Computing the Mordell-Weil rank of Jacobians of curves of genus two.

Daniel M. Gordon [*]
Department of Computer Science
University of Georgia
Athens, GA 30602 USA
and
David Grant [†]
Department of Mathematics
University of Colorado at Boulder
Boulder, CO 80309 USA

August 28, 1992

Abstract

We derive the equations necessary to perform a 2-descent on the Jacobians of curves of genus two with rational Weierstrass points. We compute the Mordell-Weil rank of the Jacobian of some genus two curves defined over the rationals, and discuss the practicality of using this method.

1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11Y50; Secondary 14K15.

[*] Partially supported by a University of Georgia Faculty Research Grant.
[†] Supported by a NATO Postdoctoral Fellowship.

Introduction

Let C be a curve of genus two defined over a number field K, and J its Jacobian variety. The Mordell-Weil theorem states that $J(K)$ is a finitely-generated Abelian group, but except in a few special cases, it has never been explicitly determined. Recent work of Vojta [24], Faltings [9], and Bombieri [3] relates the number of rational points on C to the rank of $J(K)$, increasing the interest in computing the latter. Further conjectures and results relating $C(K)$ and $J(K)$ can be found in [17] and [23].

In addition, elliptic curves have recently been applied to many computational problems, such as primality testing and factorization [15], and cryptography [14]. There are indications that curves of higher genus have similar uses. They have been proposed for better primality tests [1] and new cryptosystems [13]. However, the lack of explicit knowledge of the properties of these curves have slowed their widespread use. The recent formulations of the group law on the Jacobian by Cantor in [4] and the second author in [11] are a beginning, but more remains to be done.

In this paper we show how to compute the rank of $J(K)$ for a wide class of genus two curves, namely those which have all their Weierstrass points defined over K, and whose Jacobians have no 2-torsion in their Tate-Shafarevich groups. The former constraint could be removed by performing a Galois descent from $K(J[2])$ to K. This would take us too far afield, so we refrain from making this descent now. The latter, however, is a serious constraint, for what we actually compute is the 2-Selmer group of J.

In principle, it is well-known how to compute the Selmer group: much of this work was done by Cassels [6]. One missing ingredient there was the defining equations for J, which have now been worked out by Flynn in [10] and the second author in [11]. For computational reasons, more work has to be done beyond that stated in [6]: indeed, it is beneficial to find equations that define projective models of the homogeneous spaces of J. In the first section we will give an overview of the descent machinery, paralleling the exposition in [22] and [5]. In the following section we will present the necessary geometry to compute the requisite homogeneous spaces. In section 3 we outline the method used to perform computations, and some examples for curves defined over the rationals are explained in section 4.

This research was undertaken while the second author was enjoying the hospitality of Cambridge University.

1 The Descent Machinery

Let C be a curve of genus two defined over a number field K, all of whose Weierstrass points are rational over K. Then C has a model of the form:

$$\begin{aligned} y^2 &= (x-a_1)(x-a_2)(x-a_3)(x-a_4)(x-a_5) \\ &= x^5 + b_1x^4 + b_2x^3 + b_3x^2 + b_4x + b_5, \end{aligned}$$

where the a_i $(i = 1, \ldots, 5)$ are distinct elements of K. The normalization of C has one point at infinity, which is rational over K, and which we denote as ∞. The curve has a hyperelliptic involution I which maps a point (x, y) to $(x, -y)$. Let J be the Jacobian variety of C, which we will always take to be defined by the model given in [11] and described in the next section. We embed C into J via the divisor class map

$$P \longrightarrow Cl(P - \infty),$$

and denote its image by Θ, a theta divisor. The origin O of J lies on Θ, and every point Q on J other than O can be uniquely represented by a divisor

$$P_1 + P_2 - 2\infty,$$

for some unordered pair of points P_1, P_2 on C, with P_2 not equal to $I(P_1)$. Note that $Q \neq O$ lies on Θ if and only if P_1 or P_2 is ∞. We let U be the open complement of Θ on J.

The group $J[2]$ of 2-torsion points on J has sixteen elements. The divisors 0 and $e_i = a_i - \infty$ $(1 \leq i \leq 5)$ represent the six 2-torsion points which lie on Θ. The remaining 2-torsion points are represented by the divisors $e_{ij} = a_i + a_j - 2\infty$ $(1 \leq i < j \leq 5)$. Since the a_i all lie in K, all the 2-torsion points are K-rational. Let $\overline{K}$ be an algebraic closure of K, and let G be the Galois group of $\overline{K}$ over K.

Using the exact sequence of Galois modules,

$$0 \longrightarrow J[2] \xrightarrow{i} J(\overline{K}) \xrightarrow{[2]} J(\overline{K}) \longrightarrow 0,$$

where i is the natural injection, and [2] the multiplication-by-2 endomorphism, we get from the long exact sequence of Galois cohomology:

$$0 \longrightarrow J(K)/2J(K) \xrightarrow{\delta} H^1(G, J[2]) \xrightarrow{i} H^1(G, J)[2] \longrightarrow 0. \qquad (1.1)$$

Let M_K be a complete set of inequivalent absolute values on K. For each v in M_K, let K_v denote the localization of K at v. Picking an extension of v to $\overline{K}$ fixes a decomposition group G_v. As before, we get an exact sequence

$$0 \longrightarrow J(K_v)/2J(K_v) \xrightarrow{\delta} H^1(G_v, J[2]) \xrightarrow{i} H^1(G_v, J)[2] \longrightarrow 0. \quad (1.2)$$

The inclusions $G_v \subseteq G$, $J(\overline{K}) \subseteq J(\overline{K_v})$ give us restriction maps

$$res_v : H^1(G, J) \longrightarrow H^1(G_v, J).$$

The 2-Selmer group is defined as

$$S_2(J/K) = \ker \left\{ H^1(G, J[2]) \overset{\prod(\mathrm{res}_v \circ\ i)}{\longrightarrow} \prod_{v \in M_K} H^1(G_v, J) \right\},$$

and the Tate-Shafarevich group is

$$Ш\ (J/K) = \ker \left\{ H^1(G, J) \overset{\prod \mathrm{res}_v}{\longrightarrow} \prod_{v \in M_K} H^1(G_v, J) \right\}.$$

For all $v \in M_K$ the restriction maps define a map from sequence (1.1) to (1.2), so we get the exact sequence

$$0 \longrightarrow J(K)/2J(K) \xrightarrow{\delta} S_2(J/K) \xrightarrow{i} Ш\ (J/K)[2] \longrightarrow 0.$$

Let S be the finite set of places of K consisting of all the primes at which J has bad reduction, the primes dividing 2, and all the infinite places. Let $H^1(G, J[2]; S)$ denote the subgroup of $H^1(G, J[2])$ consisting of cocycles unramified outside S. The proof of the weak Mordell-Weil theorem shows that $H^1(G, J[2]; S)$ is finite, and that it contains $S_2(J/K)$. In our case, since all the 2-torsion is rational, $J[2] \cong (\mu_2)^4$ as Galois modules, so we have the Kummer theory isomorphism,

$$H^1(G, J[2]) \cong \left(K^*/(K^*)^2\right)^4,$$

and the isomorphism allows to to identify the classes which are unramified outside S. Specifically, $D^4 \cong H^1(G, J[2]; S)$, where

$$D = \{x \in K^* \mid \mathrm{ord}_v(x) \equiv 0 \pmod 2\ \forall v \notin S\}/(K^*)^2.$$

Therefore

$$\delta(J(K)/2J(K)) \subseteq S_2(J/K) \subseteq D^4.$$

We identify $H^1(G,J)$ and $H^1(G_v,J_v)$ with the Weil-Châtelet group of (principal) homogeneous spaces for J over K and K_v, respectively. Recall that a homogeneous space represents the trivial class if and only if it has a rational point.

Now for all $v \notin S$, $J[2]$ is an unramified G_v module, so it follows from a theorem of Tate that the image of $H^1(G,J[2];S)$ in $H^1(G_v,J)$ is zero [19].

Hence we have

$$S_2(J/K) = \ker\left\{(D^4) \overset{\prod(\mathrm{res}_v o\ i)}{\longrightarrow} \prod_{v\in S} H^1(G_v,J)\right\}.$$

This is how we will compute $S_2(J/K)$ – for every element in D^4 we compute the corresponding homogeneous space and test to see whether it is locally trivial at all v in S. This is an effective procedure which will be described in the following two sections. In many cases, we can identify $J(K)/2J(K)$ with $S_2(J/K)$, and describe $J(K)$ precisely. However, whenever $\text{Ш}\ (J/K)[2] \neq 0$, there are homogeneous spaces which are not trivial, yet are everywhere locally trivial.

Remark: Cassels [6] has already made great progress on the problem of computing the rank of the Jacobian of a curve of genus 2. He outlined a plan for general curves, with or without rational Weierstrass points, which we will summarize, since it sheds light on our somewhat different approach.

In the case where the Weierstass points are rational, he computed a map

$$J(K)/2J(K) \longrightarrow D^5. \tag{1.3}$$

The components of the map are given generically for points on U by:

$$(x_1,y_1)+(x_2,y_2)-2\infty \longrightarrow (x_1-a_i)(x_2-a_i) \pmod{(K^*)^2}, \quad (1 \le i \le 5),$$

and for points on Θ by:

$$(x,y)-\infty \longrightarrow (x-a_i) \pmod{(K^*)^2}, \quad (1 \le i \le 5).$$

The map is determined by its values for $1 \le i \le 4$, and it must be modified if any of the points on C specializes to a Weierstrass point (see [6] or Corollary 2 of the next section).

This almost gives a way to compute the 2-Selmer group, once the equations defining J are known. If $f_1, ..., f_n$ are polynomials which define U, and $g_1, ..., g_m$ are polynomials defining C, then for $d = (d_1, d_2, d_3, d_4)$ representing an element in D^4 we can form the auxiliary varieties

$$F_d : f_j = 0 \quad (1 \leq j \leq n); \quad (x_1 - a_i)(x_2 - a_i) = d_i z_i^2 \quad (1 \leq i \leq 4),$$

and

$$G_d : g_k = 0 \quad (1 \leq k \leq m); \quad (x - a_i) = d_i z_i^2 \quad (1 \leq i \leq 4).$$

Then d will be the image of a point in $J(K)/2J(K)$ (except in the aforementioned special cases) precisely when F_d or G_d has a K-rational solution with $z_1 z_2 z_3 z_4$ non-zero. However, it is very hard to test (even locally) whether a number is zero, so for computational reasons, it is expedient to modify this approach.

The problem is that F_d is birational to but not isomorphic to an open subvariety of a homogeneous space corresponding to d. To remove the condition on $z_1 z_2 z_3 z_4$, we need only to take the normalization of F_d in the extension of $K(U)$ generated by z_1, z_2, z_3, and z_4. But since F_d is not projective, one must search for rational points instead of integral points. Therefore, we choose in the next section to tackle the problem afresh. This serves the dual purposes of making our argument self-contained from Cassels's approach, and also of showing off some of the beauty of the underlying geometry.

2 Homogeneous Spaces

Let $d = (d_1, d_2, d_3, d_4)$ be a fixed element of $(K^*)^4$ representing a class in D^4. In the last section we defined a map i

$$D^4 \cong H^1(G, J[2]; S) \xrightarrow{i} H^1(G, J)$$

which associates to each d a cocycle $i(d)$. The goal of this section is to determine the homogeneous space of J corresponding to $i(d)$, which we will denote by $H(d)$.

Let Y be the pullback of $[2] : J \longrightarrow J$ along the embedding of C into J,

$$\begin{tikzcd}
Y \arrow[r] \arrow[d] & J \arrow[d, "{[2]}"] \\
C \arrow[r] & J
\end{tikzcd}$$

and let E be its open complement in J. We will consider Y as embedded in J. Then Y and E are respectively étale covers of Θ and U. We have,

$$\mathrm{Gal}(E/U) \simeq \mathrm{Gal}(Y/C) \simeq J[2],$$

given by defining an automorphism σ_e in $\mathrm{Gal}(E/U)$ as the translation-by-e map $T_e : J \to J$ for some e in $J[2]$. If we so choose, we can twist J by twisting Y and E separately to spaces $Y(d)$ and $E(d)$. Equations for these twists are given in Corollary 1 and in the remark following Corollary 2. Testing them separately provides one way to test $H(d)$ for local triviality. But this requires checking for non-integral local points, which is impractical. We choose instead to give a projective model for $H(d)$ by taking the projective closure of $E(d)$.

The equations defining E are not too difficult to calculate. The underlying geometry is described by Mumford in [20], but we will develop all the explicit material we need in a series of lemmas.

For an affine subvariety V of J, we let $A(V)$ denote its ring of regular functions. For a function f on J we let (f) denote its divisor. For a divisor W on J, we let $L(W)$ denote the vector space of functions f on J such that that $(f) + W$ is effective.

Lemma 1 *The ring A(E) is generated by L(Y).*

Proof: The divisor Θ is symmetric, hence by [21], $Y = [2]^*\Theta$ is linearly equivalent to 4Θ, which is very ample.

Our tasks, therefore, are first to find a K-basis for $L(Y)$, and then to find all the relations among the basis elements. We begin by recalling a set of equations that define U.

For a point $z = (x_1, y_1) + (x_2, y_2) - 2\infty$, there are functions defined in [11]:

$$X_{22}(z) = x_1 + x_2,$$
$$X_{12}(z) = -x_1 x_2,$$
$$X_{11} =$$
$$\frac{X_{22}X_{12}^2 + 2b_1X_{12}^2 - b_2X_{22}X_{12} - 2b_3X_{12} + b_4X_{22} + 2b_5 - 2y_1y_2}{X_{22}^2 + 4X_{12}},$$
$$X_{222}(z) = (y_1 - y_2)/(x_1 - x_2),$$
$$X_{122}(z) = (x_1y_2 - x_2y_1)/(x_1 - x_2),$$

which are regular on U, and generate $A(U)$. It was proven in [11] that

$$g_1: \quad X_{122}^2 = X_{22}X_{12}^2 - X_{11}X_{12} + b_1X_{12}^2 + b_5,$$
$$g_2: \quad X_{222}^2 = X_{22}^3 + X_{12}X_{22} + b_1X_{22}^2 + b_2X_{22} + X_{11} + b_3,$$
$$g_3: \quad 2X_{122}X_{222} = 2X_{12}X_{22}^2 - X_{11}X_{22} + X_{12}^2 + 2b_1X_{12}X_{22} + b_2X_{12} + b_4.$$

are a set of defining equations for U in 5-dimensional affine space.

For notational convenience, we also introduce the following functions from [11]. Set

$$g_4: \quad X_{112} = X_{12}X_{222} - X_{22}X_{122},$$
$$g_5: \quad X_{111} = -X_{11}X_{222} - X_{12}X_{122} + 2X_{22}X_{112} + 2b_1X_{112} - b_2X_{122},$$
$$g_6: \quad X = \tfrac{1}{2}(X_{11}X_{22} - X_{12}^2 + b_2X_{12} - b_4).$$

Then $g_1, ..., g_6$ define a variety in 8-dimensional affine space isomorphic to U.

For $1 \le i \le 5$, define $h_{e_i}(z)$ by

$$h_{e_i}(z) = -X_{12}(z) - a_iX_{22}(z) + a_i^2 = (x_1 - a_i)(x_2 - a_i). \tag{2.1}$$

Then $(h_{e_i}(z)) = 2T_{e_i}^*\Theta - 2\Theta$, so automatically $h_{e_i}([2]z)$ is the square of a function in $\overline{K}(J)$. In fact, it is a square in $K(J)$ (see [6] Theorem 4.2):

Lemma 2 *For $1 \le i \le 5$, there are even functions t_{e_i} in $K(J)$, which lie in $L(Y)$, such that*

$$h_{e_i}([2]z) = (t_{e_i}(z))^2.$$

Proof: Let $w = x - a_i$. Then C is defined by

$$y^2 = w^5 + c_1w^4 + c_2w^3 + c_3w^2 + c_4w,$$

for some $c_1, ..., c_4$ in K. If $z = (w_1, y_1) + (w_2, y_2) - 2\infty$, then the even function $h_{e_i}(z) = w_1w_2$. Suppose that $P_1 = (w_1, y_1)$ and $P_2 = (w_2, y_2)$ are independent generic points of C over K. Then $P = P_1 + P_2 - 2\infty$ is a generic point of J over K, and we can compute $[2]P$ as follows. There is a function in $K(C)$

$$g = y - \alpha_1(P)w^3 - \alpha_2(P)w^2 - \alpha_3(P)w - \alpha_4(P),$$

where $\alpha_1, ..., \alpha_4$ are odd functions in $K(J)$, such that the divisor of g is $2P + Q$ for some $Q = (w_3, y_3) + (w_4, y_4) - 2\infty$. Then $[2]P = -Q$, and $h_{e_i}([2]P) = w_3w_4$. Now

$$(\alpha_1w^3 + \alpha_2w^2 + \alpha_3w + \alpha_4)^2 = w^5 + c_1w^4 + c_2w^3 + c_3w^2 + c_4w$$

is a polynomial whose roots (with multiplicity) are w_1, w_1, w_2, w_2, w_3 and w_4. Comparing constant terms gives $w_3w_4 = \alpha_4^2/\alpha_1^2w_1^2w_2^2$. Therefore $h_{e_i}([2]z)$ is the square of the even function $t_{e_i}(z) = \alpha_4(z)/\alpha_1(z)h_{e_i}(z)$ in $K(J)$.

Now for any $1 \leq i < j \leq 5$, we define $t_{e_{ij}}(z)$ by the relation

$$X_{112}([2]z)+(a_i+a_j)X_{122}([2]z)+a_ia_jX_{222}([2]z) = t_{e_i}(z)t_{e_j}(z)t_{e_{ij}}(z). \qquad (2.2)$$

Since $X_{112}, X_{122}, X_{222}$ are odd and t_{e_i}, t_{e_j} are even, $t_{e_{ij}}$ is an odd function. Squaring (2.2) and using g_1, g_2, g_3, g_4 and (2.1) gives us the relation

$$h_{e_{ij}}([2]z) = (t_{e_{ij}}(z))^2, \qquad (2.3)$$

where

$$h_{e_{ij}}(z) = X_{11}(z) - X_{11}(e_{ij}) + (a_i + a_j)X_{12}(z) + a_ia_jX_{22}(z),$$

so $t_{e_{ij}}$ is in $K(J)$, and $L(Y)$ as well. It follows from the group law in [11] that $h_{e_{ij}}(z)$ has divisor $2T^*_{e_{ij}}\Theta - 2\Theta$. We will soon prove that $1, t_{e_i}$ $(1 \leq i \leq 5), t_{e_{ij}}$ $(1 \leq i < j \leq 5)$ form a K-basis for $L(Y)$. We first need to describe the action of $\mathrm{Gal}(E/U)$ on these functions, which is given via the Weil pairing [21].

Since J is principally-polarized, we can define the Weil pairing on $J[2]$ as a map

$$w : J[2] \times J[2] \to \mu_2,$$

given as in [21]. For O in $J[2]$ we define $h_O = t_O = 1$. Then for any e in $J[2]$ we have $(h_e(z)) = 2T_e^*\Theta - 2\Theta$, and $h_e([2]z) = (t_e(z))^2$, so $w(e', e'')$ for e', e'' in $J[2]$ is given by

$$w(e', e'') = \frac{t_{e'}(z + e'')}{t_{e'}(z)}, \tag{2.4}$$

for those z in J for which (2.4) is defined. The pairing is bilinear, non-degenerate, and $w(e, e) = 1$ for all e in $J[2]$. Therefore the pairing is alternating, and since it takes its values in μ_2, it is also symmetric.

Lemma 3 *Let i, j, k be distinct elements of $\{1, 2, 3, 4, 5\}$. Then*

$$a)\ w(e_i, e_{jk}) = 1,$$

$$b)\ w(e_i, e_j) = -1.$$

Proof: The divisor of $t_{e_i}(z)$ is $[2]^{-1}(T_{e_i}^*\Theta - \Theta)$. Since e_{jk} is not contained in the support of $T_{e_i}^*\Theta - \Theta$, we can pick a z' in $[2]^{-1}e_{jk}$ so that (2.4) is defined at z'. Since $z' + e_{jk} = -z'$, and t_{e_i} is even, we get $w(e_i, e_{jk}) = 1$, establishing (a). By bilinearity, $w(e_i, O) = 1$, and $w(e_i, e_i) = 1$, so we have found 8 elements e of $J[2]$ such that $w(e_i, e) = 1$. Since the pairing is non-degenerate, $w(e_i, e_j) = -1$, establishing (b). Alternatively, one can compute the pairing by evaluating functions on the curve, see [2], p. 283.

For any e'' in $J[2]$, we define a character on $J[2]$ by

$$\chi_{e''}(e') = w(e', e'').$$

Then the action of $\mathrm{Gal}(E/U)$ is given by

$$\sigma_{e'}(t_{e''}) = w(e'', e')t_{e''} = w(e', e'')t_{e''} = \chi_{e''}(e')t_{e''}.$$

By the non-degeneracy of the Weil pairing, these are precisely the 16 distinct characters of order dividing 2 on $J[2]$.

Lemma 4 *The vector space $L(Y)$ has a K-basis given by the functions*

$$1,\ t_{e_i}\ \ (1 \le i \le 5), \quad \textit{and} \quad t_{e_{ij}}\ \ (1 \le i < j \le 5).$$

Proof: We have already shown that the functions are in $L(Y)$. Since the 16 functions are all in different isotypical components for the action of $\mathrm{Gal}(E/U)$ on $L(Y)$, they are linearly independent.

We will prove that $t_{e_1}, t_{e_2}, t_{e_3}, t_{e_4}, t_{e_{15}}, t_{e_{25}}, t_{e_{35}}$, and $t_{e_{45}}$ generate $L(Y)$ as a K-algebra. First we need to derive some relations among the variables. As a convention we will let i, j, k denote any three elements of the set $\{1, 2, 3, 4, 5\}$, and let l and m stand for the complementary elements.

Lemma 5

$$\begin{aligned}-t_{e_{ij}}(z)t_{e_{ik}}(z)t_{e_{jk}}(z) = {} & X_{111}([2]z) + (a_i + a_j + a_k)X_{112}([2]z) \\ & + (a_ia_j + a_ia_k + a_ja_k)X_{122}([2]z) + a_ia_ja_kX_{222}([2]z), \quad (2.5)\end{aligned}$$

$$\begin{aligned}t_{e_i}(z)t_{e_{jk}}(z)t_{e_{lm}}(z) = {} & -X([2]z) + a_iX_{11}([2]z) \\ & + (a_ja_k + a_la_m + a_i(a_j + a_k + a_l + a_m))X_{12}([2]z) + a_i(a_ja_k + a_la_m)X_{22}([2]z) \\ & - a_i(a_ja_ka_l + a_ja_ka_m + a_ja_la_m + a_ka_la_m + a_i(a_la_m + a_ja_k)). \quad (2.6)\end{aligned}$$

Proof: Using $g_1, ..., g_6$ and Lemma 2, one can verify that (2.5) follows from multiplying together (2.2) for each of $(i, j), (i, k), (j, k)$ and then dividing by (2.1) for i, j, and k. Likewise (2.6) follows from multiplying (2.2) for each of (j, k) and (l, m) and (2.1) for i, and then dividing by $y_1y_2([2]z) = t_{e_i}(z)t_{e_j}(z)t_{e_k}(z)t_{e_l}(z)t_{e_m}(z)$ (which can be derived from the definition of X_{11}). In fact, both these relations were discovered by using the analytic theory of the Jacobian as outlined in [11].

Lemma 6 *We have six types of equations:*

$$\begin{aligned}\textit{Type } I(i,j,k): \quad & (a_j - a_i)t_{e_k}^2 + (a_i - a_k)t_{e_j}^2 + (a_k - a_j)t_{e_i}^2 \\ & = (a_j - a_i)(a_k - a_i)(a_k - a_j).\end{aligned}$$

$$\textit{Type } II(i,j,k): \quad t_{e_{ij}}^2 - t_{e_{ik}}^2 = (a_k - a_j)(t_{e_i}^2 - (a_i - a_l)(a_i - a_m)).$$

$$\textit{Type } III(i,j,l,m): \quad t_{e_{il}}t_{e_{im}} - t_{e_{jl}}t_{e_{jm}} = (a_j - a_i)t_{e_l}t_{e_m}.$$

$$\textit{Type } IV(i,j,k,l,m): \quad t_{e_i}t_{e_{jk}} - t_{e_j}t_{e_{ik}} = (a_i - a_j)t_{e_{lm}}.$$

$$\textit{Type } V(i,j,k,l,m): \quad t_{e_{jk}}t_{e_{lm}} - t_{e_{jl}}t_{e_{km}} = (a_j - a_m)(a_l - a_k)t_{e_i}.$$

$$\textit{Type } VI(i,j,k,l): \quad (a_j - a_k)t_{e_{il}}t_{e_i} + (a_k - a_i)t_{e_{jl}}t_{e_j} + (a_i - a_j)t_{e_{kl}}t_{e_k} = 0.$$

Proof:

Type I: Take (2.1) and Lemma 2 for i, j, and k, and eliminate X_{12} and X_{22}.

Type II: Take (2.3) for (i, j) and (i, k) and eliminate X_{11}. This gives a multiple of (2.1) for i plus a constant. Then apply Lemma 2.

Type III: Take (2.5) with (i, l, m) and (j, l, m) to eliminate X_{111}. This leaves a multiple of (2.2) for (l, m).

Type IV: Take (2.6) for (i, j, k, l, m) and (j, i, k, l, m) and eliminate X. This gives a multiple of (2.3) for (l, m).

Type V: Take (2.6) for (i, j, k, l, m) and (i, j, l, k, m) and eliminate X. This gives a multiple of (2.1) for i. Then apply Lemma 2.

Type VI: Take (2.2) for $(i, l), (j, l)$ and (k, l), and eliminate X_{122} and X_{222} using the definition of X_{112}. Then divide by t_{e_l}.

We will also need an equation of Type VII:

$$\begin{aligned} VII(i,j,k,l): \quad & t_{e_{il}}^2(a_k - a_j) + t_{e_{jl}}^2(a_i - a_k) + t_{e_{kl}}^2(a_j - a_i) \\ = \; & (a_j - a_i)(a_k - a_i)(a_k - a_j)(a_l - a_m), \end{aligned}$$

which is a linear combination of $II(l, i, j)$ and $II(l, i, k)$.

Let $\mathbf{T}$ denote the set $\{t_{e_1}, t_{e_2}, t_{e_3}, t_{e_4}, t_{e_{15}}, t_{e_{25}}, t_{e_{35}}, t_{e_{45}}\}$.

Proposition 1 *The ring $A(E) \cong K[\mathbf{T}]/R$, where R is the ideal of relations generated by:* I(1,2,3), I(1,2,4), VI(1,2,3,5), VI(1,2,4,5), VII(1,2,3,5), and VII(1,2,4,5).

A smooth model for E in 8-dimensional affine space is given by these 6 equations.

Proof: First we note that $L(Y)$ is contained in the algebra generated by $\mathbf{T}$. Indeed, *IV(k,l,5,i,j)* for $1 \le i < j \le 4$ shows that $t_{e_{ij}}$ are in the algebra, and then *V(5,1,2,3,4)* shows that t_{e_5} is in it, as well.

Since E is the pullback of U under [2], its affine ring is the normalization of $K(U)$ in the field gotten by adjoining $\mathbf{T}$. Since the normalization is unique, and non-singular varieties are normal, it suffices to show that the

Jacobian matrix M of the 6 equations generating R with respect to $\mathbf{T}$ has rank 6 at all points of E.

Suppose that 2 or more of the variables in $\mathbf{T}$ are zero. This only happens at points of E which cover a 2-torsion point e on U. Since *I(1,3,4), I(2,3,4), VI(1,3,4,5), VI(2,3,4,5), VII(1,3,4,5)*, and *VII(2,3,4,5)* are easily seen to be in R, there is a symmetry among the variables of $\mathbf{T}$ gotten by permuting the indices $\{1,2,3,4\}$. So we need only check 2 possibilities, that e is e_{12} or e_{15}.

When $e = e_{12}$, $t_{e_1} = t_{e_2} = t_{e_{35}} = t_{e_{45}} = 0$, and all the other variables in $\mathbf{T}$ are non-zero. In this case, it is not hard to find the six-by-six minor in M which has a non-vanishing determinant.

When $e = e_{15}$, $t_{e_1} = t_{e_{15}} = 0$, and all the other variables in $\mathbf{T}$ are non-zero. The variables $t_{e_{12}}, t_{e_{13}}$, and $t_{e_{14}}$ are non-zero, as well. In this case, 2 columns of M contain all zeroes, so there is only one six-by-six minor, N, whose determinant could be non-vanishing. A calculation using equations of Type V shows that the determinant is

$$16(a_1-a_2)^4(a_1-a_3)(a_1-a_4)(a_2-a_3)(a_2-a_4)(a_3-a_4)t_{e_{12}}t_{e_{13}}t_{e_{14}},$$

which is non-zero.

Finally, if one or none of the variables in $\mathbf{T}$ is zero, then $t_{e_{il}}t_{e_{jl}}t_{e_{kl}}$ must be non-zero for some permutation (i,j,k,l) of $\{1,2,3,4\}$. By symmetry, we can assume $(i,j,k,l) = (1,2,3,4)$, and so again the determinant of N is non-zero.

We are now almost in a position to find the equations defining $E(d)$, the twist of E by the cocycle $i(d)$. First we must describe the cocycle $i(d)$ precisely.

The Kummer theory isomorphism from $K^*/(K^*)^2$ to $H^1(G,\mu_2)$ is defined by taking a non-zero k in K and assigning to it the quadratic character χ_k on G defined by $\chi_k(g) = g(\sqrt{k})/\sqrt{k}$. Let $\psi : \mu_2 \xrightarrow{\sim} \mathbf{Z}/2\mathbf{Z}$.

Lemma 7 *For every $d = (d_1,d_2,d_3,d_4)$ in D^4, the cocycle $i(d)$ in $H^1(G,J)$ is given by*

$$g \longrightarrow a_g, \text{ where}$$

$$a_g = \psi(\chi_{d_1}(g))e_1 + \psi(\chi_{d_2}(g))e_2 + \psi(\chi_{d_3}(g))e_3 + \psi(\chi_{d_4}(g))e_4.$$

Proof: Using Lemma 3 and the Weil pairing, we see that e_i, $i = 1,2,3,4$, gives a $\mathbf{Z}/2\mathbf{Z}$-basis for $J[2]$. Given this choice of basis, the lemma now follows by identifying $H^1(G, J[2]) \cong H^1(G, \mathbf{Z}/2\mathbf{Z})^4 \cong H^1(G, \mu_2)^4$, and mapping the cocycle into $H^1(G, J)$.

To perform the twist, we use the isomorphism

$$J[2] \simeq \mathrm{Gal}(E/U)$$

to induce an action of G on $A(E)$ via $i(d)(g)$. We must determine which functions in $\overline{K}(E)$ are invariant under G.

Recall that $d = (d_1, d_2, d_3, d_4) \in (K^*)^4$ is a fixed representative for a class in D^4. We will now let d_5 be a fixed element in K^* such that $d_5 \equiv d_1 d_2 d_3 d_4 \bmod (K^*)^2$. To make this choice explicit, we will often abuse notation and write $d = (d_1, d_2, d_3, d_4, d_5)$ for the corresponding element in D^5. We can now define an involution on D^4 by picking $d^* = (d_1^*, d_2^*, d_3^*, d_4^*)$ to be a fixed element in $(K^*)^4$ representing $(d_5/d_1, d_5/d_2, d_5/d_3, d_5/d_4)$. Note that the map is an involution since $d_5^* \equiv d_1^* d_2^* d_3^* d_4^* \equiv d_1 d_2 d_3 d_4 \equiv d_5 \bmod (K^*)^2$.

Let $\sqrt{d_i^*}$ $(1 \le i \le 5)$ denote a fixed choice for the square root of d_i^*.

Lemma 8 *The functions of $\overline{K}(E)$ which are invariant under the action of $i(d)$ are generated over K by*

$$z_i = t_{e_i}/\sqrt{d_i^*}, \quad (1 \le i \le 5),$$

$$\text{and } z_{ij} = t_{e_{ij}}/\sqrt{d_i^*}\sqrt{d_j^*}, \quad (1 \le i < j \le 5).$$

Proof: If g is in G, then by Lemma 7, for any $e \in J[2]$,

$$g(t_e) = \sigma_{a_g} t_e,$$

$$= (\prod_{1 \le i \le 4} w(\psi(\chi_{d_i}(g))e_i, e))t_e,$$

$$= (\prod_{1 \le i \le 4} w(e_i, e)^{\psi(\chi_{d_i}(g))})t_e.$$

Now by Lemma 3, if $e = e_j$ for $1 \le j \le 4$,

$$g(t_{e_j}) = (\prod_{i \ne j} \chi_{d_i}(g))t_e = \chi_{d_j^*}(g)t_{e_j}.$$

If $e = e_5$, then

$$g(t_5) = (\prod_{1 \leq i \leq 4} \chi_{d_i}(g))t_e = \chi_{d_5^*}(g)t_{e_5}.$$

Since $g(\sqrt{d_i^*}) = \chi_{d_i^*}(g)\sqrt{d_i^*}$, for any $1 \leq i \leq 5$, z_i is G-invariant. Likewise, if $e = e_{ij}$ for $1 \leq i < j \leq 4$, then

$$g(t_{e_{ij}}) = \chi_{d_i}(g)\chi_{d_j}(g)t_{e_{ij}} = \chi_{d_i^* d_j^*}(g)t_{e_{ij}},$$

and if $1 \leq i \leq 4$,

$$g(t_{e_{i5}}) = \chi_{d_i}(g)t_{e_{i5}} = \chi_{d_i^* d_5^*}(g)t_{e_{i5}},$$

hence z_{ij} is also G-invariant. Since $K(E)$ is generated over K by $t_{e_i}(1 \leq i \leq 5)$, and $t_{e_{ij}}(1 \leq i < j \leq 5)$, the $z_i(1 \leq i \leq 5)$, and $z_{ij}(1 \leq i < j \leq 5)$, generate a field K_d over K which is isomorphic over $\bar{K}$ to $\bar{K}(E)$. Hence K_d is the function field of the twist of E by $i(d)$, and therefore it is also the field of all G-invariant functions of $\bar{K}(E)$.

Corollary 1 *A smooth model for $E(d^*)$ in 8-dimensional affine space is given by*

$$\begin{aligned}
&(a_2 - a_1)d_3 z_3^2 + (a_1 - a_3)d_2 z_2^2 + (a_3 - a_2)d_1 z_1^2 \\
&\quad = (a_2 - a_1)(a_3 - a_1)(a_3 - a_2), \\
&(a_2 - a_1)d_4 z_4^2 + (a_1 - a_4)d_2 z_2^2 + (a_4 - a_2)d_1 z_1^2 \\
&\quad = (a_2 - a_1)(a_4 - a_1)(a_4 - a_2), \\
&(a_2 - a_3)d_1 z_{15} z_1 + (a_3 - a_1)d_2 z_{25} z_2 + (a_1 - a_2)d_3 z_{35} z_3 = 0, \\
&(a_2 - a_4)d_1 z_{15} z_1 + (a_4 - a_1)d_2 z_{25} z_2 + (a_1 - a_2)d_4 z_{45} z_4 = 0, \\
&d_1 d_5 z_{15}^2(a_3 - a_2) + d_2 d_5 z_{25}^2(a_1 - a_3) + d_3 d_5 z_{35}^2(a_2 - a_1) \\
&\quad = \ (a_2 - a_1)(a_3 - a_1)(a_3 - a_2)(a_5 - a_4), \\
&d_1 d_5 z_{15}^2(a_4 - a_2) + d_2 d_5 z_{25}^2(a_1 - a_4) + d_4 d_5 z_{45}^2(a_2 - a_1) \\
&\quad = \ (a_2 - a_1)(a_4 - a_1)(a_4 - a_2)(a_5 - a_3).
\end{aligned}$$

Proof: These equations are gotten by twisting those listed in Proposition 1 and replacing d by d^*. These equations clearly define a variety which is isomorphic to E over $\bar{K}$.

Theorem 1 *Let $s = \sqrt{d_1}\sqrt{d_2}\sqrt{d_3}\sqrt{d_4}\sqrt{d_5}$. A smooth, projective model for $H(d^*)$ is given by the following 72 equations:*

$$I(d^*)(z): \ (a_j - a_i)d_k z_k^2 + (a_i - a_k)d_j z_j^2 + (a_k - a_j)d_i z_i^2$$
$$= (a_j - a_i)(a_k - a_i)(a_k - a_j)z_0^2,$$
$$\textit{where } (i,j,k) = (1,2,3),\ (1,2,4),\ (1,2,5).$$

$$II(d^*)(z): \quad d_i d_j z_{ij}^2 - d_i d_k z_{ik}^2 = (a_k - a_j)(d_i z_i^2 - (a_i - a_l)(a_i - a_m)z_0^2),$$
$$\textit{where } (i,j,k) \ =$$
$$(1,2,3),(1,2,4),(1,2,5),(2,1,3),(2,1,4),(2,1,5),(3,1,4),(3,1,5),(4,1,5).$$

$$III(d^*)(z): \quad d_i z_{il} z_{im} - d_j z_{jl} z_{jm} = (a_j - a_i)z_l z_m,$$
$$\textit{where } \{l,m\} \textit{ is any pair of indices, and } \{i,j\} \textit{ is taken in turn to be}$$
$$\textit{any } 2 \textit{ pairs chosen from the remaining } 3 \textit{ indices.}$$

$$IV(d^*)(z): \quad s(z_i z_{jk} - z_j z_{ik}) = (a_i - a_j)d_l d_m z_{lm} z_0.$$
$$\textit{where } \{l,m\} \textit{ is any pair of indices, and } \{i,j\} \textit{ is taken in turn to be}$$
$$\textit{any } 2 \textit{ pairs chosen from the remaining } 3 \textit{ indices.}$$

$$V(d^*)(z): \quad s(z_{jk} z_{lm} - z_{jl} z_{km}) = (a_j - a_m)(a_l - a_k)d_i z_i z_0,$$
$$\textit{where } i \textit{ is any index, and } \{\{j,k\},\{l,m\}\} \textit{ is taken in turn to be}$$
$$\textit{any } 2 \textit{ partitions of the remaining } 4 \textit{ indices into pairs.}$$

$$VI(d^*)(z): \quad (a_j - a_k)d_i z_{il} z_i + (a_k - a_i)d_j z_{jl} z_j + (a_i - a_j)d_k z_{kl} z_k = 0,$$
$$\textit{where } l \textit{ is any index, and } \{i,j,k\} \textit{ is taken in turn to be}$$
$$\textit{any } 2 \textit{ triplets chosen from the remaining } 4 \textit{ indices.}$$

These give a minimal set of defining equations for the embedding determined by $L(Y(d^*))$.

Proof: Let $V(d^*)$ be the variety defined by these 72 equations. The first thing that we note is that the affine open subvariety V_0 defined by $z_0 \neq 0$ is isomorphic to $E(d^*)$. Indeed, all the equations in Corollary 1 are gotten from the 72 by eliminating z_5. Conversely, in Proposition 1 we showed that z_5, z_{12}, z_{13}, z_{14}, z_{23}, z_{24} and z_{34} are elements in the algebra generated by the 8 coordinate functions given in Corollary 1. So by Lemmas 6 and 8, all 72 equations in the statement of the theorem are homogenizations of those contained in the ideal generated by those in Corollary 1. It now suffices to show that these 72 equations define the projective closure of V_0. It is enough to show that each element of the open cover

$$V_0,\ V_i \ = \ (z_i \neq 0), \ \ (1 \leq i \leq 5), \ \ V_{ij} \ = \ (z_{ij} \neq 0) \ \ (1 \leq i < j \leq 5)$$

is a non-singular variety. In (1.1) we defined a map $\delta : J(K)/2J(K) \ \rightarrow \ D^4$. Let $\delta_i = \delta(e_i)$, $\delta_{ij} = \delta(e_{ij})$. The theorem will follow from the establishment of the following claim:

Claim: V_i is isomorphic to a non-singular model of $E(d^*\delta_i)$, and V_{ij} is isomorphic to a non-singular model of $E(d^*\delta_{ij})$.

For the moment, we will think of $H(d^*)$ as the twist of J by a cocycle in $H^1(G, J[2])$. In [5], Cassels equates $H^1(G, J[2])$ with equivalence classes of "λ-coverings" (here λ is the [2]-map). There he produces a diagram

$$\begin{tikzcd}
J \arrow[r, "\theta_{d^*}"] \arrow[d, "{[2]}"'] & H(d^*) \arrow[dl, "\Lambda"] \\
J &
\end{tikzcd}$$

where Λ is defined over K, and θ_{d^*} is an isomorphism defined over $\overline{K}$. He also shows that for $P \in J(K)$, there is a K-rational map

$$\phi(P) \ : \ H(d^*) \rightarrow H(d^*\delta(P))$$

defined by the commutativity of

$$\begin{tikzcd} J \arrow[r, "T_P"] \arrow[d, "\theta_{d^*}"] & J \arrow[d, "\theta_{d^*\delta(P)}"] \\ H(d^*) \arrow[r, "\phi(P)"] & H(d^*\delta(P)) \end{tikzcd}$$

where T_P denotes the translation-by-P map. We will prove the first part of the claim by considering the map $\phi_i = \phi(e_i)$; indeed we will compute the effect of ϕ_i on every coordinate functions of $V(d^*)$. We will let small letters denote functions on $V(d^*)$ and will use capital letters to denote those on $V(d^*\delta_i)$. By comparing divisors, we can see that up to constants $c_0, c_i, c_j, c_{ij}, c_{jk}$, the map must be defined by:

$$\phi_i(z_0) = c_0 Z_i, \tag{2.7}$$

$$\phi(z_i) = c_i Z_0,$$

$$\phi_i(z_j) = c_j Z_{ij},$$

$$\phi_i(z_{ij}) = c_{ij} Z_j,$$

$$\phi_i(z_{jk}) = c_{jk} Z_{lm},$$

for $i \neq j \neq k \neq i$, and l, m complementary to i, j, k in the set $\{1, 2, 3, 4, 5\}$. We can compute the constants by evaluating (2.7) at carefully-chosen 2-torsion points. The twist is uniquely determined by the condition that ϕ_i is defined over K, so we can compute the constants and the twist simultaneously. The computation shows that $c_0 = 1$, $c_i = d_i$, $c_j = (a_j - a_i)d_j$, $c_{ij} = d_i d_j$, and $c_{jk} = d_j d_k$, with $d^*\delta_i = \Delta = (\Delta_1, \Delta_2, \Delta_3, \Delta_4, \Delta_5)$ defined by

$$\Delta_j \;=\; d_j(a_i - a_j), \text{ for } i \neq j, \text{ and } \Delta_i \;=\; d_i \prod_{j \neq i} (a_i - a_j).$$

Let fixed square roots $\sqrt{\Delta_i}$ be chosen so that

$$\prod_{1 \leq i \leq 5} \sqrt{\Delta_i} = s \prod_{i \neq j} (a_i - a_j).$$

It is then straightforward to verify that every equation of Types $I{-}VI(d^*)(z)$ gets transformed under ϕ_i into a linear combination of equations of Types $I - VI(\Delta)(Z)$, and that V_i gets mapped into $(Z_0 \neq 0) \cong E(\Delta)$. Replacing d^* by $d^*\delta_i$ gives an inverse map to ϕ_i, hence we get the desired isomorphism. The second part of the claim now follows from the first by replacing d^* by $d^*\delta_j$, and considering the composite $\phi(e_{ij}) = \phi_i\phi_j$.

We have shown that 72 relations among 136 monomials serve to generate all the relations for the homogeneous coordinate ring of $H(d^*)$. Setting $z_0 = 1$ specializes each of the monomials to a function in $L(2Y(d^*))$. But this space has dimension 64, since $2Y$ is linearly equivalent to 8Θ. Therefore no fewer than 72 relations suffice to generate all relations.

Remark: Setting $d = (1, 1, 1, 1, 1)$, $s = 1$, we recover in our special case a projective transformation of the equations discovered by Flynn [10], who placed no rationality restrictions on the Weierstrass points of C. See also [7].

We can now rederive the explicit form of the map (1.3) given in [6] and verify that it agrees with (1.1)

Corollary 2 *1)* $\delta_i = \delta(e_i) = (\Delta_1, \Delta_2, \Delta_3, \Delta_4, \Delta_5)$ *where*

$$\Delta_j \ = \ (a_i - a_j), \text{ for } i \neq j, \text{ and } \Delta_i \ = \ \prod_{j \neq i}(a_i - a_j).$$

2) For $P \in J(K)$, *let* $\delta(P) = (P_1, P_2, P_3, P_4, P_5)$. *If* $P = (x_1, y_1) + (x_2, y_2) - 2\infty$ *is in* U, *then for* $1 \leq j \leq 5$,

$$P_j \ \equiv \ (x_1 - a_j)(x_2 - a_j) \ (\text{mod } (K^*)^2), \text{ if } x_1 \ \neq \ a_j, \ x_2 \ \neq \ a_j,$$

and if $P = (x, y) - \infty$ *is on* Θ *with* $x \neq a_j$,

$$P_j \ \equiv \ (x - a_j) \ (\text{mod } (K^*)^2).$$

By linearity, this determines $\delta(P)$ *for all* $P \in J(K)$.

Proof: Statement (1) follows directly from the proof of the theorem by setting $d = (1, 1, 1, 1, 1)$. To establish (2), let P be in $J(K)$, and $P = [2]Q$ for some $Q \in J(\overline{K})$. We can think of $H(\delta(P))$ as the twist of J corresponding to the cocycle β_g in $H^1(G, J[2])$ defined by $\beta_g = g(Q) - Q$ for $g \in G$. Since $g(Q) = Q + \beta_g$, it follows immediately from the corresponding λ-covering

$$\begin{tikzcd}
J \arrow[r, "\theta_{\delta(P)}"] \arrow[d, "{[2]}"'] & H(\delta(P)) \arrow[dl, "\Lambda"] \\
J &
\end{tikzcd}$$

that $\theta_{\delta(P)}(Q)$ is K-rational. But for P on U, Λ is given by Lemmas 2 and 8. So if $P = (x_1, y_1) + (x_2, y_2) - 2\infty$, with $x_1 \neq a_j$, $x_2 \neq a_j$, then

$$(x_1 - a_j)(x_2 - a_j) \;=\; -X_{12}(P) \;- a_j X_{22}(P) \;+ a_j^2 \;=\; P_j z_j(Q)^2,$$

with $z_j(Q) \in K^*$. If x_1 or x_2 is a_j, then by linearity and (1) we can reduce to the case that P is on Θ. Now if P is on Θ, and $P \in J[2]$, $\delta(P)$ is given by (1). Finally, if P in on Θ, and $P \notin J[2]$, then the corollary follows by linearity and (1) after computing $\delta(P + e_k)$ for some $k \neq j$.

Remark: The twists of $Y(d^*)$ are easy to calculate – these are essentially the heterogeneous spaces discussed in [8]. We include them for completeness and omit their derivation.

A non-singular model for $Y(d^*)$ in 5-dimensional projective space is given by:

$$d_5{z_5}^2 - d_i{z_i}^2 = (a_i - a_5){z_0}^2,$$

for $i = 1, 2, 3, 4$.

3 Calculating the Rank over Q

Suppose now that the curve C is defined over the rational numbers $\mathbf{Q}$. Then we can find a model $y^2 = q(x)$ for C, where $q(x)$ is a monic quintic in $\mathbf{Z}[x]$. For each $d \in D^4$, we need to determine whether the 72 equations of Theorem 1 defining $H(d^*)$ have a solution over $\mathbf{Q}$. To check the space for everywhere local triviality, it suffices to test for solutions over the real numbers $\mathbf{R}$ and over the p-adic numbers $\mathbf{Q}_p$ for each prime p of bad reduction. If $H(d^*)$ has solutions over these local fields, then either a global rational solution exists, or the space is an element of order two in the Tate-Shafarevich group.

Since the map δ defined in Section 1 is a homomorphism, we need only consider cosets of the known rational points. For any curve with rational Weierstrass points, we have sixteen spaces corresponding to the 2-torsion points on J. Each time a new rational point on J is discovered, the coset of rational points doubles in size, and the number of spaces which must be tested is cut in half.

It is easiest to test for real solutions. The answer depends only on the signs of d_1, d_2, d_3, d_4, so there are only 16 sign configurations to investigate. Suppose that the a_i's are given in increasing order. Checking the signs of the coefficients of the type I and II equations shows that each have solutions over $\mathbf{R}$ for only 14 of these configurations. Combining these constraints shows that the only possible signs for the d_1, d_2, d_3, d_4 are:

$$(+,-,-,-),$$

$$(+,-,-,+),$$

$$(+,+,+,-),$$

$$(+,+,+,+).$$

This immediately eliminates three-fourths of the homogeneous spaces. Looking at the spaces corresponding to $J[2]$ shows that the remaining one-quarter spaces do indeed have real solutions.

Since $H(d^*)$ is projective, to search for solutions over $\mathbf{Q}_p$, we need only search each part of an affine cover for p-adic integral solutions. By Hensel's lemma, this reduces to a finite amount of work, for then it suffices to search for solutions in $\mathbf{Z}/p^r\mathbf{Z}$ for some sufficiently large r. However, this is a formidable task. While it is often possible to perform a 2-descent on elliptic curves by hand, it is not feasible to do the same for the Jacobians of curves of genus two. Even with a computer, the tests must be organized efficiently, using faster, weaker tests at first, and only then going onto to stronger, more time-consuming tests when the remaining set of homogeneous spaces has been pruned to a reasonable number.

To minimize r, we will always assume that d_1, d_2, d_3, d_4, and d_5 are squarefree integers. Further, we rescale each equation to make sure that every coefficient is a p-adic integer, with at least one coefficient being a unit. Even with these precautions, with sixteen variables, exhaustive tests modulo primes larger than two are infeasible.

However, there are ways to reduce the number of cases which have to be examined. For instance, the Type I equations involve only the variables z_0, z_1, z_2, z_3, z_4, and z_5. For many possible assignments of these variables $\pmod{p^r}$ there will be no solution to the Type I equations, so $H(d^*)$ may be eliminated without considering the other 10 variables.

Also since the function field of J is generated by only a few variables (for example, by z_1, z_2, z_3, z_4, and z_{12}), once the assignment of a few variables are made, others are determined. This could involve dividing by p, but in practice, not too many assignments have to be made before the others are determined. To automate this process, it proved convenient to consider the cases $z_0 \not\equiv 0 \pmod{p}$ and $z_0 \equiv 0 \pmod{p}$ separately (the latter correspond to points on $Y(d^*)$).

In the examples we now present, checking each homogeneous space using the tests over $\mathbf{R}$, checking the full set of equations $\pmod{p}$ for each of the primes of bad reduction, and considering the Type I equations $\pmod{p^2}$ were sufficient to eliminate all of the homogeneous spaces without solutions over $\mathbf{Q}$, and could be done in a reasonable amount of time.

4 Some examples

Let C be a curve of genus two defined over $\mathbf{Q}$ with rational Weierstrass points. Suppose that C has bad reduction at primes $p_1, p_2, \ldots, p_k$. Then there are $k + 1$ places in S, and 2^{4k+4} homogeneous spaces which need to be tested for local-triviality. For $k = 3$, there are 65,536 spaces, which in our examples were tested on a SUN Sparcstation in a few hours. For $k = 4$, there are 1,048,576 spaces, which could be done in a reasonable amount of time on a larger computer. The size of the primes of bad reduction also has a large effect on the running time.

Since the Weierstrass points are rational, the curve necessarily has bad reduction at 2 and at 3. In our examples, comparatively quick tests (mod 2) and (mod 3) (and (mod 4) and (mod 9) on the Type I equations) eliminated the vast majority of the spaces.

We give two examples of the method:

Theorem 2 *Let C be the curve*

$$y^2 = x(x-1)(x-2)(x-5)(x-6),$$

and J its Jacobian. Then $J(\mathbf{Q}) \cong \mathbf{Z} \oplus (\mathbf{Z}/2\mathbf{Z})^4$.

Proof: The curve C has bad reduction at 2, 3 and 5. Therefore there are $16^4 = 65,536$ homogeneous spaces to check. The five affine Weierstrass points on C map to the homogeneous spaces which correspond to the following elements of D^4:

$$\begin{aligned}
(0,0) - \infty &\rightarrow (15,-1,-2,-5)\\
(1,0) - \infty &\rightarrow (1,-5,-1,-1)\\
(2,0) - \infty &\rightarrow (2,1,6,-3)\\
(5,0) - \infty &\rightarrow (5,1,3,-15)\\
(6,0) - \infty &\rightarrow (6,5,1,1)
\end{aligned}$$

A test for solutions over $\mathbf{R}$ left $2^{14} = 16,384$ potentially everywhere locally trivial spaces. Tests (mod 2) and (mod 4) reduced the number to 2048. Performing tests (mod 9) on the Type I equations left only 128 spaces, and checking the Type I equations (mod 25) eliminated all but 32 spaces. Sixteen of these spaces correspond to $J[2]$, so the rank of $J(\mathbf{Q})$ is at most one. A short search fortunately found the integral points (3,6) and (10,120) on C, with

$$\begin{aligned}
(3,6) - \infty &\rightarrow (3,2,1,-2)\\
(10,120) - \infty &\rightarrow (10,1,2,5).
\end{aligned}$$

Note that $P = (3,6) - \infty$ is not in the coset of the 2-torsion points, so the other 16 spaces correspond to $(P+Q)$, where Q is in $J[2]$. For example, $(10,120) - \infty$ is equal to $(2,0) + (5,0) - 2\infty$ in $J(\mathbf{Q})/2J(\mathbf{Q})$, and using the addition law on J it is quickly discovered that

$$(10,120) - \infty = 2P + (2,0) + (5,0) - 2\infty.$$

To prove that $J(\mathbf{Q})$ actually has rank 1, it suffices to show that P has infinite order. We found via an exhaustive search that:

$$|J(\mathbf{F}_7)| = 48,$$

$$|J(\mathbf{F}_{11})| = 176.$$

(As the referee notes, there is an easier way to compute $|J(\mathbf{F}_p)|$, since it is just $\frac{1}{2}|C(\mathbf{F}_{p^2})| + \frac{1}{2}|C(\mathbf{F}_p)|^2 - p$. This follows either from comparing the zeta functions of C and J over $\mathbf{F}_p$, or by considering J with the origin blown up as the symmetric product of C with itself.) When $p > 2$ is a prime of good reduction, the torsion group of $J(\mathbf{Q})$ injects into $J(\mathbf{F}_p)$ (This follows by considering the formal group on the kernel of reduction of J (mod p). For the general result, see [16] p. 135). Since $\gcd(48, 176) = 16$, the torsion group consists only of the 2-torsion points, and $J(\mathbf{Q})$ has rank 1.

We do not know whether P is a generator of $J(\mathbf{Q})/J(\mathbf{Q})_{tor}$. It would be nice to have the theory of heights on Jacobians of curves of genus two worked out sufficiently explicitly to afford answers to such questions.

Theorem 3 *Let C be the curve*

$$y^2 = x(x-3)(x-4)(x-6)(x-7),$$

and J its Jacobian. Then $J(\mathbf{Q}) \cong (\mathbf{Z}/2\mathbf{Z})^4$.

Proof: The curve C has bad reduction at 2, 3 and 7. The affine Weierstrass points on C map to the homogeneous spaces:

$$\begin{array}{lcl}
(0,0)-\infty & \to & (14,-3,-1,-6) \\
(3,0)-\infty & \to & (3,-1,-1,-3) \\
(4,0)-\infty & \to & (1,1,6,-2) \\
(6,0)-\infty & \to & (6,3,2,-1) \\
(7,0)-\infty & \to & (7,1,3,1)
\end{array}$$

The test for solutions over $\mathbf{R}$ left 16,384 spaces. Tests (mod 2) and (mod 4) eliminated all but 2048 spaces. Performing tests (mod 9) on the Type I equations left 384 spaces.

Doing tests (mod 7) on the Type I equations reduced the number to 80 spaces, or five cosets of $J[2]$. Testing all the equations (mod 3) left only two cosets. The representative $d = (2, 42, 21, -42)$ of the last potentially everywhere locally trivial coset had no solution to the Type I equations (mod 49). Therefore the Jacobian has no rational points other than the 2-torsion points and the curve has no rational points other than its Weierstrass points.

References

[1] L.M. Adleman and M.A. Huang, Recognizing primes in random polynomial time, preprint.

[2] E. Arbarello, M. Cornalba, P. A. Griffiths, J. Harris, *Geometry of Algebraic Curves. I.*, Springer-Verlag, New York, 1985.

[3] E. Bombieri, The Mordell conjecture revisited, preprint.

[4] D.G. Cantor, Computing in the Jacobian of a hyperelliptic curve, *Math. Comp.*, **48** (1987) 95-101.

[5] J.W.S. Cassels, Diophantine Equations with Special Reference to Elliptic Curves, *J. London Math. Soc.*, **41** (1966) 193-291.

[6] J.W.S. Cassels, The Mordell-Weil Group of Curves of Genus 2, in *Arithmetic and Geometry*, Prog. in Math Vol. 35, Birkhaüser, Boston, 1983.

[7] J.W.S. Cassels, Arithmetic of curves of genus 2, in *Number Theory and Applications*, ed. R. A. Mollin, Kluwer, 1989.

[8] K.R. Coombes and D.R. Grant, On heterogeneous spaces, *J. London Math. Soc. (2)*, **40** (1989) 385-397.

[9] G. Faltings, Diophantine approximation on abelian varieties, *Annals of Math.*, to appear.

[10] E.V. Flynn, The Jacobian and formal group of a curve of genus 2 over an arbitrary ground field, *Math. Proc. Camb. Phil. Soc.*, **107** (1990) *no. 3*, 425-441.

[11] D. Grant, Formal groups in genus two, *J. reine angew. Math.*, **411** (1990) 96-121.

[12] M.J. Greenberg, *Lectures on Forms in Many Variables*, W.A. Benjamin, Inc., New York, 1969.

[13] N. Koblitz, Hyperelliptic cryptosystems, *Journal of Cryptology*, **3** (1989) 139-150.

[14] N. Koblitz, Elliptic curve cryptosystems, *Math. Comp.*, **48** (1987) 203-209.

[15] H.W. Lenstra, Elliptic curves and number-theoretic algorithms, *Proceedings of the ICM, Berkeley, Cal., 1986*, Amer. Math. Soc., Providence, 1987, pp. 99-120.

[16] B. Mazur, Rational isogenies of prime degree, *Invent. Math.*, **44** (1978) 129-162.

[17] B. Mazur, Arithmetic on Curves, *Bull. Amer. Math. Soc. (N. S.)*, **14** (1986) *no. 2,* 207-259.

[18] V. Miller, Use of elliptic curves in cryptography, *Advances in Cryptography - Crypto '85*, Springer-Verlag, New York, 1986, pp. 417-426.

[19] J. S. Milne, *Arithmetic Duality Theorems*, Academic Press, Orlando, 1986.

[20] D. Mumford, On equations defining Abelian varieties. I., *Invent. Math.*, **1** (1966) 287-354.

[21] D. Mumford, *Abelian Varieties*, Oxford University Press, Oxford, 1970.

[22] J.H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1986.

[23] J.H. Silverman, Lower bounds for the canonical heights on elliptic curves, *Duke Math. J.*, **48** (1981) 633-648.

[24] P. Vojta, Siegel's theorem in the compact case, *Annals of Math.*, to appear.