AN EXPLICIT ALGEBRAIC FAMILY OF GENUS-ONE CURVES VIOLATING THE HASSE PRINCIPLE

BJORN POONEN

Abstract. We prove that for any $t \in \mathbf{Q}$, the curve

$$5x^3 + 9y^3 + 10z^3 + 12\left(\frac{t^2+82}{t^2+22}\right)^3 (x+y+z)^3 = 0$$

in $\mathbf{P}^2$ is a genus 1 curve violating the Hasse principle. An explicit Weierstrass model for its Jacobian E_t is given. The Shafarevich-Tate group of each E_t contains a subgroup isomorphic to $\mathbf{Z}/3 \times \mathbf{Z}/3$.

1. Introduction

One says that a variety X over $\mathbf{Q}$ *violates the Hasse principle* if $X(\mathbf{Q}_v) \neq \emptyset$ for all completions $\mathbf{Q}_v$ of $\mathbf{Q}$ (i.e., $\mathbf{R}$ and $\mathbf{Q}_p$ for all primes p) but $X(\mathbf{Q}) = \emptyset$. Hasse proved that degree 2 hypersurfaces in $\mathbf{P}^n$ *satisfy* the Hasse principle. In particular, if X is a genus 0 curve, then X satisfies the Hasse principle, since the anticanonical embedding of X is a conic in $\mathbf{P}^2$.

Around 1940, Lind [Lin] and (independently, but shortly later) Reichardt [Re] discovered examples of genus 1 curves over $\mathbf{Q}$ that violate the Hasse principle, such as the nonsingular projective model of the affine curve

$$2y^2 = 1 - 17x^4.$$

Later, Selmer [Se] gave examples of diagonal plane cubic curves (also of genus 1) violating the Hasse principle, including

$$3x^3 + 4y^3 + 5z^3 = 0$$

in $\mathbf{P}^2$.

O'Neil [O'N, §6.5] constructs an interesting example of an algebraic *family* of genus 1 curves each having $\mathbf{Q}_p$-points for all $p \leq \infty$. Some fibers in her family violate the Hasse principle, by failing to have a $\mathbf{Q}$-point. In other words, these fibers represent nonzero elements of the Shafarevich-Tate groups of their Jacobians.

In [CP], Colliot-Thélène and the present author prove, among other things, the existence of non-isotrivial families of genus 1 curves over the base $\mathbf{P}^1$, smooth over a dense open subset, such that the fiber over *each* rational point of $\mathbf{P}^1$ is a smooth plane cubic violating the Hasse principle. In more concrete terms, this implies that there exists a family of plane cubics depending on a parameter t, such that the j-invariant is a non-constant function of t, and such that substituting *any* rational number for t results in a smooth plane cubic over $\mathbf{Q}$ violating the Hasse principle.

Date: March 18, 2000.

This research was supported by National Science Foundation grant DMS-9801104, an Alfred P. Sloan Fellowship, and a David and Lucile Packard Fellowship.

The purpose of this paper is to produce an explicit example of such a family. Our example, presented as a family of cubic curves in $\mathbf{P}^2$ with homogeneous coordinates x, y, z, is

$$5x^3 + 9y^3 + 10z^3 + 12\left(\frac{t^2+82}{t^2+22}\right)^3 (x+y+z)^3 = 0.$$

Remark. Noam Elkies pointed out to me that the existence of non-trivial families with *constant* j-invariant could be easily deduced from previously known results. In Case I of the proof of Theorem X.6.5 in [Si], one finds a proof (based on ideas of Lind and Mordell) that $2y^2 = 1 - Nx^4$ represents a nontrivial element of $Ш[2]$ of its Jacobian, when $N \equiv 1 \pmod 8$ is a prime for which 2 is not a quartic residue. The same argument works if $N = c^4 N'$ where $c \in \mathbf{Q}^*$ and N' is a product of primes $p \equiv 1 \pmod 8$, provided that 2 is not a quartic residue for at least one p appearing with odd exponent in N'. One can check that if $N = a^4 + 16b^4$ for some $a, b \in \mathbf{Q} \cap \mathbf{Z}_2^*$, then N has this form. One can now substitute rational functions for a and b mapping $\mathbf{P}^1(\mathbf{Q}_2)$ into $\mathbf{Z}_2^*$, with a/b not constant. For instance, the choices $a = 1 + 2/(t^2+t+1)$ and $b = 1$ lead to the family

$$2y^2 = 1 - \left[(t^2+t+3)^4 + 16(t^2+t+1)^4\right] x^4$$

of genus 1 curves of j-invariant 1728 violating the Hasse principle.

2. The cubic surface construction

Let us review briefly the construction in [CP]. Swinnerton-Dyer [SD] proved that there exist smooth cubic surfaces V in $\mathbf{P}^3$ over $\mathbf{Q}$ violating the Hasse principle; choose one. If L is a line in $\mathbf{P}^3$ meeting V in exactly 3 geometric points, and W denotes the blowup of V along $V \cap L$, then projection from L induces a fibration $W \to \mathbf{P}^1$ whose fibers are hyperplane sections of V. Moreover, if L is sufficiently general, then $W \to \mathbf{P}^1$ will be a Lefschetz pencil, meaning that the only singularities of fibers are nodes. In fact, for most L, all fibers will be either smooth plane cubic curves, or cubic curves with a single node.

For some $N \geq 1$, the above construction can be done with models over $\operatorname{Spec} \mathbf{Z}[1/N]$ so that for each prime $p \not| N$, reduction mod p yields a family of plane cubic curves each smooth or with a single node. One then proves that if $p \not| N$, each fiber above an $\mathbf{F}_p$-point has a smooth $\mathbf{F}_p$-point, so Hensel's Lemma constructs a $\mathbf{Q}_p$-point on the fiber W_t of $W \to \mathbf{P}^1$ above any $t \in \mathbf{P}^1(\mathbf{Q})$.

There is no reason that such W_t should have $\mathbf{Q}_p$-points for $p|N$, but the existence of $\mathbf{Q}_p$-points on V implies that at least for t in a nonempty p-adically open subset U_p of $\mathbf{P}^1(\mathbf{Q}_p)$, $W_t(\mathbf{Q}_p)$ will be nonempty. We obtain the desired family by base-extending $W \to \mathbf{P}^1$ by a rational function $f : \mathbf{P}^1 \to \mathbf{P}^1$ such that $f(\mathbf{P}^1(\mathbf{Q}_p)) \subseteq U_p$ for each $p|N$.

More details of this construction can be found in [CP].

3. Lemmas

Lemma 1. *Let V be a smooth cubic surface in $\mathbf{P}^3$ over an algebraically closed field k. Let L be a line in $\mathbf{P}^3$ intersecting V in exactly 3 points. Let W be the blowup of V at these points. Let $W \to \mathbf{P}^1$ be the fibration of W by plane cubics induced by the projection $\mathbf{P}^3 \setminus L \to \mathbf{P}^1$ from L. Assume that some fiber of $\pi : W \to \mathbf{P}^1$ is smooth. Then at most 12 fibers are singular, and if there are exactly 12, each is a nodal plane cubic.*

We give two approaches towards this result, one via explicit calculations with the discriminant of a ternary cubic form, and the other via Euler characteristics. The first has

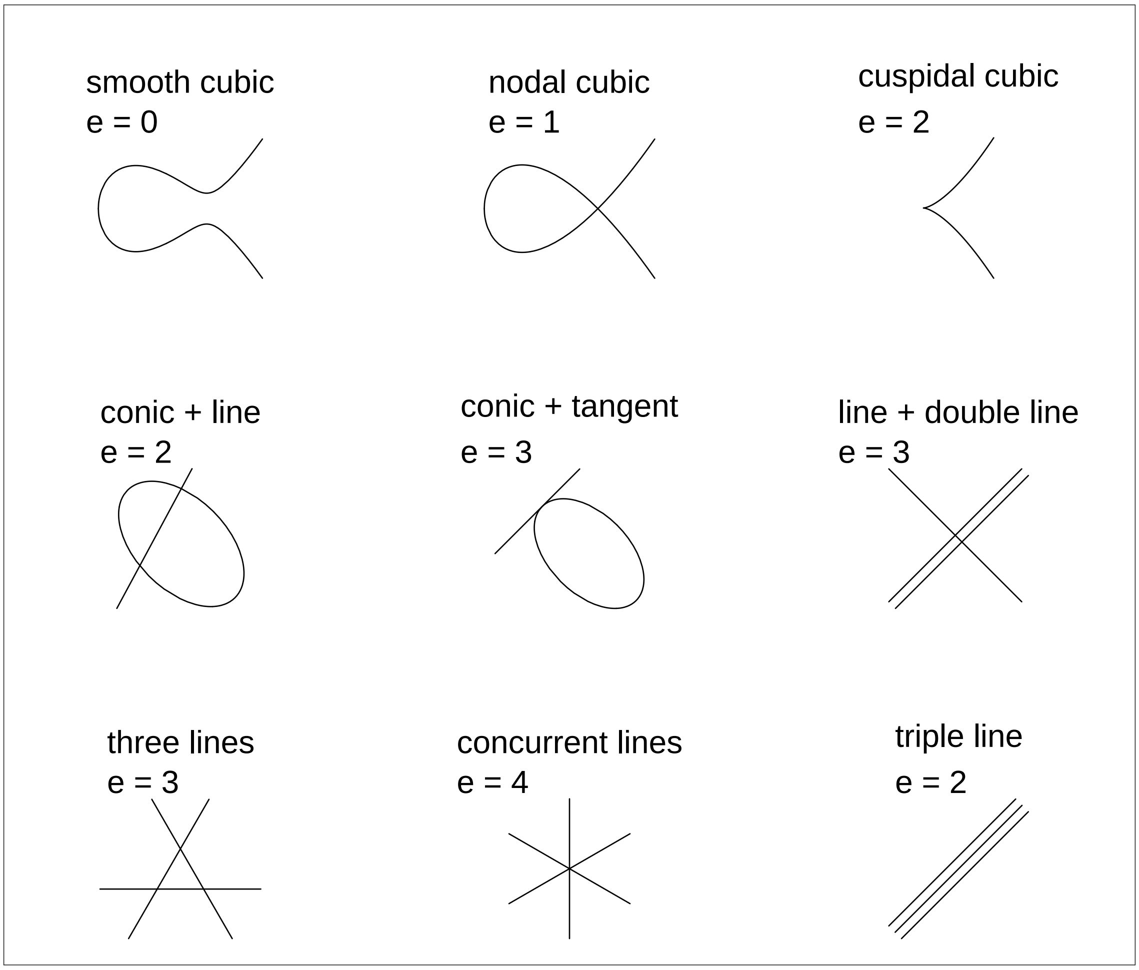

FIGURE 1. Plane cubic curves with their Euler characteristics.

the advantage of requiring much less machinery, but we complete this proof only under the assumption that L does not meet any of the 27 lines on V. (With more work, one could probably prove the general case too, but we have not tried too seriously, since the special case proved is all we need for our application, and also since the second proof works generally.) The second proof can be interpreted as explaining the order of vanishing of the discriminant of the family in terms of the Euler characteristic of a bad fiber.

First proof of Lemma 1, assuming that L does not meet the 27 lines. Let

$$\begin{aligned} F(x,y,z) &= a_0x^3 + a_1x^2y + a_2xy^2 + a_3y^3 \\ &\quad + a_4x^2z + a_5xyz + a_6y^2z \\ &\quad + a_7xz^2 + a_8yz^2 \\ &\quad + a_9z^3 \end{aligned}$$

be the generic ternary cubic form, with indeterminates $a_0, \dots, a_9$ as coefficients. Let $H(x,y,z)$ be the Hessian of F, i.e., the determinant of the 3×3 matrix of second partial derivatives of F. Let Δ be $2^{-9}3^{-3}$ times the determinant of the 6×6 obtained by writing each of $\partial F/\partial x$, $\partial F/\partial y$, $\partial F/\partial z$, $\partial H/\partial x$, $\partial H/\partial y$, $\partial H/\partial z$ in terms of the basis x^2, xy, y^2, xz, yz, z^2. (This is a special case of a classical formula for the resultant of three quadratic forms in three variables, which is reproduced in [St], for instance.) One computes that Δ is a homogeneous polynomial of degree 12 in $\mathbf{Z}[a_0, \ldots, a_9]$.

If we specialize F to the homogenization of $y^2 - (x^3 + Ax + B)$, we find that Δ becomes the usual discriminant $-16(4A^3 + 27B^2)$ of the elliptic curve [Si, p. 50]. Because Δ is an invariant for the action of $\mathrm{GL}_3(k)$, it follows that F gives the usual discriminant for any elliptic curve in general Weierstrass form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

at least in characteristic zero, and hence in any characteristic. Every smooth plane cubic is projectively equivalent to such an elliptic curve, so Δ is nonvanishing whenever the curve $F = 0$ is smooth.

On the other hand, if $F = 0$ is singular at $(0 : 0 : 1)$, so that $a_7 = a_8 = a_9 = 0$, we compute that Δ becomes 0. Again using the invariance of Δ, we deduce that $\Delta = 0$ if and only if $F = 0$ is singular.[1]

Since a cubic surface is isomorphic to $\mathbf{P}^2$ blown up at 6 points ([Ma, Theorem IV.24.4], for example), and W is the blowup of V at 3 points, we obtain a birational morphism $W \to \mathbf{P}^2$. Taking the product of this with the fibration map $W \to \mathbf{P}^1$ yields a morphism $\Psi : W \to \mathbf{P}^2 \times \mathbf{P}^1$ birational onto its image. The morphism Ψ separates points, since $W \to \mathbf{P}^2$ separates points except for 9 lines which contract to points, and these project isomorphically to the second factor $\mathbf{P}^1$, because by assumption L does not meet the 6 lines contracted by the morphism $V \to \mathbf{P}^2$. To verify that Ψ separates tangent vectors, we need only observe that at a point $P \in W$ on one of the 9 lines, a tangent vector transverse to the line through P maps to a nonzero tangent vector at the image point in $\mathbf{P}^2$, while a tangent vector at P along the line maps to the zero tangent vector at the image point in $\mathbf{P}^2$ but to a nonzero tangent vector at the image point in $\mathbf{P}^1$. Hence Ψ is a closed immersion, so we may view the given family $W \to \mathbf{P}^1$ as a family of curves in $\mathbf{P}^2$. By assumption, there exists a fiber of $W \to \mathbf{P}^1$ that is a smooth cubic curve. It follows that the divisor W in $\mathbf{P}^2 \times \mathbf{P}^1$ is of type $(3, 1)$, and hence W is given by a bihomogeneous equation $q(x_0, x_1, x_2, x_3; t_0, t_1) = 0$ of degree 3 in x_0, x_1, x_2, x_3 and of degree 1 in t_0, t_1. In other words, we may view the fibration $W \to \mathbf{P}^1$ as a family of cubic plane curves where the coefficients $a_0, \ldots, a_9$ are linear polynomials in the homogeneous coordinates t_0, t_1 on the base $\mathbf{P}^1$. Hence Δ for this family is a homogeneous polynomial of degree 12 in t_0, t_1, and it is nonvanishing because of the assumption that at least one fiber is smooth. Thus at most 12 fibers are singular.

To finish the proof, we need only show that if a fiber is singular and not with just a single node, then $\Delta(b_0, b_1)$ vanishes to order at least 2 at the corresponding point on $\mathbf{P}^1$. To prove this, we enumerate the combinatorial possibilities for a plane cubic, corresponding to the degrees of the factors of the cubic polynomial: see Figure 1.

In the "three lines" case, after a linear change of variables with constant coefficients we may assume that the three intersection points on the bad fiber are $(1 : 0 : 0)$, $(0 : 1 : 0)$, and $(0 : 0 : 1)$, so that the fiber is $xyz = 0$. We compute that if G is a general ternary cubic and t is an indeterminate, representing the uniformizer at a point on the base $\mathbf{P}^1$, then Δ for $xyz + tG$ is divisible by t^3. In the "conic + line" case, we assume that the two intersection points are the points $(1 : 0 : 0)$, $(0 : 1 : 0)$ so that the conic is a rectangular

[1] Facts such as this are undoubtedly classical, at least over $\mathbf{C}$, but it seems easier to reprove them than to find a suitable reference.

hyperbola and the line is the line $z = 0$ "at infinity." We can then translate the center of the hyperbola to $(0:0:1)$ and scale to assume that the fiber is $(xy - z^2)z = 0$. This time, Δ for $(xy - z^2)z + tG$ is divisible by t^2.

In the "cuspidal cubic" and "conic + tangent" cases, we may change coordinates so that the singularity is at $(0:0:1)$ and the line $x = 0$ is tangent to the branches of the curve there, so that $a_5 = a_6 = a_7 = a_8 = a_9 = 0$. In the remaining cases, "line + double line," "concurrent lines," and "triple line," we may move a point of multiplicity 3 to $(0:0:1)$, and again we will have at least $a_5 = a_6 = a_7 = a_8 = a_9 = 0$. We check that Δ vanishes to order 2 in all five of these cases, by substituting $a_i = tb_i$ for $i = 5, 6, 7, 8, 9$ in the generic formula for Δ, and verifying that the specialized Δ is divisible by t^2. $\square$

Second proof of Lemma 1. Let p be the characteristic of k, and choose a prime $\ell \neq p$. Let

$$\chi(V) = \sum_{i=0}^{2\dim V} (-1)^i \dim_{\mathbf{F}_\ell} \mathrm{H}^i_{\text{ét}}(V, \mathbf{F}_\ell)$$

denote the Euler characteristic. Since V is isomorphic to the blowup of $\mathbf{P}^2$ at 6 points, and W is the blowup of V at 3 points,

$$\chi(W) = \chi(\mathbf{P}^2) + 6 + 3 = 3 + 6 + 3 = 12.$$

On the other hand, combining the Leray spectral sequence

$$\mathrm{H}^p(\mathbf{P}^1, \mathrm{R}^q\pi_*\mathbf{F}_\ell) \implies \mathrm{H}^{p+q}(W, \mathbf{F}_\ell)$$

with the Grothendieck-Ogg-Shafarevich formula ([Ra, Théorème 1] or [Mi, Theorem 2.12]) yields

$$\chi(W) = \chi(W_\eta)\,\chi(\mathbf{P}^1) + \sum_{t \in \mathbf{P}^1(k)} \left[\chi(W_t) - \chi(W_\eta) - \mathrm{sw}_t(\mathrm{H}^*_{\text{ét}}(W_\eta, \mathbf{F}_\ell))\right], \tag{1}$$

where W_η is the generic fiber, W_t is the fiber above t, and

$$\mathrm{sw}_t(\mathrm{H}^*_{\text{ét}}(W_\eta, \mathbf{F}_\ell)) := \sum_{i=0}^{2} (-1)^i \,\mathrm{sw}_t(\mathrm{H}^i_{\text{ét}}(W_\eta, \mathbf{F}_\ell))$$

is the alternating sum of the Swan conductors of $\mathrm{H}^i_{\text{ét}}(W_\eta, \mathbf{F}_\ell)$ considered as a representation of the inertia group at t of the base $\mathbf{P}^1$. Since W_η is a smooth curve of genus $g = 1$, $\chi(W_\eta) = 2 - 2g = 0$. If $t \in \mathbf{P}^1(k)$ is such that W_t is smooth, then all terms within the brackets on the right side of (1) are 0, so the sum is finite. The Swan conductor of

$$\mathrm{H}^0_{\text{ét}}(W_\eta, \mathbf{F}_\ell) \cong \mathrm{H}^2_{\text{ét}}(W_\eta, \mathbf{F}_\ell) \cong \mathbf{F}_\ell$$

is trivial. Hence (1) becomes

$$12 = \sum_{t\colon W_t \text{ is singular}} \left[\chi(W_t) + \mathrm{sw}_t(\mathrm{H}^1_{\text{ét}}(W_\eta, \mathbf{F}_\ell))\right],$$

Since $\mathrm{sw}_t(\mathrm{H}^1_{\text{ét}}(W_\eta, \mathbf{F}_\ell))$ is a dimension, it is nonnegative, so the lemma will follow from the following claim: if W_t is singular, $\chi(W_t) \geq 1$ with equality if and only if W_t is a nodal cubic. To prove this, we again check the cases listed in Figure 1. The Euler characteristic for each, which is unchanged if we pass to the associated reduced scheme C, is computed using the formula

$$\chi(C) = \sum_i (2 - 2g_{\tilde{C}_i}) + \#C_{\text{sing}} - \#\alpha^{-1}(C_{\text{sing}}), \tag{2}$$

where $\alpha : \tilde{C} \to C$ is the normalization of C, $g_{\tilde{C}_i}$ is the genus of the i-th component of $\tilde{C}$, and C_{sing} is the set of singular points of C. For example, for the "conic + tangent," formula (2) gives

$$3 = \sum_{i=1}^{2} (2 - 2 \cdot 0) + 1 - 2.$$

□

Lemma 2. *If $F(x, y, z) \in \mathbf{F}_p[x, y, z]$ is a nonzero homogeneous cubic polynomial such that F does not factor completely into linear factors over $\overline{\mathbf{F}}_p$, then the subscheme X of $\mathbf{P}^2$ defined by $F = 0$ has a smooth $\mathbf{F}_p$-point.*

Proof. The polynomial F must be squarefree, since otherwise F would factor completely. Hence X is reduced. If X is a smooth cubic curve, then it is of genus 1, and $X(\mathbf{F}_p) \neq \emptyset$ by the Hasse bound.

Otherwise, enumerating possibilities as in Figure 1 shows that X is a nodal or cuspidal cubic, or a union of a line and a conic. The Galois action on components is trivial, because when there is more than one, the components have different degrees. There is an open subset of X isomorphic over $\mathbf{F}_p$ to $\mathbf{P}^1$ with at most two geometric points deleted. But $\#\mathbf{P}^1(\mathbf{F}_p) \geq 3$, so there remains a smooth $\mathbf{F}_p$-point on X. □

4. The example

We will carry out the program in Section 2 with the cubic surface

$$V: \ 5x^3 + 9y^3 + 10z^3 + 12w^3 = 0$$

in $\mathbf{P}^3$. Cassels and Guy [CG] proved that V violates the Hasse principle. Let L be the line $x + y + z = w = 0$. The intersection $V \cap L$ as a subscheme of $L \cong \mathbf{P}^1$ with homogeneous coordinates x, y is defined by

$$5x^3 + 9y^3 - 10(x + y)^3,$$

which has discriminant $242325 = 3^3 \cdot 5^2 \cdot 359 \neq 0$, so the intersection consists of three distinct geometric points. This remains true in characteristic p, provided that $p \notin \{3, 5, 359\}$.

The projection $V \dashrightarrow \mathbf{P}^1$ from L is given by the rational function $u := w/(x + y + z)$ on V. Also, W is the surface in $\mathbf{P}^3 \times \mathbf{P}^1$ given by the $((x, y, z, w); (u_0, u_1))$-bihomogeneous equations

$$\begin{aligned} W: \ 5x^3 + 9y^3 + 10z^3 + 12w^3 &= 0 \\ u_0 w &= u_1(x + y + z). \end{aligned} \tag{3}$$

The morphism $W \to \mathbf{P}^1$ is simply the projection to the second factor, and the fiber W_u above $u \in \mathbf{Q} = \mathbf{A}^1(\mathbf{Q}) \subseteq \mathbf{P}^1(\mathbf{Q})$ can also be written as the plane cubic

$$W_u: \ 5x^3 + 9y^3 + 10z^3 + 12u^3(x + y + z)^3 = 0. \tag{4}$$

The dehomogenization

$$h(x, y) = 5x^3 + 9y^3 + 10 + 12u^3(x + y + 1)^3,$$

defines an affine open subset in $\mathbf{A}^2$ of W_u. Eliminating x and y from the equations

$$h = \frac{\partial h}{\partial x} = \frac{\partial h}{\partial y} = 0$$

shows that this affine variety is singular when $u \in \overline{\mathbf{Q}}$ satisfies

$$2062096u^{12} + 6065760u^9 + 4282200u^6 + 999000u^3 + 50625 = 0. \tag{5}$$

The fiber above $u = 0$ is smooth, so by Lemma 1, the 12 values of u satisfying (5) give the *only* points in $\mathbf{P}^1(\overline{\mathbf{Q}})$ above which the fiber W_u is singular, and moreover each of these singular fibers is a nodal cubic. (Alternatively, one could calculate that Δ of the first proof of Lemma 1 for (4) equals $-2^4 3^{13} 5^4$ times the polynomial (5). One can easily verify that in any characteristic $p \notin \{2,3,5\}$, L does not meet any of the 27 lines on V.) The polynomial (5) is irreducible over $\mathbf{Q}$, so W_u is smooth for all $u \in \mathbf{P}^1(\mathbf{Q})$.

The discriminant of (5) is $2^{146} \cdot 3^{92} \cdot 5^{50} \cdot 359^4$. Fix a prime $p \notin \{2,3,5,359\}$, and a place $\overline{\mathbf{Q}} \dashrightarrow \overline{\mathbf{F}}_p$. The 12 singular u-values in $\mathbf{P}^1(\overline{\mathbf{Q}})$ reduce to 12 distinct singular u-values in $\mathbf{P}^1(\overline{\mathbf{F}}_p)$ for the family $\overline{W} \to \mathbf{P}^1$ defined by the two equations (3) over $\overline{\mathbf{F}}_p$. Moreover, the fiber above $u = 0$ is smooth in characteristic p. By Lemma 1, all the fibers of $\overline{W} \to \mathbf{P}^1$ in characteristic p are smooth plane cubics or nodal plane cubics. By Lemma 2 and Hensel's Lemma, W_u has a $\mathbf{Q}_p$-point for all $u \in \mathbf{P}^1(\mathbf{Q}_p)$.

Proposition 3. *If $u \in \mathbf{Q}$ satisfies $u \equiv 1 \pmod{p\mathbf{Z}_p}$ for $p \in \{2,3,5\}$ and $u \in \mathbf{Z}_{359}$, then the fiber W_u has a $\mathbf{Q}_p$-point for all completions $\mathbf{Q}_p$, $p \le \infty$.*

Proof. Existence of real points is automatic, since W_u is a plane curve of odd degree. Existence of $\mathbf{Q}_p$-points for $p \notin \{2,3,5,359\}$ was proved just above the statement of Proposition 3.

Consider $p = 359$. A Gröbner basis calculation shows that there do not exist a_1, a_2, b_1, b_2, c_1, c_2, $\overline{u} \in \overline{\mathbf{F}}_{359}$ such that

$$5x^3 + 9y^3 + 10z^3 + 12\overline{u}^3(x+y+z)^3 \tag{6}$$

and

$$(5x + a_1 y + a_2 z)(x + b_1 y + b_2 z)(x + c_1 y + c_2 z)$$

are identical. Hence Lemma 2 applies to show that for any $\overline{u} \in \mathbf{F}_{359}$, the plane cubic defined by (6) over $\mathbf{F}_{359}$ has a smooth $\mathbf{F}_{359}$-point, and Hensel's Lemma implies that W_u has a $\mathbf{Q}_{359}$-point at least when $u \in \mathbf{Z}_{359}$.

When $u \equiv 1 \pmod{5\mathbf{Z}_5}$, the curve reduced modulo 5,

$$\overline{W}_{\overline{u}} : \; 4y^3 + 2(x+y+z)^3 = 0,$$

consists of three lines through $P := (1:0:-1) \in \mathbf{P}^2(\mathbf{F}_5)$, so it does not satisfy the conditions of Lemma 2, but one of the lines, namely $y = -2(x+y+z)$, is defined over $\mathbf{F}_5$, and every $\mathbf{F}_5$-point on this line except P is smooth on $\overline{W}_{\overline{u}}$. Hence W_u has a $\mathbf{Q}_5$-point.

The same argument shows that W_u has a $\mathbf{Q}_2$-point whenever $u \equiv 1 \pmod{2\mathbf{Z}_2}$, since the curve reduced modulo 2 is $x^3 + y^3 = 0$, which contains $x + y = 0$.

Finally, when $u \equiv 1 \pmod{3\mathbf{Z}_3}$, the point $(1:2:1)$ satisfies the equation (4) modulo 3^2, and Hensel's Lemma gives a point $(x_0 : 2 : 1) \in W_u(\mathbf{Q}_3)$ with $x_0 \equiv 1 \pmod{3\mathbf{Z}_3}$. This completes the proof. $\square$

We now seek a non-constant rational function $\mathbf{P}^1 \to \mathbf{P}^1$ that maps $\mathbf{P}^1(\mathbf{Q}_p)$ into $1+p\mathbf{Z}_p$ for $p \in \{2,3,5\}$ and into $\mathbf{Z}_{359}$ for $p = 359$. Since $\left(\frac{-22}{p}\right) = -1$ for $p \in \{3,5,359\}$, the function

$$u = 1 + \frac{60}{t^2+22} = \frac{t^2+82}{t^2+22}$$

has the desired property. Substituting into (4), we see that

$$X_t:\ 5x^3 + 9y^3 + 10z^3 + 12\left(\frac{t^2+82}{t^2+22}\right)^3 (x+y+z)^3 = 0 \tag{7}$$

has $\mathbf{Q}_p$-points for all $p \le \infty$. On the other hand, $X_t(\mathbf{Q}) = \emptyset$, because $V(\mathbf{Q}) = \emptyset$. Finally, the existence of nodal fibers in the family implies as in [CP] that the j-invariant of the family has poles, and hence is non-constant.

5. The Jacobians

For $t \in \mathbf{Q}$, let E_t denote the Jacobian of X_t. The papers [AKMMMP] and [RVT] each contain a proof that the classical formulas of Salmon for invariants of a plane cubic yield coefficients of a Weierstrass model of the Jacobian. We used a GP-PARI implementation of these by Fernando Rodriguez-Villegas, available electronically at

`ftp://www.ma.utexas.edu/pub/villegas/gp/inv-cubic.gp`

to show that our E_t has a Weierstrass model $y^2 = x^3 + Ax + B$ where

$$A = 145800(t^2+82)^3(t^2+22)$$

and

$$\begin{aligned} B = &-6129675t^{12} - 96155100t^{10} + 359349979500t^8 + 65556113292000t^6 \\ &+ 4990338518958000t^4 + 180317231391182400t^2 + 2572729234128532800. \end{aligned}$$

Because the non-existence of rational points on V is explained by a Brauer-Manin obstruction, Section 3.5 and in particular Proposition 3.5 of [CP] show that there exists a *second family* of genus 1 curves Y_t with the same Jacobians such that the Cassels-Tate pairing satisfies $\langle X_t, Y_t\rangle = 1/3$ for all $t \in \mathbf{Q}$. In particular, for all $t \in \mathbf{Q}$, the Shafarevich-Tate group $Ш(E_t)$ contains a subgroup isomorphic to $\mathbf{Z}/3 \times \mathbf{Z}/3$.

Although we will not find explicit equations for the second family here, we can at least outline how this might be done, following [CP], except using Galois cohomology over number fields and $\mathbf{Q}(t)$ wherever possible in place of étale cohomology over open subsets of $\mathbf{P}^1$:

(1) Let $k = \mathbf{Q}(\sqrt{-3})$ and $V_k = V \times_{\mathbf{Q}} k$. On pages 66–67 of [CTKS] an element A_k of $\operatorname{Br}(V_k)$ giving a Brauer-Manin obstruction over k is described by parameters ϵ, η for a 2-cocycle ξ representing the image of A_k in $\mathrm{H}^2(\operatorname{Gal}(K/k), K(V)^*)$ for a certain finite abelian extension K of k. We may map ξ to an element of $\mathrm{H}^2(k, \overline{\mathbf{Q}}(V)^*)$.

(2) Apply the corestriction $\operatorname{cores}_{k/\mathbf{Q}}$ to A_k to obtain an element $A \in \operatorname{Br}(V)$ giving a Brauer-Manin obstruction for V over $\mathbf{Q}$. (See the proof of Lemme 4(ii) in [CTKS].) In practice, all elements of Brauer groups are to be represented by 2-cocycles analogous to ξ, and all operations are actually performed on these cocycles.

(3) Pull back A under the morphisms $X_\eta \to X \to V$, where X_η over $\mathbf{Q}(t)$ is the generic fiber of our final family $X \to \mathbf{P}^1$ of genus 1 curves, to obtain an element A_η of $\operatorname{Br}(X_\eta)$.

(4) Let $\overline{X_\eta}$ denote $X_\eta \times_{\mathbf{Q}(t)} \overline{\mathbf{Q}(t)}$. Find the image of A_η in $\mathrm{H}^1(\mathbf{Q}(t), \operatorname{Pic}\overline{X_\eta})$, by writing the divisor of the 2-cocycle representing the image of A_η in $\mathrm{H}^2(\mathbf{Q}(t), \overline{\mathbf{Q}(t)}(X_\eta)^*)$ as the coboundary of a 1-cochain, which becomes a 1-cocycle representing an element of $\mathrm{H}^1(\mathbf{Q}(t), \operatorname{Pic}\overline{X_\eta})$.

(5) Observe that the newly discovered 1-cocycle actually takes values in $\operatorname{Pic}^0 \overline{X_\eta} = E_\eta(\overline{\mathbf{Q}(t)})$, where E_η is the Jacobian of X_η over $\mathbf{Q}(t)$.

(6) Reconstruct the principal homogeneous space Y_η of E_η over $\mathbf{Q}(t)$ from this 1-cocycle, by computing the function field of Y_η as in Section X.2 of [Si].

(7) Find the minimal model of Y_η over $\mathbf{P}^1_{\mathbf{Q}}$, if desired, to obtain a model smooth over the same open subset of $\mathbf{P}^1$ as X.

Acknowledgements

I thank Ahmed Abbes for explaining the formula (1) to me, Antoine Ducros for making a comment that led to a simplification of the rational function used at the end of Section 4, and Noam Elkies for suggesting the first proof of Lemma 1 and the remark at the end of the introduction. I thank Bernd Sturmfels for the expression for the discriminant Δ of a plane cubic as a 6×6 determinant, and for providing Maple code for it. I thank also Bill McCallum and Fernando Rodriguez-Villegas, for providing Salmon's formulas for invariants of plane cubics in electronic form. The calculations for this paper were mostly done using Maple, Mathematica, and GP-PARI on a Sun Ultra 2. The values of A and B in Section 5 and their transcription into LaTeX were checked by pasting the LaTeX formulas into Mathematica, plugging them into the formulas for the j-invariant from GP-PARI, and comparing the result against the j-invariant of X_t as computed directly by Mark van Hoeij's Maple package "IntBasis" at

`http://www.math.fsu.edu/~hoeij/compalg/IntBasis/index.html`

for a few values of $t \in \mathbf{Q}$.

References

[AKMMMP] S. Y. An, S. Y. Kim, D. Marshall, S. Marshall, W. McCallum, A. Perlis, *Jacobians of genus one curves*, preprint, 1999.

[CG] J. W. S. Cassels and M. J. T. Guy, *On the Hasse principle for cubic surfaces*, Mathematika **13** (1966), 111–120.

[CTKS] J.-L. Colliot-Thélène, D. Kanevsky, et J.-J. Sansuc, *Arithmétique des surfaces cubiques diagonales*, pp. 1–108 in *Diophantine approximation and transcendence theory (Bonn, 1985)*, Lecture Notes in Math., 1290, Springer, Berlin, 1987.

[CP] J.-L. Colliot-Thélène and B. Poonen, *Algebraic families of nonzero elements of Shafarevich-Tate groups*, J. Amer. Math. Soc. **13** (2000), 83–99.

[Lin] C.-E. Lind, *Untersuchungen über die rationalen Punkte der ebenen kubischen Kurven vom Geschlecht Eins*, Thesis, University of Uppsala, 1940.

[Ma] Yu. I. Manin, *Cubic forms*, Translated from the Russian by M. Hazewinkel, Second edition, North-Holland, Amsterdam, 1974.

[Mi] J. Milne, *Étale cohomology*, Princeton Univ. Press, Princeton, N.J., 1980.

[O'N] C. O'Neil, *Jacobians of curves of genus one*, Thesis, Harvard University, 1999.

[Ra] M. Raynaud, *Caractéristique d'Euler-Poincaré d'un faisceau et cohomologie des variétés abéliennes*, Séminaire Bourbaki, Exposé **286** (1965).

[Re] H. Reichardt, *Einige im Kleinen überall lösbare, im Grossen unlösbare diophantische Gleichungen*, J. Reine Angew. Math. **184** (1942), 12–18.

[RVT] F. Rodriguez-Villegas and J. Tate, *On the Jacobian of plane cubics*, in preparation, 1999.

[Se] E. Selmer, *The diophantine equation* $ax^3 + by^3 + cz^3 = 0$, Acta Math. **85** (1951), 203–362 and **92** (1954), 191–197.

[Si] J. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics **106**, Springer-Verlag, New York-Berlin, 1986.

[St] B. Sturmfels, *Introduction to resultants*, Applications of computational algebraic geometry (San Diego, CA, 1997), 25–39, Proc. Sympos. Appl. Math. **53**, Amer. Math. Soc., Providence, RI, 1998.

[SD] H. P. F. Swinnerton-Dyer, *Two special cubic surfaces*, Mathematika **9** (1962), 54–56.

Department of Mathematics, University of California, Berkeley, CA 94720-3840, USA

E-mail address: `poonen@math.berkeley.edu`