Comments on the subtopic of "visualizing elements in the Shafarevich-Tate group".

Introduction. Much of this commentary is taken from the beginning sections of the two articles [C-M] and [M] in the bibliography. To get perspective on the topic, here is the problem in simplest terms.

Consider the theory of curves of genus *zero* over a field k. We have a beautiful and complete theory of these. First, there is the *paradigm* such curve of genus zero, namely the projective line $\mathbf{P}^1$, and all others are "twists" of this paradigm. ANY curve of genus zero is isomorphic (over k) to a plane conic and the isomorphism can be effected in a fairly concrete way once you provide yourself with a meromorphic differential form on the curve of genus zero. Any curve of genus zero over k is isomorphic (over k) to $\mathbf{P}^1$ if and only if it possesses at least one k-rational point. If k is a numberfield, then a curve of genus zero is isomorphic to $\mathbf{P}^1$ over k if and only if it possesses a k_v-rational point for every place v of k (where k_v is the completion of k at v). Any curve of genus zero over a number field k *does* possess a k_v-rational point for all but a finite *even* number of places v of k. Given a particular plane conic C, we can rapidly determine a particular set S of places of k such that S contains all but a finite number of places of k, and C has a k_v-rational point for every place v of k. Moreover, over each k_v there are precisely two isomorphism classes of plane conics (determined by *local invariants*), and given any curve of genus zero over k_v we have a perfectly well-working theory to tell us which of the two conics it is. Thus the problem of determining whether or not your plane conic C has a k-rational point is effective. We know that for any finite set Σ of places of k of even cardinality there is one and only one plane conic (up to isomorphism) which has no k_v-rational point for the v's in Σ and which has k_v-rational points for the other v's. Moreover, there is no problem in giving the formulas for these plane conics. Full stop.

We are now ready for the comparison of this simple and clean theory, with our present concern: curves of genus 1, and elliptic curves, over a number field K. As for the arithmetic of an elliptic curves E over a number field K, we have two basic arithmetic invariants:

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 $(T,\, \iota)$ 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 $\iota : E \to \text{jac}\ T$ 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. 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 topic is to develop strategies that might enable us to "visualize" the underlying curves of genus 1 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).

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.

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 $N = \text{conductor}(E)$ for the minimal heights of all elements of order 3 in Ш$(E/\mathbf{Q})$.

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 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.

From curves of genus one to their jacobian elliptic curves: 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] 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-K-M-M-M-P] being presently written by McCallum and some of the graduate students at the University of Arizona (Sang Yook An, Seog Young Kim, David Marshall, Susan Marshall and Alex Perlis).

For $n = 5$ 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.

From elliptic curves E one to locally trivial curves of genus one with jacobian equal to E : There are fewer results of an explicit nature "going this 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. One of the specific questions in our subtopic is:

For any field (of characteristic zero) K, can one find the curves of genus 1 over K corresponding to the elements of order 3 in Shafarevich-Tate groups of elliptic curves over K as curves in abelian surfaces over K?

The answer to this is yes! (See [M].)

In the case where the elliptic curve E is an abelian subvariety of the of the jacobian $J_0(N)$ of a modular curve, can one find the curves of genus 1 over K corresponding to at least some of the elements of the Shafarevich-Tate group of E as curves in $J_0(N)$?

Here the surprise is exactly how much of the Shafarevich-Tate groups (at least of elliptic curves of conductor $N < 5500$, as computed so far) can be visualized this way! (See [C-M].)

More generally, how much of the Shafarevich-Tate group of sub-abelian factors of $J_0(N)$ can be so accounted?

For this, see [A] and [St].

References.

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

[**A-K-M-M-M-P**] **(WORK-IN-PROG)** An, S.Y., Kim S.Y., M., McCallum, W., Marshall, D., Marshall, S., Perlis, A.: On the Jacobian of a Curve of Genus One , in preparation.

[**C-M**] **(WEB) (TEX)** Cremona, J., Mazur, B.: Visualizing elements in the Shafarevich-Tate group, to appear in 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]

[**M**] **(TEX)** Mazur, B.: Visualizing elements of order three in the Shafarevich-Tate group, to appear in the Journal of Asian Mathematics.

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

[**O**] O'Neil, C.: On the jacobians of curves of genus 1 in $\mathbf{P}^1 \times \mathbf{P}^1$ (WORK-IN-PROG)

[**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**] **(WEB)** Stein, W.: (A table of visible sha for higher-dimensional factors of the modular jacobian) http://math.berkeley.edu/ was/visible.html where you can view the document online.

[**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