Testing Equivalence of Ternary Cubics

Tom Fisher

University of Cambridge, DPMMS, Centre for Mathematical Sciences,
Wilberforce Road, Cambridge CB3 0WB, UK
T.A.Fisher@dpmms.cam.ac.uk

Abstract. Let C be a smooth plane cubic curve with Jacobian E. We give a formula for the action of the 3-torsion of E on C, and explain how it is useful in studying the 3-Selmer group of an elliptic curve defined over a number field.

We work over a field K of characteristic zero, with algebraic closure $\overline{K}$.

1 The Invariants of a Ternary Cubic

Let $X_3 = \mathbf{A}^{10}$ be the space of all ternary cubics

$$U(X,Y,Z) = aX^3 + bY^3 + cZ^3 + a_2X^2Y + a_3X^2Z + b_1XY^2 + b_3Y^2Z + c_1XZ^2 + c_2YZ^2 + mXYZ \ .$$

The co-ordinate ring of X_3 is the polynomial ring

$$K[X_3] = K[a, b, c, a_2, a_3, b_1, b_3, c_1, c_2, m] \ .$$

There is a natural action of GL_3 on X_3 given by

$$(gU)(X,Y,Z) = U(g_{11}X + g_{21}Y + g_{31}Z, \ldots, g_{13}X + g_{23}Y + g_{33}Z) \ .$$

The ring of invariants is

$$K[X_3]^{\mathrm{SL}_3} = \{F \in K[X_3] : F \circ g = F \text{ for all } g \in \mathrm{SL}_3(\overline{K})\} \ .$$

A homogeneous invariant F satisfies

$$F \circ g = \chi(g)F \tag{1}$$

for all $g \in \mathrm{GL}_3(\overline{K})$, for some rational character $\chi : \mathrm{GL}_3 \to \mathbf{G}_{\mathrm{m}}$. But the only rational characters of GL_3 are of the form $\chi(g) = (\det g)^k$ for k an integer. We say that F is an invariant of weight k. Taking g a scalar matrix in (1) shows that F has weight equal to its degree. The following facts are well known: see [1], [10], [15].

Theorem 1.1. *There are invariants c_4, c_6 and Δ of weights 4, 6 and 12, related by $c_4^3 - c_6^2 = 1728\Delta$, with the following properties:*
(i) The invariants of

$$U_E(X,Y,Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3$$

are given by the standard formulae: see [14, Chap. III].
(ii) The ring of invariants is a polynomial ring in two variables, generated by c_4 and c_6.
(iii) A ternary cubic U is non-singular if and only if $\Delta(U) \neq 0$.
(iv) If the plane cubic $\{U = 0\} \subset \mathbf{P}^2$ is non-singular then it has Jacobian

$$y^2 = x^3 - 27c_4(U)x - 54c_6(U) \ .$$

The Hessian of $U(X,Y,Z)$ is

$$H(X,Y,Z) = (-1/2) \times \begin{vmatrix} \frac{\partial^2 U}{\partial X^2} & \frac{\partial^2 U}{\partial X \partial Y} & \frac{\partial^2 U}{\partial X \partial Z} \\ \frac{\partial^2 U}{\partial X \partial Y} & \frac{\partial^2 U}{\partial Y^2} & \frac{\partial^2 U}{\partial Y \partial Z} \\ \frac{\partial^2 U}{\partial X \partial Z} & \frac{\partial^2 U}{\partial Y \partial Z} & \frac{\partial^2 U}{\partial Z^2} \end{vmatrix} \ .$$

The factor $-1/2$, although not standard, is a choice we find convenient. The Hessian is a polynomial map $H : X_3 \to X_3$ satisfying

$$H \circ g = (\det g)^2 g \circ H$$

for all $g \in \mathrm{GL}_3(\overline{K})$. We say it is a covariant of weight 2. Putting $c_4 = c_4(U)$, $c_6 = c_6(U)$ and $H = H(U)$ we find

$$H(\lambda U + \mu H) = 3(c_4\lambda^2\mu + 2c_6\lambda\mu^2 + c_4^2\mu^3)U + (\lambda^3 - 3c_4\lambda\mu^2 - 2c_6\mu^3)H \ .$$

This formula is classical: see [7], [11]. It is easily verified by restricting to any family of plane cubics covering the j-line. It also gives a convenient way of computing the invariants c_4 and c_6.

2 The 3-Selmer Group

Definition 2.1. *Let U_1 and U_2 be ternary cubics over K.*
(i) U_1 and U_2 are equivalent if $U_2 = \lambda(gU_1)$ for some $\lambda \in K^\times$ and $g \in \mathrm{GL}_3(K)$.
(ii) U_1 and U_2 are properly equivalent if $U_2 = (\det g)^{-1}(gU_1)$ for some $g \in \mathrm{GL}_3(K)$.

Lemma 2.2. *Let U_1 and U_2 be non-singular ternary cubics over K. If U_1 and U_2 are properly equivalent then they have the same invariants. If $K = \overline{K}$ then the converse is also true.*

Proof. The first statement follows from the fact that a homogeneous invariant has weight equal to its degree. For the second statement we may assume

$$U_1(X,Y,Z) = Y^2Z - (X^3 + a_1XZ^2 + b_1Z^3)$$
$$U_2(X,Y,Z) = Y^2Z - (X^3 + a_2XZ^2 + b_2Z^3)$$

for some $a_1, b_1, a_2, b_2 \in \overline{K}$. Since U_1 and U_2 have the same invariants, it follows by Theorem 1.1(i) that $U_1 = U_2$. □

We consider pairs $(C \to S, \omega)$ where $C \to S$ is a morphism from a smooth curve of genus one C to a Brauer-Severi variety S, and ω is a regular 1-form on C. An isomorphism between $(C_1 \to S_1, \omega_1)$ and $(C_2 \to S_2, \omega_2)$ is a pair of isomorphisms $\phi : C_1 \cong C_2$ and $\psi : S_1 \cong S_2$ such that $\phi^*\omega_2 = \omega_1$ and the diagram

$$\begin{array}{ccc} C_1 & \longrightarrow & S_1 \\ {\scriptstyle\phi}\downarrow & & \downarrow{\scriptstyle\psi} \\ C_2 & \longrightarrow & S_2 \end{array}$$

commutes.

Let $n \geq 2$ be an integer. Let E/K be an elliptic curve with invariant differential ω_E. We map $E \to \mathbf{P}^{n-1}$ via the complete linear system $|n.0_E|$. We recall that objects defined over K are called twists if they are isomorphic over $\overline{K}$.

Lemma 2.3. *The twists of $(E \to \mathbf{P}^{n-1}, \omega_E)$, up to K-isomorphism, are parametrised by $H^1(K, E[n])$.*

Proof. The automorphisms α of E with $\alpha^*\omega_E = \omega_E$ are the translation maps. If $\tau_P : E \to E$ is translation by $P \in E(\overline{K})$, we know that $\tau_P^*(n.0_E) \sim n.0_E$ if and only if $nP = 0_E$. So $\mathrm{Aut}(E \to \mathbf{P}^{n-1}, \omega_E) \cong E[n]$. An injective map from the isomorphism classes of twists to $H^1(K, E[n])$ is given by comparing an isomorphism defined over $\overline{K}$ with its Galois conjugates. It remains to prove surjectivity. This follows from the well known facts that the twists of E are parametrised by $H^1(K, \mathrm{Isom}(E))$ and the twists of $\mathbf{P}^{n-1}$ are parametrised by $H^1(K, \mathrm{PGL}_n)$. □

Remark 2.4. This interpretation of $H^1(K, E[n])$ is a variant of one given in [4], [9]. If $\phi : C \to E$ is an isomorphism of curves defined over $\overline{K}$ with $\phi^*\omega_E = \omega$ then we make C a torsor under E via $(P, Q) \mapsto \phi^{-1}(P + \phi(Q))$. This action depends on ω but not on ϕ.

The obstruction map, defined in [9], is

$$\mathrm{Ob} : H^1(K, E[n]) \to \mathrm{Br}(K)$$
$$(C \to S, \omega) \mapsto [S] \ .$$

In general this map is not a group homomorphism. Nevertheless we write $\ker(\mathrm{Ob})$ for the inverse image of the identity. We specialise to the case $n = 3$.

Theorem 2.5. *Let $U_E = 0$ be a Weierstrass equation for E. Then the ternary cubics with the same invariants as U_E, up to proper K-equivalence, are parametrised by* $\ker(\mathrm{Ob}) \subset H^1(K, E[3])$.

Proof. A ternary cubic U determines a plane cubic $C = \{U = 0\} \subset \mathbf{P}^2$ and a regular 1-form on C

$$\omega = \frac{Z^2 d(Y/Z)}{\frac{\partial U}{\partial X}(X,Y,Z)} \ .$$

Conversely, every twist $(C \to S, \omega)$ of $(E \to \mathbf{P}^2, \omega_E)$ with $S \cong \mathbf{P}^2$ arises in this way. In view of Lemmas 2.2 and 2.3 it only remains to show that ternary cubics U_1 and U_2 are properly equivalent if and only if they determine isomorphic pairs $(C_1 \to \mathbf{P}^2, \omega_1)$ and $(C_2 \to \mathbf{P}^2, \omega_2)$. This is immediate from the next lemma, or more precisely the special case of it where $g \in \mathrm{GL}_3(K)$. □

Lemma 2.6. *Let U_1 and U_2 be non-singular ternary cubics, determining pairs $(C_1 \to \mathbf{P}^2, \omega_1)$ and $(C_2 \to \mathbf{P}^2, \omega_2)$. If $gU_1 = U_2$ for some $g \in \mathrm{GL}_3(\overline{K})$ then the isomorphism induced by g, namely*

$$\gamma : C_2 \to C_1 \, ; \quad (X : Y : Z) \mapsto (g_{11}X + g_{21}Y + g_{31}Z : \ldots),$$

satisfies $\gamma^* \omega_1 = (\det g)\omega_2$.

Proof. If the lemma is true for $g_1, g_2 \in \mathrm{GL}_3(\overline{K})$ then it is true for $g_1 g_2$. So it suffices to let g run over a set of generators for $\mathrm{GL}_3(\overline{K})$. The result is already clear for matrices of the form

$$g = \begin{pmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_2 & 0 \\ 0 & \mu & \lambda_3 \end{pmatrix} \ .$$

Then for

$$g = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \quad \text{and} \quad g = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

we use the identities

$$\frac{Z}{Y} d\left(\frac{Y}{Z}\right) + \frac{Y}{Z} d\left(\frac{Z}{Y}\right) = 0$$

and

$$\frac{1}{Z^2}\frac{\partial U}{\partial X}(X,Y,Z) d\left(\frac{X}{Z}\right) + \frac{1}{Z^2}\frac{\partial U}{\partial Y}(X,Y,Z) d\left(\frac{Y}{Z}\right) = 0 \ .$$

□

Remark 2.7. The subset $\ker(\mathrm{Ob}) \subset H^1(K, E[3])$ contains the identity and is closed under taking inverses. A ternary cubic U represents the identity if and only if it has a K-rational point of inflection. The inverse of U is $-U$.

Remark 2.8. We claim that if K is a number field then the everywhere locally soluble ternary cubics with the same invariants as U_E, up to proper K-equivalence, are parametrised by the 3-Selmer group $S^{(3)}(E/K)$. It is shown in [9] that $S^{(3)}(E/K) \subset \ker(\mathrm{Ob})$, so this claim is a special case of Theorem 2.5.

This interpretation of $S^{(3)}(E/K)$ becomes more useful if we can find algorithms for performing the following tasks. We write $[U]$ for the proper equivalence class of U.

1. Given U test whether $[U] = 0$.
2. Given U_1, U_2 test whether $[U_1] = [U_2]$. If so find the change of co-ordinates that relates them.
3. Given U_1, U_2, U_3 test whether $[U_1] + [U_2] = [U_3]$.
4. Given U_1, U_2 determine whether there exists U_3 with $[U_1] + [U_2] = [U_3]$. If so compute U_3.

The analogues of these problems for the 2-Selmer group have been solved in [3].

3 The Etale Algebra

Let R be the étale algebra of $E[3]$. It is a product of field extensions of K, one for each orbit for the action of $\mathrm{Gal}(\overline{K}/K)$ on $E[3]$. It is shown in [6], [12] that there is an injective group homomorphism

$$w_1 : H^1(K, E[3]) \to R^\times/(R^\times)^3 \ .$$

According to [4, Paper I, Corollary 3.12] the restriction to $\ker(\mathrm{Ob})$ is given by

$$(C \to \mathbf{P}^2, \omega) \mapsto \alpha = \det M$$

where $M \in \mathrm{GL}_3(R) = \mathrm{Map}_K(E[3], \mathrm{GL}_3(\overline{K}))$ describes the action of $E[3]$ on $C \to \mathbf{P}^2$. (Recall that C is a torsor under E.)

In joint work [4] we describe a method for converting elements of $\ker(\mathrm{Ob})$ represented by $\alpha \in R^\times$ to elements of $\ker(\mathrm{Ob})$ represented by a ternary cubic $U(X, Y, Z)$. In this article we work in the opposite direction. We start with a ternary cubic $U(X, Y, Z)$ and convert it to $\alpha \in R^\times$. We also give a formula for the matrix $M \in \mathrm{GL}_3(R)$. This enables us to solve the problems listed at the end of Sect. 2.

4 The Hesse Family

Let C be a smooth plane cubic with Jacobian E. Let $\zeta \in \overline{K}$ be a primitive cube root of unity. Let S, T be a basis for $E[3]$ with $e_3(S, T) = \zeta$, where e_3 is the Weil pairing. Making a suitable choice of co-ordinates over $\overline{K}$ we may assume

$$M_S = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \zeta & 0 \\ 0 & 0 & \zeta^2 \end{pmatrix}, \quad M_T = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \ .$$

Then C has equation

$$U(X,Y,Z) = a(X^3+Y^3+Z^3) - 3bXYZ \ .$$

The invariants of this ternary cubic are

$$\begin{aligned} c_4(a,b) &= 3^4(8a^3+b^3)b \\ c_6(a,b) &= 3^6(8a^6+20a^3b^3-b^6) \\ \Delta(a,b) &= -3^9a^3(a^3-b^3)^3 \ . \end{aligned}$$

The Hessian is

$$H(X,Y,Z) = 27ab^2(X^3+Y^3+Z^3) - 27(4a^3-b^3)XYZ \ .$$

Taking $0_C = (0:1:-1)$ the elliptic curve $(C, 0_C)$ has Weierstrass equation

$$y^2z = x^3 - 27c_4(a,b)xz^2 - 54c_6(a,b)z^3 \ .$$

An explicit isomorphism is given by

$$\begin{aligned} x &= -27(4a^3-b^3)X - 81ab^2(Y+Z) \\ y &= 972a(a^3-b^3)(Y-Z) \\ z &= bX + a(Y+Z) \ . \end{aligned} \tag{2}$$

5 The Syzygetic Triangles

Let $U(X,Y,Z)$ be a non-singular ternary cubic with Jacobian E. The pencil of cubics spanned by U and its Hessian is a twist of the Hesse family. So there are exactly 4 singular fibres, and each singular fibre is a triangle. The sides of each triangle are the fixed lines for the action of M_T on $\mathbf{P}^2$ for some $0 \neq T \in E[3]$. So there is a Galois equivariant bijection between the syzygetic triangles and

$$\mathbf{P}(E[3]) = \frac{E[3] \setminus \{0\}}{\{\pm 1\}} \ .$$

Lemma 5.1. *Let U be a non-singular ternary cubic with invariants c_4, c_6 and Hessian H. Let $T = (x_T, y_T)$ be a non-zero 3-torsion point on the Jacobian*

$$E: \quad y^2 = x^3 - 27c_4x - 54c_6 \ .$$

Then the syzygetic triangle corresponding to $\pm T$ has equation

$$\mathcal{T} = \tfrac{1}{3}x_T U + H$$

and this equation satisfies $H(\mathcal{T}) = \frac{1}{27}y_T^2\mathcal{T}$.

Proof. We may assume that U belongs to the Hesse family with T the image of $(0:\zeta:-\zeta^2)$ under (2). The lemma follows by direct calculation. □

Remark 5.2. The Hessian of a triangle is a non-zero multiple of the triangle. So in Lemma 5.1 we have $y_T \neq 0$. This is no surprise, since a non-zero 3-torsion point on E cannot also be a 2-torsion point.

6 The Invariants of a Triangle

Let S_3 act on $\mathbf{Q}[\alpha_1, \alpha_2, \alpha_3, \beta_1, \beta_2, \beta_3]$ by simultaneously permuting the α_i and the β_i. The ring of invariants has Hilbert series

$$h(t) = \frac{1 + t^2 + 2t^3 + t^4 + t^6}{(1-t)^2(1-t^2)^2(1-t^3)^2} \ .$$

Let s_1, s_2, s_3 (respectively t_1, t_2, t_3) be the elementary symmetric polynomials in the α_i (respectively β_i). According to MAGMA the primary invariants are $s_1, s_2, s_3, t_1, t_2, t_3$. The remaining coefficients of

$$\mathcal{T}_1(X, Y, Z) = \prod_{i=1}^{3}(X + \alpha_i Y + \beta_i Z)$$

are

$$\begin{aligned} u &= \alpha_1(\beta_2 + \beta_3) + \alpha_2(\beta_3 + \beta_1) + \alpha_3(\beta_1 + \beta_2) \\ v &= \alpha_1\alpha_2\beta_3 + \alpha_1\beta_2\alpha_3 + \beta_1\alpha_2\alpha_3 \\ w &= \alpha_1\beta_2\beta_3 + \beta_1\alpha_2\beta_3 + \beta_1\beta_2\alpha_3 \ . \end{aligned}$$

The secondary invariants are $1, u, v, w, u^2, vw$. So as a $\mathbf{Q}$-algebra, the ring of invariants is generated by the coefficients of $\mathcal{T}_1$. There are 5 relations. These are obtained by writing uv, uw, v^2, w^2, u^3 as linear combinations of the secondary invariants. In fact MAGMA can rewrite any invariant as a $\mathbf{Q}[s_1, s_2, s_3, t_1, t_2, t_3]$-linear combination of the secondary invariants. For example

$$\begin{aligned} (\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1) &\begin{vmatrix} 1 & \alpha_1 & \beta_1 \\ 1 & \alpha_2 & \beta_2 \\ 1 & \alpha_3 & \beta_3 \end{vmatrix} \\ &= 2s_1^2 v - s_1 s_2 u - 6 s_1 s_3 t_1 + 2 s_2^2 t_1 - 6 s_2 v + 9 s_3 u \ . \end{aligned}$$

7 Formulae

Let C be a smooth plane cubic defined over K, with Jacobian E. Let L/K be any field extension. Given $T \in E[3](L)$ we aim to compute $M_T \in \mathrm{GL}_3(L)$ describing the action of T on C. We start with an equation $U = 0$ for C. Then we construct the syzygetic triangle $\mathcal{T} = \frac{1}{3} x_T U + H$ as described in Lemma 5.1. Making a change of co-ordinates if necessary, we may assume $\mathcal{T}(1, 0, 0) \neq 0$. Then factoring over the algebraic closure gives

$$\mathcal{T}(X, Y, Z) = r \prod_{i=1}^{3}(X + \alpha_i Y + \beta_i Z) \ . \tag{3}$$

We put

$$P = \begin{pmatrix} 1 & \alpha_1 & \beta_1 \\ 1 & \alpha_2 & \beta_2 \\ 1 & \alpha_3 & \beta_3 \end{pmatrix}$$

and $\xi = \alpha_1 + \zeta\alpha_2 + \zeta^2\alpha_3$.

Theorem 7.1. *If $\xi \neq 0$ then the matrix*

$$M_T = r\xi P^{-1} \begin{pmatrix} 1 & 0 & 0 \\ 0 & \zeta^2 & 0 \\ 0 & 0 & \zeta \end{pmatrix} P$$

belongs to $\mathrm{GL}_3(L)$ *and describes the action of* T *(or* $-T$*) on* C*.*

Proof. The required matrix has image in PGL_3 of order 3, and acts on $\mathbf{P}^2$ with fixed lines the sides of $\mathcal{T} = 0$. So the second statement is clear. We must check that M_T has coefficients in L.

We write $r^{-1}(\det P)M_T = A + (\zeta - \zeta^2)B$ where A and B are matrices with entries in $\mathbf{Q}[\alpha_1, \alpha_2, \alpha_3, \beta_1, \beta_2, \beta_3]$. We find $\sigma(A) = \mathrm{sign}(\sigma)A$ and $\sigma(B) = B$ for all $\sigma \in S_3$. So the entries of $(\det P)A$ and B are polynomials in the coefficients of $\mathcal{T}_1 = r^{-1}\mathcal{T}$. As discussed in Sect. 6 we can compute these polynomials using MAGMA.

By (3) we have $H(\mathcal{T}) = -r^2(\det P)^2\mathcal{T}$. Comparing with Lemma 5.1 it follows that $y_T = \pm 3(\zeta - \zeta^2)r \det P$. Therefore

$$(\det P)^2 M_T = r(\det P)A \pm \tfrac{1}{3} y_T B$$

and M_T has entries in L as required. □

We write

$$\begin{aligned} \mathcal{T}(X,Y,Z) = rX^3 + s_1X^2Y + s_2XY^2 + s_3Y^3 \\ + t_1X^2Z + t_2XZ^2 + t_3Z^3 \\ + YZ(uX + vY + wZ) \ . \end{aligned} \tag{4}$$

Theorem 7.2. $\det(M_T) = \frac{1}{2}(R \pm \frac{27r}{y_T}S)$ *where*

$$\begin{aligned} R &= 2s_1^3 - 9rs_1s_2 + 27r^2s_3 \\ S &= 2s_1^2v - s_1s_2u - 6s_1s_3t_1 + 2s_2^2t_1 - 6rs_2v + 9rs_3u \ . \end{aligned}$$

Proof. Comparing coefficients in (3) and (4) we find

$$\begin{aligned} \det(M_T) &= r^3(\alpha_1 + \zeta\alpha_2 + \zeta^2\alpha_3)^3 \\ &= \tfrac{1}{2}(R - 3(\zeta - \zeta^2)r^3\delta) \end{aligned}$$

where $\delta = (\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1)$. By the example in Sect. 6 we have $r^3\delta \det P = S$. Finally we recall from the proof of Theorem 7.1 that $y_T = \pm 3(\zeta - \zeta^2)r \det P$. □

Remark 7.3. The formulae of Theorems 7.1 and 7.2 sometimes fail and give zero. (The situation is analogous to the proof of Hilbert's theorem 90 using Lagrange resolvents.) However if they fail for both T and $-T$ then

$$\alpha_1 + \zeta\alpha_2 + \zeta^2\alpha_3 = 0$$

and

$$\alpha_1 + \zeta^2\alpha_2 + \zeta\alpha_3 = 0 \ .$$

From these we deduce $\det P = 0$, contradicting that (3) is the equation of a syzygetic triangle. So if our formula for M_T fails then we can use $(M_{-T})^{-1}$ instead.

8 Galois Actions

The formulae of Sect. 7 are slightly easier to use in the case E does not admit a rational 3-isogeny.

Lemma 8.1. *If E does not admit a rational 3-isogeny and $[U] \neq 0$, then we are guaranteed that $\mathcal{T}(1,0,0) \neq 0$.*

Proof. We recall that $\mathcal{T} = \frac{1}{3}x_T U + H$. By hypothesis $x_T \notin K$. So if $\mathcal{T}(1,0,0) = 0$ then $U(1,0,0) = H(1,0,0) = 0$. But then $(1:0:0)$ is a K-rational point of inflection and $[U] = 0$. □

Let $G \subset \mathrm{GL}_2(\mathbf{F}_3) \cong \mathrm{Aut}(E[3])$ be the image of Galois.

Lemma 8.2. *If E does not admit a rational 3-isogeny then $-I_2 \in G$.*

Proof. By hypothesis the image of G in $\mathrm{PGL}_2(\mathbf{F}_3) \cong S_4$ acts on $\mathbf{P}^1(\mathbf{F}_3)$ without fixed points. If this image is A_4 or S_4 then G contains $\mathrm{SL}_2(\mathbf{F}_3)$ by [13, IV, §3.4, Lemma 2]. Otherwise G is a 2-group, and so conjugate to a subgroup of the Sylow 2-subgroup generated by

$$a = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \quad \text{and} \quad b = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

The only non-trivial subgroups of $\langle a, b\rangle$, not containing $-I_2$, are the conjugates of $\langle b\rangle$. These possibilities for G are again ruled out by the assumption that E does not admit a rational 3-isogeny. □

If $-I_2 \in G$ then our formula for M_T works if and only if our formula for M_{-T} works. According to Remark 7.3 they cannot both fail, so they must both work.

9 Applications

In our examples we take $K = \mathbf{Q}$. Elliptic curves over $\mathbf{Q}$ are referenced by their labellings in [2].

9.1 Testing Proper Equivalence

We are given non-singular ternary cubics U_1 and U_2, and must decide whether they are properly equivalent. First we check that they have the same invariants c_4 and c_6. Then the plane cubics $U_1 = 0$ and $U_2 = 0$ each have Jacobian

$$E: \quad y^2 = x^3 - 27c_4x - 54c_6 \ .$$

We compute $\alpha_1, \alpha_2 \in R^\times$ by using Theorem 7.2 once for each orbit for the action of $\mathrm{Gal}(\overline{K}/K)$ on $E[3]$. Then U_1 and U_2 are properly equivalent if and only if $\alpha_1/\alpha_2 \in (R^\times)^3$.

For example the ternary cubics

$$U_1(X,Y,Z) = X^3 - 180Y^3 + 24Z^3 + 8X^2Y - 3X^2Z \\ + 3XY^2 - 148Y^2Z + 76XZ^2 - 280YZ^2 + 59XYZ$$

and

$$U_2(X,Y,Z) = 32X^3 + 48Y^3 + 32Z^3 - 14X^2Y - 17X^2Z \\ + 14XY^2 + 68Y^2Z - 34XZ^2 + 34YZ^2 - 91XYZ$$

each have invariants $c_4 = 1073512497$ and $c_6 = 35173095391575$. The Jacobian is

$$2534e2: \quad y^2 + xy + y = x^3 - x^2 - 22364844x - 40704009937 \ .$$

A non-trivial 3-torsion point is $T = (x_T, y_T)$ where

$$x_T = \tfrac{1}{12}(289u^6 + 765u^4 + 24567u^2 + 22035)$$
$$y_T = -\tfrac{1}{312}(239307u^7 + 3757u^6 + 638911u^5 + 9945u^4 \\ + 20357181u^3 + 319371u^2 + 45909405u + 286611)$$

and u is a root of $X^8 + 78X^4 - 36X^2 - 507 = 0$. We have $R = \mathbf{Q} \times L$ where $L = \mathbf{Q}(u)$ is a number field of degree 8. The first factor of $\mathbf{Q}$ may be ignored. Using Theorem 7.2 we compute

$$\alpha_1 = \tfrac{144}{13}(548276415600669u^7 - 912344032067546u^6 \\ +1459379319052681u^5 - 2428439574347826u^4 \\ +4665007562221020 3u^3 - 77626752951639190u^2 \\ +104433275464300347u - 173779291524426198)$$

$$\alpha_2 = \tfrac{1152}{13}(23737183831720776u^7 + 38664498064205221u^6 \\ +63182645951465768u^5 + 102915548856548337u^4 \\ +201967728414338 5464u^3 + 328976712978620 0531u^2 \\ +452135422005312 6264u + 7364643132168529779) \ .$$

We find $\alpha_1/\alpha_2 = b^3$ where

$$b = \tfrac{1}{31499104}(-35980u^7 + 9880u^6 - 90181u^5 + 294515u^4 \\ -2820090u^3 + 1603888u^2 - 6288205u + 17147429) \ .$$

It follows that U_1 and U_2 are properly equivalent.

Remark 9.1. Suppose we are given non-singular ternary cubics U and U' with invariants c_4, c_6 and c_4', c_6'. To test for equivalence we first find all $\lambda \in K^\times$ satisfying $c_4' = \lambda^4 c_4$ and $c_6' = \lambda^6 c_6$. Then for each such λ we test whether λU and U' are properly equivalent.

9.2 Finding Equivalences

We continue with the example of the last subsection and find the change of coordinates relating U_1 and U_2. Following the proof of Theorem 7.1 we compute

matrices $M_1, M_2 \in \mathrm{GL}_3(L)$ describing the action of T on $U_1 = 0$ and $U_2 = 0$. Since $\alpha_1/\alpha_2 \in (L^\times)^3$ we may arrange that $\det M_1 = \det M_2$. We are looking for $g \in \mathrm{GL}_3(K)$ with $U_2 = (\det g)^{-1}(gU_1)$. We must have

$$M_1 g^T = c g^T M_2$$

for some $c \in L^\times$. Taking determinants gives $c^3 = 1$. Since L contains no non-trivial cube roots of unity it follows that $c = 1$. Solving for g by linear algebra we find

$$g = \begin{pmatrix} 19 & -1 & 6 \\ -8 & -8 & 0 \\ 22 & -2 & -4 \end{pmatrix} \quad .$$

Remark 9.2. If $E[3](K) \neq 0$ then there will be more than one change of coordinates relating U_1 and U_2. These will correspond to different choices for the constant c. Indeed by the Weil pairing there is an inclusion $E[3](K) \subset \mu_3(R)$.

9.3 Addition of Selmer Group Elements

The rank 0 elliptic curve

$$E = 4343b1: \quad y^2 + y = x^3 - 325259x - 71398995$$

has Tate-Shafarevich group of analytic order 9. The following two elements of $S^{(3)}(E/\mathbf{Q})$ are visible in the rank 1 elliptic curves $21715a1$ and $117261k1$. (We will explain these calculations more fully in subsequent work. The concept of visibility was introduced in [5].)

$$\begin{aligned} U_1(X,Y,Z) &= X^3 + 15Y^3 - 17Z^3 - 8X^2Y + 4X^2Z \\ &\quad + 15XY^2 - 13Y^2Z + 32XZ^2 + 26YZ^2 + 4XYZ \\ U_2(X,Y,Z) &= 7X^3 - 13Y^3 - 17Z^3 + 7X^2Y + 3X^2Z \\ &\quad - 4XY^2 - 2Y^2Z + 12XZ^2 - 15YZ^2 - 30XYZ \end{aligned}$$

We use Theorem 7.2 to compute $\alpha_1, \alpha_2 \in R^\times$. We find that α_1, α_2 are independent in $R^\times/(R^\times)^3$. Applying the work of [4] to $\alpha_1\alpha_2$ and α_1/α_2 we obtain

$$\begin{aligned} U_3(X,Y,Z) &= -5X^3 + 12Y^3 + 31Z^3 + 3X^2Y - 5X^2Z \\ &\quad + 5XY^2 + 2Y^2Z + 4XZ^2 + 26YZ^2 + 40XYZ \\ U_4(X,Y,Z) &= -11X^3 + 8Y^3 - 13Z^3 - 9X^2Y + 11X^2Z \\ &\quad - 15XY^2 - Y^2Z - 16XZ^2 - 3YZ^2 - 38XYZ \quad . \end{aligned}$$

Assuming the Birch Swinnerton-Dyer conjecture, we have

$$Ш(E/\mathbf{Q}) = \{0, \pm[U_1], \pm[U_2], \pm[U_3], \pm[U_4]\} \quad .$$

We have found these equations without the need to compute the class group or unit group of any number field.

9.4 Testing Global Solubility

We show that the ternary cubic

$$U_1(X,Y,Z) = 7X^3 + 9Y^3 + 16Z^3 + 2X^2Y \\ + 5Y^2Z + 5XZ^2 - 7YZ^2 - 31XYZ$$

is insoluble over $\mathbf{Q}$. The Jacobian

$$E = 35882a1: \quad y^2 + xy = x^3 - x^2 - 156926x - 24991340$$

has Mordell-Weil group $E(\mathbf{Q}) \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}$. A point of infinite order is $P = (693, 13750)$. Embedding $E \subset \mathbf{P}^2$ via $|2.0_E + P|$ we obtain

$$U_2(X,Y,Z) = 15Y^3 + 1254Z^3 + X^2Z - XY^2 \\ + 674Y^2Z + 10XZ^2 - 291YZ^2 + XYZ \ .$$

We use Theorem 7.2 to compute $\alpha_1, \alpha_2 \in R^\times$. We then check that α_1, α_2 are independent in $R^\times/(R^\times)^3$. Since U_2 is soluble over $\mathbf{Q}$ and $E(\mathbf{Q})/3E(\mathbf{Q}) \cong \mathbf{Z}/3\mathbf{Z}$, it follows that U_1 is insoluble over $\mathbf{Q}$.

Alternatively this could be checked using the explicit formulae for the covering map given in [1].

9.5 Reduction of Ternary Cubics

It is desirable to be able to replace an integer coefficient ternary cubic by an equivalent one with smaller coefficients. One method, explained to me by Michael Stoll, first computes a certain inner product, and then uses standard lattice reduction techniques. By an inner product on a complex vector space we mean a positive definite Hermitian form. We recall the Weyl unitary trick.

Lemma 9.3. *Let V be an irreducible complex representation of a finite group G. Then (up to scalars) there is a unique G-invariant inner product $\langle\ ,\ \rangle : V \times V \to \mathbf{C}$.*

Proof. Let $\langle\ ,\ \rangle_0$ be any inner product on V. Then

$$\langle u, v\rangle = \sum_{g \in G} \langle gu, gv\rangle_0$$

is a G-invariant inner product. By Schur's lemma the complex vector space of G-invariant sesquilinear forms on V is 1-dimensional. □

We now take $C \subset \mathbf{P}^2$ a smooth plane cubic defined over $\mathbf{Q}$ with Jacobian E. The action of $E[3]$ on C extends to $\mathbf{P}^2$ to give $\chi : E[3] \to \mathrm{PGL}_3$. Lifting to SL_3 we obtain a diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mu_3 & \longrightarrow & H_3 & \longrightarrow & E[3] & \longrightarrow & 0 \\ & & \| & & \downarrow & & \downarrow{\scriptstyle \chi} & & \\ 0 & \longrightarrow & \mu_3 & \longrightarrow & \mathrm{SL}_3 & \longrightarrow & \mathrm{PGL}_3 & \longrightarrow & 0 \ . \end{array}$$

The Heisenberg group H_3 is a non-abelian group of order 27. For the reduction of ternary cubics, we use the unique Heisenberg-invariant inner product. Theorem 7.1 gives a convenient way of computing this inner product. Indeed if $M_1 \in \mathrm{SL}_3(\mathbf{R})$ and $M_2 \in \mathrm{SL}_3(\mathbf{C})$ generate the action of $E[3]$ on C then the required inner product on $\mathbf{C}^3$ has Gram matrix

$$\sum_{r=0}^{2} (\overline{M_2}^r)^T \left(\sum_{s=0}^{2} (M_1^s)^T M_1^s \right) M_2^r \ .$$

Acknowledgements

I would like to thank John Cremona, Cathy O'Neil and Michael Stoll for many useful discussions. All computer calculations in support of this work were performed using MAGMA [8]. The examples in Sect. 9 were prepared with the assistance of some programs written by Michael Stoll in connection with the joint work [4].

References

1. S.Y. An, S.Y. Kim, D.C. Marshall, S.H. Marshall, W.G. McCallum and A.R. Perlis. Jacobians of genus one curves. *J. Number Theory* **90** (2001), no. 2, 304–315.
2. J.E. Cremona. *Algorithms for modular elliptic curves.* Cambridge University Press, 1997. See also `http://www.maths.nott.ac.uk/personal/jec/ftp/data`
3. J.E. Cremona. Classical invariants and 2-descent on elliptic curves. *J. Symbolic Comput.* **31** (2001), no. 1-2, 71–87.
4. J.E. Cremona, T.A. Fisher, C. O'Neil, D. Simon and M. Stoll. *Explicit n-descent on elliptic curves*, I Algebra, II Geometry, III Algorithms. In preparation.
5. J.E. Cremona, B. Mazur. Visualizing elements in the Shafarevich-Tate group. *Experiment. Math.* **9** (2000), no. 1, 13–28.
6. Z. Djabri, E.F. Schaefer and N.P. Smart, Computing the p-Selmer group of an elliptic curve, *Trans. Amer. Math. Soc.* **352** (2000), no. 12, 5583–5597.
7. D. Hilbert. *Theory of algebraic invariants.* Cambridge University Press, 1993.
8. MAGMA is described in W. Bosma, J. Cannon and C. Playoust. The Magma algebra system I: The user language. *J. Symbolic Comput.* **24**, 235–265 (1997). See also `http://magma.maths.usyd.edu.au/magma/`
9. C. O'Neil. The period-index obstruction for elliptic curves, *J. Number Theory* **95** (2002), no. 2, 329–339.
10. B. Poonen. An explicit algebraic family of genus-one curves violating the Hasse principle. *J. Théor. Nombres Bordeaux* **13** (2001), no. 1, 263–274.
11. G. Salmon. *A treatise on the higher plane curves.* Third edition, Hodges, Foster and Figgis, Dublin, 1879.
12. E.F. Schaefer and M. Stoll. How to do a p-descent on an elliptic curve. *Trans. Amer. Math. Soc.* **356** (2004), no. 3, 1209–1231.
13. J.-P. Serre. *Abelian ℓ-adic representations and elliptic curves.* McGill University lecture notes, W. A. Benjamin, Inc., New York-Amsterdam, 1968.
14. J.H. Silverman. *The arithmetic of elliptic curves.* Springer GTM **106**, 1986.
15. B. Sturmfels. *Algorithms in invariant theory.* Texts and Monographs in Symbolic Computation, Springer-Verlag, Vienna, 1993.