

## EMPIRICAL EVIDENCE FOR THE BIRCH AND SWINNERTON-DYER CONJECTURES FOR MODULAR JACOBIANS OF GENUS 2 CURVES

E. VICTOR FLYNN, FRANCK LEPRÉVOST, EDWARD F. SCHAEFER,  
WILLIAM A. STEIN, MICHAEL STOLL, AND JOSEPH L. WETHERELL

ABSTRACT. This paper provides empirical evidence for the Birch and Swinnerton-Dyer conjectures for modular Jacobians of genus 2 curves. The second of these conjectures relates six quantities associated to a Jacobian over the rational numbers. One of these six quantities is the size of the Shafarevich-Tate group. Unable to compute that, we computed the five other quantities and solved for the last one. In all 32 cases, the result is very close to an integer that is a power of 2. In addition, this power of 2 agrees with the size of the 2-torsion of the Shafarevich-Tate group, which we could compute.

### 1. INTRODUCTION

The conjectures of Birch and Swinnerton-Dyer, originally stated for elliptic curves over  $\mathbf{Q}$ , have been a constant source of motivation for the study of elliptic curves, with the ultimate goal being to find a proof. This has resulted not only in a better theoretical understanding, but also in the development of better algorithms for computing the analytic and arithmetic invariants that are so intriguingly related by them. We now know<sup>1</sup> that the first and, up to a nonzero rational factor, the second conjectures hold for modular elliptic curves over  $\mathbf{Q}$  in the analytic rank 0 and 1 cases (see [GZ, Ko, Wal1, Wal2]). Furthermore, a number of people have provided numerical evidence for the conjectures for a large number of elliptic curves; see for example [BGZ, BSD, Ca, Cr2].

---

Received by the editor August 16, 1999.

2000 *Mathematics Subject Classification*. Primary 11G40; Secondary 11G10, 11G30, 14H25, 14H40, 14H45.

*Key words and phrases*. Birch and Swinnerton-Dyer conjecture, genus 2, Jacobian, modular abelian variety.

The first author thanks the Nuffield Foundation (Grant SCI/180/96/71/G) for financial support.

The second author did some of the research at the Max-Planck Institut für Mathematik and the Technische Universität Berlin.

The third author thanks the National Security Agency (Grant MDA904-99-1-0013).

The fourth author was supported by a Sarah M. Hallam fellowship.

The fifth author did some of the research at the Max-Planck-Institut für Mathematik.

The sixth author thanks the National Science Foundation (Grant DMS-9705959). The authors had useful conversations with John Cremona, Qing Liu, Karl Rubin and Peter Swinnerton-Dyer. The authors are grateful to Xiangdong Wang and Michael Müller for making data available to them and to the referee for helpful suggestions.

<sup>1</sup>It has recently been announced by Breuil, Conrad, Diamond and Taylor that they have extended Wiles' results and shown that all elliptic curves over  $\mathbf{Q}$  are modular (see [BCDT]).

By now, our theoretical and algorithmic knowledge of curves of genus 2 and their Jacobians has reached a state that makes it possible to conduct similar investigations. The Birch and Swinnerton-Dyer conjectures have been generalized to arbitrary abelian varieties over number fields by Tate [Ta]. If  $J$  is the Jacobian of a genus 2 curve over  $\mathbf{Q}$ , then the first conjecture states that the order of vanishing of the  $L$ -series of the Jacobian at  $s = 1$  (the *analytic rank*) is equal to the Mordell-Weil rank of the Jacobian. The second conjecture is that

$$(1.1) \quad \lim_{s \rightarrow 1} (s-1)^{-r} L(J, s) = \Omega \cdot \text{Reg} \cdot \prod_p c_p \cdot \#\text{III}(J, \mathbf{Q}) \cdot (\#J(\mathbf{Q})_{\text{tors}})^{-2}.$$

In this equation,  $L(J, s)$  is the  $L$ -series of the Jacobian  $J$ , and  $r$  is its analytic rank. We use  $\Omega$  to denote the integral over  $J(\mathbf{R})$  of a particular differential 2-form; the precise choice of this differential is described in Section 3.5.  $\text{Reg}$  is the regulator of  $J(\mathbf{Q})$ . For primes  $p$ , we use  $c_p$  to denote the size of  $J(\mathbf{Q}_p)/J^0(\mathbf{Q}_p)$ , where  $J^0(\mathbf{Q}_p)$  is defined in Section 3.4. We let  $\text{III}(J, \mathbf{Q})$  be the Shafarevich-Tate group of  $J$  over  $\mathbf{Q}$ , and we let  $J(\mathbf{Q})_{\text{tors}}$  denote the torsion subgroup of  $J(\mathbf{Q})$ .

As in the case of elliptic curves, the first conjecture assumes that the  $L$ -series can be analytically continued to  $s = 1$ , and the second conjecture additionally assumes that the Shafarevich-Tate group is finite. Neither of these assumptions is known to hold for arbitrary genus 2 curves. The analytic continuation of the  $L$ -series, however, is known to exist for modular abelian varieties over  $\mathbf{Q}$ , where an abelian variety is called *modular* if it is a quotient of the Jacobian  $J_0(N)$  of the modular curve  $X_0(N)$  for some level  $N$ . For simplicity, we will also call a genus 2 curve *modular* when its Jacobian is modular in this sense. So it is certainly a good idea to look at modular genus 2 curves over  $\mathbf{Q}$ , since we then at least know that the statement of the first conjecture makes sense. Moreover, for many modular abelian varieties it is also known that the Shafarevich-Tate group is finite; therefore the statement of the second conjecture also makes sense. As it turns out, all of our examples belong to this class. An additional benefit of choosing modular genus 2 curves is that one can find lists of such curves in the literature.

In this article, we provide empirical evidence for the Birch and Swinnerton-Dyer conjectures for such modular genus 2 curves. Since there is no known effective way of computing the size of the Shafarevich-Tate group, we computed the other five terms in equation (1.1) (in two different ways, if possible). This required several different algorithms, some of which were developed or improved while we were working on this paper. If one of these algorithms is already well described in the literature, then we simply cite it. Otherwise, we describe it here in some detail (in particular, algorithms for computing  $\Omega$  and  $c_p$ ).

For modular abelian varieties associated to newforms whose  $L$ -series have analytic rank 0 or 1, the first Birch and Swinnerton-Dyer conjecture has been proven. In such cases, the Shafarevich-Tate group is also known to be finite and the second conjecture has been proven, up to a nonzero rational factor. This all follows from results in [GZ, KL, Wal1, Wal2]. In our examples, all of the analytic ranks are either 0 or 1. Thus we already know that the first conjecture holds. Since the Jacobians we consider are associated to a quadratic conjugate pair of newforms, the analytic rank of the Jacobian is twice the analytic rank of either newform (see [GZ]).

The second Birch and Swinnerton-Dyer conjecture has not been proven for the cases we consider. In order to verify equation (1.1), we computed the five terms

other than  $\#\text{III}(J, \mathbf{Q})$  and solved for  $\#\text{III}(J, \mathbf{Q})$ . In each case, the value is an integer to within the accuracy of our calculations. This number is a power of 2, which coincides with the independently computed size of the 2-torsion subgroup of  $\text{III}(J, \mathbf{Q})$ . Hence, we have verified the second Birch and Swinnerton-Dyer conjecture for our curves at least numerically, if we assume that the Shafarevich-Tate group consists of 2-torsion only. (This is an ad hoc assumption based only on the fact that we do not know better.) See Section 6 for circumstances under which the verification is exact.

The curves are listed in Table 1, and the numerical results can be found in Table 2.

## 2. THE CURVES

Each of the genus 2 curves we consider is related to the Jacobian  $J_0(N)$  of the modular curve  $X_0(N)$  for some level  $N$ . When only one of these genus 2 curves arises from a given level  $N$ , then we denote this curve by  $C_N$ ; when there are two curves coming from level  $N$ , we use the notation  $C_{N,A}$ ,  $C_{N,B}$ . The relationship of, say,  $C_N$  to  $J_0(N)$  depends on the source. Briefly, from Hasegawa [Hs] we obtain quotients of  $X_0(N)$  and from Wang [Wan] we obtain curves whose Jacobians are quotients of  $J_0(N)$ . In both cases the Jacobian  $J_N$  of  $C_N$  is isogenous to a 2-dimensional factor of  $J_0(N)$ . (When not referring to a specific curve, we will typically drop the subscript  $N$  from  $J$ .) In this way we can also associate  $C_N$  with a 2-dimensional subspace of  $S_2(N)$ , the space of cusp forms of weight 2 for  $\Gamma_0(N)$ .

We now discuss the precise source of the genus 2 curves we will consider. Hasegawa [Hs] has provided exact equations for all genus 2 curves which are quotients of  $X_0(N)$  by a subgroup of the Atkin-Lehner involutions. There are 142 such curves. We are particularly interested in those where the Jacobian corresponds to a subspace of  $S_2(N)$  spanned by a quadratic conjugate pair of newforms. There are 21 of these with level  $N \leq 200$ . For these curves we will provide evidence for the second conjecture. There are seven more such curves with  $N > 200$ . We can classify the other 2-dimensional subspaces into four types. There are 2-dimensional subspaces of oldforms that are irreducible under the action of the Hecke algebra. There are also 2-dimensional subspaces that are reducible under the action of the Hecke algebra and are spanned by two oldforms, two newforms or one of each. The Jacobians corresponding to the latter three kinds are always isogenous, over  $\mathbf{Q}$ , to the product of two elliptic curves. Given the small levels, these are elliptic curves for which Cremona [Cr2] has already provided evidence for the Birch and Swinnerton-Dyer conjectures. In Table 5, we describe the kind of cusp forms spanning the 2-dimensional subspace and the signs of their functional equations from the level at which they are newforms. The analytic and Mordell-Weil ranks were always the smallest possible given those signs.

The second set of curves was created by Wang [Wan] and is further discussed in [FM]. This set consists of 28 curves that were constructed by considering the spaces  $S_2(N)$  with  $N \leq 200$ . Whenever a subspace spanned by a pair of quadratic conjugate newforms was found, these newforms were integrated to produce a quotient abelian variety  $A$  of  $J_0(N)$ . These quotients are *optimal* in the sense of [Ma], in that the kernel of the quotient map is connected.

The period matrix for  $A$  was created using certain intersection numbers. When all of the intersection numbers have the same value, then the polarization on  $A$

induced from the canonical polarization of  $J_0(N)$  is equivalent to a principal polarization. (Two polarizations are *equivalent* if they differ by an integer multiple.) Conversely, every 2-dimensional optimal quotient of  $J_0(N)$  in which the induced polarization is equivalent to a principal polarization is found in this way.

Using theta functions, numerical approximations were found for the Igusa invariants of the abelian surfaces. These numbers coincide with rational numbers of fairly small height within the limits of the precision used for the computations. Wang then constructed curves defined over  $\mathbf{Q}$  whose Igusa invariants are the rational numbers found. (There is one abelian surface at level  $N = 177$  for which Wang was not able to find a curve.) If we assume that these rational numbers are the true Igusa invariants of the abelian surfaces, then it follows that Wang's curves have Jacobians isomorphic, over  $\overline{\mathbf{Q}}$ , to the principally polarized abelian surfaces in his list. Since the classification given by these invariants is only up to isomorphism over  $\overline{\mathbf{Q}}$ , the Jacobians of Wang's curves are not necessarily isomorphic to, but can be twists of, the optimal quotients of  $J_0(N)$  over  $\mathbf{Q}$  (see below).

There are four curves in Hasegawa's list which do not show up in Wang's list (they are listed in Table 1 with an  $H$  in the last column). Their Jacobians are quotients of  $J_0(N)$ , but are not optimal quotients. It is likely that there are modular genus 2 curves which neither are Atkin-Lehner quotients of  $X_0(N)$  (in Hasegawa's sense) nor have Jacobians that are optimal quotients. These curves could be found by looking at the optimal quotient abelian surfaces and checking whether they are isogenous to a principally polarized abelian surface over  $\mathbf{Q}$ .

For 17 of the curves in Wang's list, the 2-dimensional subspace spanned by the newforms is the same as that giving one of Hasegawa's curves. In all of those cases, the curve given by Wang's equation is isomorphic, over  $\mathbf{Q}$ , to that given by Hasegawa. This verifies Wang's equations for these 17 curves. They are listed in Table 1 with  $HW$  in the last column.

The remaining eleven curves (listed in Table 1 with a  $W$  in the last column) derive from the other eleven optimal quotients in Wang's list. These are described in more detail in Section 2.1 below.

With the exception of curves  $C_{63}$ ,  $C_{117,A}$  and  $C_{189}$ , the Jacobians of all of our curves are absolutely simple, and the canonically polarized Jacobians have automorphism groups of size two. We showed that these Jacobians are absolutely simple using an argument like those in [Le, Sto1]. The automorphism group of the canonically polarized Jacobian of a hyperelliptic curve is isomorphic to the automorphism group of the curve (see [Mi2, Theorem 12.1]). Each automorphism of a hyperelliptic curve induces a linear fractional transformation on  $x$ -coordinates (see [CF, p. 1]). Each automorphism also permutes the six Weierstrass points. Once we believed we had found all of the automorphisms, we were able to show that there are no more by considering all linear fractional transformations sending three fixed Weierstrass points to any three Weierstrass points. In each case, we worked with sufficient accuracy to show that other linear fractional transformations did not permute the Weierstrass points.

Let  $\zeta_3$  denote a primitive third root of unity. The Jacobians of curves  $C_{63}$ ,  $C_{117,A}$  and  $C_{189}$  are each isogenous to the product of two elliptic curves over  $\mathbf{Q}(\zeta_3)$ , though not over  $\mathbf{Q}$ , where they are simple. These genus 2 curves have automorphism groups of size 12. In the following table we list the curve at the left. On the right we give one of the elliptic curves which is a factor of its Jacobian. The second factor is the

conjugate.

$$\begin{aligned} C_{63} : & \quad y^2 = x(x^2 + (9 - 12\zeta_3)x - 48\zeta_3) \\ C_{117,A} : & \quad y^2 = x(x^2 - (12 + 27\zeta_3)x - (48 + 48\zeta_3)) \\ C_{189} : & \quad y^2 = x^3 + (66 - 3\zeta_3)x^2 + (342 + 81\zeta_3)x + 105 + 21\zeta_3 \end{aligned}$$

Note that these three Jacobians are examples of abelian varieties ‘with extra twist’ as discussed in [Cr1], where they can be found in the tables on page 409.

**2.1. Models for the Wang-only curves.** As we have already noted, a modular genus 2 curve may be found by either, both, or neither of Wang’s and Hasegawa’s techniques. Hasegawa’s method allows for the exact determination, over  $\mathbf{Q}$ , of the equation of any modular genus 2 curve it has found. On the other hand, if Wang’s technique detects a modular genus 2 curve  $C_N$ , his method produces real approximations to a curve  $C'_N$  which is defined over  $\mathbf{Q}$  and is isomorphic to  $C_N$  over  $\overline{\mathbf{Q}}$ . We will call  $C'_N$  a *twisted modular genus 2 curve*.

In this section we attempt to determine equations for the eleven modular genus 2 curves detected by Wang but not by Hasegawa. If we assume that Wang’s equations for the twisted modular genus 2 curves are correct, we find that we are able to determine the twists. In turn, this gives us strong evidence that Wang’s equations for the twisted curves were correct. Undoing the twist, we determine probable equations for the modular genus 2 curves. We end by providing further evidence for the correctness of these equations.

In what follows, we will use the notation of [Cr2] and recommend it as a reference on the general results that we assume here and in Section 4 and the appendix. Fix a level  $N$  and let  $f(z) \in S_2(N)$ . Then  $f$  has a Fourier expansion

$$f(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z} .$$

For a newform  $f$ , we have  $a_1 \neq 0$ ; so we can normalize it by setting  $a_1 = 1$ . In our cases, the  $a_n$ ’s are integers in a real quadratic field. For each prime  $p$  not dividing  $N$ , the corresponding Euler factor of the  $L$ -series  $L(f, s)$  is  $1 - a_p p^{-s} + p^{1-2s}$ . Let  $N(a_p)$  and  $Tr(a_p)$  denote the norm and trace of  $a_p$ . The product of this Euler factor and its conjugate is  $1 - Tr(a_p) p^{-s} + (N(a_p) + 2p) p^{-2s} - p Tr(a_p) p^{-3s} + p^2 p^{-4s}$ . Therefore, the characteristic polynomial of the  $p$ -Frobenius on the corresponding abelian variety over  $\mathbf{F}_p$  is  $x^4 - Tr(a_p) x^3 + (N(a_p) + 2p) x^2 - p Tr(a_p) x + p^2$ . Let  $C$  be a curve, over  $\mathbf{Q}$ , whose Jacobian, over  $\mathbf{Q}$ , comes from the space spanned by  $f$  and its conjugate. Then we know that  $p + 1 - \#C(\mathbf{F}_p) = Tr(a_p)$  and  $\frac{1}{2}(\#C(\mathbf{F}_p)^2 + \#C(\mathbf{F}_{p^2})) - (p + 1)\#C(\mathbf{F}_p) - p = N(a_p)$  (see [MS, Lemma 3]). For the odd primes less than 200, not dividing  $N$ , we computed  $\#C(\mathbf{F}_p)$  and  $\#C(\mathbf{F}_{p^2})$  for each curve given by one of Wang’s equations. From these we could compute the characteristic polynomials of Frobenius and see if they agreed with those predicted by the  $a_p$ ’s of the newforms.

Of the eleven curves, the characteristic polynomials agreed for only four. In each of the remaining seven cases we found a twist of Wang’s curve whose characteristic polynomials agreed with those predicted by the newform for all odd primes less than 200 not dividing  $N$ . Four of these twists were quadratic and three were of higher degree. It is these twists that appear in Table 1.

We can provide further evidence that these equations are correct. For each curve given in Table 1, it is easy to determine the primes of singular reduction. In

Section 3.4 we will provide techniques for determining which of those primes divides the conductor of its Jacobian. In each case, the primes dividing the conductor of the Jacobian of the curve are exactly the primes dividing the level  $N$ ; this is necessary. With the exception of curve  $C_{188}$ , all the curves come from odd levels. We used Liu's `genus2reduction` program (<ftp://megrez.math.u-bordeaux.fr/pub/liu>) to compute the conductor of the curve. In each case (other than curve  $C_{188}$ ), the conductor is the square of the level; this is also necessary. For curve  $C_{188}$ , the odd part of the conductor of the curve is the square of the odd part of the level.

In addition, since the Jacobians of the Wang curves are optimal quotients, we can compute  $k \cdot \Omega$  (where  $k$  is the Manin constant, conjectured to be 1) using the newforms. In each case, these agree (to within the accuracy of our computations) with the  $\Omega$ 's computed using the equations for the curves. We can also compute the value of  $c_p$  for optimal quotients from the newforms, when  $p$  exactly divides  $N$  and the eigenvalue of the  $p$ th Atkin-Lehner involution is  $-1$ . When  $p$  exactly divides  $N$  and the eigenvalue of the  $p$ th Atkin-Lehner involution is  $+1$ , the component group is either  $0$ ,  $\mathbf{Z}/2\mathbf{Z}$ , or  $(\mathbf{Z}/2\mathbf{Z})^2$ . These results are always in agreement with the values computed using the equations for the curves. The algorithms based on the newforms are described in Section 4; those based on the equations of the curves are described in Section 3.

Lastly, we were able to compute the Mordell-Weil ranks of the Jacobians of the curves given by ten of these eleven equations. In each case it agrees with the analytic rank of the Jacobian, as deduced from the newforms.

It should be noted that curve  $C_{125,B}$  is the  $\sqrt{5}$ -twist of curve  $C_{125,A}$ ; the corresponding statement holds for the associated 2-dimensional subspaces of  $S_2(125)$ . Since curve  $C_{125,A}$  is a Hasegawa curve, this proves that the equation given in Table 1 for curve  $C_{125,B}$  is correct.

The  $a_p$ 's and other information concerning Wang's curves are currently kept in a database at the Institut für experimentelle Mathematik in Essen, Germany. Most recently, this database was under the care of Michael Müller. William Stein also keeps a database of  $a_p$ 's for newforms.

*Remark 2.1.* For the remainder of this paper we will assume that the equations for the curves given in Table 1 are correct, that is, that they are equations for the curves whose Jacobians are isogenous to a factor of  $J_0(N)$  in the way described above. Some of the quantities can be computed either from the newform or from the equation for the curve. We performed both computations whenever possible and view this duplicate effort as an attempt to verify our implementation of the algorithms rather than an attempt to verify the equations in Table 1. For most quantities, one method or the other is not guaranteed to produce a value; in this case, we simply quote the value from whichever method did succeed. The reader who is disturbed by this philosophy should ignore the Wang-only curves, since the equations for the Hasegawa curves can be proven to be correct.

### 3. ALGORITHMS FOR GENUS 2 CURVES

In this section, we describe the algorithms that are based on the given models for the curves. We give algorithms that compute all terms on the right-hand side of equation (1.1), with the exception of the size of the Shafarevich-Tate group. We describe, however, how to find the size of its 2-torsion subgroup. Note that these algorithms are for general genus 2 curves and do not depend on modularity.

**3.1. Torsion subgroup.** The computation of the torsion subgroup of  $J(\mathbf{Q})$  is straightforward. We used the technique described in [CF, pp. 78–82]. This technique is not always effective, however. For an algorithm working in all cases see [Sto3].

**3.2. Mordell-Weil rank and  $\text{III}(J, \mathbf{Q})[2]$ .** The group  $J(\mathbf{Q})$  is a finitely generated abelian group and so is isomorphic to  $\mathbf{Z}^r \oplus J(\mathbf{Q})_{\text{tors}}$  for some  $r$  called the Mordell-Weil rank. As noted above (see Section 1), we justifiably use  $r$  to denote both the analytic and Mordell-Weil ranks since they agree for all curves in Table 1.

We used the algorithm described in [FPS] to compute  $\text{Sel}_{\text{fake}}^2(J, \mathbf{Q})$  (notation from [PSc]), which is a quotient of the 2-Selmer group  $\text{Sel}^2(J, \mathbf{Q})$ . More details on this algorithm can be found in [Sto2]. Theorem 13.2 of [PSc] explains how to get  $\text{Sel}^2(J, \mathbf{Q})$  from  $\text{Sel}_{\text{fake}}^2(J, \mathbf{Q})$ . Let  $M[2]$  denote the 2-torsion of an abelian group  $M$  and let  $\dim V$  denote the dimension of an  $\mathbf{F}_2$  vector space  $V$ . We have  $\dim \text{Sel}^2(J, \mathbf{Q}) = r + \dim J(\mathbf{Q})[2] + \dim \text{III}(J, \mathbf{Q})[2]$ . In other words,

$$\dim \text{III}(J, \mathbf{Q})[2] = \dim \text{Sel}^2(J, \mathbf{Q}) - r - \dim J(\mathbf{Q})[2].$$

In all 30 cases where  $\dim \text{III}(J, \mathbf{Q})[2] \leq 1$ , we were able to compute the Mordell-Weil rank independently from the analytic rank. The cases where  $\dim \text{III}(J, \mathbf{Q})[2] = 1$  are discussed in more detail in Section 6. For both of the remaining cases we have  $\dim \text{III}(J, \mathbf{Q})[2] = 2$ . One of these cases is  $C_{125,B}$ . For this curve we computed  $\text{Sel}^{\sqrt{5}}(J_{125,B}, \mathbf{Q})$  using the technique described in [Sc]. From this, we were able to determine that the Mordell-Weil rank is 0 independently from the analytic rank. For the other case,  $C_{133,A}$ , we could show that  $r$  had to be either 0 or 2 from the equation, but we needed the analytic computation to show that  $r = 0$ .

**3.3. Regulator.** When the Mordell-Weil rank is 0, then the regulator is 1. When the Mordell-Weil rank is positive, then to compute the regulator, we first need to find generators for  $J(\mathbf{Q})/J(\mathbf{Q})_{\text{tors}}$ . The regulator is the determinant of the canonical height pairing matrix on this set of generators. An algorithm for computing the generators and canonical heights is given in [FS]; it was used to find generators for  $J(\mathbf{Q})/J(\mathbf{Q})_{\text{tors}}$  and to compute the regulators. In that article, the algorithm for computing height constants at the infinite prime is not clearly explained and there are some errors in the examples. A clear algorithm for computing infinite height constants is given in [Sto3]. In [Sto4], some improvements of the results and algorithms in [FS] and [Sto3] are discussed. The regulators in Table 2 have been double-checked using these improved algorithms.

**3.4. Tamagawa numbers.** Let  $\mathcal{O}$  be the integer ring in  $K$  which will be  $\mathbf{Q}_p$  or  $\mathbf{Q}_p^{\text{unr}}$  (the maximal unramified extension of  $\mathbf{Q}_p$ ). Let  $\mathcal{J}$  be the Néron model of  $J$  over  $\mathcal{O}$ . Define  $\mathcal{J}^0$  to be the open subgroup scheme of  $\mathcal{J}$  whose generic fiber is isomorphic to  $J$  over  $K$  and whose special fiber is the identity component of the closed fiber of  $\mathcal{J}$ . The group  $\mathcal{J}^0(\mathcal{O})$  is isomorphic to a subgroup of  $J(K)$  which we denote  $J^0(K)$ . The group  $J(\mathbf{Q}_p^{\text{unr}})/J^0(\mathbf{Q}_p^{\text{unr}})$  is the component group of  $\mathcal{J}$  over  $\mathcal{O}_{\mathbf{Q}_p^{\text{unr}}}$ . We are interested in computing  $c_p = \#J(\mathbf{Q}_p)/J^0(\mathbf{Q}_p)$ , which is sometimes called the Tamagawa number. Since Néron models are stable under unramified base extension, the  $\text{Gal}(\mathbf{Q}_p^{\text{unr}}/\mathbf{Q}_p)$ -invariant subgroup of  $J^0(\mathbf{Q}_p^{\text{unr}})$  is  $J^0(\mathbf{Q}_p)$ . Since  $H^1(\text{Gal}(\mathbf{Q}_p^{\text{unr}}/\mathbf{Q}_p), J^0(\mathbf{Q}_p^{\text{unr}}))$  is trivial (see [Mi1, p. 58]) we see that the  $\text{Gal}(\mathbf{Q}_p^{\text{unr}}/\mathbf{Q}_p)$ -invariant subgroup of  $J(\mathbf{Q}_p^{\text{unr}})/J^0(\mathbf{Q}_p^{\text{unr}})$  is  $J(\mathbf{Q}_p)/J^0(\mathbf{Q}_p)$ .

There exist several discussions in the literature on constructing the group  $J(\mathbf{Q}_p^{\text{unr}})/J^0(\mathbf{Q}_p^{\text{unr}})$  starting with an integral model of the underlying curve. For our purposes, we especially recommend Silverman's book [Si], Chapter IV, Sections 4 and 7. For a more detailed treatment, see [BLR, Chapter 9] and [Ed2, §2]. One can find justifications for what we will do in these sources. While constructing such groups, we ran into a number of difficulties that we did not find described anywhere. For that reason, we will present examples of such difficulties that arose, as well as our methods of resolution. We do not claim that we will describe all situations that could arise.

When computing  $c_p$  we need a proper, regular model  $\mathcal{C}$  for  $C$  over  $\mathbf{Z}_p$ . Let  $\mathbf{Z}_p^{\text{unr}}$  denote the ring of integers of  $\mathbf{Q}_p^{\text{unr}}$  and note that  $\mathbf{Z}_p^{\text{unr}}$  is a pro-étale Galois extension of  $\mathbf{Z}_p$  with Galois group  $\text{Gal}(\mathbf{Z}_p^{\text{unr}}/\mathbf{Z}_p) = \text{Gal}(\mathbf{Q}_p^{\text{unr}}/\mathbf{Q}_p)$ . It follows that giving a model for  $C$  over  $\mathbf{Z}_p$  is equivalent to giving a model for  $C$  over  $\mathbf{Z}_p^{\text{unr}}$  that is equipped with a Galois action. We have found it convenient to always work with the latter description. Thus for us, giving a model over  $\mathbf{Z}_p$  will always mean giving a model over  $\mathbf{Z}_p^{\text{unr}}$  together with a Galois action.

In order to find a proper, regular model for  $C$  over  $\mathbf{Z}_p$ , we start with the models in Table 1. Technically, we consider the curves to be the two affine pieces  $y^2 + g(x)y = f(x)$  and  $v^2 + u^3g(1/u)v = u^6f(1/u)$ , glued together by  $ux = 1$ ,  $v = u^3y$ . We blow them up at all points that are not regular until we have a regular model. (A point is *regular* if the cotangent space there has two generators.) These curves are all proper, and this is not affected by blowing up.

Let  $\mathcal{C}_p$  denote the special fiber of  $\mathcal{C}$  over  $\mathbf{Z}_p^{\text{unr}}$ . The group  $J(\mathbf{Q}_p^{\text{unr}})/J^0(\mathbf{Q}_p^{\text{unr}})$  is isomorphic to a quotient of the degree 0 part of the free group on the irreducible components of  $\mathcal{C}_p$ . Let the irreducible components be denoted  $\mathcal{D}_i$  for  $1 \leq i \leq n$ , and let the multiplicity of  $\mathcal{D}_i$  in  $\mathcal{C}_p$  be  $d_i$ . Then the degree 0 part of the free group has the form

$$L = \left\{ \sum_{i=1}^n \alpha_i \mathcal{D}_i \mid \sum_{i=1}^n d_i \alpha_i = 0 \right\}.$$

In order to describe the group that we quotient out by, we must discuss the intersection pairing. For components  $\mathcal{D}_i$  and  $\mathcal{D}_j$  of the special fiber, let  $\mathcal{D}_i \cdot \mathcal{D}_j$  denote their intersection pairing. In all of the special fibers that arise in our examples, distinct components intersect transversally. Thus, if  $i \neq j$ , then  $\mathcal{D}_i \cdot \mathcal{D}_j$  equals the number of points at which  $\mathcal{D}_i$  and  $\mathcal{D}_j$  intersect. The case of self-intersection ( $i = j$ ) is discussed below.

The kernel of the map from  $L$  to  $J(\mathbf{Q}_p^{\text{unr}})/J^0(\mathbf{Q}_p^{\text{unr}})$  is generated by divisors of the form

$$[\mathcal{D}_j] = \sum_{i=1}^n (\mathcal{D}_j \cdot \mathcal{D}_i) \mathcal{D}_i$$

for each component  $\mathcal{D}_j$ . We can deduce  $\mathcal{D}_j \cdot \mathcal{D}_j$  by noting that  $[\mathcal{D}_j]$  must be contained in the group  $L$ . This follows from the fact that the intersection pairing of  $\mathcal{C}_p = \sum d_i \mathcal{D}_i$  with any irreducible component is 0.

**Example 1.** Curve  $C_{65,B}$  over  $\mathbf{Z}_2$ .

The Jacobian of  $C_{65,B}$  is a quotient of the Jacobian of  $X_0(65)$ . Since 65 is odd,  $J_0(65)$  has good reduction at 2; however,  $C_{65,B}$  has singular reduction at 2. Since the equation for this curve is conjectural (it is a Wang-only curve), it will be nice to

verify that 2 does not divide the conductor of its Jacobian, i.e., that the Jacobian has good reduction at 2. In addition, we will need a proper, regular model for this curve in order to find  $\Omega$ .

We start with the arithmetic surface over  $\mathbf{Z}_2^{\text{unr}}$  given by the two pieces  $y^2 = f(x) = -x^6 + 10x^5 - 32x^4 + 20x^3 + 40x^2 + 6x - 1$  and  $v^2 = u^6 f(1/u)$ . (Here and in the following we will not specify the gluing maps.) This arithmetic surface is regular at  $u = 0$  so we focus our attention on the first affine piece. The special fiber of  $y^2 = f(x)$  over  $\mathbf{Z}_2^{\text{unr}}$  is given by  $(y + x^3 + 1)^2 = 0 \pmod{2}$ ; this is a genus 0 curve of multiplicity 2 that we denote  $A$ . This model is not regular at the two points  $(x - \alpha, y, 2)$ , where  $\alpha$  is a root of  $x^2 - 3x - 1$ . The current special fiber is in Figure 1 and is labelled *Fiber 1*.

We fix  $\alpha$  and move  $(x - \alpha, y, 2)$  to the origin using the substitution  $x_0 = x - \alpha$ . We get

$$y^2 = -x_0^6 + (-6\alpha + 10)x_0^5 + (5\alpha - 47)x_0^4 + (-28\alpha + 60)x_0^3 + (-11\alpha - 2)x_0^2 + (-24\alpha - 16)x_0$$

which we rewrite as the pair of equations

$$\begin{aligned} g_1(x_0, y, p) &= -x_0^6 + (-3\alpha + 5)px_0^5 + (5\alpha - 47)x_0^4 + (-7\alpha + 15)p^2x_0^3 \\ &\quad + (-11\alpha - 2)x_0^2 + (-3\alpha - 2)p^3x_0 - y^2 \\ &= 0, \\ p &= 2. \end{aligned}$$

To blow up at  $(x_0, y, p)$ , we introduce projective coordinates  $(x_1, y_1, p_1)$  with  $x_0y_1 = x_1y$ ,  $x_0p_1 = x_1p$ , and  $yp_1 = y_1p$ . We look in three affine pieces that cover the blow-up of  $g_1(x_0, y, p) = 0$ ,  $p = 2$  and check for regularity.

$x_1 = 1$ : We have  $y = x_0y_1$ ,  $p = x_0p_1$ . We get  $g_2(x_0, y_1, p_1) = 0$ ,  $x_0p_1 = 2$ , where

$$\begin{aligned} g_2(x_0, y_1, p_1) &= x_0^{-2}g_1(x_0, x_0y_1, x_0p_1) \\ &= -x_0^4 + (-3\alpha + 5)p_1x_0^4 + (5\alpha - 47)x_0^2 + (-7\alpha + 15)p_1^2x_0^3 \\ &\quad + (-11\alpha - 2) + (-3\alpha - 2)p_1^3x_0^2 - y_1^2. \end{aligned}$$

In the reduction we have either  $x_0 = 0$  or  $p_1 = 0$ .

$x_0 = 0$ :  $(y_1 + \alpha + 1)^2 = 0$ . This is a new component which we denote  $B$ . It has genus 0 and multiplicity 2. We check regularity along  $B$  at  $(x_0, y_1 + \alpha + 1, p_1 - t, 2)$ , with  $t$  in  $\mathbf{Z}_2^{\text{unr}}$ , and find that  $B$  is nowhere regular.

$p_1 = 0$ :  $(y_1 + x_0^2 + \alpha x_0 + (\alpha + 1))^2 = 0$ . Using the gluing maps, we see that this is  $A$ .

$y_1 = 1$ : We get no new information from this affine piece.

$p_1 = 1$ : We have  $x_0 = x_1p$ ,  $y = y_1p$ . We get  $g_3(x_1, y_1, p) = p^{-2}g_1(x_1p, y_1p, p) = 0$ ,  $p = 2$ . In the reduction we have

$p = 0$ :  $(y_1 + (\alpha + 1)x_1)^2 = 0$ . Using the gluing maps, we see that this is  $B$ . It is nowhere regular.

The current special fiber is in Figure 1 and is labelled *Fiber 2*. It is not regular along  $B$  and at the other point on  $A$  which we have not yet blown up. The component  $B$  does not lie entirely in any one affine piece so we will blow up the affine pieces  $x_1 = 1$  and  $p_1 = 1$  along  $B$ .

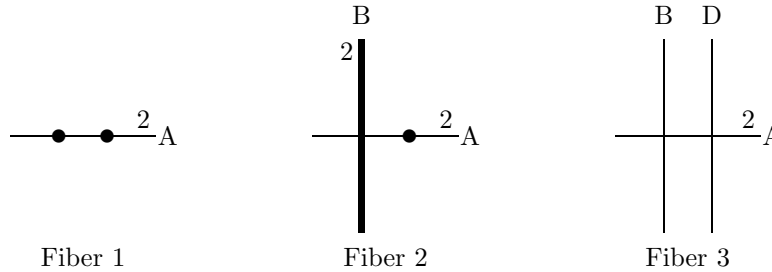


FIGURE 1. Special fibers of curve  $C_{65,B}$  over  $\mathbf{Z}_2$ ; points not regular are thick

To blow up  $x_1 = 1$  along  $B$  we make the substitution  $y_2 = y_1 + \alpha + 1$  and replace each factor of 2 in a coefficient by  $x_0p_1$ . We have  $g_4(x_0, y_2, p_1) = 0$  and  $x_0p_1 = 2$ , and we want to blow up along the line  $(x_0, y_2, 2)$ . Blowing up along a line is similar to blowing up at a point: since we are blowing up at  $(x_0, y_2, 2) = (x_0, y_2)$ , we introduce projective coordinates  $x_3, y_3$  together with the relation  $x_0y_3 = x_3y_2$ . We consider two affine pieces that cover the blow-up of  $x_1 = 1$ .

- $x_3 = 1$ : We have  $y_2 = y_3x_0$ . We get  $g_5(x_0, y_3, p_1) = x_0^{-2}g_4(x_0, y_3x_0, p_1) = 0$  and  $x_0p_1 = 2$ . In the reduction we have
- $x_0 = 0$ :  $y_3^2 + (\alpha + 1)y_3p_1 + \alpha p_1^3 + p_1^2 + \alpha + 1 = 0$ . This is  $B$ . It is now a nonsingular genus 1 curve.
- $p_1 = 0$ :  $(x_0 + y_3 + \alpha)^2 = 0$ . This is  $A$ . The point where  $B$  meets  $A$  transversally is regular.
- $y_3 = 1$ : We get no new information from this affine piece.

When we blow up  $p_1 = 1$  along  $B$ , we get essentially the same thing and all points are again regular.

The other nonregular point on  $A$  is the conjugate of the one we blew up. Therefore, after performing the conjugate blow ups, it too will be a genus 1 component crossing  $A$  transversally. We denote this component  $D$ ; it is conjugate to  $B$ .

We now have a proper, regular model  $\mathcal{C}$  of  $C$  over  $\mathbf{Z}_2$ . Let  $\mathcal{C}_2$  be the special fiber of this model; a diagram of  $\mathcal{C}_2$  is in Figure 1 and is labelled *Fiber 3*. We can use  $\mathcal{C}$  to show that the Néron model  $\mathcal{J}$  of the Jacobian  $J = J_{65,B}$  has good reduction at 2.

We know that the reduction of  $\mathcal{J}^0$  is the extension of an abelian variety by a connected linear group. Since  $\mathcal{C}$  is regular and proper, the abelian variety part of the reduction is the product of the Jacobians of the normalizations of the components of  $\mathcal{C}_2$  (see [BLR, 9.3/11 and 9.5/4]). Thus, the abelian variety part is the product of the Jacobians of  $B$  and  $D$ . Since this is 2-dimensional, the reduction of  $\mathcal{J}^0$  is an abelian variety. In other words, since the sum of the genera of the components of the special fiber is equal to the dimension of  $J$ , the reduction is an abelian variety. It follows that  $\mathcal{J}$  has good reduction at 2, that the conductor of  $J$  is odd, and that  $c_2 = 1$ . As noted above, this gives further evidence that the equation given in Table 1 is correct.

**Example 2.** Curve  $C_{63}$  over  $\mathbf{Z}_3$ .

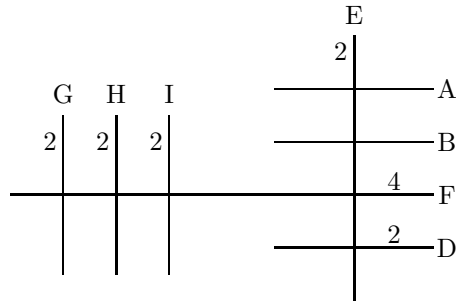


FIGURE 2. Special fiber of curve  $C_{63}$  over  $\mathbf{Z}_3$

The Tamagawa number is often found using the intersection matrix and sub-determinants. This is not entirely satisfactory for cases where the special fiber has several components and a nontrivial Galois action. Here is an example of how to resolve this (see also [BL]).

When we blow up curve  $C_{63}$  over  $\mathbf{Z}_3^{\text{unr}}$ , we get the special fiber shown in Figure 2. Elements of  $\text{Gal}(\mathbf{Q}_3^{\text{unr}}/\mathbf{Q}_3)$  that do not fix the quadratic unramified extension of  $\mathbf{Q}_3$  switch  $H$  and  $I$ . The other components are defined over  $\mathbf{Q}_3$ . All components have genus 0. The group  $J(\mathbf{Q}_3^{\text{unr}})/J^0(\mathbf{Q}_3^{\text{unr}})$  is isomorphic to a quotient of

$$L = \{ \alpha A + \beta B + \delta D + \epsilon E + \phi F + \gamma G + \eta H + \iota I \mid \alpha + \beta + 2\delta + 2\epsilon + 4\phi + 2\gamma + 2\eta + 2\iota = 0 \}.$$

The kernel is generated by the following divisors.

$$\begin{aligned} [A] &= -2A + E & [B] &= -2B + E \\ [D] &= -D + E & [E] &= A + B + D - 4E + F \\ [F] &= E - 2F + G + H + I & [G] &= F - 2G \\ [H] &= F - 2H & [I] &= F - 2I \end{aligned}$$

When we project away from  $A$ , we find that  $J(\mathbf{Q}_3^{\text{unr}})/J^0(\mathbf{Q}_3^{\text{unr}})$  is isomorphic to

$$\langle B, D, E, F, G, H, I \mid E = 0, E = 2B, D = E, 4E = B + D + F, 2F = E + G + H + I, F = 2G = 2H = 2I \rangle.$$

At this point, it is straightforward to simplify the representation by elimination. Note that we projected away from  $A$ , which is Galois-invariant. It is best to continue eliminating Galois-invariant elements first. We find that this group is isomorphic to  $\langle H, I \mid 2H = 2I = 0 \rangle$  and elements of  $\text{Gal}(\mathbf{Q}_3^{\text{unr}}/\mathbf{Q}_3)$  that do not fix the quadratic unramified extension of  $\mathbf{Q}_3$  switch  $H$  and  $I$ . Therefore

$$J(\mathbf{Q}_3^{\text{unr}})/J^0(\mathbf{Q}_3^{\text{unr}}) \cong \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z} \quad \text{and} \quad c_3 = \#J(\mathbf{Q}_3)/J^0(\mathbf{Q}_3) = 2.$$

**3.5. Computing  $\Omega$ .** By an *integral differential* (or *integral form*) on  $J$  we mean the pullback to  $J$  of a global relative differential form on the Néron model of  $J$  over  $\mathbf{Z}$ . The set of integral  $n$ -forms on  $J$  is a full-rank lattice in the  $\mathbf{Q}$ -vector space of global holomorphic  $n$ -forms on  $J$ . Since  $J$  is an abelian variety of dimension 2, the integral 1-forms are a free  $\mathbf{Z}$ -module of rank 2 and the integral 2-forms are a free  $\mathbf{Z}$ -module of rank 1. Moreover, the wedge of a basis for the integral 1-forms is

a generator for the integral 2-forms. The quantity  $\Omega$  is the integral, over the real points of  $J$ , of a generator for the integral 2-forms. (We choose the generator that leads to a positive integral.)

We now translate this into a computation on the curve  $C$ . Let  $\{\omega_1, \omega_2\}$  be a  $\mathbf{Q}$ -basis for the holomorphic differentials on  $C$  and let  $\{\gamma_1, \gamma_2, \gamma_3, \gamma_4\}$  be a  $\mathbf{Z}$ -basis for the homology of  $C(\mathbf{C})$ . Create a  $2 \times 4$  complex matrix  $M_{\mathbf{C}} = [\int_{\gamma_j} \omega_i]$  by integrating the differentials over the homology and let  $M_{\mathbf{R}} = \text{Tr}_{\mathbf{C}/\mathbf{R}}(M_{\mathbf{C}})$  be the  $2 \times 4$  real matrix whose entries are traces from the complex matrix. The columns of  $M_{\mathbf{R}}$  generate a lattice  $\Lambda$  in  $\mathbf{R}^2$ . If we make the standard identification between the holomorphic 1-forms on  $J$  and the holomorphic differentials on  $C$  (see [Mi2]), then the notation  $\int_{J(\mathbf{R})} |\omega_1 \wedge \omega_2|$  makes sense and its value can be computed as the area of a fundamental domain for  $\Lambda$ .

If  $\{\omega_1, \omega_2\}$  is a basis for the integral 1-forms on  $J$ , then  $\int_{J(\mathbf{R})} |\omega_1 \wedge \omega_2| = \Omega$ . On the other hand, the computation of  $M_{\mathbf{C}}$  is simplest if we choose  $\omega_1 = dX/Y$ , and  $\omega_2 = X dX/Y$  with respect to a model for  $C$  of the form  $Y^2 = F(X)$ ; in this case we obtain  $\Omega$  by a simple change-of-basis calculation. This assumes, of course, that we know how to express a basis for the integral 1-forms in terms of the basis  $\{\omega_1, \omega_2\}$ ; this is addressed in more detail below.

It is worth mentioning an alternate strategy. Instead of finding a  $\mathbf{Z}$ -basis for the homology of  $C(\mathbf{C})$  one could find a  $\mathbf{Z}$ -basis  $\{\gamma'_1, \gamma'_2\}$  for the subgroup of the homology that is fixed by complex conjugation (call this the real homology). Integrating would give us a  $2 \times 2$  real matrix  $M'_{\mathbf{R}}$  and the determinant of  $M'_{\mathbf{R}}$  would equal the integral of  $\omega_1 \wedge \omega_2$  over the connected component of  $J(\mathbf{R})$ . In other words, the number of real connected components of  $J$  is equal to the index of the  $\mathbf{C}/\mathbf{R}$ -traces in the real homology.

We now come to the question of determining the differentials on  $C$  which correspond to the integral 1-forms on  $J$ . Call these the integral differentials on  $C$ . This computation can be done one prime at a time. At each prime  $p$  this is equivalent to determining a  $\mathbf{Z}_p^{\text{unr}}$ -basis for the global relative differentials on any proper, regular model for  $C$  over  $\mathbf{Z}_p^{\text{unr}}$ . In fact a more general class of models can be used; see the discussion of models with rational singularities in [BLR, §6.7] and [Li, §4.1].

We start with the model  $y^2 + g(x)y = f(x)$  given in Table 1. Note that the substitution  $X = x$  and  $Y = 2y + g(x)$  gives us a model of the form  $Y^2 = F(X)$ . For integration purposes, our preferred differentials are  $dX/Y = dx/(2y + g(x))$  and  $X dX/Y = x dx/(2y + g(x))$ . It is not hard to show that at primes of non-singular reduction for the  $y^2 + g(x)y = f(x)$  model, these differentials will generate the integral 1-forms. For each prime  $p$  of singular reduction we give the following algorithm. All steps take place over  $\mathbf{Z}_p^{\text{unr}}$ .

- Step 1:** Compute explicit equations for a proper, regular model  $\mathcal{C}$ .
- Step 2:** Diagram the configuration of the special fiber of  $\mathcal{C}$ .
- Step 3:** (Optional) Identify exceptional components and blow them down in the configuration diagram. Repeat step 3 as necessary.
- Step 4:** (Optional) Remove components with genus 0 and self-intersection  $-2$ . Since  $C$  has genus greater than 1, there will be a component that is not of this kind.

(This step corresponds to contracting the given components. The model obtained would no longer be regular; it would, however, be a proper model

with rational singularities. We will not need a diagram of the resulting configuration.)

**Step 5:** Determine a  $\mathbf{Z}_p^{\text{unr}}$ -basis for the integral differentials. It suffices to check this on a dense open subset of each surviving component. Note that we have explicit equations for a dense open subset of each of these components from the model  $\mathcal{C}$  in step 1. A pair of differentials  $\{\eta_1, \eta_2\}$  will be a basis for the integral differentials (at  $p$ ) if the following three statements are true.

- a:** The pair  $\{\eta_1, \eta_2\}$  is a basis for the holomorphic differentials on  $C$ .
- b:** The reductions of  $\eta_1$  and  $\eta_2$  produce well-defined differentials mod  $p$  on an open subset of each surviving component.
- c:** If  $a_1\eta_1 + a_2\eta_2 = 0 \pmod{p}$  on all surviving components, then  $p|a_1$  and  $p|a_2$ .

Techniques for explicitly computing a proper, regular model are discussed in Section 3.4. A configuration diagram should include the genus, multiplicity and self-intersection number of each component and the number and type of intersections between components. Note that when an exceptional component is blown down, all of the self-intersection numbers of the components intersecting it will go up (towards 0). In particular, components which were not exceptional before may become exceptional in the new configuration.

Steps 3 and 4 are intended to make this algorithm more efficient for a human. They are entirely optional. For a computer implementation it may be easier to simply check every component than to worry about manipulating configurations.

The curves in Table 1 are given as  $y^2 + g(x)y = f(x)$ . We assumed, at first, that  $dx/(2y + g(x))$  and  $x dx/(2y + g(x))$  generate the integral differentials. We integrated these differentials around each of the four paths generating the complex homology and found a provisional  $\Omega$ . Then we checked the proper, regular models to determine if these differentials really do generate the integral differentials and adjusted  $\Omega$  when necessary. There were three curves where we needed to adjust  $\Omega$ . We describe the adjustment for curve  $C_{65,B}$  in the following example. For curve  $C_{63}$ , we used the differentials  $3 dx/(2y + g(x))$  and  $x dx/(2y + g(x))$ . For curve  $C_{65,A}$ , we used the differentials  $3 dx/(2y + g(x))$  and  $3x dx/(2y + g(x))$ .

**Example 3.** Curve  $C_{65,B}$ .

The primes of singular reduction for curve  $C_{65,B}$  are 2, 5 and 13. In Example 1 of Section 3.4, we found a proper, regular model  $\mathcal{C}$  for  $C$  over  $\mathbf{Z}_2^{\text{unr}}$ . The configuration for the special fiber of  $\mathcal{C}$  is sketched in Figure 1 under the label *Fiber 3*. Component  $A$  is exceptional and can be blown down to produce a model in which  $B$  and  $D$  cross transversally. Since  $B$  and  $D$  both have genus 1, we cannot eliminate either of these components. Furthermore, it suffices to check  $B$ , since  $D$  is its Galois conjugate.

To get from the equation of the curve listed in Table 1 to an affine containing an open subset of  $B$  we need to make the substitutions  $x = x_0 + \alpha$  and  $y = x_0(y_3x_0 - \alpha - 1)$ . We also have  $x_0p_1 = 2$ . Using the substitutions and the relation  $dx_0/x_0 = -dp_1/p_1$ , we get

$$\frac{dx}{2y} = \frac{-dp_1}{2p_1(y_3x_0 - \alpha - 1)} \quad \text{and} \quad \frac{x dx}{2y} = \frac{-(x_0 + \alpha) dp_1}{2p_1(y_3x_0 - \alpha - 1)}.$$

Note that  $p_1 - t$  is a uniformizer at  $p_1 = t$  almost everywhere on  $B$ . When we multiply each differential by 2, then the denominator of each is almost everywhere

nonzero; thus,  $dx/y$  and  $x dx/y$  are integral at 2. Moreover, although the linear combination  $(x - \alpha) dx/y$  is identically zero on  $B$ , it is not identically zero on  $D$  (its Galois conjugate is not identically zero on  $B$ ). Thus, our new basis is correct at 2. We multiply the provisional  $\Omega$  by 4 to get a new provisional  $\Omega$  which is correct at 2.

Similar (but somewhat simpler) computations at the primes 5 and 13 show that no adjustment is needed at these primes. Thus,  $dx/y$  and  $x dx/y$  form a basis for the integral differentials of curve  $C_{65,B}$ , and the correct value of  $\Omega$  is 4 times our original guess.

#### 4. MODULAR ALGORITHMS

In this section, we describe the algorithms that were used to compute some of the data from the newforms. This includes the analytic rank and leading coefficient of the  $L$ -series. For optimal quotients, the value of  $k \cdot \Omega$  can also be found ( $k$  is the Manin constant), as well as partial information on the Tamagawa numbers  $c_p$  and the size of the torsion subgroup.

**4.1. Analytic rank of  $L(J, s)$  and leading coefficient at  $s = 1$ .** Fix a Jacobian  $J$  corresponding to the 2-dimensional subspace of  $S_2(N)$  spanned by quadratic conjugate, normalized newforms  $f$  and  $\bar{f}$ . Let  $W_N$  be the Fricke involution. The newforms  $f$  and  $\bar{f}$  have the same eigenvalue  $\epsilon_N$  with respect to  $W_N$ , namely  $+1$  or  $-1$ . In the notation of Section 2, let

$$L(f, s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

be the  $L$ -series of  $f$ ; then  $L(\bar{f}, s)$  is the Dirichlet series whose coefficients are the conjugates of the coefficients of  $L(f, s)$ . (Recall that the  $a_n$  are integers in some real quadratic field.) The order of  $L(f, s)$  at  $s = 1$  is even when  $\epsilon_N = -1$  and odd when  $\epsilon_N = +1$ . We have  $L(J, s) = L(f, s)L(\bar{f}, s)$ . Thus the analytic rank of  $J$  is 0 modulo 4 when  $\epsilon_N = -1$  and 2 modulo 4 when  $\epsilon_N = +1$ . We found that the ranks were all 0 or 2. To prove that the analytic rank of  $J$  is 0, we need to show  $L(f, 1) \neq 0$  and  $L(\bar{f}, 1) \neq 0$ . In the case that  $\epsilon_N = +1$ , to prove that the analytic rank is 2, we need to show that  $L'(f, 1) \neq 0$  and  $L'(\bar{f}, 1) \neq 0$ . When  $\epsilon_N = -1$ , we can evaluate  $L(f, 1)$  as in [Cr2, §2.11]. When  $\epsilon_N = +1$ , we can evaluate  $L'(f, 1)$  as in [Cr2, §2.13]. Each appropriate  $L(f, 1)$  or  $L'(f, 1)$  was at least 0.1 and the errors in our approximations were all less than  $10^{-67}$ . In this way we determined the analytic ranks, which we denote  $r$ . As noted in the introduction, the analytic rank equals the Mordell-Weil rank if  $r = 0$  or  $r = 2$ . Thus, we can simply call  $r$  the rank, without fear of ambiguity.

To compute the leading coefficient of  $L(J, s)$  at  $s = 1$ , we note that

$$\lim_{s \rightarrow 1} L(J, s)/(s-1)^r = L^{(r)}(J, 1)/r!.$$

In the  $r = 0$  case, we simply have  $L(J, 1) = L(f, 1)L(\bar{f}, 1)$ . In the  $r = 2$  case, we have  $L''(J, s) = L''(f, s)L(\bar{f}, s) + 2L'(f, s)L'(\bar{f}, s) + L(f, s)L''(\bar{f}, s)$ . Evaluating both sides at  $s = 1$  we get  $\frac{1}{2}L''(J, 1) = L'(f, 1)L'(\bar{f}, 1)$ .

**4.2. Computing  $k \cdot \Omega$ .** Let  $J$ ,  $f$  and  $\bar{f}$  be as in Section 4.1 and assume  $J$  is an optimal quotient. Let  $V$  be the 2-dimensional space spanned by  $f$  and  $\bar{f}$ . Choose a basis  $\{\omega_1, \omega_2\}$  for the subgroup of  $V$  consisting of forms whose  $q$ -expansion coefficients lie in  $\mathbf{Z}$ . Let  $k \cdot \Omega$  be the volume of the real points of the quotient of  $\mathbf{C} \times \mathbf{C}$  by the lattice of period integrals  $(\int_\gamma \omega_1, \int_\gamma \omega_2)$  with  $\gamma$  in the integral homology  $H_1(X_0(N), \mathbf{Z})$ . The rational number  $k$  is called the *Manin constant*. In practice we compute  $k \cdot \Omega$  using modular symbols and a generalization to dimension 2 of the algorithm for computing periods described in [Cr2, §2.10]. When  $L(J, 1) \neq 0$ , the method of [Cr2, §2.11] coupled with Sections 4.1 and 4.3 can also be used to compute  $k \cdot \Omega$ .

A slight generalization of the argument of Proposition 2 of [Ed1] proves that  $k$  is, in fact, an integer. This generalization can be found in [AS2], where one also finds a conjecture that  $k$  must equal 1 for all optimal quotients of Jacobians of modular curves, which generalizes the longstanding conjecture of Manin that  $k$  equals 1 for all optimal elliptic curves. In unpublished work, Edixhoven has partially proven Manin’s conjecture.

The computations of the present paper verify that  $k$  equals 1 for the optimal quotients that we are considering. Specifically, we computed  $k \cdot \Omega$  as above and  $\Omega$  as described in Section 3.5. The quotient of the two values was always well within 0.5 of 1.

**4.3. Computing  $L(J, 1)/(k \cdot \Omega)$ .** We compute the rational number  $L(J, 1)/(k \cdot \Omega)$ , for optimal quotients, using the algorithm in [AS1]. This algorithm generalizes the algorithm described in [Cr2, §2.8] to dimension greater than 1.

**4.4. Tamagawa numbers.** In this section we assume that  $p$  is a prime which exactly divides the conductor  $N$  of  $J$ . Under these conditions, Grothendieck [Gr] gave a description of the component group of  $J$  in terms of a monodromy pairing on certain character groups. (For more details, see Ribet [Ri, §2].) If, in addition,  $J$  is a new optimal quotient of  $J_0(N)$ , one deduces the following. When the eigenvalue for  $f$  of the Atkin-Lehner involution  $W_p$  is  $+1$ , then the rational component group of  $J$  is a subgroup of  $(\mathbf{Z}/2\mathbf{Z})^2$ . Furthermore, when the eigenvalue of  $W_p$  is  $-1$ , the algorithm described in [KS] can be used to compute the value of  $c_p$ .

**4.5. Torsion subgroup.** To compute an integer divisible by the order of the torsion subgroup of  $J$  we make use of the following two observations. First, it is a consequence of the Eichler-Shimura relation [Sh, §7.9] that if  $p$  is a prime not dividing the conductor  $N$  of  $J$  and  $f(T)$  is the characteristic polynomial of the endomorphism  $T_p$  of  $J$ , then  $\#J(\mathbf{F}_p) = f(p+1)$  (see [Cr2, §2.4] for an algorithm to compute  $f(T)$ ). Second, if  $p$  is an odd prime at which  $J$  has good reduction, then the natural map

$$J(\mathbf{Q})_{\text{tors}} \rightarrow J(\mathbf{F}_p)$$

is injective (see [CF, p. 70]). This does not depend on whether  $J$  is an optimal quotient. To obtain a lower bound on the torsion subgroup for optimal quotients, we use modular symbols and the Abel-Jacobi theorem [La, IV.2] to compute the order of the image of the rational point  $(0) - (\infty) \in J_0(N)$ .

## 5. TABLES

In Table 1, we list the 32 curves described in Section 2. We give the level  $N$  from which each curve arose, an integral model for the curve, and list the source(s) from which it came ( $H$  for Hasegawa [Ha],  $W$  for Wang [Wan]). Throughout the paper, the curves are denoted  $C_N$  (or  $C_{N,A}$ ,  $C_{N,B}$ ).

TABLE 1. Levels, integral models and sources for curves

$N$	Equation	Source
23	$y^2 + (x^3 + x + 1)y = -2x^5 - 3x^2 + 2x - 2$	HW
29	$y^2 + (x^3 + 1)y = -x^5 - 3x^4 + 2x^2 + 2x - 2$	HW
31	$y^2 + (x^3 + x^2 + 1)y = -x^5 - 5x^4 - 5x^3 + 3x^2 + 2x - 3$	HW
35	$y^2 + (x^3 + x)y = -x^5 - 8x^3 - 7x^2 - 16x - 19$	H
39	$y^2 + (x^3 + 1)y = -5x^4 - 2x^3 + 16x^2 - 12x + 2$	H
63	$y^2 + (x^3 - 1)y = 14x^3 - 7$	W
65,A	$y^2 + (x^3 + 1)y = -4x^6 + 9x^4 + 7x^3 + 18x^2 - 10$	W
65,B	$y^2 = -x^6 + 10x^5 - 32x^4 + 20x^3 + 40x^2 + 6x - 1$	W
67	$y^2 + (x^3 + x + 1)y = x^5 - x$	HW
73	$y^2 + (x^3 + x^2 + 1)y = -x^5 - 2x^3 + x$	HW
85	$y^2 + (x^3 + x^2 + x)y = x^4 + x^3 + 3x^2 - 2x + 1$	H
87	$y^2 + (x^3 + x + 1)y = -x^4 + x^3 - 3x^2 + x - 1$	HW
93	$y^2 + (x^3 + x^2 + 1)y = -2x^5 + x^4 + x^3$	HW
103	$y^2 + (x^3 + x^2 + 1)y = x^5 + x^4$	HW
107	$y^2 + (x^3 + x^2 + 1)y = x^4 - x^2 - x - 1$	HW
115	$y^2 + (x^3 + x + 1)y = 2x^3 + x^2 + x$	HW
117,A	$y^2 + (x^3 - 1)y = 3x^3 - 7$	W
117,B	$y^2 + (x^3 + 1)y = -x^6 - 3x^4 - 5x^3 - 12x^2 - 9x - 7$	W
125,A	$y^2 + (x^3 + x + 1)y = x^5 + 2x^4 + 2x^3 + x^2 - x - 1$	HW
125,B	$y^2 + (x^3 + x + 1)y = x^6 + 5x^5 + 12x^4 + 12x^3 + 6x^2 - 3x - 4$	W
133,A	$y^2 + (x^3 + x + 1)y = -2x^6 + 7x^5 - 2x^4 - 19x^3 + 2x^2 + 18x + 7$	W
133,B	$y^2 + (x^3 + x^2 + 1)y = -x^5 + x^4 - 2x^3 + 2x^2 - 2x$	HW
135	$y^2 + (x^3 + x + 1)y = x^4 - 3x^3 + 2x^2 - 8x - 3$	W
147	$y^2 + (x^3 + x^2 + x)y = x^5 + 2x^4 + x^3 + x^2 + 1$	HW
161	$y^2 + (x^3 + x + 1)y = x^3 + 4x^2 + 4x + 1$	HW
165	$y^2 + (x^3 + x^2 + x)y = x^5 + 2x^4 + 3x^3 + x^2 - 3x$	H
167	$y^2 + (x^3 + x + 1)y = -x^5 - x^3 - x^2 - 1$	HW
175	$y^2 + (x^3 + x^2 + 1)y = -x^5 - x^4 - 2x^3 - 4x^2 - 2x - 1$	W
177	$y^2 + (x^3 + x^2 + 1)y = x^5 + x^4 + x^3$	HW
188	$y^2 = x^5 - x^4 + x^3 + x^2 - 2x + 1$	W
189	$y^2 + (x^3 - 1)y = x^3 - 7$	W
191	$y^2 + (x^3 + x + 1)y = -x^3 + x^2 + x$	HW

TABLE 2. Conjectured sizes of  $\text{III}(J, \mathbf{Q})$

$N$	$r$	$\lim_{s \rightarrow 1} \frac{L(J, s)}{(s-1)^r}$	$\Omega$	Reg	$c_p$ 's	$\Phi$	III?	error
23	0	0.24843	2.7328	1	11	11	1	
29	0	0.29152	2.0407	1	7	7	1	
31	0	0.44929	2.2464	1	5	5	1	
35	0	0.37275	2.9820	1	16,2	16	1	$< 10^{-25}$
39	0	0.38204	10.697	1	28,1	28	1	$< 10^{-25}$
63	0	0.75328	4.5197	1	2,3	6	1	
65,A	0	0.45207	6.3289	1	7,1	14	2	
65,B	0	0.91225	5.4735	1	1,3	6	2	
67	2	0.23410	20.465	0.011439	1	1	1	$< 10^{-50}$
73	2	0.25812	24.093	0.010713	1	1	1	$< 10^{-49}$
85	2	0.34334	9.1728	0.018715	4,2	2	1	$< 10^{-26}$
87	0	1.4323	7.1617	1	5,1	5	1	
93	2	0.33996	18.142	0.0046847	4,1	1	1	$< 10^{-49}$
103	2	0.37585	16.855	0.022299	1	1	1	$< 10^{-49}$
107	2	0.53438	11.883	0.044970	1	1	1	$< 10^{-49}$
115	2	0.41693	10.678	0.0097618	4,1	1	1	$< 10^{-50}$
117,A	0	1.0985	3.2954	1	4,3	6	1	
117,B	0	1.9510	1.9510	1	4,1	2	1	
125,A	2	0.62996	13.026	0.048361	1	1	1	$< 10^{-50}$
125,B	0	2.0842	2.6052	1	5	5	4	
133,A	0	2.2265	2.7832	1	5,1	5	4	
133,B	2	0.43884	15.318	0.028648	1,1	1	1	$< 10^{-49}$
135	0	1.5110	4.5331	1	3,1	3	1	
147	2	0.61816	13.616	0.045400	2,2	2	1	$< 10^{-50}$
161	2	0.82364	11.871	0.017345	4,1	1	1	$< 10^{-47}$
165	2	0.68650	9.5431	0.071936	4,2,2	4	1	$< 10^{-26}$
167	2	0.91530	7.3327	0.12482	1	1	1	$< 10^{-47}$
175	0	0.97209	4.8605	1	1,5	5	1	
177	2	0.90451	13.742	0.065821	1,1	1	1	$< 10^{-45}$
188	2	1.1708	11.519	0.011293	9,1	1	1	$< 10^{-44}$
189	0	1.2982	3.8946	1	1,3	3	1	
191	2	0.95958	17.357	0.055286	1	1	1	$< 10^{-44}$

In Table 2, we list the curve  $C_N$  simply by  $N$ , the level from which it arose. Let  $r$  denote the rank. We list

$$\lim_{s \rightarrow 1} (s - 1)^{-r} L(J, s),$$

where  $L(J, s)$  is the  $L$ -series for the Jacobian  $J$  of  $C_N$  and round off the results to five digits. The symbol  $\Omega$  was defined in Section 3.5 and is also rounded to five digits. Let Reg denote the regulator, also rounded to five digits. We list the  $c_p$ 's

TABLE 3. Generators of  $J(\mathbf{Q})/J(\mathbf{Q})_{\text{tors}}$  in rank 2 cases

$N$	Generators of $J(\mathbf{Q})/J(\mathbf{Q})_{\text{tors}}$	
67	$[(0, 0) - \infty_{-1}]$	$[(0, 0) - (0, -1)]$
73	$[(0, -1) - \infty_{-1}]$	$[(0, 0) - \infty_{-1}]$
85	$[(1, 1) - \infty_{-1}]$	$[(-1, 3) - \infty_0]$
93	$[(-1, 1) - \infty_0]$	$[(1, -3) - (-1, -2)]$
103	$[(0, 0) - \infty_{-1}]$	$[(0, -1) - (0, 0)]$
107	$[\infty_{-1} - \infty_0]$	$[(-1, -1) - \infty_{-1}]$
115	$[(1, -4) - \infty_0]$	$[(1, 1) - (-2, 2)]$
125,A	$[\infty_{-1} - \infty_0]$	$[(-1, 0) - \infty_{-1}]$
133,B	$[\infty_{-1} - \infty_0]$	$[(0, -1) - \infty_{-1}]$
147	$[\infty_{-1} - \infty_0]$	$[(-1, -1) - \infty_0]$
161	$[(1, 2) - (-1, 1)]$	$[(\frac{1}{2}, -3) - (1, 2)]$
165	$[(1, 1) - \infty_{-1}]$	$[(0, 0) - \infty_0]$
167	$[(-1, 1) - \infty_0]$	$[(i, 0) + (-i, 0) - \infty_0 - \infty_{-1}]$
177	$[(0, -1) - \infty_0]$	$[(0, 0) - (0, -1)]$
188	$[(0, -1) - \infty]$	$[(0, 1) - (1, -2)]$
191	$[\infty_{-1} - \infty_0]$	$[(0, -1) - \infty_0]$

by primes of increasing order dividing the level  $N$ . We denote  $J(\mathbf{Q})_{\text{tors}} = \Phi$  and list its size. We use  $\text{III}^?$  to denote the size of

$$\left(\lim_{s \rightarrow 1} (s - 1)^{-r} L(J, s)\right) \cdot (\#J(\mathbf{Q})_{\text{tors}})^2 / (\Omega \cdot \text{Reg} \cdot \prod c_p),$$

rounded to the nearest integer. We will refer to this as the *conjectured size of*  $\text{III}^?(J, \mathbf{Q})$ . For rank 0 optimal quotients this integer equals the (a priori) rational number

$$(L(J, 1)/(k \cdot \Omega)) \cdot ((\#J(\mathbf{Q})_{\text{tors}})^2 / \prod c_p);$$

of course there is no rounding error in this computation. For all other cases the last column gives a bound on the accuracy of the computations; all values of  $\text{III}^?$  were at least this close to the nearest integer before rounding.

In Table 3 are generators of  $J(\mathbf{Q})/J(\mathbf{Q})_{\text{tors}}$  for the curves whose Jacobians have Mordell-Weil rank 2. The generators are given as divisor classes. Whenever possible, we have chosen generators of the form  $[P - Q]$  where  $P$  and  $Q$  are rational points on the curve. Curve 167 is the only example where this is not the case, since the degree zero divisors supported on the (known) rational points on  $C_{167}$  generate a subgroup of index two in the full Mordell-Weil group. Affine points are given by their  $x$  and  $y$  coordinates in the model given in Table 1. There are two points at infinity in the normalization of the curves described by our equations, with the exception of curve  $C_{188}$ . These are denoted by  $\infty_a$ , where  $a$  is the value of the function  $y/x^3$  on the point in question. The (only) point at infinity on curve  $C_{188}$  is simply denoted  $\infty$ .

TABLE 4. Namikawa and Ueno classification of special fibers

$N$	Prime	Type	Prime	Type
23	23	$I_{3-2-1}$		
29	29	$I_{3-1-1}$		
31	31	$I_{2-1-1}$		
35	5	$I_{3-2-2}$	7	$I_{2-1-0}$
39	3	$I_{6-2-2}$	13	$I_{1-1-0}$
63	3	$2I_0^* - 0$	7	$I_{1-1-1}$
65,A	3	$I_0 - I_0 - 1$	5	$I_{3-1-1}$
65,A	13	$I_{1-1-0}$		
65,B	2	$I_0 - I_0 - 1$	5	$I_{3-1-0}$
65,B	13	$I_{1-1-1}$		
67	67	$I_{1-1-0}$		
73	73	$I_{1-1-0}$		
85	5	$I_{2-2-0}$	17	$I_{2-1-0}$
87	3	$I_{2-1-1}$	29	$I_{1-1-0}$
93	3	$I_{2-2-0}$	31	$I_{1-1-0}$
103	103	$I_{1-1-0}$		
107	107	$I_{1-1-0}$		
115	5	$I_{2-2-0}$	23	$I_{1-1-0}$
117,A	3	$III - III^* - 0$	13	$I_{1-1-1}$
117,B	3	$I_{3-1-1}^*$	13	$I_{1-1-0}$
125,A	5	$VIII - 1$		
125,B	5	$IX - 3$		
133,A	7	$I_{2-1-1}$	19	$I_{1-1-0}$
133,B	7	$I_{1-1-0}$	19	$I_{1-1-0}$
135	3	$III$	5	$I_{3-1-0}$
147	3	$I_{2-1-0}$	7	$VII$
161	7	$I_{2-2-0}$	23	$I_{1-1-0}$
165	3	$I_{2-2-0}$	5	$I_{2-1-0}$
165	11	$I_{2-1-0}$		
167	167	$I_{1-1-0}$		
175	5	$II - II - 0$	7	$I_{2-1-1}$
177	3	$I_{1-1-0}$	59	$I_{1-1-0}$
188	2	$IV - IV - 0$	47	$I_{1-1-0}$
189	3	$II - IV^* - 0$	7	$I_{1-1-1}$
191	191	$I_{1-1-0}$		

In Table 4 are the reduction types, from the classification of [NU], of the special fibers of the minimal, proper, regular models of the curves for each of the primes of singular reduction for the curve. They are the same as the primes dividing the level except that curve  $C_{65,A}$  has singular reduction at the prime 3 and curve  $C_{65,B}$  has singular reduction at the prime 2.

6. DISCUSSION OF SHAFAREVICH-TATE GROUPS  
AND EVIDENCE FOR THE SECOND CONJECTURE

From Section 3.2 we have  $\dim \text{III}(J, \mathbf{Q})[2] = \dim \text{Sel}^2(J, \mathbf{Q}) - r - \dim J(\mathbf{Q})[2]$ . With the exception of curves  $C_{65,A}$ ,  $C_{65,B}$ ,  $C_{125,B}$ , and  $C_{133,A}$  we have  $\dim \text{III}(J, \mathbf{Q})[2] = 0$ . Thus we expect  $\#\text{III}(J, \mathbf{Q})$  to be an odd square. In each case, the conjectured size of  $\text{III}(J, \mathbf{Q})$  is 1. For curves  $C_{65,A}$ ,  $C_{65,B}$ ,  $C_{125,B}$  and  $C_{133,A}$  we have  $\dim \text{III}(J, \mathbf{Q})[2] = 1, 1, 2$  and  $2$  and the conjectured size of  $\text{III}(J, \mathbf{Q}) = 2, 2, 4$  and  $4$ , respectively. We see that in each case, the (conjectured) size of the odd part of  $\text{III}(J, \mathbf{Q})$  is 1 and the 2-part is accounted for by its 2-torsion.

Recall that for rank 0 optimal quotients we are able to exactly determine the value which the second Birch and Swinnerton-Dyer conjecture predicts for  $\text{III}(J, \mathbf{Q})$ . From the previous paragraph, we then see that equation (1.1) holds if and only if  $\text{III}(J, \mathbf{Q})$  is killed by 2.

The size of  $\text{III}(J, \mathbf{Q})[2]$  is related to deficient primes. A prime  $p$  is *deficient* with respect to a curve  $C$  of genus 2, if  $C$  has no degree 1 rational divisor over  $\mathbf{Q}_p$ . From [PSt], the number of deficient primes has the same parity as  $\dim \text{III}(J, \mathbf{Q})[2]$ , if  $\text{III}(J, \mathbf{Q})$  is finite. In any case,  $\text{III}(J, \mathbf{Q})[2]$  is nontrivial if there is an odd number of deficient primes. Curve  $C_{65,A}$  has one deficient prime 3. Curve  $C_{65,B}$  has one deficient prime 2. Curve  $C_{117,B}$  has two deficient primes 3 and  $\infty$ . The rest of the curves have no deficient primes.

Since we have found  $r$  (analytic rank) independent points on each Jacobian, we have a direct proof that the Mordell-Weil rank must equal the analytic rank if  $\dim \text{III}(J, \mathbf{Q})[2] = 0$ . For curves  $C_{65,A}$  and  $C_{65,B}$ , the presence of an odd number of deficient primes gives us a similar result. For  $C_{125,B}$  we used a  $\sqrt{5}$ -Selmer group to get a similar result. Thus, we have an independent proof of equality between analytic and Mordell-Weil ranks for all curves except  $C_{133,A}$ .

The 2-Selmer groups have the same dimensions for the pairs  $C_{125,A}$ ,  $C_{125,B}$  and  $C_{133,A}$ ,  $C_{133,B}$ . For each pair, the Mordell-Weil rank is 2 for one curve and the 2-torsion of the Shafarevich-Tate group has dimension 2 for the other. In addition, the two Jacobians, when canonically embedded into  $J_0(N)$ , intersect in their 2-torsion subgroups, and one can check that their 2-Selmer groups become equal under the identification of  $H^1(\mathbf{Q}, J_{N,A}[2])$  with  $H^1(\mathbf{Q}, J_{N,B}[2])$  induced by the identification of the 2-torsion subgroups. Thus these are examples of the principle of a ‘visible part of a Shafarevich-Tate group’ as discussed in [CM].

APPENDIX: OTHER HASEGAWA CURVES

In Table 5 is data concerning all 142 of Hasegawa’s curves in the order presented in his paper. Let us explain the entries. The first column in each set of three columns gives the level,  $N$ . The second column gives a classification of the cusp forms spanning the 2-dimensional subspace of  $S_2(N)$  corresponding to the Jacobian. When that subspace is irreducible with respect to the action of the Hecke algebra and is spanned by two newforms or two oldforms, we write  $2n$  or  $2o$ , respectively. When that subspace is reducible and is spanned by two oldforms, two newforms or one of each, we write  $oo$ ,  $nn$  and  $on$ , respectively. The third column contains the sign of the functional equation at the level  $M$  at which the cusp form is a newform. This is the negative of  $\epsilon_M$  (described in Section 4.1). The order of the two signs in the third column agrees with that of the forms listed in the second column. We include this information for those who would like to further study these curves. The curves with  $N < 200$  classified as  $2n$  appeared already in Table 1.

TABLE 5. Spaces of cusp forms associated to Hasegawa’s curves

22	oo	++	58	nn	+-	87	2o	++	129	on	--	198	2o	+-
23	2n	++	60	oo	++	88	on	+-	130	on	+-	204	2o	+-
26	nn	++	60	2o	++	90	on	++	132	oo	++	205	2n	--
28	oo	++	60	2o	++	90	oo	++	133	2n	--	206	2o	--
29	2n	++	62	2o	++	90	oo	++	134	2o	--	209	2n	--
30	on	++	66	nn	++	90	oo	++	135	on	+-	210	on	+-
30	oo	++	66	2o	++	91	nn	--	138	nn	+-	213	2n	--
30	on	++	66	2o	++	93	2n	--	138	on	+-	215	on	--
31	2n	++	66	on	++	98	oo	++	140	oo	++	221	2n	--
33	on	++	67	2n	--	100	oo	++	142	nn	+-	230	2o	--
35	2n	++	68	oo	++	102	on	+-	143	on	+-	255	2o	--
37	nn	+-	69	2o	++	102	on	+-	146	2o	--	266	2o	--
38	on	++	70	on	++	103	2n	--	147	2n	--	276	2o	+-
39	2n	++	70	2o	++	104	2o	++	150	on	++	284	2o	+-
40	on	++	70	2o	++	106	on	--	153	on	+-	285	on	--
40	oo	++	70	2o	++	107	2n	--	154	on	--	286	on	--
42	on	++	72	on	++	110	on	++	156	oo	++	287	2n	--
42	oo	++	72	oo	++	111	oo	+-	158	on	--	299	2n	--
42	on	++	73	2n	--	112	on	+-	161	2n	--	330	2o	--
42	oo	++	74	oo	+-	114	oo	+-	165	2n	--	357	2n	--
44	2o	++	77	on	+-	115	2n	--	166	on	--	380	2o	+-
46	2o	++	78	oo	++	116	2o	+-	167	2n	--	390	on	--
48	on	++	78	2o	++	117	2o	++	168	2o	++			
48	oo	++	80	oo	++	120	oo	++	170	2o	--			
50	nn	++	84	oo	++	120	on	++	177	2n	--			
52	oo	++	84	oo	++	121	on	+-	180	2o	++			
52	oo	++	84	oo	++	122	on	--	184	on	+-			
54	on	++	84	oo	++	125	2n	--	186	2o	--			
57	on	+-	85	2n	--	126	oo	++	190	on	+-			
57	on	+-	87	2n	++	126	on	++	191	2n	--			

The smallest possible Mordell-Weil ranks corresponding to ++, +-, -+ and --, predicted by the first Birch and Swinnerton-Dyer conjecture, are 0, 1, 1 and 2 respectively. In all cases, those were, in fact, the Mordell-Weil ranks. This was determined by computing 2-Selmer groups with a computer program based on [Sto2]. Of course, these are cases where the first Birch and Swinnerton-Dyer conjecture is already known to hold. In the cases where the Mordell-Weil rank is positive, the Mordell-Weil group has a subgroup of finite index generated by degree zero divisors supported on rational points with  $x$ -coordinates with numerators bounded by 7 (in absolute value) and denominators by 12 with one exception. On the second curve with  $N = 138$ , the divisor class  $[(3 + 2\sqrt{2}, 80 + 56\sqrt{2}) + (3 - 2\sqrt{2}, 80 - 56\sqrt{2}) - 2\infty]$  generates a subgroup of finite index in the Mordell-Weil group.

REFERENCES

[AS1] A. Agashé and W.A. Stein, *Some abelian varieties with visible Shafarevich-Tate groups*, preprint, 2000.  
 [AS2] A. Agashé, and W.A. Stein, *The generalized Manin constant, congruence primes, and the modular degree*, in preparation, 2000.  
 [BSD] B. Birch and H.P.F. Swinnerton-Dyer, *Notes on elliptic curves. II*, J. Reine Angew. Math., **218** (1965), 79–108. MR **31**:3419

- [BL] S. Bosch and Q. Liu, *Rational points of the group of components of a Néron model*, Manuscripta Math, **98** (1999), 275–293. MR **2000i**:11094
- [BLR] S. Bosch, W. Lütkebohmert and M. Raynaud, *Néron models*, Springer-Verlag, Berlin, 1990. MR **91i**:14034
- [BCDT] C. Breuil, B. Conrad, F. Diamond and R. Taylor *On the modularity of elliptic curves over  $\mathbf{Q}$ : Wild 3-adic exercises*. [http://abel.math.harvard.edu/HTML/Individuals/Richard\\_Taylor.html](http://abel.math.harvard.edu/HTML/Individuals/Richard_Taylor.html) (2000).
- [BGZ] J. Buhler, B.H. Gross and D.B. Zagier, *On the conjecture of Birch and Swinnerton-Dyer for an elliptic curve of rank 3*. Math. Comp., **44** (1985), 473–481. MR **86g**:11037
- [Ca] J.W.S. Cassels, *Arithmetic on curves of genus 1. VIII. On conjectures of Birch and Swinnerton-Dyer.*, J. Reine Angew. Math., **217** (1965), 180–199. MR **31**:3420
- [CF] J.W.S. Cassels and E.V. Flynn, *Prolegomena to a middlebrow arithmetic of curves of genus 2*, London Math. Soc., Lecture Note Series 230, Cambridge Univ. Press, Cambridge, 1996. MR **97i**:11071
- [Cr1] J.E. Cremona, *Abelian varieties with extra twist, cusp forms, and elliptic curves over imaginary quadratic fields*, J. London Math. Soc. (2), **45** (1992), 404–416. MR **93h**:11056
- [Cr2] J.E. Cremona, *Algorithms for modular elliptic curves. 2nd edition*, Cambridge Univ. Press, Cambridge, 1997. MR **93m**:11053
- [CM] J.E. Cremona and B. Mazur, *Visualizing elements in the Shafarevich-Tate group, Experiment. Math.* **9** (2000) 13–28. CMP 2000:12
- [Ed1] B. Edixhoven, *On the Manin constants of modular elliptic curves*, Arithmetic algebraic geometry (Texel, 1989), Progr. Math., 89, Birkhauser Boston, Boston, MA, 1991, pp. 25–39. MR **92a**:11066
- [Ed2] B. Edixhoven, *L'action de l'algèbre de Hecke sur les groupes de composantes des jacobiniennes des courbes modulaires est "Eisenstein"*, Astérisque, No. 196–197 (1992), 159–170. MR **92k**:11059
- [FPS] E.V. Flynn, B. Poonen and E.F. Schaefer, *Cycles of quadratic polynomials and rational points on a genus-two curve*, Duke Math. J., **90** (1997), 435–463. MR **98j**:11048
- [FS] E.V. Flynn and N.P. Smart, *Canonical heights on the Jacobians of curves of genus 2 and the infinite descent*, Acta Arith., **79** (1997), 333–352. MR **98f**:11066
- [FM] G. Frey and M. Müller, *Arithmetic of modular curves and applications*, in *Algorithmic algebra and number theory*, Ed. Matzat et al., Springer-Verlag, Berlin, 1999, pp. 11–48. MR **00a**:11095
- [GZ] B.H. Gross and D.B. Zagier, *Heegner points and derivatives of L-series*, Invent. Math., **84** (1986), 225–320. MR **87j**:11057
- [Gr] A. Grothendieck, *Groupes de monodromie en géométrie algébrique*, SGA 7 I, Exposé IX, Lecture Notes in Math. vol. 288, Springer, Berlin–Heidelberg–New York, 1972, pp. 313–523. MR **50**:7134
- [Ha] R. Hartshorne, *Algebraic geometry*, Grad. Texts in Math. 52, Springer-Verlag, New York, 1977. MR **57**:3116
- [Hs] Y. Hasegawa, *Table of quotient curves of modular curves  $X_0(N)$  with genus 2*, Proc. Japan. Acad., **71** (1995), 235–239. MR **97e**:11071
- [KS] D.R. Kohel and W.A. Stein, *Component groups of quotients of  $J_0(N)$* , in: Algorithmic number theory (Leiden, The Netherlands, 2000), Lecture Notes in Computer Science, 1838, Ed. W. Bosma, Springer, Berlin, 2000, 405–412.
- [Ko] V.A. Kolyvagin, *Finiteness of  $E(\mathbf{Q})$  and  $\text{III}(E, \mathbf{Q})$  for a subclass of Weil curves*, Izv. Akad. Nauk SSSR Ser. Mat., **52** (1988), 522–540. MR **89m**:11056
- [KL] V.A. Kolyvagin and D.Y. Logachev, *Finiteness of the Shafarevich-Tate group and the group of rational points for some modular abelian varieties*, Leningrad Math J., **1** (1990), 1229–1253. MR **91c**:11032
- [La] S. Lang, *Introduction to modular forms*, Springer-Verlag, Berlin, 1976. MR **55**:2751
- [Le] F. Lépervost, *Jacobiniennes de certaines courbes de genre 2: torsion et simplicité*, J. Théor. Nombres Bordeaux, **7** (1995), 283–306. MR **98a**:11078
- [Li] Q. Liu, *Conducteur et discriminant minimal de courbes de genre 2*, Compos. Math., **94** (1994), 51–79. MR **96b**:14038
- [Ma] B. Mazur, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math., **44** (1978), 129–162. MR **80h**:14022

- [MS] J.R. Merriman and N.P. Smart, *Curves of genus 2 with good reduction away from 2 with a rational Weierstrass point*, Math. Proc. Cambridge Philos. Soc., **114** (1993), 203–214. MR **94h**:14031
- [Mi1] J.S. Milne, *Arithmetic duality theorems*, Academic Press, Boston, 1986. MR **88e**:14028
- [Mi2] J.S. Milne, *Jacobian varieties*, in: *Arithmetic geometry*, Ed. G. Cornell, G. and J.H. Silverman, Springer-Verlag, New York, 1986, pp. 167–212. MR **89b**:14029
- [NU] Y. Namikawa and K. Ueno, *The complete classification of fibres in pencils of curves of genus two*, Manuscripta Math., **9** (1973), 143–186. MR **51**:5595
- [PSc] B. Poonen and E.F. Schaefer, *Explicit descent for Jacobians of cyclic covers of the projective line*, J. Reine Angew. Math., **488** (1997), 141–188. MR **98k**:11087
- [PSt] B. Poonen and M. Stoll, *The Cassels-Tate pairing on polarized abelian varieties*, Ann. of Math. (2), **150** (1999), 1109–1149. MR **2000m**:11048
- [Ri] K. Ribet, *On modular representations of  $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$  arising from modular forms*, Invent. Math., **100** (1990), 431–476. MR **91g**:11066
- [Sc] E.F. Schaefer, *Computing a Selmer group of a Jacobian using functions on the curve*, Math. Ann., **310** (1998), 447–471. MR **99h**:11063
- [Sh] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Princeton University Press, 1994. MR **95e**:11048
- [Si] J.H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Grad. Texts in Math. 151, Springer-Verlag, New York, 1994. MR **96b**:11074
- [Sto1] M. Stoll, *Two simple 2-dimensional abelian varieties defined over  $\mathbf{Q}$  with Mordell-Weil rank at least 19*, C. R. Acad. Sci. Paris, Sér. I, **321** (1995), 1341–1344. MR **96j**:11084
- [Sto2] M. Stoll, *Implementing 2-descent for Jacobians of hyperelliptic curves*, to appear in Acta Arith.
- [Sto3] M. Stoll, *On the height constant for curves of genus two*, Acta Arith., **90** (1999), 183–201. MR **2000h**:11069
- [Sto4] M. Stoll, *On the height constant for curves of genus two, II*, in preparation.
- [Ta] J. Tate, *On the conjectures of Birch and Swinnerton-Dyer and a geometric analog*. Séminaire Bourbaki, **306** 1965/1966. CMP 98:09
- [Wal1] J.-L. Waldspurger, *Correspondances de Shimura*, Proceedings of the International Congress of Mathematicians, Vol. 1, 2, (Warsaw, 1983), 1984, pp. 525–531. MR **86m**:11036
- [Wal2] J.-L. Waldspurger, *Sur les coefficients de Fourier des formes modulaires de poids demi-entier*, J. Math. Pures Appl. (9), **60** (1981), 375–484. MR **83h**:10061
- [Wan] X. Wang, *2-dimensional simple factors of  $J_0(N)$* , Manuscripta Math., **87** (1995), 179–197. MR **96h**:11059

DEPARTMENT OF MATHEMATICAL SCIENCES, UNIVERSITY OF LIVERPOOL, P.O.BOX 147, LIVERPOOL L69 3BX, ENGLAND

*E-mail address:* [evflynn@liverpool.ac.uk](mailto:evflynn@liverpool.ac.uk)

UNIVERSITÉ GRENOBLE I, INSTITUT FOURIER, BP 74, F-38402 SAINT MARTIN D'HÈRES CEDEX, FRANCE

*E-mail address:* [leprevot@math.jussieu.fr](mailto:leprevot@math.jussieu.fr)

DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE, SANTA CLARA UNIVERSITY, SANTA CLARA, CALIFORNIA 95053

*E-mail address:* [eschaefe@math.scu.edu](mailto:eschaefe@math.scu.edu)

DEPARTMENT OF MATHEMATICS, HARVARD UNIVERSITY, ONE OXFORD STREET, CAMBRIDGE, MASSACHUSETTS 02138

*E-mail address:* [was@math.berkeley.edu](mailto:was@math.berkeley.edu)

MATHEMATISCHES INSTITUT DER HEINRICH-HEINE-UNIVERSITÄT, UNIVERSITÄTSSTR. 1, 40225 DÜSSELDORF, GERMANY

*E-mail address:* [stoll@math.uni-duesseldorf.de](mailto:stoll@math.uni-duesseldorf.de)

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF SOUTHERN CALIFORNIA, 1042 W. 36TH PLACE, LOS ANGELES, CALIFORNIA 90089-1113

*E-mail address:* [jlwether@alum.mit.edu](mailto:jlwether@alum.mit.edu)