Studying the Birch and Swinnerton-Dyer Conjecture for Modular Abelian Varieties Using Magma

William Stein

Harvard University, Cambridge, Massachusetts, USA

1 Introduction

In this paper we describe the Birch and Swinnerton-Dyer conjecture in the case of modular abelian varieties and how to use Magma to do computations with some of the quantities that appear in the conjecture. We assume the reader has some experience with algebraic varieties and number theory, but do not assume the reader has proficiency working with elliptic curves, abelian varieties, modular forms, or modular symbols.

In Section 2 we quickly survey abelian varieties, modular forms, Hecke algebras, modular curves, and modular Jacobians, then discuss Shimura's construction of abelian varieties attached to modular forms. In Section 3 we survey many quantities associated to an abelian variety, including the Mordell-Weil group, torsion subgroup, regulator, Tamagawa numbers, real volume, and Shafarevich-Tate group, and use these to state the full Birch and Swinnerton-Dyer conjecture for modular abelian varieties. Section 4 contains some computational results from other papers about the Birch and Swinnerton-Dyer conjecture.

The rest of the paper is about how to use the package that I wrote for Magma to carry out an explicit computational study of modular abelian varieties. Section 5 is about modular symbols and how to compute with them in Magma. In Section 6 we state a theorem that allows us to use Magma to compute subgroups of Shafarevich-Tate groups of abelian varieties. In Section 7 we discuss computation of special values of L-functions. Section 8 is about computing Tamagawa numbers, and in Section 9 we describe how to compute a divisor and multiple of the order of the torsion subgroup. All these computations are pulled together in Section 10 to obtain a conjectural divisor and multiple of the order of the Shafarevich-Tate group of a modular abelian variety of dimension 20. We finish with Section 11, which contains an example in which the level is composite and elements of the Shafarevich-Tate group only becomes "visible" at higher level.

Taken together, these computations give evidence for the Birch and Swinnerton-Dyer conjecture and increase our explicit understanding of modular abelian varieties.

2 Modular Abelian Varieties

An elliptic curve E over the rational numbers $\mathbf{Q}$ is a one-dimensional commutative compact algebraic group. Such a curve is usually given as the projective closure of an affine curve $y^2 = x^3 + ax + b$, with a and b in $\mathbf{Q}$. The points over the real numbers $\mathbf{R}$ of $y^2 = x^3 - x + 1$ are illustrated in Figure 1. If P and Q

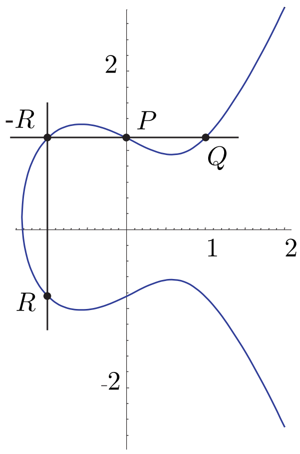

Fig. 1. Adding $P = (0, 1)$ to $Q = (1, 1)$ to get $R = (-1, -1)$ on $y^2 = x^3 - x + 1$

are two distinct points on E, we find their sum as follows: draw the unique line through them and let (x, y) be the third point of intersection of this line with E. Then the sum of P and Q is $R = (x, -y)$, as illustrated in Figure 1. For more about elliptic curves, see [33, 34].

This paper is about abelian varieties, which are compact (commutative) algebraic groups of dimension possibly greater than 1. For example, the Cartesian product of two elliptic curves is an abelian variety of dimension 2.

Explicit equations for abelian varieties are vastly more complicated than for elliptic curves, so algorithms for computing with abelian varieties without recourse to explicit algebraic equations are of great value. In this paper we focus on such algorithms in the case when the abelian variety is endowed with extra structure coming from modular forms.

A cuspidal modular form of weight 2 for

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}) : N \mid c \right\}$$

is a holomorphic function $f(z)$ on the upper half plane such that for all $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$ we have

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^2 f(z),$$

and which satisfies certain vanishing conditions at the cusps (see [13, pg. 42] for a precise definition). We denote the finite dimensional complex vector space of all cuspidal modular forms of weight 2 for $\Gamma_0(N)$ by $S_2(\Gamma_0(N))$. Because $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma_0(N)$, cuspidal modular forms have a Fourier series representation

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

The Hecke algebra

$$\mathbf{T} = \mathbf{Z}[T_1, T_2, T_3, \ldots] \subset \mathrm{End}(S_2(\Gamma_0(N)))$$

is a commutative ring that is free of rank equal to $\dim_{\mathbf{C}} S_2(\Gamma_0(N))$ (for the definition and basic properties of the Hecke operators T_n, see [13, §3] and the references therein).

A newform is a modular form

$$f = q + \sum_{n \geq 2} a_n q^n$$

that is a simultaneous eigenvector for every element of the Hecke algebra and such that the coefficients $\{a_p : p \nmid N\}$ are not the prime-index coefficients of another eigenform of some level that strictly divides N.

The group $\Gamma_0(N)$ acts as a discrete group of linear fractional transformations on the upper half plane; the quotient of the upper half plane by this action is a non-compact Riemann surface. Its compactification has the structure of algebraic curve over $\mathbf{Q}$, i.e., the compactification is the set of complex points of an algebraic curve $X_0(N)$ defined by polynomial equations with coefficients in $\mathbf{Q}$.

A divisor on an algebraic curve X is an element of the free abelian group generated by the points of X. For example, if f is a rational function on X then

$$(f) = (\text{formal sum of poles of } f) - (\text{formal sum of zeros of } f)$$

is a divisor on X, where the sums are with multiplicity. Two divisors D_1 and D_2 are linearly equivalent if there is a rational function f on X such that

$D_1 - D_2 = (f)$. The Jacobian J of an algebraic curve X is an abelian variety of dimension equal to the genus (number of holes in the Riemann surface $X(\mathbf{C})$) of X such that the underlying group of J is naturally isomorphic to the group of divisor classes of degree 0 on X. Let $J_0(N)$ denote the Jacobian of $X_0(N)$.

Similarly, let

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}) : N \mid c \text{ and } a \equiv 1 \pmod{N} \right\},$$

define $X_1(N)$ similarly, and let $J_1(N)$ be the Jacobian of $X_1(N)$.

A modular abelian variety is an abelian variety A for which there exists a surjective morphism $J_1(N) \to A$. Modular abelian varieties are appealing objects to study. For example, it is a deep theorem that every elliptic curve over $\mathbf{Q}$ is modular (see [7, 40, 41]), and this implies Fermat's Last Theorem (see [25, Cor. 1.2]). In [27], Ken Ribet conjectured that the simple abelian varieties over $\mathbf{Q}$ of "GL_2-type" are exactly the simple modular abelian varieties. A closely related conjecture of Serre (see [29, pg. 179] and [28]) asserts that every odd irreducible Galois representation

$$\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\overline{\mathbf{F}}_p)$$

is "modular"; this conjecture is equivalent to the assertion that ρ can be realized (up to twist) as the action of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ on a subgroup of the points on some $J_1(N)$ (see [28, §3.3.1] for a partial explanation). Though Serre's conjecture is still far from proved, it implies Ribet's conjecture (see [27, Thm. 4.4]).

We now return to considering $\Gamma_0(N)$, though we could consider $\Gamma_1(N)$ for everything in the rest of this section. The Hecke algebra $\mathbf{T}$, which we introduced above as a ring of linear transformations on $S_2(\Gamma_0(N))$, also acts via endomophisms on $J_0(N)$.

In order to construct Galois representations attached to modular forms, Goro Shimura (see [31, §1] and [32, §7.14]) associated to each newform $f = \sum a_n q^n$ a simple abelian variety A_f defined over $\mathbf{Q}$. Let I_f be the ideal of elements of $\mathbf{T}$ that annihilate f. Then

$$A_f = J_0(N)/I_f J_0(N).$$

The dimension of A_f equals the degree of the field generated over $\mathbf{Q}$ by the coefficients a_n of f. Note that A_f need not be simple over $\overline{\mathbf{Q}}$.

We will frequently mention the dual $A_f^\vee$ below. The dual can be considered as an abelian subvariety of $J_0(N)$, by using that Jacobians are canonically self dual and the dual of the quotient map $J_0(N) \to A_f$ is an inclusion $A_f^\vee \hookrightarrow J_0(N)$. Note that $A_f^\vee$ is the connected component of the intersection of the kernels of all elements of I_f.

We say that a newform g is a Galois conjugate of f if there is σ in $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ such that $g = \sum \sigma(a_n) q^n$. If g is a Galois conjugate of f, then

$A_f = A_g$; if g is not a conjugate of f then the only homomorphism from A_f to A_g is the zero map. (A nonzero homomorphism $A_f \to A_g$ would induce an isogeny of Tate modules, from which one could deduce that f and g are Galois conjugate.)

We will concern ourselves almost entirely with these modular abelian varieties attached to newforms, because, as mentioned above, there are a number of algorithms for computing with them that do not require explicit algebraic equations (see [2, 3, 9, 10, 15, 19, 37, 35]). Also, it follows from standard results about constructing spaces of cusp forms from newforms, which can be found in [4, 22], that every modular abelian variety is isogenous to a product of abelian varieties of the form A_f. (An isogeny of abelian varieties is a surjective homomorphism with finite kernel.)

3 The Birch and Swinnerton-Dyer Conjecture

In the 1960s Bryan Birch and Peter Swinnerton-Dyer did computations with elliptic curves at Cambridge University on the EDSAC computer (see, e.g., [5]). These computations led to earth-shattering conjectures about the arithmetic of elliptic curves over $\mathbf{Q}$. Tate [39] formulated their conjectures in a more functorial way that generalized them to abelian varieties over global fields (such as the rational numbers). We now state their conjectures below for modular abelian varieties over $\mathbf{Q}$.

Let A_f be a modular abelian variety. Mordell and Weil proved that the abelian group $A_f(\mathbf{Q})$ of rational points on A_f is finitely generated, so it is isomorphic to $\mathbf{Z}^r \times T$ where T is the finite group $A_f(\mathbf{Q})_{\mathrm{tor}}$ of all elements of finite order in $A_f(\mathbf{Q})$. The exponent r is called the Mordell-Weil rank of A_f.

If f is a newform, the L-function of f is defined by the Dirichlet series $L(f,s) = \sum_{n\geq 1} a_n n^{-s}$. Hasse showed that $L(f,s)$ has an analytic continuation to a holomorphic function on the whole complex plane. The Hasse-Weil L-function of A_f is

$$L(A_f, s) = \prod L(g, s)$$

where the product is over the Galois conjugates g of f. The analytic rank of A_f is $\mathrm{ord}_{s=1} L(A_f, s)$.

We are now ready to state the first part of the conjecture.

Conjecture 3.1 (Birch and Swinnerton-Dyer) *The analytic rank of A_f is equal to the Mordell-Weil rank of A_f.*

Remark 1.

1. It is an open problem to give, with proof, an example of an elliptic curve with analytic rank at least 4. No examples with analytic rank at least 3 were known until the deep theorem of [16, Prop. 7.4].

2. When A_f is an elliptic curve, Conjecture 3.1 is the Clay Mathematics Institute Millennium Prize Problem from arithmetic geometry [17], so it has received much publicity.

In order to explain the conjecture of Birch and Swinnerton-Dyer about the leading coefficient of $L(A_f, s)$ at $s = 1$, we introduce the regulator, real volume, Tamagawa numbers, and Shafarevich-Tate group of A_f. Most of what we say below is true for a general abelian variety over a global field; the notable exceptions are that we do not know that the L-function is defined on the whole complex plane, and there are hardly any cases in general when the Shafarevich-Tate group is known to be finite.

Let $A_f(\mathbf{Q})/_{\mathrm{tor}}$ denote the quotient of $A_f(\mathbf{Q})$ by its torsion subgroup, so $A_f(\mathbf{Q})/_{\mathrm{tor}}$ is isomorphic to $\mathbf{Z}^r$, where r is the Mordell-Weil rank of A_f. The height pairing is a nondegenerate bilinear pairing h on $A_f(\mathbf{Q})/_{\mathrm{tor}}$. The regulator Reg_{A_f} of A_f is the absolute value of the determinant of a matrix who entries are $h(P_i, P_j)$, where $P_1, \ldots, P_r$ are a basis for $A_f(\mathbf{Q})/_{\mathrm{tor}}$. When $A_f(\mathbf{Q})$ has rank zero, the regulator is 1.

We use a certain integral model of A_f to define the real volume and Tamagawa numbers of A_f. The Néron model $\mathcal{A}$ of A_f, whose existence was established by Néron in [24] (see also [6, Ch. 1]), is a canonical object associated to A_f that is defined over $\mathbf{Z}$. The Néron model can be reduced modulo p for every prime p, and when base extended to $\mathbf{Q}$, the Néron model is isomorphic to A_f. The Néron model $\mathcal{A}$ is determined, up to unique isomorphism, by the following properties, which the reader unfamiliar with schemes can safely ignore: $\mathcal{A}$ is a smooth commutative group scheme over $\mathbf{Z}$ such that whenever S is a smooth scheme over $\mathbf{Z}$ the restriction map

$$\mathrm{Hom}(S, \mathcal{A}) \to \mathrm{Hom}_{\mathbf{Q}}(S_{\mathbf{Q}}, A)$$

is a bijection.

The real volume Ω_{A_f} of A_f is the absolute value of the integral over $A_f(\mathbf{R})$ of $h_1 \wedge \cdots \wedge h_d$ where $h_1, \ldots, h_d$ are a basis for the holomorphic 1-forms on $\mathcal{A}$. Using various identifications as in [1, §2.2.2] one sees that the $\mathbf{Z}$-span M of $h_1, \ldots, h_d$ can be viewed as a submodule of

$$W = S_2(\Gamma_0(N), \mathbf{Z}) \cap (\mathbf{C}f_1 \oplus \cdots \oplus \mathbf{C}f_d)$$

where $f_1, \ldots, f_d$ are the $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ conjugates of f. We call the index of M in W the Manin constant of A_f, and conjecture (see [1]) that the Manin constant is 1. This conjecture would imply that a basis $h_1, \ldots, h_d$ can be computed, since W can be computed.

The reduction modulo p of $\mathcal{A}$ is an algebraic group $\mathcal{A}_{\mathbf{F}_p}$ over the finite field $\mathbf{F}_p$ with p elements. If p does not divide N, then this group is connected, but when p divides N, the reduction $\mathcal{A}_{\mathbf{F}_p}$ need not be connected. Let

$$\Phi_{A,p} = \mathcal{A}_{\mathbf{F}_p}/\mathcal{A}^0_{\mathbf{F}_p}$$

be the finite group of components. The Tamagawa number of A_f at p, denoted c_p, is the number of $\mathbf{F}_p$-rational components of the reduction of $\mathcal{A}$ modulo p, so $c_p = \#\Phi_{A,p}(\mathbf{F}_p)$.

The only object left to define before we state the second part of the Birch and Swinnerton-Dyer conjecture is the Shafarevich-Tate group of A_f. This is a group that measures the failure of a certain local-to-global principle for A_f. To give an exact description, we let $\mathrm{H}^1(\mathbf{Q}, A_f)$ be the first Galois cohomology group of A_f, which is a torsion group with infinitely many elements of any order bigger than 1 (see [30] for a proof in the case when A_f is an elliptic curve; the top of page 278 of [8] also purports to contain a proof). More precisely, $\mathrm{H}^1(\mathbf{Q}, A_f)$ is the set of equivalence classes of maps $c : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to A_f(\overline{\mathbf{Q}})$, with finite image, such that $c(\sigma\tau) = c(\sigma) + \sigma c(\tau)$, and two classes c_1 and c_2 are equivalent if there exists P in $A_f(\overline{\mathbf{Q}})$ such that $c_1(\sigma) - c_2(\sigma) = \sigma(P) - P$ for all $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. For each prime p we define $\mathrm{H}^1(\mathbf{Q}_p, A_f)$ analogously, but with the rational numbers $\mathbf{Q}$ replaced by the p-adic numbers $\mathbf{Q}_p$. Also, we allow $p = \infty$, in which case $\mathbf{Q}_p = \mathbf{R}$. Then

$$Ш(A_f) = \ker\left(\mathrm{H}^1(\mathbf{Q}, A_f) \longrightarrow \bigoplus_{\text{primes } p \leq \infty} \mathrm{H}^1(\mathbf{Q}_p, A_f)\right).$$

We are now ready to state the full Birch and Swinnerton-Dyer conjecture for modular abelian varieties A_f.

Conjecture 3.2 *Let $A = A_f$ be a modular abelian variety attached to a newform, and let $r = \mathrm{ord}_{s=1} L(A, s)$ be the analytic rank of A. Then*

$$\frac{L^{(r)}(A,1)}{r!} = \frac{\prod c_p \cdot \Omega_A \cdot \mathrm{Reg}_A}{\#A(\mathbf{Q})_{\mathrm{tor}} \cdot \#A^\vee(\mathbf{Q})_{\mathrm{tor}}} \cdot \#Ш(A).$$

Recall that $L^{(r)}(A_f, 1)$ makes sense at $s = 1$ because A_f is attached to a modular form. Also Kato established in [18, Cor. 14.3] that if $L(A_f, 1) \neq 0$ then $Ш(A_f)$ is finite, and Kolyvagin-Logachev ([20, Thm. 0.3]) proved that if f is a modular form in $S_2(\Gamma_0(N))$ and $\mathrm{ord}_{s=1} L(f, s) \leq 1$, then $Ш(A_f)$ is finite. When the theorems of Kato, Kolyvagin, and Logachev do not apply, we do not know even one example of a modular abelian variety A_f for which $Ш(A_f)$ is provably finite. John Tate once remarked that Conjecture 3.2 (for arbitrary abelian varieties) relates the value of a function where it is not known to be defined to the order of a group that is not known to be finite.

The rest of this paper is about how to use Magma to gather computational evidence for Conjecture 3.2, a task well worth pursuing. Elliptic curves are naturally surrounded by modular abelian varieties, so we want to understand modular abelian varieties well in order to say something about Conjectures 3.1–3.2 for elliptic curves. Doing explicit computations about these conjectures results in stimulating tables of data about modular abelian varieties, which could never be obtained except by direct computation. Until [2, 15] there were very few nontrivial computational examples of Conjecture 3.2 for abelian varieties in the literature, so it is important to test the conjecture since we might find a counterexample. Trying to compute information about a conjecture stimulates development of algorithms and theorems about that conjecture. Finally, our computations may lead to refinements of Conjecture 3.2 in the special case of modular abelian varieties; for example, most objects in Conjecture 3.2 are modules over the Hecke algebra so there should be more precise module-theoretic versions of the conjecture.

4 Some Computational Results

In [2] we use MAGMA to compute some of the arithmetic invariants of the 19608 abelian variety quotients A_f of $J_0(N)$ with $N \leq 2333$. Over half of these A_f have analytic rank 0, and for these we compute a divisor and a multiple of the order of $Ш(A_f)$ predicted by Conjecture 3.2. We find that there are at least 168 abelian varieties A_f such that the Birch and Swinnerton-Dyer Conjecture implies that $\#Ш(A_f)$ is divisible by an odd prime, and we use MAGMA to show that for 37 of these the odd part of the conjectural order of $Ш(A_f)$ divides $\#Ш(A_f)$ by constructing nontrivial elements of $Ш(A_f)$ using visibility theory. The challenge remains to show that the remaining 131 abelian varieties A_f have odd part of $Ш(A_f)$ divisible by the odd part of the conjectural order of $Ш(A_f)$ (we successfully take up this challenge for one example of level 551 in Section 11 of the present paper).

In [9, §2 and §7] we investigate Conjecture 3.1–3.2 when A_f is a quotient of $J_1(p)$ with p prime. In particular, we compute some of the invariants of every A_f for $p \leq 71$.

It was once thought by some mathematicians that Shafarevich-Tate groups of abelian varieties would have order a perfect square (or at least twice a perfect square). This is false, as we showed in the paper [36], where we use MAGMA to prove that for every odd prime $p < 25000$ there is an abelian variety whose Shafarevich-Tate group has order pn^2 with n an integer.

Much of the data mentioned above is of interest even if the full Birch and Swinnerton-Dyer conjecture were known since this data could probably never be discovered without considerable computation, even assuming the conjectures were true.

The rest of this paper is about how to use MAGMA to do computations with newform quotients A_f of $J_0(N)$ as in [2]. These computations involve modular symbols, which underly most algorithms for working with modular abelian varieties. (I hope to add functionality to a future release of MAGMA for computing directly with modular abelian varieties, so that no explicit mention of modular symbols is required.)

Remark 2. From a computational point of view, it is difficult to give evidence for Conjecture 3.1 when the dimension is greater than 1 in cases not covered by the general theorems of Kato, Kolyvagin, and Logachev. To give new evidence we would have to consider a modular abelian variety A_f with either f a newform in $S_2(\Gamma_0(N))$ and $\mathrm{ord}_{s=1} L(f,s) > 1$, or f a newform in $S_2(\Gamma_1(N))$ but not in $S_2(\Gamma_0(N))$ and $\mathrm{ord}_{s=1} L(f,s) > 0$. We would then show that $A_f(\mathbf{Q})$ is infinite, and more precisely that it has the rank predicted by Conjecture 3.1. In the above 2 cases the only known way to show that $A_f(\mathbf{Q})$ is infinite is to exhibit a point of infinite order in $A_f(\mathbf{Q})$, and this seems to require knowing equations for A_f. Also when $L(A_f,1) = 0$, Conjecture 3.2 involves a regulator term, which we do not know how to compute without explicitly finding the points on a model for A_f. Thus we will focus on giving evidence for Conjecture 3.2 in the case when $L(f,1) \neq 0$.

5 Modular Symbols

In this section we describe how modular symbols are related to homology of modular curves, and illustrate how to compute with modular symbols in Magma. We also discuss computing decomposition of modular symbols spaces and, for efficiency reasons, computing in the +1 quotient.

Let N be a positive integer. The integral homology $\mathrm{H}_1(X_0(N),\mathbf{Z})$ of the modular curve $X_0(N)$ is a free abelian group of rank equal to the genus of $X_0(N)$. The Hecke algebra $\mathbf{T} = \mathbf{Z}[T_1, T_2, T_3, \ldots]$ acts on a $\mathrm{H}_1(X_0(N),\mathbf{Z})$ as a ring of homomorphisms and makes $\mathrm{H}_1(X_0(N),\mathbf{Z})$ into a $\mathbf{T}$-module. This section is concerned with how to compute with this module using Magma. Section 12 contains a complete log of all Magma computations given below.

Modular symbols provide a finite computable presentation for the homology of $X_0(N)$ along with the action of the Hecke algebra $\mathbf{T}$ on this homology. The relative rational homology $\mathrm{H}_1(X_0(N),\mathbf{Q},\mathrm{cusps})$ is the rational homology of $X_0(N)$ relative to the cusps; it is the finitely generated free abelian group of homology equivalence classes of geodesic paths from α to β, where α and β lie in $\mathbf{P}^1(\mathbf{Q}) = \mathbf{Q} \cup \{\infty\}$. A finite presentation for $\mathrm{H}_1(X_0(N),\mathbf{Q},\mathrm{cusps})$ can be found in [23]. For simplicity, we typically compute $\mathrm{H}_1(X_0(N),\mathbf{Q},\mathrm{cusps})$ first, then find $\mathrm{H}_1(X_0(N),\mathbf{Z})$ inside $\mathrm{H}_1(X_0(N),\mathbf{Q},\mathrm{cusps})$ if it is needed. By definition, We now illustrate how Magma can compute a basis for $\mathrm{H}_1(X_0(N),\mathbf{Q},\mathrm{cusps})$, and, given arbitrary α and β in $\mathbf{P}^1(\mathbf{Q})$, find an equivalent linear combination of basis elements.

```
M := ModularSymbols(389);
Basis(M);
```

The output of Basis(M) begins with the symbol $\{-1/337, 0\}$. Figure 2 on page 10 illustrates how the expression $\{-1/337, 0\}$ represents the relative rational homology class determined by a geodesic path from $-1/337$ to 0 in the upper half plane. The cusps determined by $-1/337$ and 0 are equivalent by an element of $\Gamma_0(389)$, so the image of the geodesic path in the 32 holed torus $X_0(389)(\mathbf{C})$ is a closed loop.

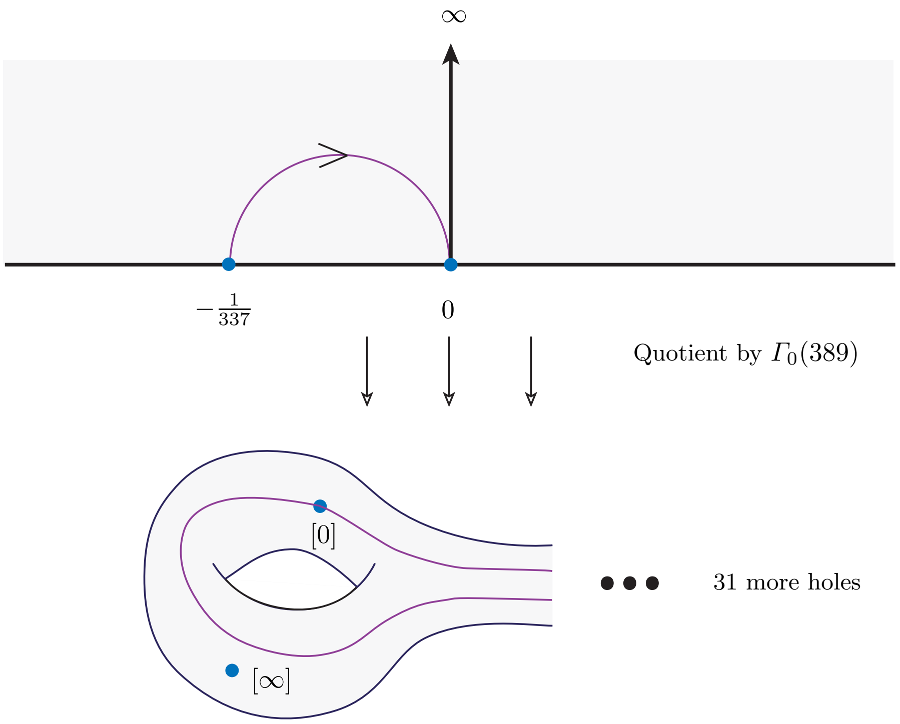

Fig. 2. The Modular Symbol $\{-1/337, 0\}$

The following MAGMA code illustrates how to find the image in the relative homology of an arbitrary path between cusps. The extra $<$ and $>$ are needed because we are considering modular symbols of weight $k = 2$; in general there is a coefficient which is a homogenous polynomial of degree $k - 2$, which is the first argument to the coercion. The Cusps()| part of the expression is needed so that the sequence is a sequence of cusps (this is not required if both cusps are rational numbers).

```
M ! <1, [Cusps() | -1/337, Infinity()] > ;
```

For more about computing with modular symbols, see [11, 12, 23, 37, 35].

Precise relationships between $\mathrm{H}_1(X_0(N), \mathbf{Q})$ and $S_2(\Gamma_0(N))$, along with some linear algebra, make it possible for us to compute a basis of $S_2(\Gamma_0(N))$

from knowledge about $\mathrm{H}_1(X_0(N), \mathbf{Q})$ as a $\mathbf{T}$-module. The following code, which computes a basis for $S_2(\Gamma_0(389))$, computes $\mathrm{H}_1(X_0(389), \mathbf{Q})$ and uses it to deduce the basis.

```
S := CuspForms(389);
SetPrecision(S, 40);
Basis(S);
```

The SetPrecision command sets the output precision for q-expansions. The computed basis consists of q-expansions with coefficients in $\mathbf{Z}$.

Using NewformDecomposition, we find the submodules of $\mathrm{H}_1(X_0(389), \mathbf{Q})$ that correspond to Galois-conjugacy classes of newforms. These in turn correspond to the modular abelian varieties A_f attached to newforms. Magma excels at dense linear algebra over $\mathbf{Q}$ and is highly optimized for computing these decompositions. The following commands compute a decomposition of the new subspace of $\mathrm{H}_1(X_0(389), \mathbf{Q})$ corresponding to newforms.

```
M := ModularSymbols(389);
N := NewSubspace(CuspidalSubspace(M));
NewformDecomposition(N);
```

Since 389 is prime, the NewSubspace command is not necessary since everything is automatically new (there are no nonzero cusp forms of level 1 and weight 2). The decomposition consists of five factors of dimensions 2, 4, 6, 12, and 40; these correspond to newforms defined over fields of degrees 1, 2, 3, 6, and 20, respectively, which in turn correspond to abelian varieties over $\mathbf{Q}$ of dimensions 1, 2, 3, 6, and 20, respectively.

Remark 3. When information about the powers of 2 appearing in Conjecture 3.2 is not needed, we can instead do all computations in the "+1 quotient" of the space of modular symbols, which has half the dimension.

```
M := ModularSymbols(389, 2, +1);    // the plus one quotient
```

6 Visibility Theory

Mazur introduced the notion of visibility to unify diverse ideas for constructing elements of Shafarevich-Tate groups. In this section we define what it means for an element of the Shafarevich-Tate group to be visible, state a theorem that allows us to compute pieces of this visible subgroup in some cases, and illustrate the theorem with a 20 dimensional abelian variety of level 389.

Suppose $i : A \to J$ is an injective morphism of abelian varieties over $\mathbf{Q}$. Then the visible subgroup of $Ш(A)$ is the kernel of the induced map $Ш(A) \to Ш(J)$.

Our interest in visibility in the present paper is that it allows us to obtain a provable divisor of $\#Ш(A)$, which is useful in giving evidence for Conjecture 3.2. The following theorem is proved in [3, Thm. 3.1] for abelian varieties over number fields.

Theorem 6.1 *Let A and B be abelian subvarieties of an abelian variety J over $\mathbf{Q}$ such that $A(\overline{\mathbf{Q}})\cap B(\overline{\mathbf{Q}})$ is finite. (Note that J need not be a Jacobian.) Let N be an integer divisible by the residue characteristics of primes of bad reduction for B (so if A and B are modular then N is the level). Suppose p is an odd prime and that*

$$p \nmid N \cdot \#(J/B)(\mathbf{Q})_{\mathrm{tor}} \cdot \#B(\mathbf{Q})_{\mathrm{tor}} \cdot \prod_{p} c_{A,p} \cdot c_{B,p},$$

where $c_{A,p} = \#\Phi_{A,p}(\mathbf{F}_p)$ (resp., $c_{B,p}$) is the Tamagawa number of A (resp., B) at p. Suppose furthermore that $B(\overline{\mathbf{Q}})[p] \subset A(\overline{\mathbf{Q}})$, where both are viewed as subgroups of $J(\overline{\mathbf{Q}})$. Then there is a natural map

$$\varphi : B(\mathbf{Q})/pB(\mathbf{Q}) \to Ш(A)[p]$$

such that

$$\dim_{\mathbf{F}_p} \ker(\varphi) \leq \dim_{\mathbf{Q}} A(\mathbf{Q}) \otimes \mathbf{Q}.$$

In particular, if A has Mordell-Weil rank 0, then φ is injective.

Let A be the 20 dimensional quotient of $J_0(389)$ attached to a newform and B the elliptic curve quotient of $J_0(389)$. We use MAGMA to verify the hypothesis of Theorem 6.1 for $J = A^\vee + B^\vee \subset J_0(389)$ with $p = 5$, and hence deduce that $B(\mathbf{Q})/5B(\mathbf{Q}) = (\mathbf{Z}/5\mathbf{Z}) \times (\mathbf{Z}/5\mathbf{Z})$ injects into $Ш(A)$.

Since A and B are quotients of $J_0(389)$, we have $N = 389$. Next we construct the corresponding spaces A and B of modular symbols.

```
M := ModularSymbols(389);
N := NewSubspace(CuspidalSubspace(M));
D := SortDecomposition(NewformDecomposition(N));
A := D[5]; B := D[1];
```

The command IntersectionGroup computes the group structure of the intersection of two abelian subvarieties. In our case these are the abelian varieties $A^\vee$ and $B^\vee$, and we find that $A^\vee \cap B^\vee = (\mathbf{Z}/20\mathbf{Z}) \times (\mathbf{Z}/20\mathbf{Z})$. In particular, $B^\vee[5] = (\mathbf{Z}/5\mathbf{Z}) \times (\mathbf{Z}/5\mathbf{Z})$ is contained in $A^\vee$ as abelian subvarieties of $J_0(389)$.

```
IntersectionGroup(A, B);
```

Using the TorsionBound command (see Section 9 below), we obtain a multiple of the order of the torsion subgroup of B (it is 1) and of J/B (it is 97).

```
TorsionBound(A, 7);
TorsionBound(B, 7);
```

Neither torsion subgroup has order divisible by 5, as required to apply Theorem 6.1. The reason that TorsionBound$(A, 7)$ is a multiple of the order of the torsion subgroup of J/B is because TorsionBound is an isogeny invariant and A is isogenous to J/B. (The kernel of the natural map from A to J/B is $A \cap B = (\mathbf{Z}/20\mathbf{Z}) \times (\mathbf{Z}/20\mathbf{Z})$, which is finite.)

Finally, we compute the Tamagawa numbers of A and B and obtain 97 and 1, respectively (see Section 8 below).

```
TamagawaNumber(A, 389);
TamagawaNumber(B, 389);
```

Putting everything together we see that $B(\mathbf{Q})/5B(\mathbf{Q})$ is a subgroup of $Ш(A)$. Finally, using the Rank command on the elliptic curve attached to B, we see that $B(\mathbf{Q})/5B(\mathbf{Q}) = (\mathbf{Z}/5\mathbf{Z}) \times (\mathbf{Z}/5\mathbf{Z})$.

```
E := EllipticCurve(B);
Rank(E);
```

Thus 25 divides $\#Ш(A)$, which gives evidence for Conjecture 3.2, as we will see in Section 10.

Frequently not all of $Ш(A)$ can be constructed using Theorem 6.1 and abelian subvarieties B of $J_0(N)$. One obstruction to visibility arises from a canonical homomorphism from $A^\vee$ to A. Jacobians of curves are canonically isomorphic to their dual abelian variety and the composition $A^\vee \to J_0(389)^\vee \cong J_0(389) \to A$ defines a homomorphism from $A^\vee$ to A. According to [3, §5.3], if p does not divide the kernel of $A^\vee \to A$, then no element of order p in $Ш(A)$ is visible in $J_0(N)$. The command ModularKernel computes the group structure of the kernel of $A^\vee \to A$.

```
G := ModularKernel(A);
Factorization(#G);
```

We find that the modular kernel has order $2^{24}5^2$, so any element of $Ш(A^\vee)$ that is visible in $J_0(389)$ has order divisible only by 2 and 5.

7 Computing Special Values of Modular L-function

This section is about computing the quotient $L(A_f, 1)/\Omega_{A_f}$. We discuss the Manin constant and the LRatio command.

Let $A = A_f$ for some newform f and assume that $L(A, 1) \neq 0$. We can then rewrite Conjecture 3.2 as follows:

$$\frac{L(A,1)}{\Omega_A} = \frac{\prod c_p \cdot \#Ш(A)}{\#A(\mathbf{Q})_{\mathrm{tor}} \cdot \#A^\vee(\mathbf{Q})_{\mathrm{tor}}}.$$

We do not know an algorithm, in general, to compute $L(A, 1)/\Omega_A$. However, we can compute $c_A \cdot L(A, 1)/\Omega_A$, where c_A is the Manin constant, which is defined in [1, §2.2]. We conjecture that $c_A = 1$, and prove in [1, §2.2.2] that if f is a newform on $\Gamma_0(N)$ then c_A is an integer divisible only by primes whose square divides $4N$. Moreover, if N is odd then $2^{\dim A}$ is the largest power of 2 that can divide c_A. See also [14] for results when A has dimension 1, and [9, §6.1.2] for a proof that c_A is an integer when $\Gamma_0(N)$ is replaced by $\Gamma_1(N)$.

The algorithm described in [9, §2.1.3], [2, §4] and [37, §3.10] to compute $c_A \cdot L(A,1)/\Omega_A$ is implemented in MAGMA via the LRATIO command. For example, if A is as in Section 6, then $c_A \cdot L(A,1)/\Omega_A = 2^{11} \cdot 5^2/97$.

LRATIO$(A, 1)$

8 Computing Tamagawa Numbers

In this section we discuss computing Tamagawa numbers when $p \mid\mid N$ and some bounds when $p^2 \mid N$. We also discuss issues that arise in going from the order of the component group to the Tamagawa number when $p \mid\mid N$.

Let $A = A_f$ be a modular abelian variety attached to a newform $f \in S_2(\Gamma_0(N))$. When $p \mid\mid N$, [10, §2.1] contains a computable formula for $\#\Phi_{A,p}(\overline{\mathbf{F}}_p)$ and for $c_p = \#\Phi_{A,p}(\mathbf{F}_p)$, where the latter formula is in some cases only valid up to a bounded power of 2. Also [19] is about how to compute these orders. Note that the Tamagawa number of A at p is the same as the Tamagawa number of $A^\vee$ at p.

When $p^2 \mid N$ the authors do not know an algorithm to compute c_p. However, in this case Lenstra and Oort proved in [21, Cor. 1.15] that

$$\sum_{\ell \neq p} (\ell - 1)\mathrm{ord}_\ell(\#\Phi_{A,p}(\overline{\mathbf{F}}_p)) \leq 2\dim(A_f),$$

so if $\ell \mid \#\Phi_{A,p}(\overline{\mathbf{F}}_p)$ then $\ell \leq 2 \cdot \dim(A_f) + 1$ or $\ell = p$. (Here $\mathrm{ord}_\ell(x)$ denotes the exponent of the largest power of ℓ that divides x.)

Using [10], when $p \mid\mid N$ we know how to compute the order of the component group over the algebraic closure, but not its structure as a group. The command COMPONENTGROUPORDER computes the order of $\Phi_{A,p}(\overline{\mathbf{F}}_p)$. The command TAMAGAWANUMBER computes $c_p = \#\Phi_{A,p}(\mathbf{F}_p)$ when the subgroup of elements of $\Phi_{A,p}(\overline{\mathbf{F}}_p)$ fixed by the Galois group has order that does not depend on the underlying group structure. By computing the Atkin-Lehner involution on modular symbols, we can decide whether the Galois group acts trivially or by -1 on $\Phi_{A,p}(\overline{\mathbf{F}}_p)$ since the Atkin-Lehner involution acts as the negative of the canonical generator Frobenius of $\mathrm{Gal}(\overline{\mathbf{F}}_p/\mathbf{F}_p)$. We can thus compute $\#\Phi_{A,p}(\mathbf{F}_p)$ when the Galois group acts trivially. When the Galois group acts nontrivially, $\Phi_{A,p}(\mathbf{F}_p)$ is the 2-torsion subgroup of $\Phi_{A,p}(\overline{\mathbf{F}}_p)$, whose order we know as long as 4 does not divide $\#\Phi_{A,p}(\overline{\mathbf{F}}_p)$. It is an open problem to given an algorithm to compute the group structure of $\Phi_{A,p}(\overline{\mathbf{F}}_p)$ or the order of $\Phi_{A,p}(\mathbf{F}_p)$ in general.

Section 11 contains an example of an abelian variety of dimension 18 in which the author is only able to find the Tamagawa number up to a controlled power of 2.

9 Computing the Torsion Subgroup

In this section we describe how to compute a divisor and multiple of the order of the torsion subgroup and explain how knowing a divisor of $\#A_f(\mathbf{Q})_{\rm tor}$ yields a divisor of $\#A_f^\vee(\mathbf{Q})_{\rm tor}$.

The papers [2, §3.5–3.6] and [9, §2.1.1] contain discussions of how to compute a divisor and multiple of the order of the torsion subgroup $A_f(\mathbf{Q})_{\rm tor}$ of $A_f(\mathbf{Q})$, and likewise for $A_f^\vee(\mathbf{Q})_{\rm tor}$. (The multiple of $\#A_f^\vee(\mathbf{Q})_{\rm tor}$ is the same as for $A_f(\mathbf{Q})_{\rm tor}$, and the divisor can be computed as described below.) We compute the multiple by using that $A_f(\mathbf{Q})_{\rm tor}$ injects into $A_f(\mathbf{F}_p)$ for all p not dividing $2N$, and that $\#A_f(\mathbf{F}_p)$ is fairly easy to compute, though we do not know how to compute the group structure. We compute the lower bound by considering the subgroup of elements of $J_0(N)(\mathbf{Q})_{\rm tor}$ generated by rational cusps on $X_0(N)$ (see [38, §1.3]), and taking its image in $A_f(\mathbf{Q})_{\rm tor}$ or intersecting its image with $A_f^\vee(\mathbf{Q})_{\rm tor} \subset J_0(N)(\mathbf{Q})_{\rm tor}$. Note that there is no reason for the subgroup generated by rational cusps to equal the rational subgroup of the group generated by all cusps, and one might want to compute and work with this possibly larger group instead.

Let A and B be as in Section 6, where we showed that the torsion subgroup of B is trivial and the order of $B(\mathbf{Q})$ and $B^\vee(\mathbf{Q})$ divides 97. In Section 10, we give an example in which the divisor and multiple of the order of the torsion subgroup differ by a power of 2.

```
RationalCuspidalSubgroup(A);    // subgroup of A(Q)
```

As mentioned in Section 6, there is a homomorphism $A^\vee \to A$ of degree $2^{24} \cdot 5^2$, which implies that 97 also divides $\#A_f^\vee(\mathbf{Q})_{\rm tor}$. Thus $\#A_f(\mathbf{Q})_{\rm tor} = \#A_f^\vee(\mathbf{Q})_{\rm tor} = 97$.

Remark 4. Computation of a nontrivial divisor of $\#A_f^\vee(\mathbf{Q})_{\rm tor}$ directly using rational cusps is not yet implemented in Magma, though in principle this should not be difficult to implement.

10 A Divisor and Multiple of the Order of the Shafarevich-Tate Group

In this section we substitute the values computed above into Conjecture 3.2 to obtain a conjectural divisor and multiple of the order of a Shafarevich-Tate group. We then remark that the visibility computation of Section 6 gives evidence for Conjecture 3.2. This example is also discussed in [3, §4.2].

To obtain evidence for Conjecture 3.2, we consider an abelian variety A_f with $L(A_f, 1) \neq 0$ and combine the invariants whose computation is described above with Conjecture 3.2 to obtain a conjectural divisor and multiple of the order of $Ш(A_f)$. We then observe that this divisor and multiple is consistent with Conjecture 3.2.

We now combine the computations from the previous sections for the 20 dimensional quotient A of $J_0(389)$. Recall that Conjecture 3.2 asserts that

$$\frac{L(A,1)}{\Omega_A} = \frac{\prod c_p \cdot \#Ш(A)}{\#A(\mathbf{Q})_{\mathrm{tor}} \cdot \#A^\vee(\mathbf{Q})_{\mathrm{tor}}}.$$

This equation becomes

$$\frac{2^n \cdot 2^{11} \cdot 5^2}{97} = \frac{97 \cdot \#Ш(A)}{97^2}$$

where $0 \leq n \leq 20$ (using the bound from [1, Thm. 2.7]). Thus the conjecture asserts that $\#Ш(A) = 5^2 \cdot 2^{11+n}$, and we have computed a conjectural divisor $5^2 \cdot 2^{11}$ and a conjectural multiple $5^2 \cdot 2^{31}$ of $\#Ш(A)$. Using visibility theory from Section 6 we have proved that $5^2 \mid \#Ш(A)$, which provides evidence for Conjecture 3.2.

11 An Element of the Shafarevich-Tate Group that Becomes Visible at Higher Level

We finish this paper by considering the 18-dimensional newform quotient A of $J_0(551)$. In this example, the level $551 = 19 \cdot 29$ is composite, the Shafarevich-Tate group is conjecturally nontrivial, and the methods of Section 6 do not produce nontrivial elements of the Shafarevich-Tate group at level 551.

This example is striking because it is, in some sense, the simplest known example of "visibility only at a higher level"; more precisely, the methods of Section 6 do produce a nontrivial element at the rather small level 1102. For a similar example, see [3, §4.3], where the levels involved are much larger.

We first compute the space of modular symbols corresponding to A:

```
M := ModularSymbols(551);
N := NewSubspace(CuspidalSubspace(M));
D := SortDecomposition(NewformDecomposition(N));
A := D[8];
```

Next we compute a divisor and a multiple of the order of the torsion subgroup of $A(\mathbf{Q})$ and $A^\vee(\mathbf{Q})$. Using odd primes $p \leq 7$ we obtain the multiple 160, and using the rational cuspidal subgroup we obtain the divisor 40.

```
TorsionBound(A,7);
RationalCuspidalSubgroup(A);
```

Since the divisor and multiple are different, we try more finite fields. For $p \leq 29$ the multiple we obtain is still 160; however, for $p = 31$ the multiple is 80, which is where it appears to stabilize.

```
TorsionBound(A,31);
```

We conclude that $40 \mid \#A(\mathbf{Q})_{\mathrm{tor}} \mid 80$ and $5 \mid \#A^{\vee}(\mathbf{Q})_{\mathrm{tor}} \mid 80$. We know that 5 divides $\#A^{\vee}(\mathbf{Q})_{\mathrm{tor}}$ because, as we will see below, there is a homomorphism $A^{\vee} \to A$ of degree not divisible by 5.

Next we compute the modular kernel, which is of order $2^{44} \cdot 13^4$.

```
Factorization(#ModularKernel(A));
```

The only possible elements of $Ш(A)$ that we can construct using Theorem 6.1 at level 551 are of order 13.

The level 551 is not prime, so computation of the Tamagawa numbers involves certain relatively slow algorithms (a minute rather than seconds) that involve arithmetic in quaternion algebras. Also, in this example, we are unable to determine the exact power of 2 that divides the Tamagawa number at 19.

```
TamagawaNumber(A,19);    // takes over a minute; gives an error
TamagawaNumber(A,29);
```

We find that $c_{29} = 40$. We also deduce that $c_{19} = 2$ or 4 by noting that the component group over $\overline{\mathbf{F}}_{19}$ has order $2^2 \cdot 13^2$ by using the command

```
ComponentGroupOrder(A,19);
```

and noting that the Galois generator Frobenius acts as -1 because

```
AtkinLehnerOperator(A,19)[1,1];
```

returns 1. Finally note that the 2 torsion in any group of order $2^2 \cdot 13^2$ is a subgroup of order either 2 or 4.

Next we find that $L(A,1)/\Omega_A = 2^n \cdot 2^2 \cdot 3^2/5$, with $0 \leq n \leq 18$, using the command

```
LRatio(A,1)
```

and the fact that the Manin constant divides $2^{\dim A}$ (see [1, Thm. 2.7]).

Putting these computations together we find that Conjecture 3.2 asserts that

$$\frac{2^n \cdot 2^2 \cdot 3^2}{5} = \frac{2^m \cdot 40 \cdot \#Ш(A)}{40 \cdot 2^r \cdot 5 \cdot 2^s},$$

where $0 \leq n \leq 18$, $1 \leq m \leq 2$, $0 \leq r \leq 1$, and $0 \leq s \leq 4$. Solving for $\#Ш(A)$, we see that Conjecture 3.2 predicts that

$$\#Ш(A) = 2^t \cdot 3^2$$

with $2 \leq t \leq 24$.

Theorem 6.1 does not construct elements of order 2 (yet), so we do not consider the factor 2^t further. As mentioned above, we cannot construct any elements of $Ш(A)$ of order 3 using visibility at level 551. We can, however, consider the images of A in $J_0(2 \cdot 551)$ under various natural maps. These natural maps are the degeneracy maps δ_1 and δ_2, which correspond to the maps $f(q) \mapsto f(q)$ and $f(q) \mapsto f(q^2)$ from $S_2(\Gamma_0(551))$ to $S_2(\Gamma_0(2 \cdot 551))$.

We next compute the space of modular symbols that corresponds to the sum $C = \delta_1(A)+\delta_2(A)$ of the images of A at level $2\cdot 551$ by the two degeneracy maps δ_1 and δ_2.

```
M := ModularSymbols(2*551,2);
N := NewSubspace(CuspidalSubspace(M));
D := SortDecomposition(NewformDecomposition(N));
M551 := ModularSymbols(M,551);
N551 := NewSubspace(CuspidalSubspace(M551));
D551 := SortDecomposition(NewformDecomposition(N551));
A551 := D551[#D551];
C := M !! A551;    // sum of images under degeneracy maps
```

The sum C contains the 3-torsion of the rank 2 elliptic curve B defined by $y^2 + xy = x^3 + x^2 - 29x + 61$, as the following computation shows.

```
IntersectionGroup(C,D[1]);
B := EllipticCurve(D[1]); B;
```

It follows that $B[3]$ is contained in C. The following computation shows that the Tamagawa numbers of B are 2, 2, and 1 and $B(\mathbf{Q}) \equiv \mathbf{Z} \times \mathbf{Z}$:

```
TamagawaNumber(B,2);
TamagawaNumber(B,19);
TamagawaNumber(B,29);
MordellWeilGroup(B);
```

Theorem 6.1 implies that $B(\mathbf{Q})/3B(\mathbf{Q}) = \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$ is a subgroup of Ш(C). By [26, §2], there is an isogeny φ from $A \times A$ to C whose kernel is isomorphic to the intersection of A with the Shimura subgroup of $J_0(551)$. The Shimura subgroup Σ is a subgroup of $J_0(N)$ that, according to [26, Prop. 2], is annihilated by $T_p - (p+1)$ for all primes $p \nmid 551$. Using MAGMA we find that $3 \nmid \det(T_3|_A - 4) = 12625812402998886400$, so the degree of φ is coprime to 3.

```
T3 := HeckeOperator(A,3);
d := Determinant(T3-4);
Valuation(d,3);
```

Since $3 \mid \#$Ш(C) it follows that $3 \mid \#$Ш(A). By [2, §5.3] the power of 3 that divides $\#$Ш(A) is even, so $9 \mid \#$Ш(A), as predicted by the Birch and Swinnerton-Dyer conjecture.

12 Complete MAGMA Log

This is a complete log of using MAGMA V2.10-6 to do all of the computations discussed in this paper. The output has been edited slightly to save space.

```
> M := ModularSymbols(389);
> Basis(M);
[
    {-1/337, 0},{-1/237, 0},{-1/342, 0},{-1/266, 0},{-1/170, 0},
    {-1/272, 0},{-1/333, 0},{-1/355, 0},{-1/270, 0},{-1/301, 0},
    {-1/293, 0},{-1/87, 0},{-1/306, 0},{-1/205, 0},{-1/209, 0},
    {-1/277, 0},{-1/383, 0},{-1/142, 0},{-1/178, 0},{-1/116, 0},
    {-1/61, 0},{-1/127, 0},{-1/235, 0},{-1/240, 0},{-1/93, 0},
    {-1/121, 0},{-1/221, 0},{-1/199, 0},{-1/213, 0},{-1/370, 0},
    {-1/282, 0},{-1/379, 0},{-1/100, 0},{-1/286, 0},{-1/165, 0},
    {-1/158, 0},{-1/376, 0},{-1/228, 0},{-1/125, 0},{-1/72, 0},
    {-1/374, 0},{-1/140, 0},{-1/81, 0},{-1/186, 0},{-1/53, 0},
    {-1/37, 0},{-1/175, 0},{-1/108, 0},{-1/183, 0},{-1/316, 0},
    {-1/363, 0},{-1/250, 0},{-1/359, 0},{-1/162, 0},{-1/106, 0},
    {-1/350, 0},{-1/216, 0},{-1/243, 0},{-1/111, 0},{-1/324, 0},
    {-1/311, 0},{-1/97, 0},{-1/259, 0},{-1/194, 0},{oo, 0}
]
> M ! <1, [Cusps() | -1/337, Infinity()]>;
{-1/337, 0} + -1*{oo, 0}
> S := CuspForms(389);
> SetPrecision(S,40);
> Basis(S);
[
    q + 474049571*q^32 + 480335856*q^33 + 984946270*q^34 +
    1338756227*q^35 + 1246938503*q^36 - 29119245*q^37 +
    1504020580*q^38 - 2463550751*q^39 + O(q^40),
    ...
]
```

```
> M := ModularSymbols(389);
> N := NewSubspace(CuspidalSubspace(M));
> NewformDecomposition(N);
[
    Modular symbols space for Gamma_0(389) of weight 2 and
    dimension 2 over Rational Field,
    Modular symbols space for Gamma_0(389) of weight 2 and
    dimension 4 over Rational Field,
    Modular symbols space for Gamma_0(389) of weight 2 and
    dimension 6 over Rational Field,
    Modular symbols space for Gamma_0(389) of weight 2 and
    dimension 12 over Rational Field,
    Modular symbols space for Gamma_0(389) of weight 2 and
    dimension 40 over Rational Field ]
```

```
> M := ModularSymbols(389,2,+1);
```

```
> M := ModularSymbols(389);
> N := NewSubspace(CuspidalSubspace(M));
> D := NewformDecomposition(N);
```

```
> A := D[5]; B := D[1];
> IntersectionGroup(A,B);
Abelian Group isomorphic to Z/20 + Z/20
> TorsionBound(A,7);
97
> TorsionBound(B,7);
1
> TamagawaNumber(A,389);
97
> TamagawaNumber(B,389);
1
> E := EllipticCurve(B);
> Rank(E);
2
> G := ModularKernel(A);
Abelian Group isomorphic to Z/2 + Z/2 + Z/2 + Z/2 + Z/2 + Z/2 +
Z/2 + Z/2 + Z/2 + Z/2 + Z/2 + Z/2 + Z/2 + Z/2 + Z/2 + Z/2 + Z/2 +
Z/2 + Z/40 + Z/40
> Factorization(#G);
[ <2, 24>, <5, 2> ]
> LRatio(A,1);
51200/97
> RationalCuspidalSubgroup(A);
Abelian Group isomorphic to Z/97
> M := ModularSymbols(551);
> N := NewSubspace(CuspidalSubspace(M));
> D := NewformDecomposition(N);
> A := D[8];
> TorsionBound(A,7);
160
> RationalCuspidalSubgroup(A);
Abelian Group isomorphic to Z/2 + Z/20
> TorsionBound(A,31);
80
> Factorization(#ModularKernel(A));
[ <2, 44>, <13, 4> ]
> TamagawaNumber(A,19);
No algorithm known to compute the Tamagawa number at 2. Use
ComponentGroupOrder instead.
> TamagawaNumber(A,29);
40
> ComponentGroupOrder(A,19);
676
> AtkinLehnerOperator(A,19)[1,1];
1
> LRatio(A,1);
36/5
> M := ModularSymbols(2*551,2);
> N := NewSubspace(CuspidalSubspace(M));
```

```
> D := SortDecomposition(NewformDecomposition(N));
> M551 := ModularSymbols(M,551);
> N551 := NewSubspace(CuspidalSubspace(M551));
> D551 := NewformDecomposition(N551);
> A551 := D551[#D551];
> C := M!!A551;
> IntersectionGroup(C,D[1]);
Abelian Group isomorphic to Z/32 + Z/32
> B := EllipticCurve(D[1]); B;
Elliptic Curve defined by y^2 + x*y = x^3 + x^2 - 29*x + 61
> TamagawaNumber(B,2);
2
> TamagawaNumber(B,19);
2
> TamagawaNumber(B,29);
1
> MordellWeilGroup(B);
Abelian Group isomorphic to Z + Z
> MordellWeilGroup(B);
Abelian Group isomorphic to Z + Z
> T3 := HeckeOperator(A,3);
> d := Determinant(T3-4);
> Valuation(d,3);
0
```

References

1. A. Agashe and W. A. Stein. The manin constant, congruence primes, and the modular degree. *Submitted*.
2. A. Agashe and W. A. Stein. Visible Evidence for the Birch and Swinnerton-Dyer Conjecture for Modular Abelian Varieties of Analytic Rank 0. *To appear in Mathematics of Computation*.
3. A. Agashe and W. A. Stein. Visibility of Shafarevich-Tate groups of abelian varieties. *J. Number Theory*, 97(1):171–185, 2002.
4. A. O. L. Atkin and J. Lehner. Hecke operators on $\Gamma_0(m)$. *Math. Ann.*, 185:134–160, 1970.
5. B. J. Birch. Conjectures concerning elliptic curves. In *Proceedings of Symposia in Pure Mathematics, VIII*, pages 106–112. Amer. Math. Soc., Providence, R.I., 1965.
6. S. Bosch, W. Lütkebohmert, and M. Raynaud. *Néron models*. Springer-Verlag, Berlin, 1990.
7. C. Breuil, B. Conrad, F. Diamond, and R. Taylor. On the modularity of elliptic curves over $\mathbf{Q}$: wild 3-adic exercises. *J. Amer. Math. Soc.*, 14(4):843–939 (electronic), 2001.
8. J. W. S. Cassels. Diophantine equations with special reference to elliptic curves. *J. London Math. Soc.*, 41:193–291, 1966.
9. B. Conrad, S. Edixhoven, and W. A. Stein. $J_1(p)$ Has Connected Fibers. *To appear in Documenta Mathematica*, 2003.

10. B. Conrad and W. A. Stein. Component Groups of Purely Toric Quotients. *To appear in Math Research Letters*, 2002.
11. J. E. Cremona. Modular symbols for $\Gamma_1(N)$ and elliptic curves with everywhere good reduction. *Math. Proc. Cambridge Philos. Soc.*, 111(2):199–218, 1992.
12. J. E. Cremona. *Algorithms for modular elliptic curves.* Cambridge University Press, Cambridge, second edition, 1997.
13. F. Diamond and J. Im. Modular forms and modular curves. In *Seminar on Fermat's Last Theorem*, pages 39–133. Providence, RI, 1995.
14. B. Edixhoven. On the Manin constants of modular elliptic curves. In *Arithmetic Algebraic Geometry*, pages 25–39 (G. van der Geer, F. Oort et al., eds.), Basel: Birkhäuser, Progress in Mathematics Volume 89, 1991.
15. 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. *Math. Comp.*, 70(236):1675–1697 (electronic), 2001.
16. B. Gross and D. Zagier. Heegner points and derivatives of L-series. *Invent. Math.*, 84(2):225–320, 1986.
17. Clay Mathematics Institute. Millennium prize problems, `http://www.claymath.org/millennium_prize_problems/`.
18. K. Kato. p-adic Hodge theory and values of zeta functions of modular forms. *Preprint*, page 244 pages.
19. D. R. Kohel and W. A. Stein. Component Groups of Quotients of $J_0(N)$. In *Proceedings of the 4th International Symposium (ANTS-IV), Leiden, Netherlands, July 2–7, 2000*, Berlin, 2000. Springer.
20. 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(5):171–196, 1989.
21. H. W. Lenstra, Jr. and F. Oort. Abelian varieties having purely additive reduction. *J. Pure Appl. Algebra*, 36(3):281–298, 1985.
22. W-C. Li. Newforms and functional equations. *Math. Ann.*, 212:285–315, 1975.
23. J. I. Manin. Parabolic points and zeta functions of modular curves. *Izv. Akad. Nauk SSSR Ser. Mat.*, 36:19–66, 1972.
24. A. Néron. Modèles minimaux des variétés abéliennes sur les corps locaux et globaux. *Inst. Hautes Études Sci. Publ.Math. No.*, 21:128, 1964.
25. K. A. Ribet. On modular representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms. *Invent. Math.*, 100(2):431–476, 1990.
26. K. A. Ribet. Raising the levels of modular representations. In *Séminaire de Théorie des Nombres, Paris 1987–88*, pages 259–271. Birkhäuser Boston, Boston, MA, 1990.
27. K. A. Ribet. Abelian varieties over $\mathbf{Q}$ and modular forms. In *Algebra and topology 1992 (Taejŏn)*, pages 53–79. Korea Adv. Inst. Sci. Tech., Taejŏn, 1992.
28. K. A. Ribet and W. A. Stein. Lectures on Serre's conjectures. In *Arithmetic algebraic geometry (Park City, UT, 1999)*, volume 9 of *IAS/Park City Math. Ser.*, pages 143–232. Amer. Math. Soc., Providence, RI, 2001.
29. J-P. Serre. Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. *Duke Math. J.*, 54(1):179–230, 1987.
30. I. R. Shafarevich. Exponents of elliptic curves. *Dokl. Akad. Nauk SSSR (N.S.)*, 114:714–716, 1957.
31. G. Shimura. On the factors of the jacobian variety of a modular function field. *J. Math. Soc. Japan*, 25(3):523–544, 1973.

32. 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.
33. J. H. Silverman. *The arithmetic of elliptic curves.* Springer-Verlag, New York, 1992. Corrected reprint of the 1986 original.
34. J. H. Silverman and J. Tate. *Rational points on elliptic curves.* Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1992.
35. W. A. Stein. An introduction to computing modular forms using modular symbols. *To appear in an MSRI Proceedings.*
36. W. A. Stein. Shafarevich-Tate groups of nonsquare order. *Proceedings of MCAV 2002, Progress of Mathematics (to appear).*
37. W. A. Stein. Explicit approaches to modular abelian varieties. *Ph.D. thesis, University of California, Berkeley*, 2000.
38. G. Stevens. *Arithmetic on modular curves.* Birkhäuser Boston Inc., Boston, Mass., 1982.
39. J. Tate. On the conjectures of Birch and Swinnerton-Dyer and a geometric analog. In *Séminaire Bourbaki, Vol. 9*, pages Exp. No. 306, 415–440. Soc. Math. France, Paris, 1995.
40. R. Taylor and A. J. Wiles. Ring-theoretic properties of certain Hecke algebras. *Ann. of Math. (2)*, 141(3):553–572, 1995.
41. A. J. Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995.