Visualizing elements in the Shafarevich-Tate group

J. E. Cremona and B. Mazur

To Bryan Birch

Introduction. Two basic arithmetic invariants of an elliptic curve E over a number field K are:

the *Mordell-Weil group* $E(K)$ – whose elements are the K-rational points of E,

and

the *Shafarevich-Tate group* $Ш(E/K)$ – whose elements are defined to be isomorphism classes of pairs (T, ι) where T is a smooth projective curve of genus 1 over K possessing a K_v-rational point for every place v of K (where K_v is the completion of K at v), and where $\iota : E \to \mathrm{jac}\, T$ is an isomorphism over K between E and the jacobian of T.

As is well known, $E(K)$ and $Ш(E/K)$ are somehow linked in the sense that it is often easier to come by information about the *Selmer group* of E over K which is built out of both $E(K)$ and $Ш(E/K)$ than it is to get information about either of these groups separately. It occurred to us that, although these two groups (Mordell-Weil and Ш) are partners, so to speak, in the arithmetic analysis of the elliptic curve E, there seems to be a slight discrepancy in their treatment in the existent mathematical literature, for this literature does a much more thorough job of helping one (at least in specific instances) to compute rational points, i.e., to exhibit elements of Mordell-Weil, than it does in helping one to find (in an explicit way) the curves of genus one which represent elements of Ш (especially if one is interested in elements of Ш of order > 2). This is perhaps understandable in that it is usually quite clear how to present a rational point (e.g., if E is given in Weierstrass form, giving just its x-coordinate determines the rational point up to sign) but it is less clear what manner one should choose to exhibit the curves of genus 1 representing the elements of Ш. Of course (for a fixed integer n) an element in Ш annihilated by multiplication by n can always be obtained by push-out, starting with an appropriate 1-cocycle on the Galois group $G_K = \mathrm{Gal}(\overline{K}/K)$ with coefficients in the finite Galois module $E[n] \subset E$, the kernel of multiplication by n in E, (the 1-cocycle being unramified outside the primes dividing n and the places of bad reduction for E) and so therefore, there is indeed, a "finitistic" way of representing these elements of Ш. Our aim here is rather to develop strategies that might enable us to "visualize" the underlying curves more concretely. There are, for example, two standard ways of representing elements of Ш, both of which we will briefly review below, and we will also suggest a third (where the curves of genus 1 in question are sought as subcurves of abelian varieties). It is this third mode of visualizing elements of the Shafarevich-Tate group together with data regarding it (See Tables 1 and 2 below) that is the principal theme of our article.

The data we tabulate strikes us as surprising, and as deserving of some explanation. However, we have *no* hypothesis to offer that would explain it, and therefore our article is not genuinely experimental in the classical sense (despite the name of the journal in which it appears), since experiments are usually expected to be the testing-grounds of explicitly articulated hypotheses.

Explicit equations for curves of genus 1 and for their jacobians, together with results regarding visibility and related matters are to be the subject of a Winter School at the University of Arizona in March 1999. See `http://www.math.arizona.edu/~swcenter/aws99/` for more details.

We are deeply grateful to A. Agashé, N. Elkies, J. de Jong, A. Logan, L. Merel, W. McCallum, C. O'Neil, N. Shepherd-Baron, and R. Taylor for comments, computations, explanations of the classical literature, and conversation, regarding this topic.

Finally, both authors would like to extend their warmest best wishes in his retirement year to Bryan Birch, to whom they owe so much.

1. Elements of Ш(E/K) represented as étale coverings of E.

Let n be a positive integer. Given T a curve of genus 1 over K with a specific identification of its jacobian with E, there is a natural action of E on T which allows us to view T as a *principal homogeneous space* (equivalent terminology: *torsor*) for E over K. If T represents an element of order n in Ш(E/K) (or more generally, an element of the "Weil-Châtelet" group $\mathrm{WC}(E/K) \cong H^1(G_K, E)$, of isomorphism classes of E-torsors over K) the quotient of T under the action of the finite subgroup $E[n] \subset E$ has a K-rational point, and is therefore K-isomorphic to E. That is, we may view T as an étale finite covering of E, of degree n^2.

2. Elements of Ш(E/K) represented as curves of degree n in projective $(n-1)$-space.

Now let us give ourselves T, a curve of genus 1 over K, with an identification of its jacobian with E, representing an element σ of order $n > 1$ in Ш(E/K), and note that for any integer $k \in \mathbf{Z}$ the curve $T^k := \mathrm{Pic}^k(T)$ of linear equivalence classes of divisors of degree k on T is again a torsor for E over K representing the element $k \cdot \sigma \in$ Ш(E/K). In particular, since $T^n \cong E$ (over K) we see that there exists a linear equivalence class of divisors of degree n on T which is K-rational. Choose such a K-rational divisor class $\mathcal{D}$, and consider the (Chow) variety V (over K) consisting of divisors on T which are in the linear equivalence class $\mathcal{D}$. Over $\overline{K}$ the variety V is a projective space, and V is therefore a (Brauer-Severi) twist of projective space over K. But since $\sigma \in$ Ш(E/K), it follows that V has a K_v-rational point for all completions K_v of K and therefore, by Global Class Field Theory (more specifically, by the Hasse Principle for Brauer-Severi varieties) V has a K-rational point; i.e., there is a K-rational divisor on T of degree n. Choose such a divisor D, and consider the mapping (of degree n) r_D of T to the $(n-1)$-dimensional projective space $\mathbf{P}^{n-1} := \mathbf{P}(H^0(T, \mathcal{O}(D)))$, defined (over K) by the linear system of D. This representation of T is independent of the rational divisor D chosen, in the sense that given another choice, D', the representation $r_{D'}$ may be obtained from r_D by composition of appropriate K-isomorphisms of domain and range. We might remark that this method of representing elements of Ш, in contrast with the first method we described, works as formulated specifically for elements of the Shafarevich-Tate group but if one were to try to extend it to a method of describing curves T representing elements of order n in the larger Weil-Châtelet group one would be required, in general, to replace the ambient projective $(n-1)$-space by an appropriate Brauer-Severi variety of dimension $n-1$ over K.

Returning to the case at hand, i.e., representing elements of Ш, when $n=2$ the above method represents T as double cover of $\mathbf{P}^1$. When $n \geq 3$ we get T as a curve, defined over K, of degree n in $\mathbf{P}^{n-1}$. In particular, when $n=3$, T is represented, in this way, as a plane cubic. There is a large body of classical literature (but, nevertheless, many still-open problems) regarding this case and the case $n=4$; we will review some of this literature below. When $n=4$, T is represented as a curve of degree 4 in $\mathbf{P}^3$ which is also the subject of significant classical work (the legacy of Jacobi). Also in more recent times, the legacy of Jacobi has been expressed in terms of the theory of theta functions via the Heisenberg representation [Mum]. If appropriately developed, this approach might yield, we believe, a fine format for presenting the equations of curves of degree n in $\mathbf{P}^{n-1}$ representing elements of Ш.

The case $n=3$. By the **height** of a plane cubic over K (i.e., a cubic in the standard projective plane, given with homogeneous coordinates X_0, X_1, X_2) let us mean the logarithmic height of the point in projective 9-space of the (ten) homogeneous coordinates of the defining equation of the cubic. To get a notion of height which is independent of the coordinatization of the projective plane, call the **minimal height** of a plane cubic over K the greatest lower bound of these heights under projective general linear changes of the homogeneous coordinates X_0, X_1, X_2 defined over K; to actually compute this minimal height would involve understanding the classical reduction theory regarding the symmetric cube representation of GL_3, and implementing algorithms for it. But given this, we then have a well-defined notion of the **minimal height** $h(\sigma)$ of an element σ of order 3 in Ш(E/K): one defines $h(\sigma)$ to be the minimal height of a plane cubic representing σ.

Problem. When $K=\mathbf{Q}$, find an upper bound as a function of $N = \mathrm{conductor}(E)$ for the minimal heights of all elements of order 3 in Ш$(E/\mathbf{Q})$.

Some literature and current work on the subject of explicit representation of curves of genus 1 and their jacobians. In search of explicit formulas, there are two directions in which it is important to go. One can start with a curve of genus 1, given by an equation, or a system of equations, and ask for the equation(s) of its jacobian. Or, and this is the more specific thrust of this article, one can try go the other way: given an elliptic curve, and a Selmer class, find the explicit equations of the curve of genus 1 representing that class. There is a wealth of material which goes in the first direction (e.g., typical of such is the result of Cassels about plane diagonal cubics: for nonzero constants a, b, c in a field of characteristic different from 3, the plane cubic curve whose equation is $aX^3 + bY^3 + cZ^3 = 0$ has jacobian isomorphic to the locus of zeroes of $X^3 + Y^3 + abcZ^3$). For the jacobian of curves of genus 1 where the curves are of order n in their Weil-Châtelet groups and for the equations of the n-fold map to the jacobian, see [W] or [Cr2] for $n=2$, [Sa1] for $n=3$, and, when $n=4$ and we have given the curve in question as an intersection of two quadrics in $\mathbf{P}^3$, see [Sa 2] or [MSS]. For the formulas for the jacobians of curves of genus 1 given as hypersurfaces of bihomogenous degree $(2,2)$ in $\mathbf{P}^1 \times \mathbf{P}^1$ see the Harvard

Ph.D. thesis (presently being written) of Catherine O'Neil who has found families $\mathcal{C}_2, \mathcal{C}_3$, and $\mathcal{C}_5$ of curves of genus one in $\mathbf{P}^1 \times \mathbf{P}^1, \mathbf{P}^2$, and $\mathbf{P}^4$ respectively such that (1) A map $\mathcal{C}_i \longrightarrow \mathrm{jac}(\mathcal{C}_i)$ is explicitly written as a linear automorphism of the ambient projective space, and (2) every curve of genus one over a field F of characteristic 0 embeddable over F in one of the projective or multi-projective spaces above, and whose jacobian has a subgroup of i-torsion isomorphic (over F) to μ_i is a member of $\mathcal{C}_i$.

The general formula in the cases $n \leq 4$ is the subject of a paper [A-H-K-K-M-M-P] being presently written by McCallum, Minhyong Kim and some of the graduate students at the University of Arizona (Sang Yook An, Susan Hammond, Seog Young Kim, David Marshall, and Alex Perlis).

For $n = 5$, as Nicholas Shepherd-Baron pointed out to one of us, the equations for a smooth curve of genus 1 of degree 5 in $\mathbf{P}^4$ can be given as the determinants of minors of a 5×5 Pfaffian matrix. The search for elliptic curves over $\mathbf{Q}$ with large 5-Selmer group is the subject of current work being done by Tom Fisher, a student of Shepherd-Baron, who does this by writing down genus 1 curves of degree 5 in $\mathbf{P}^4$, with an action of μ_5, the corresponding jacobians being the quotients of these by μ_5.

There are fewer results of an explicit nature going the "other way". Available numerical data (e.g., listings of equations of minimal height representing the elements of order 3 in the Shafarevich-Tate groups of elliptic curves of low conductor) is still fragmentary at best.

3. Elements of Ш(E/K) represented as curves in abelian varieties.

Let σ be an element in $\mathrm{WC}(E/K) \cong H^1(G_K, E)$, the Weil-Châtelet group of isomorphism classes of torsors for E over K. Suppose that we are given an embedding over K of E into an abelian variety J. Form the exact sequence of abelian varieties

$$(*) \qquad 0 \to E \to J \to B \to 0.$$

Definition. Let us say that σ is **visible** in J if σ is in the kernel of the natural homomorphism

$$\mathrm{WC}(E/K) \to \mathrm{WC}(J/K).$$

Remark 1. The element σ is visible in J if and only if there is an element $\beta \in B(K)$ such that σ is represented by a curve T of genus 1 defined over K contained in the variety J and such that T is the inverse image of the point $\beta \in B$ under the projection $J \to B$. Equivalently, T is a translation of E by a point $P \in J(\overline{K})$, the point P projecting to β under the natural mapping $J \to B$. Thus

$$T := E + P \subset J.$$

(Of course, if $\sigma \neq 0$, the point P is not rational over K despite the fact that the translate $E + P$ is defined over K.)

Proof. This follows immediately upon consideration of the exact sequence **(*)** and the induced long exact sequence of G_K-cohomology:

$$J(K) \to B(K) \to H^1(G_K, E) \to H^1(G_K, J).$$

Definition. If the above situation occurs, we shall say that the element σ is **explained by** the element $\beta \in B(K)$ of the Mordell-Weil group of B, noting that the element β playing the role required in the statement of the theorem is uniquely determined modulo the image of $J(K)$ in $B(K)$.

Since the curve T representing σ is the inverse image of an element $\beta \in B(K)$ explaining σ, the size of the coefficients of the equations for T, as, say, a curve in some projective space, is bounded by data coming from a choice of projective embedding of J, the nature of the projection mapping $J \to B$, and, finally, the height of the point β.

Remark 2. Suppose that our elliptic curve E does not have complex multiplication by $\sqrt{-1}$ or $\sqrt{-3}$, and we have an embedding of E into an abelian variety J (over K) such that there are no nontrivial homomorphisms of E to $B = J/E$ over $\overline{K}$. Then an element $\sigma \in \mathrm{WC}(E/K)$ is visible in J if and only if the curve T of genus 1 (over K) representing σ is isomorphic over K to a curve contained in the variety J.

Proof. By Remark 1, if σ is visible in J, then T occurs as a subvariety (in fact, it is a translate of E) in J. Suppose that T is isomorphic to a subvariety $T' \subset J$. The projection $J \to B$ must be constant when restricted to T', for T' is isomorphic over $\overline{K}$ to E and, by assumption, there are no nonconstant maps from E to B over $\overline{K}$. So T' is a translate of E. We must show that the structure that T' inherits from T as torsor over E coincides, up to sign, with the E-torsor structure on T' given by addition (in J). But by our assumption on E, we have that the only automorphisms of E are the scalar multiplications by ± 1, and therefore, up to sign, there is only one E-torsor structure on T', which concludes the proof of this remark.

Remark 3. As Johan de Jong explained to one of us (in the Castle pub on Castle Hill in Cambridge, England), for any element $\sigma \in \mathrm{WC}(E/K)$ there is some abelian variety J over K containing E as abelian subvariety, such that σ is visible in J. One can see this as follows. Let n be the order of σ, and represent σ as an Azumaya algebra $\mathcal{A}_F$ of rank n^2 over the field F of rational functions on the K-variety E. There is a maximal commutative sub-algebra L in $\mathcal{A}$ of rank n over F such that, if $\pi : C \to E$ is the mapping of degree n of projective smooth curves associated to the field extension L/F, then π is totally ramified at (at least) one point of E. It follows that the associated morphism of jacobians $E = J_E \to J_C$ is injective. Moreover, by construction, the induced Azumaya algebra $\mathcal{A}_L = \mathcal{A}_F \otimes_F L$ splits; i.e. σ is visible in J_C. Here are the details:

Proposition. Let K be a number field, E an elliptic curve over K and $\sigma \in \mathrm{WC}(E/K)$. Then there is some abelian variety J over K containing E as abelian subvariety, such that σ is visible in J.

Proof. Consider the natural homomorphism

$$H^1(K,E) \to \coprod_v H^1(K_v,E)$$

where v runs through all non-archimedean places of K, and where K_v is the completion of K at v. Let $\mathcal{V}$ denote the finite set of these places which have the property that the element $\sigma \in H^1(K,E)$ does *not* go to zero under the mapping $H^1(K,E) \to H^1(K_v,E)$. To have a nice geometric model to work with, let $\mathcal{O} = \mathcal{O}_K[1/m] \subset K$ be a Dedekind subdomain of the ring of integers $\mathcal{O}_K$ of K where we have inverted the non-zero integer m; the integer m is assumed to be divisible by all primes of bad reduction for E and by the residual characteristics of all $v \in \mathcal{V}$ and by the order of σ. It follows that the cohomology class σ comes by restriction from a class (which we denote by the same letter) $\sigma \in H^1(\text{Spec } \mathcal{O}, \mathcal{E})$, where $f : \mathcal{E} \to \text{Spec } \mathcal{O}$ is the Néron model of E/K over the base Spec $\mathcal{O}$, and the cohomology in question is étale cohomology. Alternatively, we may view σ as an element of the kernel of

$$H^1(K,E) \to \coprod_{v \neq \mathcal{V}} H^1(K_v,E);$$

i.e., the group denoted Ш (V,A) in section 3 of [T] for $V = \mathcal{O}$ and $A = \mathcal{E}$. We may apply Theorem 3.1 of [T] to the proper morphism $f : \mathcal{E} \to \text{Spec } \mathcal{O}$ (its fibers are of dimension 1 and $\mathcal{E}$ is regular of dimension 2) to get the exact sequence

$$0 \to \text{Br (Spec } (\mathcal{O})) \to \text{Br } (\mathcal{E}) \to Ш\ (\mathcal{O}, \mathcal{E}) \to 0.$$

By surjectivity of Br $(\mathcal{E}) \to$ Ш $(\mathcal{E})$, we may (and do) choose an element ξ in the Brauer group of $\mathcal{E}$ which projects to σ. We now "shrink" Spec $(\mathcal{O})$ further, so as to guarantee that the order (call it N) of the element ξ is not divisible by any of the residual characteristics of Spec $(\mathcal{O})$, and therefore ξ is the image of some element $\eta \in H^2(\mathcal{E}, \mu_N)$ under the mapping

$$H^2(\mathcal{E}, \mu_N) \to H^2(\mathcal{E}, \mathbf{G}_m) = \text{Br } (\mathcal{E}).$$

Now let us modify our choice of lifting ξ. Let $\hat{\mathcal{E}}$ denote the completion of (the abelian scheme) $\mathcal{E}$ along its zero-section, and let

$$z : \text{Spec } (\mathcal{O}) \hookrightarrow \hat{\mathcal{E}}$$

denote that zero-section. Let $\hat{\eta} \in H^2(\hat{\mathcal{E}}, \mu_N)$ be the pullback of the cohomology class η to $\hat{\mathcal{E}}$. The morphism z above induces an isomorphism on étale cohomology,

$$z : H^2(\hat{\mathcal{E}}, \mu_N) \cong H^2(\text{Spec } (\mathcal{O}), \mu_N),$$

and let let us denote by $\eta_o \in H^2(\text{Spec } (\mathcal{O}), \mu_N)$ the image of $\hat{\eta}$ under the isomorphism z. Let $\xi_o \in H^2(\text{Spec } (\mathcal{O}), \mathbf{G}_m) = \text{Br(Spec } (\mathcal{O}))$ be the image of η_o under the mapping $H^2(\text{Spec } (\mathcal{O}), \mu_N) \to H^2(\text{Spec } (\mathcal{O}), \mathbf{G}_m)$. Put

$$\xi' := \xi - (\text{ the image of } \xi_o \text{ in Br}(\mathcal{E})).$$

Then ξ' is also a lifting of σ, but has the added property that its pullback to Br $(\hat{\mathcal{E}})$ vanishes. Let n denote its order, and let $\mathcal{A}_{\mathcal{E}}$ denote an Azumaya algebra of rank n^2 over $\mathcal{E}$ representing ξ'. Such an Azumaya algebra exists by Corollary 2.2 of [Groth]. Moreover, the Azumaya algebra $\mathcal{A}_{\hat{\mathcal{E}}}$ is a "trivial" Azumaya algebra over $\hat{\mathcal{E}}$.

We now retract to the associated function fields: let F denote the field of rational functions on the K-variety E which we view as a discretely valued field, with the valuation given by the order of zero (or pole) at the origin of the elliptic curve E. Let F_o denote the completion of F with respect to this valuation. Thus, $F_o \cong K((t))$ is isomorphic to the field of Laurent power series in a uniformizer t. Let $\mathcal{A}_F$ be the central simple algebra (of rank n^2) over F which is obtained by change of scalars from the Azumaya algebra $\mathcal{A}_{\hat{\mathcal{E}}}$. We have that the central simple algebra $\mathcal{A}_{F_o}$ obtained from $\mathcal{A}_F$ by base change is trivial; i.e. is a total matrix algebra $\mathrm{Mat}_n(F_o)$ of all $n \times n$ matrices with entries in $F_o \cong K((t)))$. Here is how we may view this total matrix algebra. Identifying F_o with $K((t))$, let L_o/F_o be the totally ramified extension of degree n given by $L_o := K((s))$ where $s^n = t$; i.e., $L_o := K((t^{1/n}))$. Viewing L_o as (n-dimensional) vector space over F_o, we may find an isomorphism, then, between F_o-algebras:

$$\mathcal{A}_{F_o} \cong \mathrm{End}_{F_o}\ (L_o) \cong \mathrm{Mat}_n(F_o),$$

and since L_o is a maximal commutative algebra (of rank n) in $\mathrm{End}_{F_o}\ (L_o)$, its action on the F_o-vector space given by multiplication, so we have an imbedding of L_o into $\mathcal{A}_{F_o}$.

Our next task is to approximate the uniformizer

$$s \in L_o \subset \mathcal{A}_{F_o}$$

by an element $s' \in \mathcal{A}_F$. Since $\mathcal{A}_F$ is dense in the topological vector space $\mathcal{A}_{F_o}$, given any positive integer ν, we can find such an element s' with the property that

$$s' - s = t^\nu \cdot w \in \mathcal{A}_{F_o} \cong \mathrm{Mat}_n(K((t))),$$

where $w \in \mathrm{Mat}_n(K[[t]])$. If ν is taken large enough, we get that the characteristic polynomial for the action of s' is a monic polynomial of degree n which is congruent modulo a high power of t to the polynomial $X^n - t$, and therefore s' generates a maximal commutative subfield L of $\mathcal{A}_F$ (an extension of F of degree n) which is totally ramified over F_o.

We now have only to repeat the brief sketch given immediately before the statement of this proposition. Namely, let C be the smooth projective curve whose field of rational functions is L (i.e., the normalization of L over the K-scheme E) and note that since the natural projection mapping $C \to E$ is totally ramified at the origin in E, it induces an injection on jacobians $0 \to E \to J := \mathrm{jac}(C)$ and, moreover we see, by the construction of C, that the Azumaya algebra $\mathcal{A}$ splits when pulled back to C. That is, σ is visible in $J = \mathrm{jac}(C)$. ■

This construction, however, does not allow us easy viewing of the curves of genus 1 that are generated. To get a sharper image we are led to imposing very strong restrictions on the types of abelian varieties J that we wish to use, to visualize torsors over elliptic curves. For the rest of this article, we concentrate in the question of visualizing elements of Ш rather than the corresponding more general question for arbitrary E-torsors. Moreover, we will be interested in five special situations.

1. The field $K = \mathbf{Q}$, the elliptic curve E a abelian subvariety of $J_0(N) := \mathrm{jac}(X_0(N))$ the jacobian of the modular curve $X_0(N)$ for some level N, and we want to know which elements of $Ш(E/\mathbf{Q})$ are visible in $J_0(N)$.

2. We are over any number field K and we want the elements of Ш visible in abelian surfaces.

3. Same as **1** above, but considering only elliptic curves $E \subset J_0(N)$ where N is specifically the conductor of E, and we want to know the elements of Ш visible in $J_0(N)$.

4. The combination of **1,2, 3** above. That is, we are over $K = \mathbf{Q}$ and are seeking elements of Ш visible in abelian surfaces contained in $J_0(N)$ where N is the conductor of E.

5. As in **4** above, but with one more specific requirement. We are dealing, as in **4** with elliptic curves E over $K = \mathbf{Q}$ and are seeking elements of $Ш(E/\mathbf{Q})$ visible in abelian surfaces J,

$$E \subset J \subset J_0(N)$$

where N is the conductor of E, but also request that the complementary elliptic curve $A \subset J$ to E in the abelian surface J be of conductor N as well (equivalently: that J be contained in the *new* part of $J_0(N)$).

The reader might imagine that we are stacking the deck against ourselves by asking for something as stringent as **5**, but we are getting ahead of our story.

Visibility and congruence moduli. Let $0 \to E \to J \to B \to 0$ be an exact sequence of abelian varieties over K, where E is an elliptic curve. Denote by $A \subset J$ a complementary abelian variety to E in J, so that we have the exact sequence over K,

$$0 \to A \cap E \to A \oplus E \to J \to 0,$$

with $A \cap E$ a finite subgroup of the abelian varieties A and E; we embed it "anti-"diagonally in $A \oplus E$. Let m be the exponent of the finite group $(A \cap E)(\overline{K})$. We can call the integer m the **congruence modulus** of E and A in J. One immediately sees that if $\sigma \in Ш(E/K)$ is visible in J then its order divides the congruence modulus m, and, more specifically, there is an element $h \in H^1(G_K, E \cap A)$ which maps to the element $\sigma \in Ш(E/K) \subset H^1(G_K, E)$ under the homomorphism induced from the inclusion $E \cap A \hookrightarrow E$, and which maps to zero in $H^1(G_K, A)$ under the homomorphism induced from the inclusion $E \cap A \hookrightarrow A$. The set of elements of $Ш(E/K)$ visible in J is a subgroup of $Ш(E/K)$, and is a subgroup of $Ш(E/K)[m]$. Denote the subgroup of elements of $Ш(E/K)$ visible in J by

$$Ш(E/K)^{(J)} \subset Ш(E/K)[m] \subset Ш(E/K).$$

There is a converse to this description. Namely, let us give ourselves the following data:

i. an abelian variety A over K,

ii. finite, G_K-stable, subgroups $\Phi_E \subset E$ and $\Phi_A \subset A$,

iii. and a G_K-equivariant isomorphism $\iota : \Phi_E \cong \Phi_A$,

with the property that

a. $\sigma \in Ш(E/K) \subset H^1(G_K, E)$ is the image of an element $h \in H^1(G_K, \Phi_E)$, and that

b. $\iota \cdot h \in H^1(G_K, \Phi_A)$ maps to zero in $H^1(G_K, A)$ under the homomorphism induced from the inclusion $\Phi_A \hookrightarrow A$.

Then, forming J by requiring the sequence

$$0 \to \Phi_E \to A \oplus E \to J \to 0$$

to be exact, where we have embedded $\Phi_E \hookrightarrow A \oplus E$ by the injection $\iota \ \oplus -1$, the element σ is visible in J, A is a complementary abelian variety to E in J, and the congruence modulus is the exponent of the finite group $\Phi_E \cong \Phi_A$.

Referring to our list of cases above, Case **2.** occurs when the abelian variety A is an elliptic curve. Note, therefore, that one would expect there to be serious impediments to finding visible elements of Ш of large order (for fixed K) in abelian surfaces. For example we would not even expect to find pairs of non-isogenous elliptic curves E, A over $\mathbf{Q}$ with $\mathbf{Q}$-stable finite subgroups $\Phi_E \subset E$ and $\Phi_A \subset A$ which are $G_{\mathbf{Q}}$-equivariantly isomorphic and are of large exponent m (let alone with the properties requisite for visibility).

Specifically, the first author has conducted a search for non-isogenous pairs of elliptic curves E and A for which there are finite subgroups $\Phi_E \subset E$ and $\Phi_A \subset A$ which are $G_{\mathbf{Q}}$-equivariantly isomorphic of exponent m. This search has so far covered all (modular) elliptic curves of conductor $N \leq 5500$ and all prime moduli $m \leq 97$. It has yielded a large number of examples for $m \leq 7$, quite a number for $m = 11$, but has so far yielded only two examples for $m \geq 13$, both of these being for $m = 13$. Namely, there is an elliptic curve of conductor 988, labelled 988B1 in [Cr1], satisfying a 13-congruence (see below for the definition of *m-congruence*) with the elliptic curve 52A1 of conductor 52; and the elliptic curve 3952C1 satisfies a 13-congruence with the curve 208C1. Neither of these congruences involve issues of visibility. These curves all have trivial Ш and rank 0, except for 988B1 which has rank 1.

This systematic search shows that there are no m-congruences for pairs of non-isogenous (modular) elliptic curves of conductors both ≤ 5500, where m is a prime number in the range $17 \leq m \leq 97$. The question of "high congruences" satisfied by pairs of non-isogenous elliptic curves is a topic of some current interest. See, for example, the work of Kani and Schanz [K-S], and the Harvard PhD thesis of David Carlton [Ca].

Optimal (or "strong Weil") modular elliptic curves. A natural case to consider is where $K = \mathbf{Q}$, and E is a modular elliptic curve over $\mathbf{Q}$ of conductor N, contained in the jacobian of the modular curve $J = J_0(N) := \mathrm{jac}(X_0(N))$. The requirement that E be *contained* in $J_0(N)$ is, in effect, the requirement that E be the *optimal* (or equivalently, in somewhat older terminology, the *"strong Weil"*) elliptic curve in its $\mathbf{Q}$-isogeny class. It is equivalent to request that the modular parametrization

$$\pi : X_0(N) \to E$$

of smallest degree among all possible nonconstant mappings from $X_0(N)$ to E have the property that the kernel of the homomorphism induced from π on jacobians, $J_0(N) \to E$, be (geometrically) irreducible. By definition, the **modular degree** of E, denoted m_E, is the degree of the finite mapping π. Denoting its kernel $A \subset J := J_0(N)$, we have that A is an abelian variety over K which fits into the exact sequence

$$0 \to A \to J \to E \to 0$$

whose dual we identify with

$$0 \to E \to J \to B \to 0.$$

The appropriate compositions of the mappings in the exact sequences above give us isogenies $E \to E$ and $A \to B$, the first being multiplication by the modular degree, m_E, from which we deduce that the (common) kernel of these isogenies is the finite subgroup $A \cap E = E[m_E]$. In particular, the congruence modulus of E and A in J is equal to the modular degree of E.

In studying the Shafarevich-Tate groups of elliptic curves, the optimal curve is a good choice of curve to concentrate on, in that, at least as far as most of the available numerical data shows, the order of the Shafarevich-Tate group, if it varies at all within a given isogeny class, will tend to be smallest for the optimal curve in the class. The phrase "will tend" is perhaps a bit too weak to describe the state of affairs here: of the data so far analyzed by the first author (going up to level 1000), there are only two counter-examples, both at level 960, to the statement that the minimal order of the Shafarevich-Tate group is attained by the optimal member of the $\mathbf{Q}$-isogeny class of modular elliptic curves. The exceptions are the isogeny classes $960D$ and $960N$ (in the labelling of [Cr1]), where the optimal curves $960D1$ and $960N1$ both have Ш of order 4, while in each case the three other curves in the isogeny class have trivial Ш. (See [Cr3] for more details of this investigation.)

It would be interesting to determine whether these counter-examples remain "optimal" when considered as quotients of $X_1(N)$, following the ideas regarding optimality suggested by Glenn Stevens [St]. We have not yet answered this question, but we suspect that the answer in each case is "yes", for the following reason. Stevens proves in [St] that each isogeny class of elliptic curves of conductor N over $\mathbf{Q}$ contains a unique curve whose Faltings-Parshin height is minimal, or equivalently whose period lattice is strictly contained in the period lattices of the other curves in the class. He also conjectures that the curve of minimal height is always the $X_1(N)$-optimal curve in the class, and proves (by explicit computation) that this holds for $N \leq 200$. For both the classes $960D$ and $960N$, the $X_0(N)$-optimal curves have minimal height, so by Stevens' conjecture one would expect that they are also $X_1(N)$-optimal.

In any event, once one knows the Shafarevich-Tate group of one member of a $\mathbf{Q}$-isogeny class of elliptic curves, it is often not that hard to work out the Shafarevich-Tate group of any other member. In the above situation, denoting as above by B the quotient abelian variety J/E, we have most of the hypothesis requested in Remark 2 above (that there are no nontrivial homomorphisms from E to B) by the "multiplicity one" theorem.

Let us denote the subgroup of elements of the Shafarevich-Tate group of a modular elliptic curve E of conductor N which are *visible* in the modular jacobian $J = J_0(N)$ with a superscript ^{o}, so we have the inclusion of subgroups

$$Ш(E/\mathbf{Q})^o \subset Ш(E/\mathbf{Q})[m_E] \subset Ш(E/\mathbf{Q}),$$

and note also the evident fact that whenever the modular degree of E is prime to the order of the torsion group of $B(K)$, any $\sigma \in Ш(E/\mathbf{Q})^o$ is "explained by" an element $\beta \in B(K)$ of infinite order.

The relation of m-congruence. Let E and F be elliptic curves over a field K, and let $m > 0$ be a positive integer. We will say that E and F are m-**congruent** over K if there exists an isomorphism $E[m] \cong F[m]$ as $(\mathbf{Z}/m\mathbf{Z})[G_K]$-modules. Suppose E and F, now, are optimal elliptic curves over $\mathbf{Q}$ of the same conductor N and denote by

$$f_E(q) = q + a_2(E)q^2 + a_3(E)q^3 + \cdots$$

the Fourier expansion of the cuspidal modular newform of weight two on $\Gamma_0(N)$ corresponding to E, and by $f_F(q)$ the Fourier expansion of the newform corresponding to F. The newforms f_E and f_F are eigenforms for the full Hecke algebra $\mathbf{T} = \mathbf{T}_0(N)$ which acts faithfully on the space of cuspidal modular forms of weight two on $\Gamma_0(N)$ (and also on the jacobian, $J_0(N)$, of the modular curve $X_0(N)$) and which is generated by the T_l's for prime numbers l not dividing the level N together with the U_q's for primes q dividing N. Our elliptic curves E and F are both abelian subvarieties of the new part of $J_0(N)$. To simplify our discussion, suppose that $m = p$ is a prime number. Consider these five conditions.

(1) The "prime to pN" Fourier coefficients of f_E and f_F "satisfy a p-congruence", i.e., $a_n(E) \equiv a_n(F) \bmod p$ for all n such that $(n, pN) = 1$.

(2) The $G_{\mathbf{Q}}$-representations $E[p]$ and $F[p]$ have isomorphic semisimplifications.

(3) The $G_{\mathbf{Q}}$-representations $E[p]$ and $F[p]$ are isomorphic (equivalently: E and F are p-**congruent**).

(4) All the Fourier coefficients "satisfy a p-congruence", i.e., $a_n(E) \equiv a_n(F) \bmod p$ for all n.

(5) The finite subgroups $E[p]$ and $F[p]$ are equal in $J_0(N)$. That is, the abelian subvarieties $E \subset J_0(N)$ and $F \subset J_0(N)$ have the property that their intersection contains $E[p] = F[p]$.

There are some evident implications between these five conditions. But also, (1) and (2) are equivalent, and when the Galois representation $E[p]$ is irreducible (or, what amounts to the same thing, when E does not admit a rational p-isogeny) (1) (2), and (3) are equivalent. Moreover, if N is relatively prime to p, p is odd, and $E[p]$ irreducible, then (4) and (5) are equivalent (by Theorem 5.2 of [R]). We also have the equivalence of (4) and (5) when p divides N provided that p is odd, p^2 doesn't divide N, and the Galois representation on $E[p]$ is irreducible and *not finite* at p ([M-R]). The condition that E be *not finite* at p is equivalent, if p^2 does not divide N, to the requirement that $\mathrm{ord}_p(\Delta_E)$ not be congruent to zero modulo p, where Δ_E is the discriminant of E.

Let us refer to condition (5) as providing a **modular p-congruence** between E and F. So, we have (at least) two possible notions: *modular p-congruence*, and (the a priori weaker notion of) *p-congruence*.

There are two possible computational strategies for checking, for a given positive integer m, that $E[m] = F[m]$ (e.g., when $m = p$ is a prime number, for checking a "modular p-congruence").

First strategy: Computing m-congruences of period lattices. The better of the two ways is to explicitly determine a basis for the integral homology of E and of F in $H_1(X_0(N); \mathbf{Z})$, and then to demonstrate that corresponding basis elements are linearly dependent modulo m. This has the virtue of actually demonstrating that $E[m] = F[m]$. It is by this method that we establish most of the modular p-congruences listed in our table, using the modular symbol methods of [Cr1].

Second strategy: Computing congruences of Fourier coefficients, and order of vanishing of Δ. Another possible computational strategy to establish modular p-congruences is suggested by the following proposition (whose proof follows from the results already quoted in [R] and [M-R]).

Proposition. Let N be an integer, and p an odd prime number such that p^2 does not divide N. Let E and F be elliptic curves defined over $\mathbf{Q}$ both (of conductor N, and) contained as abelian subvarieties of the new part of $J_0(N)$. Suppose that the $G_{\mathbf{Q}}$-representation on $E[p]$ is irreducible.

Then $E[p] = F[p]$ as subgroups of $J_0(N)$ (and, in particular, conditions (1)–(5) all hold) if

(i) $a_n(E) \equiv a_n(F) \bmod p$ for all n, and

(ii) if p divides N, $\mathrm{ord}_p(\Delta_E)$ is not congruent to 0 mod p.

To implement this strategy for $m = p$, we must check **(i)** and **(ii)**. Of course, **(ii)** only requires a finite number of different computations and therefore it is feasible, and very easy in the cases of interest to us, to make such a check. But **(i)** involves an infinite number of distinct computations. Here we make the following convention: if we have checked that $a_\ell(E) \equiv a_\ell(F) \bmod p$ for all prime numbers $\ell < 1000$, and if, in the few cases where there are prime divisors ℓ of pN which are greater than 1000, we also have checked the

p-congruence for these ℓ's as well, we will say that the pair E and F *seem to satisfy a p-congruence.* If, further, the hypotheses of the proposition, together with **(ii)** also hold, we will then also say that such a pair E and F *seem to satisfy a modular p-congruence.* In any such instance, if one wanted to actually *prove* the existence of a p-congruence or modular p-congruence, further work would be necessary: for example, one could use the results of [Sturm] to reduce the checking of **(i)** to the checking of a finite number of congruences.

However, as we have mentioned, for most of the cases tabulated below (including all those in Table 1, where m is odd) we have been able to follow the first strategy and therefore we will have shown that the congruence $a_n(E) \equiv a_n(F) \bmod m$ does in fact hold for *all* n. When we have only established that a p-congruence, or modular p-congruence, *seems to be the case* we explicitly indicate this in the tables.

Remark. Assume the Birch and Swinnerton-Dyer Conjecture, and the Shafarevich-Tate Conjecture. If E and F are optimal, of the same conductor N, and are modular p-congruent one to another ($p > 2$) then the parity of the Mordell-Weil ranks of E and F are the same.

To see this, just note that the parity of the Mordell-Weil ranks is determined by the sign of the eigenvalue ± 1 of the operator w_N on E and F as they sit in $J_0(N)$, and since $p > 2$ this sign can be read off by the action of w_N on $E[p] = F[p]$.

The first two examples. It may very well be the case that "asymptotically" for high values of the conductor N, the subgroup $\text{Ш}(E/K)^o$ of visible elements does not account for a large portion of $\text{Ш}(E/K)$ or even of $\text{Ш}(E/K)[m_E]$. Nevertheless, we began to examine the issue by considering the" first" two instances of nontrivial Shafarevich-Tate group for optimal semi-stable elliptic curves (i.e. the two lowest conductors N for which this occurs). These are tabulated in [Cr1] and are the curves labelled $571A1$ and $681B1$ there. The curve $571A1$ has trivial Mordell-Weil group, and the Mordell-Weil group of $681B1$ consists of 2-torsion; their Shafarevich-Tate groups are isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ and to $\mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$, respectively. Checking [Cr1] one immediately finds the happy "accident" that $571A1$ admits a 2-congruence with the optimal elliptic curve factor $571B1$, whose Mordell-Weil rank is 2 and whose 2-part of Ш is trivial. And with $681B1$, a similar "accident" happens: $681B1$ seems to admit a 3-congruence with the optimal elliptic curve factor $681C1$, whose Mordell-Weil rank is 2 and whose 3-part of Ш is trivial. Further computation, using the "first strategy" given above, shows that these congruences do hold fully in both cases, in the sense that condition **5** above holds: the 2-torsion of $571A1$ and $571B1$ coincide in $J_0(571)$, and the 3-torsion of $681B1$ and $681C1$ coincide in $J_0(681)$.

The values of the orders of Ш given in [Cr1] and [Cr3] are in all cases the so-called "analytic order" of Ш, which is the order as predicted from the value of the L-series at $s = 1$ by the conjecture of Birch and Swinnerton-Dyer; hence this data, and the data that will be tabulated below should be taken as conditional on this conjecture. Let us therefore officially assume the truth of the Birch and Swinnerton-Dyer conjecture for the rest of this article.

It follows that all of $\text{Ш}(571A1/\mathbf{Q})$ is visible in the abelian surface $J := (571A1 \oplus 571B1)/\Phi$, where Φ is isomorphic to the kernel of multiplication by 2 in either $571A1$ or $571B1$, and is embedded diagonally. Moreover, the two independent generators of the Mordell-Weil group of $571B1$ *explain* the two independent generators (mod 2) of $\text{Ш}(571A1/\mathbf{Q})$. Similarly, all of $\text{Ш}(681B1/\mathbf{Q})$ is visible in the abelian surface $J := (681B1 \oplus 681C1)/\Phi$ where Φ is isomorphic to the kernel of multiplication by 3 in either $681B1$ or $681C1$, and, again, the two independent generators of the Mordell-Weil group of $681C1$ *explain* the two independent generators (mod 3) of $\text{Ш}(681B1/\mathbf{Q})$. Moreover the abelian surface $J = (681B1 \oplus 681C1)/\Phi$ is an abelian subvariety of $J_0(681)$.

About the data. To make some further tests to see whether these were two extremely lucky, but singular, occurrences, Adam Logan examined squarefree conductors $N < 3000$ with the help of data and programs of the first author (see [Cr5]). Logan showed that all elements of odd order in the Shafarevich-Tate groups of optimal semi-stable elliptic curves over $\mathbf{Q}$ of conductor $N < 2849$ are visible in abelian surfaces contained in the jacobian $J_0(N)$ (these computations being again conditional upon the conjecture of Birch and Swinnerton-Dyer, and on the assumption that certain "apparent" m-congruences are actual m-congruences). In this regard, one should also mention the surprising computations done by Amod Agashé [A] (a PhD student of Loic Merel) who, along with Merel, has been independently investigating the order of the Shafarevich-Tate group of the winding quotients of $J_0(N)$ for N prime. They find that $\text{Ш}(J_0(N))$ vanishes surprisingly often (but not always; e.g. there is an element of order 7 in $\text{Ш}(J_0(1091))$).

The first author has since continued this investigation to all levels up to 5500. In the rest of this paper we will present and discuss the data obtained.

The data in detail. It appears that all of the elliptic curves with nontrivial Shafarevich-Tate group with conductor ≤ 5500 have Mordell-Weil rank 0. Two caveats are necessary here, however: first, we have not yet made systematic tables of the (analytic) order of Ш for non-optimal curves in the higher range $1000 < N \leq 5500$ which was not already covered in [Cr3]. Second, for optimal curves of positive rank r, our claim that the analytic order of Ш is trivial is based upon the assumption that the r independent points we have (as listed in [Cr1] and supplementary computer files in [Cr5]) do generate the full Mordell-Weil group modulo torsion, rather than a subgroup of index > 1. We have only checked this in some cases.

The nontrivial Shafarevich-Tate groups for N in this range are either of order p^2 for $p = 2$, 3, 5 or 7 or else of order 16. Specifically, there are 153 occurrences of order 4, 37 of order 9, 11 of order 16, 13 of order 25 and one of order 49. In discussing the data, it is useful to distinguish between instances where the Shafarevich-Tate group is of odd order or of order a power of two, these being the only cases that arise in the range tabulated. We remark that for all the cases where Ш has order 16, a 2-descent (using the first author's program `mwrank`, see [Cr6]) shows that the 2-rank of Ш is 2.

The kernel of multiplication by the modular degree. Recall the inclusion of subgroups of the Shafarevich-Tate group of E,

$$\text{Ш}(E/\mathbf{Q})^o \subset \text{Ш}(E/\mathbf{Q})[m_E] \subset \text{Ш}(E/\mathbf{Q}).$$

We find only three cases, where the modular degree m_E does not annihilate all of $Ш(E/\mathbf{Q})$, i.e., where $Ш(E/\mathbf{Q})[m_E]$ differs from $Ш(E/\mathbf{Q})$. The first, found by Logan, is given by the curve $E = 2849A1$ which has $Ш(E/\mathbf{Q})$ of order 9, but modular degree not divisible by 3. In particular, none of $Ш(2849A1/\mathbf{Q})$ is visible in $J_0(2849)$. Similarly, $4343B1$ and $5389A1$ all have Ш of order 9 but degree not divisible by 3.

But for all other cases examined, $Ш(E/\mathbf{Q})[m_E] = Ш(E/\mathbf{Q})$ and we find much the same pattern as was exhibited by the examples given above, of conductors 571 and 681. For convenience, we divide the results into, first, the cases where Ш has odd order > 1, and second, the cases of even order.

The Shafarevich-Tate groups of odd order: For all but two of the optimal elliptic curve factors E of squarefree conductor $N \leq 5500$ with Ш of odd order p^2, other than the "invisible" cases $2849A1$, $4343B1$ and $5389A1$, we find another optimal *elliptic curve* factor F which satisfies an m-congruence with E and such that F has trivial Ш but Mordell-Weil rank 2. The exceptions are $4229A1$ (which is the only optimal curve of conductor 4229) and $5073D1$ (where none of the other optimal curves of conductor 5073 has rank 2). A similar phenomenon occurs for all but four the curves E whose conductor is in this range but is not squarefree, with Ш of order p^2. There are exceptions at levels 2392, 3364, 4914, and 5054 where we did not find any suitable congruent curve.

In most cases, F has the same conductor as E, but for $E = 3306B1$ and $E = 5136B1$, which both have Ш of order 9, the conductor of F is a proper divisor of that of E (and there is no suitable curve F at the same level). The curve $E = 3306B1$ satisfies a 3-congruence with $F = 1102A1$ which has rank 2, and $E = 5136B1$ is 3-congruent to $F = 1712D1$ of rank 2.

It would then follow that, with the exception of the exceptional cases listed above, all of $Ш(E/\mathbf{Q})$ is visible in the abelian surface $J := E \oplus F/\Phi$ where $\Phi \cong E[p] \cong F[p]$ and J is a abelian subvariety of $J_0(M)$ for some M. Usually, $M = N$, and J is even in the "new" part of $J_0(N)$, but there are exceptions to this as we have just seen.

In one case (conductor 2534) three optimal elliptic curve factors are all 3-congruent. Two of these elliptic curves ($2534E1$ and $2534F1$) have Mordell-Weil rank zero and Ш of order 9, and the third ($2534G1$) is the "explanatory" optimal factor: it has trivial Ш but Mordell-Weil rank equal to 2. The curve $4592G1$ of rank 2 explains *both* the elements of order 5 in $4592D1$, to which it is 5-congruent, and also the elements of order 3 in $4592F$, to which it is 3-congruent.

There is only one example here where Ш has order 49, namely $3364C1$. However, this curve satisfies no congruence modulo 7 to any curve in the range studied, though its degree is a multiple of 7, and neither of the other two curves at that level has rank 2. (These curves are the 29-twists of the curves 116ABC listed in [Cr1], and all have rank 0.)

The "invisible" examples. Since $2849A1$ is our first invisible example, it may be worth looking a bit more closely at it. Both Loic Merel and Richard Taylor have suggested that one test to see if its Shafarevich-Tate group becomes visible in $J_1(2849)$. We have not yet made this test. The invisibility of this example in $J_0(2849)$ is the reason for the capitalization of the word "NONE" which appears in the "F-column" of its entry in the table. Similar remarks apply to the invisible examples $4343B1$ and $5389A1$.

Examples where Ш is of even order and E does not have a rational point of order 2. Here a similar pattern is found. In Table 2, the congruences listed between curves with the same conductor are in most cases true modular 2-congruences proved using our first computational strategy. In a few such cases, and in all cases where the conductors are not equal, the first strategy failed and so we only claim that the curves "seem to" satisfy a congruence modulo 2, in the sense defined earlier. The exceptions, which are marked in the table, are: $3664J$ (for all three curves F listed), $4528C$ and $4528A$ (but the congruence between $4528C$ and $4528B$ is proved), $4776C$ and $5296C$.

One feature peculiar to the prime $p = 2$ is that it is possible for a "switch of parity" to occur; that is, it is possible for two optimal factors of $J_0(N)$ to admit a congruence modulo $p = 2$ and have the property that they have different sign in their functional equations. Among the elliptic curves not possessing a rational point of order 2, and of conductor ≤ 5500 with Ш of even order there are only two such cases which have a "parity switch". The first is $E = 3431B1$ for which the 2-congruent curve F has rank one. The order of $Ш(E/\mathbf{Q})$ is 4; E admits a 2-congruence to both of the other optimal elliptic curves $3431A1$ and $3431C1$ of its conductor, which both have rank 1 and no 2-torsion. Similarly, $3995A1$ has Ш of order 4 and is 2-congruent to $3995D1$ which has rank 1 and no 2-torsion. In the remaining cases where a corresponding F exists, F has Mordell-Weil rank 2.

There are cases where there is more than one congruent curve of rank 2 to explain the nontrivial elements of Ш. At level 5302, there are two curves, $5302B1$ and $5302J1$, which have Ш of order 4 and 16 respectively, and which satisfy a congruence modulo 2 with each other and also with the four curves $5302C1$–$D1$–$F1$–$I1$, all of which have rank 2.

As with the cases of odd order Ш , there are several examples where we find a suitable explaining congruence with an optimal curve at a different level. For example, $Ш(2045B1)$ is "explained" by the curve $4090B1$ of rank 2 to which "seems to be" 2-congruent.

Examples where Ш is of even order and E has a rational point of order two. There are 90 such elliptic curves E. All but three of these have Ш of order 4 and the remaining three, $2742B$, $3800D$, and $5335A$, have Ш of order 16. For all but eight of these 90 examples, there is another elliptic curve F of the same conductor as E which also possesses a rational point of order 2, and with positive Mordell-Weil rank. We have not yet checked which of these 82 F's are (or even "seem to be") modular 2-congruent to their corresponding E's. The eight E's which do not possess a corresponding F are $1105A$, $2145D$, $2145G$, $3069A$, $4901C$, $5135B$, $5185A$, and $5335A$.

The tables. In the two tables below, the data we have compiled is reproduced. The 128 curves E occurring in these tables comprise all optimal elliptic curves E of conductor $N \leq 5500$ with nontrivial Ш except for the ninety optimal curves which have Ш of even order and a rational point of order 2. Each of these 128 elliptic curves E is listed together with the corresponding elliptic curve F of positive Mordell-Weil rank which "explains" $Ш(E/\mathbf{Q})$ (except in the cases where F doesn't exist). If there is no indication to the contrary, the congruence modulus linking $Ш(E/\mathbf{Q})$ and F is $\sqrt{|Ш|}$. The modular degrees m_E and m_F are also tabulated: these were computed by the method of [Cr4]. To save space, we do not give here the coefficients of a minimal Weierstrass equation for the curves; these may be obtained from the first author's anonymous `ftp` site [Cr5].

The marks (1), (2), (3) and (4) in the last column refer to the notes after the tables.

Table 1. Odd $|Ш_E| > 1$, all $N \leq 5500$

E	$\sqrt{|Ш_E|}$	m_E	**F**	m_F	Remarks
681B	3	$3 \cdot 5^3$	**681C**	$2^5 \cdot 3$	
1058D	5	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 23$	**1058C**	$2^4 \cdot 5$	
1246B	5	$2^6 \cdot 3^4 \cdot 5$	**1246C**	$2^6 \cdot 5$	
1664K	5	$2^7 \cdot 5 \cdot 7$	**1664N**	$2^6 \cdot 5$	
1913B	3	$3 \cdot 103$	**1913A**	$2^2 \cdot 3 \cdot 5^2$	
2006E	3	$2^6 \cdot 3 \cdot 5 \cdot 7 \cdot 23$	**2006D**	$2^7 \cdot 3$	
2366D	3	$2^4 \cdot 3^2 \cdot 13$	**2366E**	$2^5 \cdot 3^2 \cdot 5$	**E** has rational 3-torsion
2366F	5	$2^4 \cdot 3 \cdot 5 \cdot 13 \cdot 19$	**2366E**	$2^5 \cdot 3^2 \cdot 5$	
2429B	3	$2 \cdot 3 \cdot 73$	**2429D**	$2^3 \cdot 3 \cdot 13$	
2534E	3	$2^2 \cdot 3^2 \cdot 5^3 \cdot 11$	**2534G**	$2^5 \cdot 3^2 \cdot 13$	
2534F	3	$2^2 \cdot 3^2 \cdot 5 \cdot 7$	**2534G**	$2^5 \cdot 3^2 \cdot 13$	
2541D	3	$2^6 \cdot 3^2 \cdot 7 \cdot 11$	**2541C**	$2^5 \cdot 3^2$	
2574D	5	$2^7 \cdot 3^2 \cdot 5 \cdot 7^2$	**2574G**	$2^8 \cdot 5$	
2601H	3	$2^8 \cdot 3 \cdot 17$	**2601L**	$2^8 \cdot 3$	
2674B	3	$2^4 \cdot 3^3 \cdot 13$	**2674A**	$2^4 \cdot 3^2$	
2710C	3	$2^5 \cdot 3^3 \cdot 7$	**2710B**	$2^5 \cdot 3^2$	
2718D	3	$2^6 \cdot 3 \cdot 5 \cdot 7 \cdot 29$	**2718F**	$2^6 \cdot 3 \cdot 5$	
2768C	3	$2^2 \cdot 3 \cdot 41$	**2768B**	$2^5 \cdot 3 \cdot 7$	
2834D	5	$2^2 \cdot 3 \cdot 5 \cdot 109$	**2834C**	$2^6 \cdot 3^2 \cdot 5$	
2849A	3	$2^5 \cdot 5 \cdot 61$	**NONE**	–	
2900D	5	$2^5 \cdot 3^4 \cdot 5$	**2900C**	$2^6 \cdot 3 \cdot 5$	
2932A	3	$3 \cdot 277$	**none**	–	
2955B	3	$2^3 \cdot 3^5 \cdot 5$	**2955C**	$2^6 \cdot 3^3$	
3054A	3	$2 \cdot 3 \cdot 5^2 \cdot 11$	**3054C**	$2^4 \cdot 3 \cdot 5 \cdot 7$	
3185C	5	$2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 11^2$	**3185B**	$2^4 \cdot 3 \cdot 5$	
3306B	3	$2^4 \cdot 3^3 \cdot 5^2$	**1102A**	$2^5 \cdot 3^2$	(1)
3364C	7	$2^6 \cdot 3^2 \cdot 5^2 \cdot 7$	**none**	–	
3384A	5	$2^{10} \cdot 3 \cdot 5 \cdot 11$	**3384C**	$2^8 \cdot 5$	
3536H	3	$2^9 \cdot 3^2 \cdot 5 \cdot 11$	**3536G**	$2^7 \cdot 3^2$	
3555E	3	$2^3 \cdot 3 \cdot 5 \cdot 17$	**3555D**	$2^7 \cdot 3 \cdot 5$	
3712J	3	$2^6 \cdot 3 \cdot 13$	**3712I**	$2^6 \cdot 3$	
3879E	3	$2^6 \cdot 3^4 \cdot 5$	**3879D**	$2^5 \cdot 3^3$	
3933A	3	$2^5 \cdot 3 \cdot 5 \cdot 13$	**3933B**	$2^6 \cdot 3 \cdot 5$	
3952C	5	$2^4 \cdot 3 \cdot 5 \cdot 13 \cdot 17$	**3952E**	$2^5 \cdot 3 \cdot 5$	
3954C	3	$2^4 \cdot 3 \cdot 5^3 \cdot 7^2$	**3954D**	$2^5 \cdot 3 \cdot 5$	
4092A	5	$2^7 \cdot 3 \cdot 5 \cdot 19$	**4092B**	$2^6 \cdot 3 \cdot 5$	
4229A	3	$2^3 \cdot 3 \cdot 7 \cdot 13$	**none**	–	
4343B	3	$2^4 \cdot 1583$	**NONE**	–	
4592D	5	$2^8 \cdot 3^2 \cdot 5 \cdot 17$	**4592G**	$2^6 \cdot 3^2 \cdot 5$	

4592F	3	$2^6 \cdot 3^3 \cdot 7^2$	**4592C**	$2^6 \cdot 3^3$	
4592F	3	$2^6 \cdot 3^3 \cdot 7^2$	**4592G**	$2^6 \cdot 3^2 \cdot 5$	
4606B	3	$2^8 \cdot 3^3 \cdot 5 \cdot 7$	**4606C**	$2^7 \cdot 3^3$	
4675J	3	$2^2 \cdot 3^3 \cdot 5^3$	**4675I**	$2^6 \cdot 3^3$	
4914N	3	$2^4 \cdot 3^5$	**none**	–	**E** has rational 3-torsion
4963C	3	$2^2 \cdot 3 \cdot 71$	**4963D**	$2^9 \cdot 3$	
5046H	3	$2^4 \cdot 3 \cdot 5^2 \cdot 7$	**5046J**	$2^4 \cdot 3 \cdot 5 \cdot 11$	
5054C	3	$2^3 \cdot 3^3 \cdot 11$	**none**	–	(2)
5073D	3	$2^5 \cdot 3 \cdot 5 \cdot 7 \cdot 23$	**none**	–	
5082C	5	$2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13$	**5082D**	$2^8 \cdot 3 \cdot 5$	
5136B	3	$2^4 \cdot 3 \cdot 59$	**1712D**	$2^5 \cdot 7$	(1)
5389A	3	$2^2 \cdot 2333$	**NONE**	–	
5499E	3	$2^7 \cdot 3^4 \cdot 5$	**5499F**	$2^7 \cdot 3^3$	

Table 2. Even $|\text{Ш}_E|$, no rational 2-torsion, all $N \leq 5500$

E	$\sqrt{\lvert\text{Ш}_E\rvert}$	m_E	**F**	m_F	Remarks
571A	2	$2^3 \cdot 3 \cdot 5$	**571B**	$2^4 \cdot 3$	
1058B	2	$2^4 \cdot 5 \cdot 23$	**1058C**	$2^4 \cdot 5$	
1309A	4	$2^7 \cdot 3^2 \cdot 17$	**1309B**	2^8	(cong. mod 4)
1325D	2	$2^3 \cdot 3^3 \cdot 5$	**1325E**	$2^3 \cdot 3^3$	
1613B	2	$2^4 \cdot 19$	**1613A**	$2^4 \cdot 5$	
1701I	2	$2^4 \cdot 3^4$	**1701J**	$2^4 \cdot 3^3$	(cong. mod 4)
1717A	2	$2^3 \cdot 41$	**1717B**	$2^3 \cdot 13$	
1738B	2	$2^{11} \cdot 3^3 \cdot 7$	**1738A**	2^8	(cong. mod 4)
1849D	2	$2^4 \cdot 3 \cdot 7 \cdot 11$	**1849A**	$2^3 \cdot 3 \cdot 11$	
1856G	2	$2^8 \cdot 3 \cdot 5$	**1856D**	2^8	(cong. mod 4)
1862C	2	$2^4 \cdot 3^3 \cdot 7$	**1862A**	$2^4 \cdot 3^3$	
1888B	2	$2^8 \cdot 3$	**1888A**	2^7	
1917E	2	$2^3 \cdot 3^4$	**1917C**	$2^3 \cdot 3^3$	
2023A	2	$2^4 \cdot 3^3 \cdot 17$	**2023B**	$2^4 \cdot 3^3$	
2045B	4	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 17$	**2045C**	$2^3 \cdot 3^3 \cdot 13$	(cong. mod 2)
2045B	4	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 17$	**4090B**	$2^6 \cdot 7$	(1)
2089D	2	$2^5 \cdot 3 \cdot 5$	**2089E**	$2^5 \cdot 11$	
2224E	2	$2^7 \cdot 17$	**2224F**	$2^7 \cdot 3$	(cong. mod 4)
2265A	2	$2^5 \cdot 3^2 \cdot 5^2 \cdot 7$	**2265B**	$2^5 \cdot 5 \cdot 7$	(cong. mod 4)
2409B	2	$2^9 \cdot 5^2$	**2409D**	$2^5 \cdot 7^2$	
2541A	2	$2^5 \cdot 3^4 \cdot 11$	**2541C**	$2^5 \cdot 3^2$	
2554B	2	$2^5 \cdot 13$	**2554C**	$2^4 \cdot 3^2 \cdot 7$	
2563C	2	$2^6 \cdot 3 \cdot 7$	**2563D**	$2^4 \cdot 3 \cdot 5$	
2619C	2	$2^4 \cdot 3^2 \cdot 5$	**2619D**	$2^4 \cdot 3 \cdot 5$	
2678A	4	$2^9 \cdot 3^2 \cdot 23$	**2678B**	$2^7 \cdot 3$	
2678A	4	$2^9 \cdot 3^2 \cdot 23$	**2678I**	$2^5 \cdot 3 \cdot 11$	(cong. mod 2)
2710A	2	$2^5 \cdot 3 \cdot 5^2$	**2710B**	$2^5 \cdot 3^2$	

2710A	2	$2^5 \cdot 3 \cdot 5^2$	**2710D**	$2^5 \cdot 5 \cdot 11$	
2738C	4	$2^6 \cdot 3^2 \cdot 37$	**2738D**	$2^6 \cdot 3^2$	
3017A	2	$2^3 \cdot 3^5$	**none**		
3370D	2	$2^5 \cdot 5 \cdot 7$	**3370E**	$2^5 \cdot 3^4$	(cong. mod 4)
3380A	2	$2^6 \cdot 3^3 \cdot 13$	**3380D**	$2^6 \cdot 3^2$	(cong. mod 4)
3431B	2	$2^3 \cdot 3^3 \cdot 5$	**none**	–	(3)
3479D	2	$2^6 \cdot 7 \cdot 13$	**3479E**	$2^6 \cdot 13$	
3509B	2	$2^4 \cdot 3^2 \cdot 11^2$	**3509A**	$2^4 \cdot 3 \cdot 5$	
3555C	2	$2^7 \cdot 3^3 \cdot 5 \cdot 11$	**3555D**	$2^7 \cdot 3 \cdot 5$	
3575E	2	$2^4 \cdot 3 \cdot 5^2 \cdot 7$	**3575F**	$2^4 \cdot 3 \cdot 5 \cdot 7$	
3664J	2	$2^4 \cdot 3^2 \cdot 239$	**3664D**	$2^6 \cdot 5$	(5)
3664J	2	$2^4 \cdot 3^2 \cdot 239$	**3664E**	$2^6 \cdot 13$	(5)
3664J	2	$2^4 \cdot 3^2 \cdot 239$	**3664G**	2^9	(5)
3686D	4	$2^{10} \cdot 3 \cdot 7^2$	**3686E**	2^{11}	
3718H	4	$2^8 \cdot 3 \cdot 5 \cdot 7 \cdot 13$	**3718K**	$2^8 \cdot 3$	
3742A	2	$2^4 \cdot 3^2 \cdot 5$	**3742B**	$2^4 \cdot 5 \cdot 7$	
3774G	2	$2^{10} \cdot 5 \cdot 7$	**3774D**	$2^{10} \cdot 3$	(cong. mod 4)
3883B	2	$2^3 \cdot 3^3 \cdot 37$	**3883A**	$2^3 \cdot 3 \cdot 7$	
3886B	2	$2^6 \cdot 3 \cdot 5$	**3886G**	$2^5 \cdot 3^3$	
3975B	2	$2^5 \cdot 3 \cdot 7 \cdot 17$	**3975E**	$2^5 \cdot 3 \cdot 5^2$	
3995A	2	$2^6 \cdot 5 \cdot 7 \cdot 653$	**none**	–	(4)
4046F	2	$2^6 \cdot 3^2 \cdot 7 \cdot 17$	**4046D**	$2^6 \cdot 3^2 \cdot 7$	
4396A	2	$2^3 \cdot 3 \cdot 97$	**4396C**	$2^3 \cdot 3^4$	
4428F	2	$2^3 \cdot 3^5$	**4428B**	$2^3 \cdot 3^4$	
4528C	2	$2^7 \cdot 3$	**4528A**	$2^6 \cdot 5$	(5)
4528C	2	$2^7 \cdot 3$	**4528B**	$2^6 \cdot 3$	
4544M	2	$2^8 \cdot 3^5$	**4544L**	$2^8 \cdot 5$	(cong. mod 4)
4544M	2	$2^8 \cdot 3^5$	**4544G**	$2^7 \cdot 5$	
4564C	2	$2^4 \cdot 3^2 \cdot 5^2$	**4564A**	$2^4 \cdot 3 \cdot 11$	
4617F	2	$2^4 \cdot 3^4$	**4617H**	$2^4 \cdot 3^3$	
4630A	2	$2^9 \cdot 3 \cdot 5$	**4630B**	$2^6 \cdot 3^2$	
4630A	2	$2^9 \cdot 3 \cdot 5$	**4630C**	$2^7 \cdot 3^2$	
4630D	2	$2^6 \cdot 3 \cdot 5 \cdot 13$	**4630B**	$2^6 \cdot 3^2$	
4630D	2	$2^6 \cdot 3 \cdot 5 \cdot 13$	**4630C**	$2^7 \cdot 3^2$	
4655G	2	$2^5 \cdot 3 \cdot 5 \cdot 7 \cdot 19$	**4655F**	$2^5 \cdot 3 \cdot 5$	(cong. mod 4)
4655G	2	$2^5 \cdot 3 \cdot 5 \cdot 7 \cdot 19$	**4655C**	$2^5 \cdot 3^3 \cdot 7$	
4749A	2	$2^3 \cdot 3 \cdot 19 \cdot 23$	**4749B**	$2^3 \cdot 7 \cdot 23$	
4761A	2	$2^6 \cdot 5 \cdot 23$	**4761B**	$2^6 \cdot 5$	
4776C	2	$2^6 \cdot 3^2 \cdot 5 \cdot 11$	**4776B**	$2^5 \cdot 5^2$	(5)
4878A	2	$2^5 \cdot 17 \cdot 79$	**4878C**	$2^6 \cdot 19$	
4941B	2	$2^3 \cdot 3^2 \cdot 11$	**4941C**	$2^3 \cdot 3^4$	
4975C	2	$2^6 \cdot 5 \cdot 17$	**4975B**	$2^6 \cdot 3^3$	
4975C	2	$2^6 \cdot 5 \cdot 17$	**4975D**	$2^6 \cdot 17$	
5046C	2	$2^4 \cdot 3 \cdot 5^2 \cdot 7 \cdot 29$	**5046J**	$2^4 \cdot 3 \cdot 5 \cdot 11$	

5049A	2	$2^6 \cdot 3^3 \cdot 5$	**5049B**	$2^6 \cdot 3 \cdot 5^2$	(cong. mod 4)
5067C	2	$2^3 \cdot 3 \cdot 5 \cdot 13$	**563A**	$2^2 \cdot 13$	(1)
5067C	2	$2^3 \cdot 3 \cdot 5 \cdot 13$	**1126A**	$2^4 \cdot 11$	(1)
5067C	2	$2^3 \cdot 3 \cdot 5 \cdot 13$	**4504A**	$2^6 \cdot 5$	(1)
5067C	2	$2^3 \cdot 3 \cdot 5 \cdot 13$	**4504B**	$2^5 \cdot 13$	(1)
5067C	2	$2^3 \cdot 3 \cdot 5 \cdot 13$	**4504C**	$2^5 \cdot 17$	(1)
5117C	4	$2^6 \cdot 3 \cdot 7 \cdot 37$	**5117D**	$2^6 \cdot 5$	(cong. mod 2)
5133C	2	$2^5 \cdot 31$	**5133B**	$2^5 \cdot 3 \cdot 7$	
5133C	2	$2^5 \cdot 31$	**5133D**	$2^7 \cdot 5 \cdot 11$	
5150C	2	$2^4 \cdot 3^4 \cdot 5^2$	**5150D**	$2^4 \cdot 3^2 \cdot 5^2$	
5244A	2	$2^7 \cdot 3^2 \cdot 5 \cdot 7$	**5244B**	$2^7 \cdot 3^3$	(cong. mod 4)
5296C	2	$2^4 \cdot 3 \cdot 37$	**5296B**	$2^7 \cdot 3$	(5)
5300C	2	$2^4 \cdot 3^2 \cdot 5 \cdot 23$	**5300G**	$2^4 \cdot 3^2 \cdot 23$	
5302B	2	$2^5 \cdot 3 \cdot 5^2$	**5302C**	$2^7 \cdot 5$	
5302B	2	$2^5 \cdot 3 \cdot 5^2$	**5302D**	$2^6 \cdot 3^2$	
5302B	2	$2^5 \cdot 3 \cdot 5^2$	**5302F**	$2^8 \cdot 13$	
5302B	2	$2^5 \cdot 3 \cdot 5^2$	**5302I**	$2^6 \cdot 5^2$	
5302J	4	$2^6 \cdot 101$	**5302C**	$2^7 \cdot 5$	(cong. mod 2)
5302J	4	$2^6 \cdot 101$	**5302D**	$2^6 \cdot 3^2$	(cong. mod 2)
5302J	4	$2^6 \cdot 101$	**5302F**	$2^8 \cdot 13$	(cong. mod 2)
5302J	4	$2^6 \cdot 101$	**5302I**	$2^6 \cdot 5^2$	
5312K	2	$2^8 \cdot 3 \cdot 5$	**5312F**	2^9	
5312K	2	$2^8 \cdot 3 \cdot 5$	**5312J**	$2^8 \cdot 3$	(cong. mod 4)
5390E	2	$2^5 \cdot 3 \cdot 5 \cdot 7 \cdot 19$	**5390L**	$2^5 \cdot 3 \cdot 5 \cdot 19$	
5427A	2	$2^7 \cdot 3^2$	**5427B**	$2^7 \cdot 3^2$	
5427A	2	$2^7 \cdot 3^2$	**5427F**	$2^6 \cdot 3^2$	
5427E	2	$2^6 \cdot 3^3$	**5427B**	$2^7 \cdot 3^2$	
5427E	2	$2^6 \cdot 3^3$	**5427F**	$2^6 \cdot 3^2$	
5445A	2	$2^6 \cdot 3 \cdot 5 \cdot 11$	**5445B**	$2^6 \cdot 3 \cdot 5$	
5456A	2	$2^6 \cdot 3 \cdot 5 \cdot 19$	**2728C**	$2^5 \cdot 3 \cdot 11$	(1)
5456A	2	$2^6 \cdot 3 \cdot 5 \cdot 19$	**2728D**	$2^5 \cdot 11$	(1)

Notes. (1): Curve F is congruent to curve E and has rank 2, but has a different level. If there is more than one such curve F, all are listed (on separate lines).

(2): The curve 5054C is the (-19)-twist of the curve 14A; it has a rational 3-isogeny but no rational torsion.

(3): The curve $3431B1$ is 2-congruent to both $3431A1$ and $3431C1$ which have rank 1.

(4): The curve $3995A1$ is 2-congruent to $3995D1$ which has rank 1.

(5): For these pairs, as well as all those for which E and F have different conductors, we only claim that E and F "seem to" satisfy a 2-congruence.

Asymptotic questions. We feel that these issues deserve to be investigated further. Is the prevalence of "visibility" a phenomenon occurring only in this modest range of conductors? Is most of Ш invisible? Or is most of Ш visible? It is relatively easy to find other examples where $Ш(E/\mathbf{Q})$ is *not* annihilated by m_E (and hence examples of invisible elements of $Ш(E/\mathbf{Q})$ in $J_0(N)$ where N is the conductor of E), if one searches among all twists (e.g., by quadratic Dirichlet characters) of a given modular elliptic curve.

To discuss asymptotics more specifically, if we are given a non-negative function $f(E)$ where E ranges through all, or a class of, (modular) elliptic curves defined over $\mathbf{Q}$, let us define the **upper conductor exponent of** f to be the minimal real number α having the property that for all $\epsilon > 0$ there is a finite $N(\epsilon)$ such that

$$f(E) < N^{\alpha+\epsilon}$$

if conductor$(E) = N \geq N(\epsilon)$ (putting $\alpha = \infty$ if there is no such real number). Thus, as Ram Murty has shown in [Mur], the ABC conjecture is equivalent to the statement that the upper conductor exponent of the modular degree ($f(E) = m_E$) for semistable elliptic curves is ≤ 2. See also current publications of A. Granville in this regard. Also, Goldfeld and Szpiro [G-S] have conjectured that the upper conductor exponent of the order of the Shafarevich-Tate group ($f(E) = |Ш(E/\mathbf{Q})|$) is $\leq 1/2$. See also [de W] where it is shown (conditional on the Birch-Swinnerton-Dyer conjecture and the Riemann hypothesis for Rankin-Selberg zeta functions associated to certain weight 3/2 modular forms) that the upper conductor exponent of $f(E) = |Ш(E/\mathbf{Q})|$ is $\geq 1/2$.

Problem. What are the upper conductor exponents of orders of $|Ш(E/\mathbf{Q})^{\circ}|$ and of $|Ш(E/\mathbf{Q})[m_E]|$ as E ranges through all optimal elliptic curves over $\mathbf{Q}$? What are they (i.e., are they any different) when E ranges through all semi-stable optimal elliptic curves over $\mathbf{Q}$?

If it turns out that these upper conductor exponents are small it would be *especially* interesting to understand why so much of Ш for conductors ≤ 5500 is visible, and is already visible in abelian surfaces, as our data shows.

Most of the data used in these investigations, including the coefficients of minimal equations of all the elliptic curves mentioned here, their modular degrees and traces of Frobenius, may be obtained by anonymous ftp from the first author, from the ftp site [Cr5].

REFERENCES

Printed Publications

[A] Agashé, A.: On invisible elements of the Tate-Shafarevich group, Comptes Rendues de l'Académie de Sciences, France, to appear.

[A-H-K-K-M-M-P] An, S.Y., Hammond, S., Kim S.Y., Kim, M., McCallum, W., Marshall, D., Perlis, A.: On the Jacobian of a Curve of Genus One , in preparation.

[Ca] Carlton, D.:Moduli for pairs of elliptic curves with isomorphic N-torsion, PhD thesis, M.I.T. (1998).

[Cr1] Cremona, J.E.: Algorithms for Modular Elliptic Curves (Second edition), Cambridge University Press, 1997.

[Cr2] Cremona, J.E.: Classical Invariants and 2-descent on elliptic curves, J. Symbolic Comp., to appear.

[Cr3] Cremona, J.E.: The Analytic order of Ш for Modular Elliptic Curves, Journal de Théorie des Nombres de Bordeaux 5 (1993), pp. 179–184.

[Cr4] Cremona, J.E.: Computing the degree of the modular parametrization of a Modular Elliptic Curves, Mathematics of Computation 64 (1995), pp. 1235–1250.

[G-S] Goldfeld, D., Szpiro, L.: Bounds for the order of the Tate-Shafarevich group, Comp. Math. **97** (1995) 71-87.

[Groth] Grothendieck, A.: Le Groupe de Brauer, II, (pp. 67-87) in *Dix exposés sur la cohomologie des schémas*, volume 3 of Advanced Studies in Pure Mathematics, Eds: A. Grothendieck, N.H. Kuiper, North-Holland Publishing Co. (1968)

[K-S] Kani, Schanz: Diagonal quotient surfaces, Manuscripta Math., **93** (1997) 67-108; see also their "Modular diagonal quotient surfaces" to appear in Math. Zeitschrift.

[M-R] Mazur, B., Ribet, K.: Two-dimensional representations in the arithmetic of modular curves, Astérisque **196/197** (1991) 215-255.

[MSS] Merriman, J.R., Siksek, S., and Smart, N.P.: Explicit 4-descents on an elliptic curve, Acta Arithmetica LXXVII.4 (1996), pp. 385–404.

[Mum] Mumford, D.: On the equations defining abelian varieties I. Invent. math. **1** (1966) 287-354; II. **3** (1967) 75-135; III. bf 3 (1967) 215-244.

[Mur] Murty, R.: Bounds for congruence primes, preprint.

[R] Ribet, K.: On modular representations of Gal($\bar{\mathbf{Q}}/\mathbf{Q}$) arising from modular forms. Invent. Math **100** (1990) 431-476.

[Sa 1] Salmon, G.: A Treatise on the Higher Plane Curves (3rd edition), Hodges, Foster and Figgis, Dublin 1879.

[Sa 2] Salmon, G.: A Treatise on the analytic geometry of three dimensions (7th edition), Chelsea, New York 1927.

[St] Stevens, G.: Stickelberger elements and modular parametrizations of elliptic curves, Invent. Math. 98 (1989), pp. 75–106.

[Sturm] Sturm, J.: On the congruence of modular forms, Number theory (New York, 1984-1985), 275-280, Lecture Notes in Mathematics, 1240, Springer, Berlin-New York, 1987.

[T] Tate, J.: On the conjectures of Birch and Swinnerton-Dyer and a geometric analog, Séminaire Bourbaki 1965/66, no. 306; reprinted (pp. 189-214) in *Dix exposés sur la cohomologie des schémas*, volume 3 of Advanced Studies in Pure Mathematics, Eds: A. Grothendieck, N.H. Kuiper, North-Holland Publishing Co. (1968).

[de W] de Weger, B.: $A+B=C$ and big Шs, Quart. J. Math. Oxford (2) **49** (1998) 105-128.

[W] Weil, A.: Remarques sur un memoire d'Hermite, Arch. d. Math. **5** (1954) 197-202; reprinted in pp. 111-116 of volume II of *André Weil Oeuvres Scientifiques Collected Papers* Springer 1979.

Electronic Publications

[Cr5] Cremona, J.E.: Modular elliptic curve data for conductors up to 5500, available from `ftp://euclid.ex.ac.uk/pub/cremona/data`.

[Cr6] Cremona, J.E.: `mwrank`, a program for 2-descent on elliptic curves over **Q**, available from `ftp://euclid.ex.ac.uk/pub/cremona/progs`.