Visualizing elements of order three in the Shafarevich-Tate group.

Barry Mazur

(For Sir Michael Atiyah, with admiration)

1. Introduction. If we wish to write the equations of curves of genus 1 that give elements of the Shafarevich-Tate group of an elliptic curve over a number field K, a choice of ways is open to us. For example, if the element in question is of order 3 the curve of genus 1 corresponding to it occurs as a smooth plane cubic curve over K.

In a recent article [C-M] we raised the question of when one can find the curves of genus 1 corresponding to at least *some* of the elements of Shafarevich-Tate groups as curves in abelian surfaces over K. Adam Logan, using data and programs due to Cremona, studied this question numerically for semistable optimal elliptic curves E over $\mathbf{Q}$ of square-free conductor N less than about 3000, and for the odd part of their Shafarevich-Tate group. By an "optimal" elliptic curve (or in older terminology, a "strong Weil" curve) we mean that there is a modular parametrization $\phi : J_0(N) \to E$ where $N =$ the conductor of E, $J_0(N) =$ the jacobian of the modular curve $X_0(N)$, and such that the kernel of ϕ is an abelian variety. Any modular elliptic curve is isogeneous, over $\mathbf{Q}$, to a (unique) optimal elliptic curve, and any optimal elliptic curve of conductor N is isomorphic, over $\mathbf{Q}$, to an elliptic curve in $J_0(N)$. Logan studied the elements of the Shafarevich-Tate group of such optimal elliptic curves, and sought, in effect, to realize the corresponding curves of genus 1 in question as subcurves defined over $\mathbf{Q}$ within *abelian surfaces* contained in the new part of $J_0(N)$. If E is an optimal elliptic curve for which we can successfully do this for *each of* the elements of the Shafarevich-Tate group of E, let us say that we have *visualized* the Shafarevich-Tate group of E in abelian surfaces in the new part of the modular jacobian.

With this understanding, Logan found, for all the cases *but one* of elliptic curves E that he examined (e.g., squarefree conductor < 3000 with the odd part of the Shafarevich-Tate group nontrivial) that all the elements of the Shafarevich-Tate group of these E's are visualizable in abelian surfaces in the new part of the modular jacobian. The one curve for which this is not true is the one labelled $2849A$ in Cremona's tables, which has Shafarevich-Tate group of order 9: none of the curves of genus 1 corresponding to nontrivial elements of its Shafarevich-Tate group occur as sub-curves of $J_0(2849)$, let alone occur within abelian surfaces contained in $J_0(2849)$. In performing some of these computations, the Birch and Swinnerton-Dyer conjectures were relied upon, and therefore let us officially assume that conjecture. There was also another technical "caveat" (later removed!) to these computations for a detailed discussion of which the reader should consult [C-M].

An extension of this numerical investigation is reported in [C-M], where all optimal modular elliptic curves E over $\mathbf{Q}$ of conductor $N < 5500$ are examined (N not necessarily square-free). One of the great surprises (at least to us) was that there continued to be an "unreasonably" large number of such elliptic curves E with Shafarevich-Tate group visualized in abelian surfaces. Quite often, for a given elliptic curve E, it was even the case that all the elements of its Shafarevich-Tate group were representable by curves of genus 1 in a single abelian surface contained in the new part of the modular jacobian. I say "unreasonably" since in any instance where this happens, it comes (given our present state of understanding of the phenomenon) as a very lucky accident. Moreover, (for reasons outlined in [C-M]), it is not the sort of thing we would expect to happen *at all* for the p-primary components of the Shafarevich-Tate group if p is a large prime number.

The luckiness of this data deserves explanation. In searching for such explanation (and I should say that we are still very far from a completely satisfactory one!) I was led to prove that for any number field K, any elliptic curve E over K, and any element σ of order three in the Shafarevich-Tate group of E over K, there is an abelian surface A over K containing a curve of genus 1 (over K) which represents the element σ.

Most of the present article is devoted to a proof of this result (formulated in the corollary at the end of section 2). Our proof comes from a construction which has some side benefits. For example, along the way we will produce (over any number field K) elliptic fibrations over the projective line over K, possessing no K-rational section, whose total space is birationally isomorphic to $\mathbf{P}^2$ (and therefore the elliptic surface has a large supply of K-rational points), and having the further property that every smooth fiber of the elliptic fibration that has *any* K-rational point at all, has an *infinity* of them. That is, any smooth fiber of these elliptic fibrations possessing a K-rational point has the property that it is isomorphic over K to an elliptic curve with Mordell-Weil rank over K which is ≥ 1. One is led, by the existence of such elliptic fibrations, to ask whether one can find even "better" ones. For example, for which positive integers r can one find a (non-isotrivial) elliptic fibration over $\mathbf{P}^1$ (over the base field $\mathbf{Q}$) with a Zariski-dense set of $\mathbf{Q}$-rational points, possessing no $\mathbf{Q}$-rational section, and with the property that any smooth fiber that possesses one $\mathbf{Q}$-rational point is isomorphic over $\mathbf{Q}$ to an elliptic curve with Mordell-Weil rank over $\mathbf{Q}$ which is $\geq r$?

2. Visible elements in the Shafarevich-Tate group. Let us briefly recall the basic definition of [C-M]. Let K be a number field, $\bar{K}/K$ an algebraic closure, and $G_K = \mathrm{Gal}(\bar{K}/K)$ the Galois group. If E is an elliptic curve over K, and if we are given an imbedding over K of E into an abelian variety J, we form the exact sequence of abelian varieties

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

and say that an element $\sigma \in \mathrm{WC}(E/K) \cong H^1(G_K, E)$ (the Weil-Châtelet group of isomorphism classes of torsors for E over K) is **visible** in J if σ is in the kernel of the natural homomorphism

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

As discussed in [C-M], 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 $J \to B$. Such a T is nothing more nor less than 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

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

and we might note that if $\sigma \neq 0$, the point P is not rational over K despite the fact that the translate $E + P$ is defined over K. To signal the above relationship we will sometimes say that this element β (which is well-defined modulo the image of $J(K)$ in $B(K)$) **explains** σ.

To analyze this further, suppose we are given a pair $((*), \sigma)$ consisting of an exact sequence of abelian varieties over K,

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

with E an elliptic curve, and σ an element in $\mathrm{WC}(E/K) \cong H^1(G_K, E)$ which is visible in J.

By Poincaré's complete reducibility theorem (cf. [Mum] Theorem 1, Ch VI section 19) we may find a complementary abelian variety to E in J, over K. That is, there exists $B' \subset J$, an abelian subvariety of J, defined over K, with the property that $J = E + B'$ and $E \cap B'$ is finite. Fix such a complement $B' \subset J$ and put $E' := J/B'$.

We have that the projections $B' \to B$, and $E \to E'$ are both isogenies and both of these isogenies have the same kernel– namely, the finite group $\Phi := E \cap B' \subset J$ viewed as subgroup of B' or as subgroup of E (we may think of $\Phi = E \cap B'$ as the finite G_K-module $(E \cap B')(\bar{K}) = E(\bar{K}) \cap B'(\bar{K})$).

Consider the long exact sequence in G_K-cohomology associated to the exact sequence

$$(*) \qquad 0 \to \Phi \to E \to E' \to 0,$$

and note that since $\sigma \in H^1(G_K, E)$ is visible in J and the isogeny $E \to E'$ factors through J, it follows that σ is in the image of the natural homomorphism

$$H^1(G_K, \Phi) \to H^1(G_K, E(\bar{K})).$$

Let us now, for definiteness, make the following further hypothesis:

Hypothesis. The natural homomorphism $E(K) \to E'(K)$ is surjective.

For example, in the special case where $\Phi = E[N]$ is the kernel of multiplication by a positive integer N, and the Mordell-Weil group of E over K is a finite group of order prime to N, the above hypothesis holds.

Under this hypothesis, the natural homomorphism $H^1(G_K, \Phi) \to H^1(G_K, E(\bar{K}))$ is injective, and there is a unique cohomology class $\eta \in H^1(G_K, \Phi)$ which maps to σ.

Lemma 1. Under the above hypothesis, the image of η in $H^1(G_K, B'(\bar{K}))$ is zero. If $\beta \in B(K)$ maps to η in the long cohomological exact sequence

$$B'(K) \to B(K) \to H^1(G_K, \Phi) \to H^1(G_K, B'(\bar{K})),$$

then β (in $B(K)$ modulo the image of $J(K)$) *explains* σ, in the sense introduced above.

Proof. This is a straightforward diagram-chase. The point is that we have an exact sequence of abelian varieties over K,

$$0 \to B' \to J \to E' \to 0,$$

and under our hypothesis, the mapping $J(K) \to E'(K)$ is surjective, and therefore the natural mapping $H^1(G_K, B'(\bar{K})) \to H^1(G_K, J(\bar{K}))$ is injective.

To summarize, if we are given $E \subset J$ over K and $\sigma \in H^1(G_K, E(\bar{K}))$ which is visible in J, and if in addition we are given an abelian subvariety $B' \subset J$ which is complementary to E for which the above hypothesis holds, we get a quadruple (E, B', Φ, η) where

- E is an elliptic curve, B' is an abelian variety over K, Φ is a finite G_K-module given with G_K-equivariant imbeddings $\Phi \hookrightarrow E$, $\Phi \hookrightarrow B'$ into both E and B', and
- $\eta \in H^1(G_K, \Phi)$ projects to $\sigma \in H^1(G_K, E(\bar{K}))$ and to $0 \in H^1(G_K, B'(\bar{K}))$.

There is a "converse" to the above discussion, in the following sense. Suppose we are given a *quadruple* (E, B', Φ, η) satisfying the conditions stipulated in the bullets above. In particular, we have E an elliptic curve and we can consider $\sigma \in H^1(G_K, E(\bar{K}))$, the image of η under the inclusion mapping $\Phi \to E(\bar{K})$. Running the above argument in reverse, we get:

Lemma 2. There is an abelian variety $\tilde{J}$ over K, and an injection $E \hookrightarrow \tilde{J}$ such that σ is visible in $\tilde{J}$.

Proof. Imbed Φ into the abelian surface $E \times B'$ by the "diagonal" mapping, and let $\tilde{J}$ be the abelian surface over K given by

$$\tilde{J} := (E \times B')/\Phi.$$

The inclusion of E as the first factor of $E \times B'$ induces a natural inclusion $E \subset \tilde{J}$. Letting $B := \tilde{J}/E$ be the quotient abelian variety, we get two exact sequences of G_K-modules,

$$0 \to \ \Phi \ \to B' \ \to B \ \to 0,$$

and

$$0 \to \ E \ \to \tilde{J} \ \to B \ \to 0,$$

and the proof that the image of σ in $H^1(G_K, \tilde{J})$ vanishes is a direct check, comparing the long exact sequences of cohomology coming from these exact sequences.

In the present article, we will be particularly interested in the notion of visibility in *abelian surfaces* J. Therefore we will be focussing on *quadruples* (E, B', Φ, η) as above, but where the complementary abelian variety B' is also an elliptic curve. We reserve the letter $F (= B')$ for such complementary elliptic curves. Note that in the case where the complementary abelian variety of the quadruple is an elliptic curve and the finite group Φ is equal to $E[N]$ (the kernel of multiplication by a positive integer N in E) the data of the quadruple is given simply by a pair of elliptic curves E and F over K together with a G_K-equivariant isomorphism

$$\alpha : E[N] \cong F[N]$$

between groups of N-torsion (this is signalled colloquially by saying that "E and F are N-congruent over K") and a cohomology class $\eta \in H^1(G_K, E[N])$ with the property that the image of η in $H^1(G_K, E)$ is σ while the image of $\alpha \cdot \eta \in H^1(G_K, F[N])$ in $H^1(G_K, F)$ vanishes. In this case, the above abelian surface $\tilde{J}$ containing E and rendering σ visible is given by the quotient of $E \times F$ by the finite subgroup $E[N]$ imbedded in $E \times F$ via the mapping $\iota \times \alpha \cdot \iota$ where ι refers to either of the natural inclusions, $E[N] \hookrightarrow E$ and $F[N] \hookrightarrow F$.

Here is our main result, whose proof will be completed in section **3** (see Corollary 1 there).

Proposition. Let K be any number field, E any elliptic curve over K, and $h \in H^1(G_K, E(\bar{K})[3])$ such that the induced element $\sigma = \iota \cdot h \in H^1(G_K, E(\bar{K}))$ is in the Shafarevich-Tate group of E over K, i.e., $\sigma \in \mathrm{Sha}(E/K) \subset H^1(G_K, E(\bar{K}))$. Then there is an elliptic curve F over K and a G_K-equivariant isomorphism $\alpha : E[3] \cong F[3]$ such that the image of $\alpha \cdot h \in H^1(G_K, F(\bar{K})[3])$ in $H^1(G_K, F(\bar{K}))$ vanishes.

Corollary. Let K be any number field, E any elliptic curve over K, and $\sigma \in \mathrm{Sha}(E/K)[3]$. Then there is an abelian surface $\tilde{J}$ over K containing E such that σ is visible in $\tilde{J}$.

The Corollary follows directly from the Proposition together with Lemma 2.

3. Proof of the Proposition. Let us begin by considering the modular curve $X(3)$ over $\mathbf{Q}$ classifying pairs $\{F, \alpha\}$ where F is an elliptic curve (or, to include the cusps, a "generalized elliptic curve"; cf. [D-R]) and where α is a level 3 structure on F "*based on* $\mathbf{Z}/3\mathbf{Z} \times \mu_3$" and of determinant 1 ; that is,

$$\alpha : \mathbf{Z}/3\mathbf{Z} \times \mu_3 \to F[3]$$

is an isomorphism, and the natural isomorphism it induces on wedge-squares is "the identity". It makes sense to ask that this natural isomorphism be the identity, for domain and range are canonically isomorphic: $\wedge^2(\mathbf{Z}/3\mathbf{Z} \times \mu_3)$ is naturally isomorphic to μ_3, as is $\wedge^2(F[3])$ using the Weil pairing on 3-torsion in F . Let $\mathcal{S} \to X(3)$ denote the universal elliptic curve (over the cusps this is only a "generalized elliptic curve") with level 3 structure based on $\mathbf{Z}/3\mathbf{Z} \times \mu_3$. That is, $\mathcal{S}$ represents the moduli problem of classifying isomorphism classes of triples $\{F, \alpha, P\}$ where $\{F, \alpha\}$ represents a point of $X(3)$, and P is a point of F. We find it more convenient to work with the compactification of $\mathcal{S}$ which we denote S and which, as surface over $\mathbf{Q}$, was constructed by Hesse in the late 19th century (cf. a discussion of this surface in [R-S]). The surface S (over $\mathbf{Q}$) is conveniently expressed as the bihomogeneous hypersurface in $\mathbf{P}^1 \times \mathbf{P}^2$ (of bidegree $(1, 3)$):

$$s(X^3 + Y^3 + Z^3) = tXYZ,$$

where (s,t) are homogeneous coordinates of $\mathbf{P}^1$ and (X,Y,Z) are homogeneous coordinates of $\mathbf{P}^2$. To see $\mathcal{S}$ as a "generalized elliptic curve" we must specify a section to be the *zero section*; let us choose the section $(X,Y,Z)=(1,-1,0)$ to play this role.

The coordinates (s,t) give us a rational parametrization of $X(3)\cong\mathbf{P}^1$ and the projection of S to the first factor of $\mathbf{P}^1\times\mathbf{P}^2$ is, given this identification $X(3)\cong\mathbf{P}^1$, the natural projection $S\to X(3)$. Let $Y(3)\subset X(3)$ denote the complement of the four cusps. The (s,t)-coordinates of these cusps are $(0,1)$ and $(\zeta,3)$ where ζ ranges through all three cube roots of 1. The restriction of S to $Y(3)$ is a ("genuine") elliptic curve (over $Y(3)$). The quasi-projective variety $\mathcal{S}\subset S$ which is the total space of a generalized elliptic curve over $X(3)$ is the complement of twelve points in S lying over the cusps in $X(3)$ (the (X,Y,Z)-coordinates of three of these twelve points being the cyclic permutations of $(0,0,1)$ and the nine others being of the form $(1,\zeta,\zeta')$ where ζ and ζ' run through all cube roots of 1).

The projection to the second factor of $\mathbf{P}^1\times\mathbf{P}^2$ gives us a regular mapping $S\to\mathbf{P}^2$ (over $\mathbf{Q}$) which is a birational isomorphism and which consists in blowing-down the nine curves in S given by the locus $XYZ=0$ to the nine points

$$\{(0,-1,\zeta),\ (-1,\zeta,0),\ (\zeta,0,-1)\}\subset\mathbf{P}^2$$

where ζ runs through the three cube roots of 1. These nine *exceptional* curves are, in fact, sections of $\mathcal{S}$ over $X(3)$. Each of these nine sections is rational over $\mathbf{Q}(\sqrt{-3})$, and their union is precisely $\mathcal{S}[3]$, the kernel of multiplication by 3 in the ("generalized") elliptic curve $\mathcal{S}/X(3)$. Let us refer to these nine curves/sections as

$$\mathcal{C}:=\{C_{(0,-1,\zeta)},\ C_{(-1,\zeta,0)},C_{(\zeta,0,-1)}\}.$$

It is a theorem of Igusa [I] that these nine sections comprise the entire Mordell-Weil group of $\mathcal{S}$ over the base $X(3)$, and this is true even "geometrically", i.e., even when we make the groundfield base change from $\mathbf{Q}$ to $\mathbf{C}$. (For the analogous theorem for $X(N)$ over characteristic 0 fields for all $N>2$ see [Sh]; results of Silverberg provide further generalizations of this result to families of higher-dimensional abelian varieties.)

To "name" specific generators of the group of $\bar{\mathbf{Q}}$-rational points of $\mathcal{S}[3]$, set $P_1:=(0,1,-1)$, and $Q_\zeta:=(0,-1,\zeta)$ where ζ is a primitive cube root of unity. The mapping $1\mapsto P_1$ induces an injection of the constant group scheme $\mathbf{Z}/3\mathbf{Z}$ into $\mathcal{S}[3]$ while the mapping $\zeta\mapsto Q_\zeta$ induces an injection of the multiplicative-type group scheme μ_3 into $\mathcal{S}[3]$. These mappings allow us to make the identification of the finite group scheme $\mathcal{S}[3]$ over $X(3)$ with the pullback of the group scheme $\mathbf{Z}/3\mathbf{Z}\times\mu_3$ over $\mathrm{Spec}(\mathbf{Q})$ to the $\mathbf{Q}$-scheme $X(3)$. This also gives us a convenient choice of basis $\{P_1,Q_\zeta\}$ of the two-dimensional $\mathbf{F}_3$-vector space of $\bar{\mathbf{Q}}$-rational points of $\mathcal{S}[3]$.

For consistency with conventions to be made later, let us use the notation $\tilde{S}$ to refer to the "blow-down" in S of the nine exceptional curves in $\mathcal{C}$, noting that, first, $\tilde{S}$ is naturally defined over $\mathbf{Q}$ since the set $\mathcal{C}$ of exceptional curves being blown down is $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$-stable, and second, that we have a canonical isomorphism

$$\tilde{S}\cong\mathbf{P}^2.$$

A brief digression: the Heisenberg description of S. Consider the $G_{\mathbf{Q}}$-group $\mathbf{Z}/3\mathbf{Z}\times\mu_3$ and let $t,z\in\mathbf{Z}/3\mathbf{Z}\times\mu_3$ project to the generators of the first and second factors respectively, and project to zero in the second and first factors respectively. To be specific, let t project to $1\in\mathbf{Z}/3\mathbf{Z}$ and z to the primitive cube root of 1 which we will denote $\zeta_3\in\mu_3$. Define a homomorphism of the $G_{\mathbf{Q}}$-group $\mathbf{Z}/3\mathbf{Z}\times\mu_3$ into $\mathbf{PSL}_3(\mathbf{Z}[\mu_3])$ by putting

$$t:(X,Y,Z)\mapsto(Y,Z,X)$$

and

$$z:(X,Y,Z)\mapsto(X,\zeta_3\cdot Y,\zeta_3^2\cdot Z).$$

This comes from a representation of the (Heisenberg) extension of the $G_{\mathbf{Q}}$-group $\mathbf{Z}/3\mathbf{Z}\times\mu_3$ by μ_3 to $\mathbf{GL}_3(\mathbf{Z}[\mu_3])$, so let me refer to the corresponding action of $\mathbf{Z}/3\mathbf{Z}\times\mu_3$ on $\mathbf{P}^2$ as the **Heisenberg action**. The Heisenberg action is "defined over $\mathbf{Q}$" in the sense that it comes from a homomorphism of group schemes over $\mathbf{Q}$:

$$\mathbf{Z}/3\mathbf{Z}\times\mu_3\to\underline{\mathrm{Aut}}(\mathbf{P}^2),$$

where $\underline{\mathrm{Aut}}(\mathbf{P}^2)$ is the $\mathbf{Q}$-group scheme of automorphisms of $\mathbf{P}^2$. Equivalently, the Heisenberg action comes from a $G_{\mathbf{Q}}$-equivariant homomorphism of groups with $G_{\mathbf{Q}}$-action:

$$\mathbf{Z}/3\mathbf{Z}\times\mu_3(\bar{\mathbf{Q}})\to\mathrm{Aut}_{\bar{\mathbf{Q}}}(\mathbf{P}^2),$$

where $\mathrm{Aut}_{\bar{\mathbf{Q}}}(\mathbf{P}^2)$ is the group of automorphisms of $\mathbf{P}^2$ defined over $\bar{\mathbf{Q}}$.

The (nine point) locus of zeroes in $\mathbf{P}^2$ of the ideal

$$(XYZ,X^3+Y^3+Z^3)$$

is an orbit of the Heisenberg action. Any elliptic curve F in the family S passes through this orbit of nine points, and has the property that it is preserved by the Heisenberg action, this action being identified with translation by $F[3]$.

Much of our work will be to construct *twists* of this situation. Many of the twists that we will be considering admit alternate descriptions as pencils of cubic curves in $\mathbf{P}^2$ passing through some specified K-rational orbit (call it $\mathcal{T}$) of a *twist* of the Heisenberg action. If we were to seek explicit equations to describe them, it would be natural to look for the equations $\mathcal{F}(X,Y,Z)=0$ and $\mathcal{G}(X,Y,Z)=0$ of two distinct members of this pencil, thereby exhibiting the orbit $\mathcal{T}$ in question as a complete intersection (by curves stabilized under the Heisenberg action). At the same time one would be exhibiting the corresponding twist of S as the locus in $\mathbf{P}^1\times\mathbf{P}^2$ of the equation $s'\cdot\mathcal{F}=t'\cdot\mathcal{G}$, where (s',t') are homogeneous coordinates for the parameter curve $(\mathbf{P}^1)$ of the pencil.

The first twist: description in terms of twisting 1-cocyles. Here we fix a number field $K\subset\bar{\mathbf{Q}}$ and an elliptic curve $\mathcal{E}$ defined over K. For concreteness, by the "automorphism group" $\mathrm{Aut}(\mathcal{E}[3])$ let us mean the group of automorphisms of the abelian group $\mathcal{E}[3](\bar{\mathbf{Q}})$ of $\bar{\mathbf{Q}}$-rational points in $\mathcal{E}[3]$, but we view $\mathrm{Aut}(\mathcal{E}[3])$ with the natural G_K-action on it that it inherits induced by the standard Galois action of G_K on $\bar{\mathbf{Q}}$. Alternatively, we might view $\mathrm{Aut}(\mathcal{E}[3])$ as the automorphism group of the finite étale (commutative) group scheme $\mathcal{E}[3]$ over Spec K, where $\mathrm{Aut}(\mathcal{E}[3])$ is itself viewed as finite étale (noncommutative) group scheme over Spec K. We let $\mathrm{Aut}_o(\mathcal{E}[3]) \subset \mathrm{Aut}(\mathcal{E}[3])$ denote the subgroup (of index two) of automorphisms whose determinant is 1. As an abstract group (the group of $\bar{\mathbf{Q}}$-valued points of) $\mathrm{Aut}(\mathcal{E}[3])$ is isomorphic to $\mathrm{GL}_2(\mathbf{F}_3)$, and the subgroup $\mathrm{Aut}_o(\mathcal{E}[3]) \subset \mathrm{Aut}(\mathcal{E}[3])$ is isomorphic to $\mathrm{SL}_2(\mathbf{F}_3) \subset \mathrm{GL}_2(\mathbf{F}_3)$; a specific isomorphism is obtained by choosing an $\mathbf{F}_3$-basis of the 2-dimensional $\mathbf{F}_3$-vector space, $\mathcal{E}[3]$.

In the case where we have an identification $\iota : \mathcal{E}[3]) \cong \mathbf{Z}/3\mathbf{Z} \times \mu_3$ our choice of basis $\{P_1, Q_\zeta\}$ of $\mathbf{Z}/3\mathbf{Z} \times \mu_3$ gives us such isomorphisms:

$$\mathrm{Aut}_0(\mathbf{Z}/3\mathbf{Z} \times \mu_3) \cong \mathrm{SL}_2(\mathbf{F}_3), \qquad \mathrm{Aut}(\mathbf{Z}/3\mathbf{Z} \times \mu_3) \cong \mathrm{GL}_2(\mathbf{F}_3).$$

To pin down this choice of basis, $\{P_1, Q_\zeta\}$, of course, we must specify $\zeta = \zeta_3$, a primitive cube root of unity; for convenience of notation (*alone*) we make such a specification and we will allow ourselves the identification of $\mathrm{Aut}(\mathbf{Z}/3\mathbf{Z} \times \mu_3)$ with $\mathrm{GL}_2(\mathbf{F}_3)$ and of $\mathrm{Aut}_o(\mathbf{Z}/3\mathbf{Z} \times \mu_3)$ with $\mathrm{SL}_2(\mathbf{F}_3)$ below, with the understanding that via these identifications, the groups $\mathrm{GL}_2(\mathbf{F}_3)$ and $\mathrm{SL}_2(\mathbf{F}_3)$ are equipped with a natural (continuous) G_K-actions, where the elements of G_K act as group-automorphisms.

The group $\mathrm{Aut}_o(\mathbf{Z}/3\mathbf{Z} \times \mu_3)$ $(\cong \mathrm{SL}_2(\mathbf{F}_3)$) acts on the varieties $(S, X(3), \tilde{S})$ in the natural way. Explicitly, if $\gamma \in \mathrm{Aut}_o(\mathbf{Z}/3\mathbf{Z} \times \mu_3)$ and $\{F, \alpha : \mathbf{Z}/3\mathbf{Z} \times \mu_3 \to F[3]\}$ represents a point of $X(3)$ then $\gamma \cdot \{F, \alpha\} = \{F, \gamma \cdot \alpha\}$, and similary, if $\{F, \alpha, P\}$ represents a point of S, we have $\gamma \cdot \{F, \alpha, P\} = \{F, \gamma \cdot \alpha, P\}$. The action of $\mathrm{Aut}_o(\mathbf{Z}/3\mathbf{Z} \times \mu_3)$ on S stabilizes the set $\mathcal{C}$ of exceptional curves for the blow-down to $\tilde{S}$ and therefore induces an action on $\tilde{S}$. The mappings $S \to X(3)$ and $S \to \tilde{S}$ are equivariant with respect to these actions. We will be describing continuous 1-cocycles on G_K with values in $\mathrm{Aut}_o(\mathbf{Z}/3\mathbf{Z} \times \mu_3)$ with respect to which we will be twisting the above varieties to obtain varieties

$$(\ S(\mathcal{E}),\ X(\mathcal{E}),\ \tilde{S}(\mathcal{E}),\ )$$

over K and mappings

$$S(\mathcal{E}) \to X(\mathcal{E}), \qquad S(\mathcal{E}) \to \tilde{S}(\mathcal{E}),$$

(again over K). We are denoting our twisted configuration ($S(\mathcal{E}),\ X(\mathcal{E}),\ \tilde{S}(\mathcal{E}),$) even though it depends only on $\mathcal{E}[3]$. For a brief treatment of the basic results regarding twisting algebraic varieties by 1-cocycles, see Ch. V, section 4, para. 20 of [Se 1], and for a fuller account, see [Se 2], especially Prop. 5 of section 1.3 of Ch. III there. For definiteness we will be identifying the algebraic closures $\bar{K}$ with $\bar{\mathbf{Q}}$, or equivalently, setting $G_{\mathbf{Q}} := \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$, we are thinking of $G_K \subset G_{\mathbf{Q}}$ as the subgroup fixing the subfield K. Let $r_o : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{F}_3)$ denote the homomorphism with image equal to diagonal matrices, and which is of the form $r_o : g \mapsto [1, \chi(g)]$ where $\chi : G_{\mathbf{Q}} \to \{\pm 1\}$ is the character giving the action of Galois on cube roots of unity. Let $r_{\mathcal{E}} : G_K \to \mathrm{GL}_2(\mathbf{F}_3)$ be a continuous homomorphism which is equivalent (under $\mathrm{GL}_2(\mathbf{F}_3)$-conjugation) to the representation of Galois on $\mathcal{E}[3]$. Define the 1-cocycle (on G_K with values in the non-commutative group $\mathrm{GL}_2(\mathbf{F}_3)$):

$$c : G_K \to \mathrm{GL}_2(\mathbf{F}_3)$$

by $c(g) := r_{\mathcal{E}}(g) \cdot r_o^{-1}(g)$ for all $g \in G_K$. Since both determinants of $r_{\mathcal{E}}(g)$ and of $r_o(g)$ are equal to $\chi(g)$, the 1-cocycle c takes its values in $\mathrm{SL}_2(\mathbf{F}_3) \subset \mathrm{GL}_2(\mathbf{F}_3)$ and we will regard c, therefore, as a 1-cocycle on G_K with values in the (nonabelian) group $\mathrm{SL}_2(\mathbf{F}_3)$. Given the natural action of $\mathrm{SL}_2(\mathbf{F}_3)$ on our three varieties $(S, X(3), \tilde{S})$ over $\bar{\mathbf{Q}}$ we may obtain (via composition of the 1-cocycle c with the natural homomorphism of $\mathrm{SL}_2(\mathbf{F}_3)$ to the automorphism groups of the three varieties in question) three 1-cocycles,

$$c_{S,\mathcal{E}} \in Z^1(\, G_K, \mathrm{Aut}_{\bar{\mathbf{Q}}}(S_{\bar{\mathbf{Q}}})\,),$$

$$c_{X(3),\mathcal{E}} \in Z^1(G_K, \mathrm{Aut}_{\bar{\mathbf{Q}}}(X(3)_{\bar{\mathbf{Q}}})\,),$$

and

$$c_{\tilde{S},\mathcal{E}} \in Z^1(G_K, \mathrm{Aut}_{\bar{\mathbf{Q}}}(\tilde{S}_{\bar{\mathbf{Q}}})\,),$$

where if M is a continuous (possibly non-commutative) G_K-module, $Z^1(G_K, M)$ refers to the group of continuous 1-cocyles on G_K with values in M. Twisting $\mathcal{S}$ and S by the 1-cocycle $c_{S,\mathcal{E}}$ and the remaining two varieties ($X(3)$, and $\tilde{S}$) by their corresponding 1-cocycles give us the varieties over K which we denoted $\mathcal{S}(\mathcal{E})$, $S(\mathcal{E})$, $X(\mathcal{E})$, $\tilde{S}(\mathcal{E})$. The isomorphism class of each of these varieties is dependent only on the cohomology class of the corresponding twisting 1-cocycle.

The first twist: modular description. The modular interpretation of these varieties is as follows: The K-variety $\tilde{S}(\mathcal{E})$ represents the functor associated to the "moduli problem" of classifying isomorphism classes of triples $\{F, \alpha : \mathcal{E}[3] \cong F[3], P\}$ where F is an elliptic curve (or "generalized elliptic curve") over a base K-scheme W, α is an isomorphism of determinant 1 of group schemes over W, where by "$F[3]$" above we have meant the K-group scheme $F[3]$ pulled back to W, and P is a W-valued section of the generalized elliptic curve F. The K-variety $X(\mathcal{E})$ represents the functor associated to the "moduli problem" of classifying isomorphism classes of couples $\{F, \alpha : \mathcal{E}[3] \cong F[3]\}$ where the mapping $\mathcal{S}(\mathcal{E}) \to X(\mathcal{E})$ is given by dropping the "third" piece of data (P). The K-variety $S(\mathcal{E})$ is given as the evident completion of $\mathcal{S}(\mathcal{E})$ and the K-variety $\tilde{S}(\mathcal{E})$ may be thought of as obtained from $S(\mathcal{E})$ by noting that the twisting 1-cocyle preserves the set of the nine sections $\mathcal{C} \subset S$ yielding a K-rational packet (call it $\mathcal{C}(\mathcal{E})$) which is a (K-rational) multi-section of $S(\mathcal{E}) \to X(\mathcal{E})$. Therefore we can ($K$-equivariantly) blow this down in $S(\mathcal{E})$ to obtain $\tilde{S}(\mathcal{E})$.

Perhaps we should pause to take stock of what we have so far. The curve $X(\mathcal{E})$ is a curve of genus 0 over K. Since $X(\mathcal{E})$ possesses a K-rational point (given by our "starting curve" $\mathcal{E}$) we have $X(\mathcal{E}) \cong \mathbf{P}^1$ over K. The quasi-projective surface $\mathcal{S}(\mathcal{E})$ is a generalized elliptic curve over $X(\mathcal{E})$ whose kernel of multiplication by 3 is "constantly" $\mathcal{E}[3]$, meaning that, as a group scheme over $X(\mathcal{E})$ it is the pullback of the K-group scheme $\mathcal{E}[3]$. The projective surface $\tilde{S}(\mathcal{E})$ is a twist of $\mathbf{P}^2$, i.e., is a Brauer-Severi variety over K. Since $S(\mathcal{E})$ has a K-rational point so does $\tilde{S}(\mathcal{E})$ and therefore we see that $\tilde{S}(\mathcal{E})$ is isomorphic over K to $\mathbf{P}^2$. Going back to $S(\mathcal{E})$ we then have that $S(\mathcal{E})$ is the blow-up of a certain K-rational 0-cycle (of degree 9) in $\mathbf{P}^2$.

The second twist. At this point we wish to give ourselves an extra piece of data. We keep the number field K and the elliptic curve $\mathcal{E}$ over K, but add to our initial data a cohomology class $h \in H^1(G_K, \mathcal{E}[3])$. We wish to use the class h to twist our varieties

$$\mathcal{S}(\mathcal{E}),\ S(\mathcal{E}),\ X(\mathcal{E}),\ \tilde{S}(\mathcal{E})$$

to obtain varieties

$$\mathcal{S}(\mathcal{E},h),\ S(\mathcal{E},h),\ X(\mathcal{E}),\ \tilde{S}(\mathcal{E},h)$$

over K admitting mappings

$$\mathcal{S}(\mathcal{E},h) \subset S(\mathcal{E},h) \to X(\mathcal{E}), \qquad S(\mathcal{E},h) \to \tilde{S}(\mathcal{E},h),$$

again over K.

Here (as the notation above already indicates) the K-variety $X(\mathcal{E})$ will be unperturbed by this second twist. There will be three ways to describe this twist. The first is, as before, in terms of the twisting 1-cocycle. Note that the K-group scheme $\mathcal{E}[3]$ acts on $\mathcal{S}(\mathcal{E}) \subset S(\mathcal{E})$ by translation, and therefore we have an imbedding $\mathcal{E}[3]) \subset \mathrm{Aut}(\mathcal{S}(\mathcal{E}))$ (and $\mathcal{E}[3]) \subset \mathrm{Aut}(S(\mathcal{E})))$ these imbeddings being imbeddings of G_K-groups. The cohomology class h induces classes in $H^1(\ G_K, \mathrm{Aut}_{\bar{\mathbf{Q}}}(\mathcal{S}(\mathcal{E}))\ )$ and in $H^1(\ G_K, \mathrm{Aut}_{\bar{\mathbf{Q}}}(S(\mathcal{E}))\ )$ which we use to twist $\mathcal{S}(\mathcal{E})$ and $S(\mathcal{E})$ respectively, to give us the K-varieties $\mathcal{S}(\mathcal{E},h)$ and $S(\mathcal{E},h)$. Since the action of $\mathcal{E}[3]$ (by translation) preserves the projection to $X(\mathcal{E})$ we have an induced projection $S(\mathcal{E},h) \to X(\mathcal{E})$. Since the action preserves the subvariety $\mathcal{C}(\mathcal{E}) \subset S(\mathcal{E})$ we have, after twist by h, a K-rational multisection (of degree 9) of $S(\mathcal{E},h) \to X(\mathcal{E})$ obtained by the twist of $\mathcal{C}(\mathcal{E})$ which we may denote $\mathcal{C}(\mathcal{E},h)$. We may again blow $\mathcal{C}(\mathcal{E},h)$ down K-equivariantly in $S(\mathcal{E},h)$ to obtain a variety which we denote $\tilde{S}(\mathcal{E},h)$.

Here is a second way of thinking of this twist. The quasi-projective variety $\mathcal{S}(\mathcal{E})$ is a generalized elliptic curve over the base $X(\mathcal{E})$ and $\mathcal{S}(\mathcal{E},h)$ is simply an $\mathcal{S}(\mathcal{E})$-torsor over $X(\mathcal{E})$ classified by the image of the class h under the composition

$$H^1(\ G_K, \mathcal{E}[3]) \to H^1(X(\mathcal{E}), \mathcal{E}[3])_{X(\mathcal{E})}) \cong H^1(X(\mathcal{E}), \mathcal{S}(\mathcal{E})[3]) \to H^1(X(\mathcal{E}), \mathcal{S}(\mathcal{E})).$$

The third way of describing this twist is to give the "moduli problem" that it represents. Here I will only give the briefest indication: consider isomorphism classes of quadruples

$$\{F, \alpha : \mathcal{E}[3] \cong F[3], T_h, P\},$$

where F is a generalized elliptic curve over a K-scheme W, α is as before, T_h is an F-torsor representing the cohomology class $\iota{\cdot}\alpha{\cdot}j(h) \in H^1(W,F)$ where $\iota : H^1(W,F[3]) \to H^1(W,F)$ and $j : H^1(G_K, \mathcal{E}[3]) \to H^1(W, \mathcal{E}[3])$ are the natural mappings, and P is a section of T_h over W. To give a more precise description one should say explicitly what one means here by isomorphism classes, but I will omit this. In particular, a (noncuspidal) K-rational point of $\mathcal{S}(\mathcal{E},h)$ will give us an elliptic curve F over K with a given 3-congruence to $\mathcal{E}$

(over K) such that the F-torsor classified by the cohomology class induced from h is trivial over K.

Now suppose that the cohomology class $h \in H^1(G_K, \mathcal{E}[3])$ lies in the Selmer group of $\mathcal{E}$. If this is the case, the $\mathcal{E}$-torsor obtained in the natural way from the class h is trivial over every completion K_v of K. It follows that $S(\mathcal{E}, h)$ and therefore also $\tilde{S}(\mathcal{E}, h)$ has a K_v-rational point for every completion K_v of K. But since $\tilde{S}(\mathcal{E}, h)$ is a Brauer-Severi variety, it follows that $\tilde{S}(\mathcal{E}, h)$ has, in fact, a K-rational point, and therefore is trivial. We conclude

Lemma. If $h \in H^1(G_K, \mathcal{E}[3])$ lies in the Selmer group of $\mathcal{E}$, then $\tilde{S}(\mathcal{E}, h) \cong \mathbf{P}^2$ over K.

It follows from the above Lemma that, under the above hypothesis, $S(\mathcal{E}, h)$ likewise has a dense set of K-rational points (Zariski-dense, as well as dense in the Σ-adic topology, for Σ any finite set of places of K). We should note that to prove the proposition stated earlier, all we *really* needed was that the variety $S(\mathcal{E}, h)$ satisfy the Hasse principle. But, since we have that $\tilde{S}(\mathcal{E}, h) \cong \mathbf{P}^2$ over K, we can even assert:

Corollary 1. Given any number field K, elliptic curve $\mathcal{E}$ over K and class $h \in H^1(G_K, \mathcal{E}[3])$ in the Selmer subgroup of $\mathcal{E}$ over K, there is a countably infinite set of elliptic curves F over K with distinct j-invariants having the property that F satisfies a 3-congruence over K with $\mathcal{E}$ and the F-torsor obtained from h by transport via the 3-congruence is trivial.

Our proposition immediately follows from this corollary. It seems worthwhile to record a few "extras" that one gets from this construction.

Corollary 2. Under the hypotheses of Corollary let us assume that the class h is nontrivial, and that the Mordell-Weil group $\mathcal{E}(K)$ contains no nontrivial 3-torsion. Then $\pi : S(\mathcal{E}, h) \to X(\mathcal{E})$ is an elliptic pencil over K with the following properties.

a. The pencil has no K-rational sections and has only a finite number of $\mathbf{C}$-rational sections.

b. The set of K-rational points of the domain $S(\mathcal{E}, h)$ of the pencil is dense (Zariski dense, as well as dense in the Σ-adic topology, for Σ any finite set of places of K).

c. Any nonsingular fiber of π which contains a K-rational point, contains an infinite number of K-rational points.

Proof. It is only the last property listed (i.e., **c.**) that needs proof, the rest having been either previously proved, or at least mentioned. Let e be a K-rational point of $S(\mathcal{E}, h)$ and let $\mathcal{T} \subset S(\mathcal{E}, h)$ be the fiber of π containing e. Then e is represented by a quadruple

$$\{F, \alpha, T_h, P\}$$

over K and if e doesn't lie over a cusp of $X(\mathcal{E})$ we have that F is an elliptic curve over K. The elliptic curve F satisfies a 3-congruence to $\mathcal{E}$ such that the induced F-torsor T_h

is trivial (all this being over K). The fiber $\mathcal{T}$ in question is isomorphic over K to T_h, and therefore to the elliptic curve F. Let us consider, then, the portion of the Galois cohomology exact sequence coming from multiplication by 3 on F:

$$F(K)/3F(K) \to H^1(G_K, F[3]) \to H^1(G_K, F).$$

Since the second homomorphism is not injective, we see that $F(K)/3F(K)$ doesn't vanish. But F has no nontrivial K-rational 3-torsion (since $\mathcal{E}$ has none, and $\mathcal{E}[3] \cong F[3]$ over K). It follows that $F(K)$ is of positive rank; i.e., $\mathcal{T}$ has an infinity of K-rational points.

4. Some afterthoughts.

a. Let us return to the context of Corollary 1, and consider the pencil of elliptic curves $\pi : S(\mathcal{E}, h) \to X(\mathcal{E})$ (where $h \in H^1(G_K, \mathcal{E}[3])$ is in the Selmer subgroup of $\mathcal{E}$ over K). Then the domain of π is a blow-up of $\mathbf{P}^2$, and the range of π is $\mathbf{P}^1$, and so π determines a K-isomorphism class of birational mappings of $\mathbf{P}^2$ to $\mathbf{P}^1$. Let us (partially) normalize the identification $X(\mathcal{E}) \cong \mathbf{P}^1$ by letting $\infty \in \mathbf{P}^1$ correspond to the "base point" in $X(\mathcal{E})$; i.e., the point representing the starting elliptic curve $\mathcal{E}$. As promised in our digression regarding the Heisenberg action above, the mapping π is easily seen to be given by some rational function of the form

$$\mathcal{F}(X, Y, Z)/\mathcal{G}(X, Y, Z)$$

where $\mathcal{F}$ and $\mathcal{G}$ are homogenous forms of degree 3. Here $\mathcal{G}(X, Y, Z)$ is a cubic form cutting out (in $\mathbf{P}^2$) the curve of genus 1 corresponding to the element $\sigma \in \mathrm{Sha}(\mathcal{E}/K)$ which is induced from the cohomology class h. We therefore find (surprise!) that in order to systematically understand *all* visualizations of a given element of Sha in abelian surfaces, we are again back to the problem of visualizing elements of order 3 in Sha as the locus of zeroes of cubic forms in $\mathbf{P}^2$ (and this just to get a cubic form that plays the role of $\mathcal{G}$; we would have yet more work to do to get $\mathcal{F}$). An example for $j = 0$ which one can think through to illustrate the interplay (between the problems presented by representing an element of order three of the Shafarevich-Tate group in $\mathbf{P}^2$ and in abelian surfaces) is given by the equations

$$s(3X^3 + 4Y^3 + 5Z^3) = t(XYZ).$$

Returning to the general case, to give an *explicit* description of π (and, along with π, a complete description of the collection of elliptic curves F whose Mordell-Weil groups *explain* the element σ in the Shafarevich-Tate group of $\mathcal{E}$ coming from the cohomology class h) one should (once given K, $\mathcal{E}$ and h) find some way to provide homogenous forms $\mathcal{F}(X, Y, Z)$ and $\mathcal{G}(X, Y, Z)$ that do the above job. It might be interesting to produce a (usable) computer algorithm that does this.

b. Given K, $\mathcal{E}$, and an element σ of order 3 in $\mathrm{Sha}(\mathcal{E}/K)$, Corollary 1 guarantees an infinity of elliptic curves F over K which (are 3-congruent to $\mathcal{E}$ and) have elements in their Mordell-Weil groups K which *explain* σ. The striking thing, though, that is exhibited by the data (that of Logan and the extended tables in [C-M]) is the profusion of cases where there is such an elliptic curve F *of the same conductor as* $\mathcal{E}$. Our result here gives us no further understanding about why such F's should exist so often. It would, of course, be very interesting (but probably too optimistic to hope for) if one could produce a number $\mathcal{N}$, computable simply from the original data of the problem, for which one can prove the existence of such an F with conductor $< \mathcal{N}$.

c. All the entries in the tables of [C-M] have the property that their Shafarevich-Tate groups have exponent ≤ 7. Moreover, there is only one entry with Shafarevich-Tate group of exponent > 5, and its Shafarevich-Tate group (of order 49) is one of the few which are *not*, in fact, visualizable in an abelian surfaces in the new part of the modular jacobian (of the same conductor as the elliptic curve in question). So the puzzle in our data concerns elements of Shafarevich-Tate groups of orders 2,3,4, and 5. Can one provide an analysis similar to our treatment of elements of order 3, which deals with elements of orders 2,4, and 5?

d. So far, we have twice twisted the basic "Hessian" universal elliptic curve with level 3-structure. We can produce an even more elaborate twisting of the fiber-square of this universal elliptic curve over $X(3)$. Briefly, let us give ourselves the data of a number field K, an elliptic curve $\mathcal{E}$ over K, and *two* elements $h_1, h_2 \in H^1(G_K, \mathcal{E}[3])$. We omit the details of the construction, but note that there is a projective threefold $V(\mathcal{E}, h_1, h_2)$ over K representing the moduli problem of giving sextuples

$$\{F, \alpha, T_{h_1}, T_{h_2}, P_1, P_2\}$$

where T_{h_i} is an F-torsor classified by h_i and P_i is a point on T_{h_i} (for $i = 1, 2$). There are natural projections $V(\mathcal{E}, h_1, h_2) \to S(\mathcal{E}, h_1)$ and $V(\mathcal{E}, h_1, h_2) \to S(\mathcal{E}, h_2)$ which, in both cases, have their generic fibers curves of genus 1. If $\mathcal{E}$ has no nontrivial K-rational point of order 3, and if the elements $h_1, h_2 \in H^1(G_K, \mathcal{E}[3])$ are linearly independent over $\mathbf{F}_3$ and are both elements of the Selmer group of $\mathcal{E}$ then $V(\mathcal{E}, h_1, h_2)$ is a family of elliptic curves (i.e., the generic fiber is a curve of genus 1) over $\mathbf{P}^2$ and has the property that if a fiber $\mathcal{T}$ has a K-rational point, then it is isomorphic over K to an elliptic curve with Mordell-Weil rank ≥ 2. It would be interesting to study some specific examples of these in detail. Can one find such an example for which the total space has a Zariski-dense set of K-rational points?

e. Returning to the family $\pi : S(\mathcal{E}, h) \to X(\mathcal{E})$ where h represents an element in the Selmer group of $\mathcal{E}$, so that $S(\mathcal{E}, h)$ is a blow up of $\mathbf{P}^2$ and $X(\mathcal{E}) = \mathbf{P}^1$ over K. For $x \in X(\mathcal{E})(K) = \mathbf{P}^1(K)$ denote by $h(x)$ the (normalized, logarithmic) height of x, and denote by $\mathcal{T}_x \subset S(\mathcal{E}, h)$ the fiber over x. I am thankful to Yuri Tschinkel and Bjorn Poonen for conversations about these examples, and in particular, for their comments suggesting that it would be interesting to get some idea of the asymptotics of these functions of a real variable T:

$$r(T) = \#\{x \in X(\mathcal{E})(K) = \mathbf{P}^1(K) \mid h(x) \leq T \text{ and } \mathcal{T}_x(K) \text{ nonempty}\},$$

and

$$r'(T) = \#\{x \in X(\mathcal{E})(K) = \mathbf{P}^1(K) \mid h(x) \leq T \text{ and } \mathcal{T}_x(K_v) \text{ nonempty for all places } v\}.$$

6. References.

[C-M] Cremona, J., Mazur, B.: Visualizing elements in the Shafarevich-Tate group, submitted to the Journal of Experimental Mathematics. [This article also can be downloaded as dvi or ps files from Cremona's homepage: http://www.maths.ex.ac.uk/ cremona/papers/visual.dvi or http://www.maths.ex.ac.uk/ cremona/papers/visual.ps]

[D-R] Deligne, P., Rapoport, M.: Schémas de modules des courbes elliptiques. Vol. II of the proceedings of the international school on modular functions, Antwerp (1972), *Lecture Notes in Mathematics* **349** Springer (1973)

[I] Igusa, J.: Fibre systems of Jacobian varieties. **III.** Fibre systems of elliptic curves, Am. J. **81** (1959) 453-476

[Mum] Mumford, D.: Abelian Varieties, Oxford University Press (1970)

[R-S] Rubin, K., Silverberg, A.: Mod p representations of elliptic curves, pp. 148-161 in *Elliptic curves, modular forms, and Fermat's Last Theorem*, International Press (1995)

[Se 1] Serre, J.-P.: *Groupes algébriques et corps de classes*, Hermann, Paris (1959)

[Se 2] Serre, J.-P.: *Cohomologie Galoisienne* (fifth ed.) *Lecture Notes in Mathematics* **5** Springer (reprinted: 1994)

[Sh] Shioda, T.: On elliptic modular surfaces, J. Math. Soc. Japan **24** (1972) 20-59