}} \xrightarrow{\widetilde{\phi}} Ш_{\widehat{J_e}'} \to Ш_{J_1}$. Now in the composite

$$\widehat{J_e} \xrightarrow{\pi^*} \widehat{J_e}' \hookrightarrow J_1 \xrightarrow{\pi_*} J_0 \xrightarrow{\psi} J_e, \tag{5.2}$$

which is an isogeny, the first map $\widehat{J_e} \xrightarrow{\pi^*} \widehat{J_e}'$ is also an isogeny. So the rest of (5.2), i.e., the composite

$$\widehat{J_e}' \hookrightarrow J_1 \xrightarrow{\pi_*} J_0 \xrightarrow{\psi} J_e$$

is also an isogeny and the only primes that can divide its degree are 2, 5 and 109. Attaching the automorphism ϕ, we find that the composite

$$\widehat{J_e}' \xrightarrow{\phi} \widehat{J_e}' \hookrightarrow J_1 \xrightarrow{\pi_*} J_0 \xrightarrow{\psi} J_e$$

is also an isogeny; call it f. The only primes that can divide the degree of f are 2, 5 and 109. There is an isogeny $g : J_e \to \widehat{J_e}'$ such that $g \circ f$ is multiplication by the degree of the isogeny f (e.g., see [Mil86a, §8]). Since V is killed under the sequence of maps $Ш_{\widehat{J_e'}} \xrightarrow{\widetilde{\phi}} Ш_{\widehat{J_e}'} \to Ш_{J_1}$, it is killed under the map induced by $g \circ f$, i.e., it is killed by multiplication by an integer that is not divisible by 7. But V has order 7 in $Ш_{\widehat{J_e}}$; this contradiction shows that V is an element of $Ш_{\widehat{J_e'}}$ that is not visible in J_1. □

A similar result of the existence of an invisible element was found for $p = 1429$, where 5 divides $|H_e^+/\Im e|$ (see Table 3.1). Note that as a byproduct, we have that the Shafarevich-Tate groups of $J_0(1091)$ and $J_1(1091)$ are non-trivial (assuming the Birch and Swinnerton-Dyer conjecture).

Question 5.3.6. Mazur [Maz99] showed that if E is an elliptic curve over $\mathbf{Q}$, then every element of $Ш_E$ of order 3 is visible in an abelian surface contained in the Jacobian of the modular curve of some (unknown) level. So the natural question is whether the element of $Ш_{J_e(1091)}$ that is not visible in $J_0(1091)$ is visible in $J_0(M)$ for some integer M that is a multiple of 1091. W. Stein found that $J_e(1091)$ shared a congruence mod 7 with an elliptic curve of level $2 \cdot 1091$ and rank 1, and using this one hopes to show that the element under consideration becomes visible in $J_0(2 \cdot 1091)$ (by generalizing work of Mazur: see [Maz98] and [AS99b]).

Bibliography

[Aga99] A. Agashe, *On invisible elements of the Tate-Shafarevich group*, C. R. Acad. Sci. Paris Sér. I Math. **328** (1999), no. 5, 369–374.

[AL70] A. O. L. Atkin and J. Lehner, *Hecke operators on* $\Gamma_0(m)$, Math. Ann. **185** (1970), 134–160.

[AS99a] A. Agashe and W. A. Stein, *The generalized Manin constant, congruence primes and the modular degree*, preprint (1999).

[AS99b] A. Agashe and W. A. Stein, *Visibility of Shafarevich-Tate groups of modular abelian varieties*, preprint (1999).

[Atk67] A. O. L. Atkin, *Weierstrass points at cusps* $\Gamma_0(n)$, Ann. of Math. (2) **85** (1967), 42–45.

[AU96] A. Abbes and E. Ullmo, *À propos de la conjecture de Manin pour les courbes elliptiques modulaires*, Compositio Math. **103** (1996), no. 3, 269–286.

[AW67] M. F. Atiyah and C. T. C. Wall, *Cohomology of groups*, Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), Thompson, Washington, D.C., 1967, pp. 94–115.

[BFH90] D. Bump, S. Friedberg, and J. Hoffstein, *Nonvanishing theorems for L-functions of modular forms and their derivatives*, Invent. Math. **102** (1990), no. 3, 543–618.

[BK90] S. Bloch and K. Kato, *L-functions and Tamagawa numbers of motives*, The Grothendieck Festschrift, Vol. I, Birkhäuser Boston, Boston, MA, 1990, pp. 333–400.

[BLR90] S. Bosch, W. Lütkebohmert, and M. Raynaud, *Néron models*, Springer-Verlag, Berlin, 1990.

[Bou66] N. Bourbaki, *Elements of mathematics. General topology. Part 1*, Hermann, Paris, 1966.

[Bru95] A. Brumer, *The rank of* $J_0(N)$, Astérisque (1995), no. 228, 3, 41–68, Columbia University Number Theory Seminar (New York, 1992).

[BSD63] B. J. Birch and H. P. F. Swinnerton-Dyer, *Notes on elliptic curves. I*, J. Reine Angew. Math. **212** (1963), 7–25.

[BSD65] B. J. Birch and H. P. F. Swinnerton-Dyer, *Notes on elliptic curves. II*, J. Reine Angew. Math. **218** (1965), 79–108.

[Car86] H. Carayol, *Sur les représentations l-adiques associées aux formes modulaires de Hilbert*, Ann. Sci. École Norm. Sup. (4) **19** (1986), no. 3, 409–468.

[Cas63] J. W. S. Cassels, *Arithmetic on an elliptic curve*, Proc. Internat. Congr. Mathematicians (Stockholm, 1962), Inst. Mittag-Leffler, Djursholm, 1963, pp. 234–246.

[CE98] R. F. Coleman and B. Edixhoven, *On the semi-simplicity of the U_p-operator on modular forms*, Math. Ann. **310** (1998), no. 1, 119–127.

[CM99] J. E. Cremona and B. Mazur, *Visualizing elements in the Shafarevich-Tate group*, to appear in Experiment. Math. (1999).

[Coh00] H. Cohen, *Advanced topics in computational number theory*, Springer-Verlag, New York, 2000.

[Cre97] J. E. Cremona, *Algorithms for modular elliptic curves*, second ed., Cambridge University Press, Cambridge, 1997.

[Dar97] H. Darmon, *Wiles' theorem and the arithmetic of elliptic curves*, Modular forms and Fermat's last theorem (Boston, MA, 1995), Springer, New York, 1997, pp. 549–569.

[DDT94] H. Darmon, F. Diamond, and R. Taylor, *Fermat's last theorem*, Current developments in mathematics, 1995 (Cambridge, MA), Internat. Press, Cambridge, MA, 1994, pp. 1–154.

[DI95] F. Diamond and J. Im, *Modular forms and modular curves*, Seminar on Fermat's Last Theorem (Toronto, ON, 1993–1994), Amer. Math. Soc., Providence, RI, 1995, pp. 39–133.

[Dia89] F. Diamond, *On congruence modules associated to λ-adic forms*, Compositio Math. **71** (1989), no. 1, 49–83.

[DR73] P. Deligne and M. Rapoport, *Les schémas de modules de courbes elliptiques*, Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972) (Berlin), Springer, 1973, pp. 143–316. Lecture Notes in Math., Vol. 349.

[Edi89] B. Edixhoven, *Stable models of modular curves and applications*, Thèse de doctorat à l'université d'Utrecht (1989), `http://www.maths.univ-rennes1.fr/~edix/publications/prschr.html`.

[Edi91] B. Edixhoven, *On the Manin constants of modular elliptic curves*, Arithmetic algebraic geometry (Texel, 1989), Birkhäuser Boston, Boston, MA, 1991, pp. 25–39.

[FM99] G. Frey and M. Müller, *Arithmetic of modular curves and applications*, Algorithmic algebra and number theory (Heidelberg, 1997), Springer, Berlin, 1999, pp. 11–48.

[FpS+99] E. V. Flynn, F. Leprévost, E. F. Schaefer, W. A. Stein, M. Stoll, and J. L. Wetherell, *Empirical evidence for the Birch and Swinnerton-Dyer conjectures for modular Jacobians of genus 2 curves*, submitted (1999).

[Gro82] B. H. Gross, *On the conjecture of Birch and Swinnerton-Dyer for elliptic curves with complex multiplication*, Number theory related to Fermat's last theorem (Cambridge, Mass., 1981), Birkhäuser Boston, Mass., 1982, pp. 219–236.

[GZ86] B. H. Gross and D. B. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), no. 2, 225–320.

[IR90] K. Ireland and M. Rosen, *A classical introduction to modern number theory*, second ed., Springer-Verlag, New York, 1990.

[KL89] V. A. Kolyvagin and D. Y. Logachev, *Finiteness of the Shafarevich-Tate group and the group of rational points for some modular abelian varieties*, Algebra i Analiz **1** (1989), no. 5, 171–196.

[KM85] N. M. Katz and B. Mazur, *Arithmetic moduli of elliptic curves*, Princeton University Press, Princeton, N.J., 1985.

[Lan56] S. Lang, *Algebraic groups over finite fields*, Amer. J. Math. **78** (1956), 555–563.

[Lan91] S. Lang, *Number theory. III*, Springer-Verlag, Berlin, 1991, Diophantine geometry.

[Lan95] S. Lang, *Introduction to modular forms*, Springer-Verlag, Berlin, 1995, With appendixes by D. Zagier and W. Feit, Corrected reprint of the 1976 original.

[Lig75] G. Ligozat, *Courbes modulaires de genre* 1, Société Mathématique de France, Paris, 1975, Bull. Soc. Math. France, Mém. 43, Supplément au Bull. Soc. Math. France Tome 103, no. 3.

[Man72] J. I. Manin, *Parabolic points and zeta functions of modular curves*, Izv. Akad. Nauk SSSR Ser. Mat. **36** (1972), 19–66.

[Maz77] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. (1977), no. 47, 33–186 (1978).

[Maz78] B. Mazur, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math. **44** (1978), no. 2, 129–162.

[Maz98] B. Mazur, *Three lectures about the arithmetic of elliptic curves.*, Handout at the Arizona Winter School (1998), `http://swc.math.arizona.edu/~swcenter/aws98/Abstracts.html`.

[Maz99] B. Mazur, *Visualizing elements of order three in the Shafarevich-Tate group*, Asian J. Math. **3** (1999), no. 1, 221–232, Sir Michael Atiyah: a great mathematician of the twentieth century.

[Mer94] L. Merel, *Universal Fourier expansions of modular forms*, On Artin's conjecture for odd 2-dimensional representations (Berlin), Springer, 1994, pp. 59–94.

[Mer96a] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Invent. Math. **124** (1996), no. 1-3, 437–449.

[Mer96b] L. Merel, *L'accouplement de Weil entre le sous-groupe de Shimura et le sous-groupe cuspidal de $J_0(p)$*, J. Reine Angew. Math. **477** (1996), 71–115.

[Mil80] J. S. Milne, *Étale cohomology*, Princeton University Press, Princeton, N.J., 1980.

[Mil86a] J. S. Milne, *Abelian varieties*, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 103–150.

[Mil86b] J. S. Milne, *Arithmetic duality theorems*, Academic Press Inc., Boston, Mass., 1986.

[Mil86c] J. S. Milne, *Jacobian varieties*, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 167–212.

[MM91] M. R. Murty and V. K. Murty, *Mean values of derivatives of modular L-series*, Ann. of Math. (2) **133** (1991), no. 3, 447–475.

[MO89] J.-F. Mestre and J. Oesterlé, *Courbes de Weil semi-stables de discriminant une puissance m-ième*, J. Reine Angew. Math. **400** (1989), 173–184.

[MT87] B. Mazur and J. Tate, *Refined conjectures of the "Birch and Swinnerton-Dyer type"*, Duke Math. J. **54** (1987), no. 2, 711–750.

[Oes] J. Oesterlé, *Torsion des courbes elliptiques sur les corps de nombres*, unpublished manuscript.

[Ogg78] A. P. Ogg, *On the Weierstrass points of $X_0(N)$*, Illinois J. Math. **22** (1978), no. 1, 31–35.

[Par99] P. Parent, *Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres*, J. Reine Angew. Math. **506** (1999), 85–116.

[Rib75] K. A. Ribet, *Endomorphisms of semi-stable abelian varieties over number fields*, Ann. Math. (2) **101** (1975), 555–562.

[Rib83] K. A. Ribet, *Mod p Hecke operators and congruences between modular forms*, Invent. Math. **71** (1983), no. 1, 193–205.

[Rib97] K. A. Ribet, *Images of semistable Galois representations*, Pacific J. Math. (1997), no. Special Issue, 277–297, Olga Taussky-Todd: in memoriam.

[Rub98] K. Rubin, *Euler systems and modular elliptic curves*, Galois representations in arithmetic algebraic geometry (Durham, 1996), Cambridge Univ. Press, Cambridge, 1998, pp. 351–367.

[SD67] H. P. F. Swinnerton-Dyer, *The conjectures of Birch and Swinnerton-Dyer, and of Tate*, Proc. Conf. Local Fields (Driebergen, 1966), Springer, Berlin, 1967, pp. 132–157.

[Shi77] G. Shimura, *On the periods of modular forms*, Math. Ann. **229** (1977), 211–221.

[Shi94] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Princeton University Press, Princeton, NJ, 1994, Reprint of the 1971 original, Kan Memorial Lectures, 1.

[Ste00] W. A. Stein, *Explicit approaches to modular abelian varieties*, U. C. Berkeley Ph.D. thesis (2000).

[Stu87] J. Sturm, *On the congruence of modular forms*, Number theory (New York, 1984–1985), Springer, Berlin, 1987, pp. 275–280.

[Tat95] J. Tate, *On the conjectures of Birch and Swinnerton-Dyer and a geometric analog*, Séminaire Bourbaki, Vol. 9, Soc. Math. France, Paris, 1995, pp. Exp. No. 306, 415–440.

[Til97] J. Tilouine, *Hecke algebras and the Gorenstein property*, Modular forms and Fermat's last theorem (Boston, MA, 1995), Springer, New York, 1997, pp. 327–342.

[Wil95] A. J. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), no. 3, 443–551.

[Zag85] D. Zagier, *Modular parametrizations of elliptic curves*, Canad. Math. Bull. **28** (1985), no. 3, 372–384.

List of Symbols

Symbol	Definition	Page
$L_A(s)$	L-function of an abelian variety	1
G^+		2
$c_\infty(A)$		2
Ω_A	real volume	2
$\widehat{A}$	dual abelian variety	2
R_A	regulator	2
$Ш_A$	Shafarevich-Tate group	2
$\mathcal{A}$	Néron model	2
$\mathcal{A}^0$		2
$c_p(A)$	order of arithmetic component group	2
$\lvert G\rvert$	order of a group	2
$\stackrel{?}{=}$	conjectured equality	2
N	level	2
$X_0(N)$	modular curve	2
$J_0(N)$	Jacobian of $X_0(N)$	2
$\mathbf{T}$	Hecke algebra	2
T_ℓ	Hecke operator	2
U_p	Hecke operator	2
$\Gamma_0(N)$	congruence subgroup	3
$S_2(\Gamma_0(N), R)$	cusp forms with coefficients in R	3
$M[I]$	I-torsion in M	3
ω_f		3
S_A		4
c_A	generalized Manin constant	4
disc	discriminant of a pairing	4
$\deg\phi_E$	modular degree	6
c_E	Manin constant	6
r_E	congruence number	6
J	Jacobian of $X_0(N)$	7
B_R	Néron model	7
$S_2(R)$	cusp forms with coefficients in R	7
c_A	generalized Manin constant	8

Symbol	Definition	Page
$M_0(N)$	coarse moduli scheme	8
$M_0(N)^0$	smooth part of $M_0(N)$	8
ϕ_A	modular parametrization	8
q-exp	q-expansion map	8
C_A		9
J^{new}	new quotient of $J_0(N)$	9
ϕ_2		9
ϕ_1		9
n_A	modular exponent	9
$\#G$	order of a group	10
m		10
S	$\text{Spec}(\mathbf{Z}[\frac{1}{m}])$	10
Ω	relative dualizing sheaf	10
q-exp	q-expansion map	10
q-exp	q-expansion map	10
C		11
$W(I)$		11
r_A	congruence number	11
m_A	congruence exponent	11
ϕ'	conjugate isogeny	12
e	winding element	15
I_e	winding ideal	15
$J_e(N)$	winding quotient	15
J_e	winding quotient of prime level p	15
H	homology group	16
$H_e = H[I_e]$		16
$\widehat{I_e}$		16
$\widehat{H_e}$		16
$\Im$	Eisenstein ideal	16
n	order of $(0) - (\infty)$	16
c	complex conjugation involution	18
S_e		19
$[x]$	Manin symbol	22
$F(x)$		23
$\sigma_1(i)$		23
r	Sturm bound	24
$\Phi_p(A)$	component group	29
$L(f,s)$	L-function of a modular form	32
I_f		32
A_f	Shimura quotient	32
$[L:M]$	lattice index	33
f_i	conjugate of f	33

Symbol	Definition	Page
Φ		33
n	order of the cuspidal subgroup	33
S_f		35
J_e	winding quotient of level pq	36
$a_m(f)$	mth Fourier coefficient of f	37
$\Im$		37
S_M		37
J	an abelian variety	42
π		43
π^*		43
$\widehat{J_e}'$		43
$(*)$		44
J_0	$J_0(p)$	46

Index