ON HETEROGENEOUS SPACES

KEVIN R. COOMBES AND DAVID R. GRANT

Introduction

Let C be a curve of genus $g \geqslant 2$ defined over a number field k. Faltings's proof of the Mordell conjecture [5] guarantees that $C(k)$ is finite, yet no practical effective procedure is known for bounding either the heights of the k-rational points or their number.

If $\eta: C \to D$ is a k-morphism to another curve, then η carries k-points to k-points. The problem of computing $C(k)$ is thus reduced to determining $D(k)$. However, such a cover is unlikely to exist if the genus of D is greater than 0, since the Jacobian of D would have to be isogenous to a factor in the Jacobian of C. On the other hand, there are arbitrarily many curves which cover C. Unfortunately, there is no *a priori* way to determine over which field the inverse image of k-rational points will be defined.

When $\eta: D \to C$ is an unramified cover, a classical theorem of Weil and Chevalley [2] determines a finite extension k' of k such that $\eta^{-1}(C(k))$ is contained in $D(k')$. Since D might well cover another curve E, knowledge of the arithmetic of E can be used to study the arithmetic of C. Indeed, this method was used by Chabouty [1] to bound the number of integer points on elliptic curves, and by Kubert and Lang [7] to study rational points on hyperelliptic and superelliptic curves. But in practice, for producing curves on which one can be certain that all rational points are known, the Weil–Chevalley theorem is difficult to use. Extending the groundfield makes it harder to compute rational points.

The purpose of this paper is to introduce a method by which all the rational points on certain curves can be found, not only in theory, but also in practice. We introduce certain auxiliary curves called *heterogeneous spaces*. These are unramified geometrically abelian covers $\eta: D \to C$. The main result is Theorem 1.4, which produces finite sets of heterogeneous spaces $\eta_i: D_i \to C$ such that every k-point of C is the image of a k-point on one of the D_i. Often, each D_i will cover another curve E_i, whose arithmetic is known. In this way, we can sometimes determine $C(k)$ completely without extending the ground field.

The basic results are presented in the first section, and are not very difficult to prove. The interest in the method comes from its practical applications. In Section 2 we find heterogeneous spaces which are double covers of hyperelliptic curves, and use them in Sections 3 and 4 to find all the rational points on certain curves of genus 2 and 3. Section 4 also contains the equations needed to carry out a three-descent on a general elliptic curve with a rational three-torsion point. In the final section, we use

---

Received 13 April 1988.

1980 *Mathematics Subject Classification* (1985 *Revision*) 14H25.

The first author was partially supported by NSF grant DMS 86-00036; the second by NSF grant DMS 85-02804 A04.

heterogeneous spaces which are triple covers of a genus 2 curve to determine all of its rational points.

Numerous references are made in this paper to computations of the points on elliptic curves using a descent via an isogeny of degree two. Contrary to the overriding spirit of the paper, these computations are not included. They were carried out on a Sun 3/50 workstation which was paid for by a grant from the National Science Foundation. The software to compute these descents was written by the authors of this paper, based on mathematics which is explained carefully in [**14**]. Also, the equations of three-descents in Section 4 were made tractable while running MACSYMA on the same Sun workstation.

1. *Basic results*

Let X be a smooth, projective, geometrically irreducible variety over a perfect field k. A morphism $\eta: Y \to X$ will be called *geometrically abelian* if Y is a geometrically irreducible k-variety and the induced morphism over the algebraic closure $\bar{k}$ is a Galois cover with abelian Galois group.

DEFINITION 1.1. A pair (Y, η) is called a *heterogeneous space* for X over k if $\eta: Y \to X$ is an unramified geometrically abelian cover defined over k.

Although the morphism is an essential part of the structure, we shall frequently abuse notation and refer simply to a heterogeneous space Y for X. The adjective 'heterogeneous' was chosen because these spaces play a role in descent arguments analogous to that played by principal homogeneous spaces for abelian varieties. In fact, heterogeneous spaces for abelian varieties are, in a slightly skewed sense, just homogeneous spaces.

LEMMA 1.2. *Let (H, ϕ) be a heterogeneous space, defined over a field k, covering an abelian variety A. Then there is an isogeny $\psi: B \to A$ defined over k such that H is a principal homogeneous space for B and the cover ϕ is a twisted form of the cover ψ.*

Proof. Let B be the Albanese variety of H. Then B is an abelian variety defined over k, and there is a natural isogeny ψ arising from the universal property of the Albanese. Moreover, H becomes isomorphic to B as a cover after base extension, since the only unramified abelian covers of abelian varieties are themselves abelian varieties [**10**].

Heterogeneous spaces for varieties other than abelian varieties usually get more complicated. For instance, a non-trivial heterogeneous space for a curve of genus $g \geqslant 2$ will have genus strictly larger than g. This situation is very different from the use of torsors in the study of the arithmetic of rational surfaces [**3**]. Torsors over a rational surface with structure group a torus are more likely to be k-rational, and thus simpler, than the original surface. Nevertheless, heterogeneous spaces have two redeeming features. On the one hand, geometrically more complicated varieties should (in some deliberately vague sense growing out of Mordell's conjecture and Vojta's conjecture [**17**]) have fewer rational points over number fields. On the other hand, heterogeneous spaces are essentially twisted forms of torsors with structure group a finite commutative groupscheme.

PROPOSITION 1.3. *Let C be a curve over k with $C(k)$ non-empty. Every heterogeneous space for C is isomorphic to the pullback of a heterogeneous space for its Jacobian.*

Proof. Let $\eta: D \to C$ be a heterogeneous space and let J_C denote the Jacobian of C. Suppose first that there is a twisted form $\theta: D_1 \to C$ of η which is actually abelian over k. Then, by [13], D_1 is a pullback of an isogeny $\phi: B \to J_C$ along an embedding of the curve in its Jacobian. Let G denote the Galois group of $\bar{k}/k$, and let $B[\phi]$ denote the kernel of ϕ. Since D becomes isomorphic to D_1 over $\bar{k}$, it defines a class in

$$H^1(G, \mathrm{Aut}(D_1/C)) = H^1(G, \mathrm{Aut}(B/J_C)) = H^1(G, B[\phi]).$$

Let H be the heterogeneous space over J defined by this class. Then D is the pullback of H.

Thus, it suffices to find a twist of D which is already abelian over k. Since D becomes abelian over $\bar{k}$, it also becomes isomorphic to the pullback of an isogeny $\phi: B \to J_C$. It is enough to show that ϕ is already defined over k.

Let J_D denote the Jacobian of D, and let $\alpha: J_C \to J_D$ be the natural map on Jacobians induced by pulling back divisors along η. Write $K = \mathrm{Ker}(\alpha)$. Then K is a k-groupscheme. It now suffices to show that K, viewed over the algebraic closure, is the kernel of the dual isogeny $\hat{\phi}: J_C \to B$.

Assume, therefore, that k is algebraically closed. Let d be the degree of η. The abelianized fundamental group of C is isomorphic to the Tate module of its Jacobian [6]. Since D/C is an abelian cover, there is therefore an exact sequence

$$J_D[d] \longrightarrow J_C[d] \longrightarrow \mathrm{Aut}(D/C) \longrightarrow 0.$$

The map on Jacobians here is the natural one which arises from identifying them with the Albanese varieties of the curves. Its transpose [8] is the natural map on Jacobians in the other direction whose kernel is K. The result follows.

Certain heterogeneous spaces for curves or abelian varieties are more closely related than others. If $\phi: B \to A$ is an isogeny with kernel $B[\phi]$, then there is a heterogeneous space over A, corresponding to a twist of ϕ, for each cohomology class in $H^1(G, B[\phi])$. Similarly, when $A = J_C$ is the Jacobian of a curve C, the same cohomology group parametrizes pullbacks of twists of ϕ. Two heterogeneous spaces which are twists or pullbacks of twists of the same isogeny ϕ will be said to be *associated* to ϕ.

THEOREM 1.4. *Let C be a curve defined over a number field k. Let $\phi: A \to J$ be an isogeny to the Jacobian J of C. Then there exist finitely many heterogeneous spaces $\eta_i: X_i \to C$, each of which is associated to ϕ, such that*

$$\bigcup \eta_i(X_i(k)) = C(k).$$

Proof. If $C(k)$ is empty, there is nothing to prove. Otherwise, consider the diagram

$$\begin{array}{ccccc} & & C(k) & & \\ & & \downarrow & & \\ 0 & \longrightarrow & J(k)/\phi(A(k)) & \longrightarrow & H^1(G, A[\phi]). \end{array}$$

Each k-point $P \in C$ determines a cohomology class which represents a heterogeneous space for J associated to ϕ. Pulling back defines a heterogeneous space for C also associated to ϕ, which, by definition, has a point lying over P. As in the proof of the weak Mordell–Weil theorem (see, for example, [14]), the cohomology classes which arise from this construction are unramified outside the set of infinite primes, primes of bad reduction, and primes dividing the degree of the cover. The theorem follows.

Let S be the set of primes which arises in the proof of the theorem. That is, for a given curve C and a given isogeny ϕ, let S be the finite set of primes consisting of all infinite primes, all primes of bad reduction of C, and all primes which divide the degree of ϕ. Then S gives an upper bound for the set of primes where cohomology classes corresponding to heterogeneous spaces with rational points can be ramified. In fact, we shall see below that this bound can sometimes be improved upon.

2. *Double covers of hyperelliptic curves*

Let A be an abelian variety over a perfect field k of characteristic not two, with dual abelian variety $\hat{A}$. Geometrically irreducible, unramified, double covers of A over $\bar{k}$ are classified by $H^1(A, \mathbb{Z}/2\mathbb{Z}) = H^1(A, \mu_2) = \hat{A}[2]$. By taking Galois invariants, we see that such covers over k are determined by the choice of a k-rational two-torsion point on $\hat{A}$.

Let C be a hyperelliptic curve of genus g defined by $y^2 = f(x)$. Since the Jacobian J of C is self-dual, heterogeneous spaces of degree two over C can only arise from rational two-torsion points on J. These, in turn, are generated by the Weierstrass points (where $f(x) = 0$, or possibly infinity). Hence, heterogeneous spaces of degree two are only defined when $f(x)$ factors over k.

Suppose that $f(x) = g(x)h(x)$. For each $t \in k$, define an unramified double cover D_t by the system of equations

$$tu^2 = h(x), \qquad tv^2 = g(x), \qquad tuv = y.$$

The D_t are associated heterogeneous spaces for C. Let $\eta_t : D_t \to C$ be the natural covering map.

Let k be a number field. The arithmetic of the covers enters through the choice of t. By the proof of Theorem 1.4, we only need to consider values of t such that $k(t^{\frac{1}{2}})$ is ramified at primes of bad reduction or primes dividing 2. The fundamental feature of the D_t is that each one covers another curve of smaller genus. For instance, let E_t be the curve defined by

$$tu^2 = h(x).$$

Then there is a natural projection $\lambda_t : D_t \to E_t$. Moreover, every rational point of C can be found by lifting a rational point from some E_t to a rational point on D_t, and then projecting to C.

The simplest case arises when $g(x) = x$, and $h(x)$ has even degree. Then D_t is a hyperelliptic curve of genus $2g-1$ defined by

$$D_t : tu^2 = h(tv^2),$$

but it covers a new curve

$$(*) \qquad E_t : tu^2 = h(x)$$

of genus $g-1$.

PROPOSITION 2.1. *Let $h(x)$ be a monic polynomial of degree $2g$ over the ring of integers $\mathcal{O}_k$ of a number field k, such that the curve C defined by*

$$y^2 = xh(x)$$

has genus g. Let $a = h(0)$, and let S be the set of prime divisors of $2a$. Then the k-rational points on C are contained in

$$\bigcup \eta_t \lambda_t^{-1}(E_t(k)),$$

where the union is taken over $t \in \mathcal{O}_k$ such that $k(t^{\frac{1}{2}})$ is unramified outside S.

Proof. Let $t \in k$ be such that $k(t^{\frac{1}{2}})$ is ramified at a prime outside S. Localizing at this prime and absorbing squares into u, we may assume that t is a uniformizing parameter. Since E_t is defined by (*) and $h(x)$ is monic of even degree, the incompatibility of orders of poles forces any t-adic point to be integral. But the same result must hold on D_t, where we also have $x = tv^2$. Thus, the integer x must be divisible by t. Now reducing (*) modulo t shows that there can only be points locally if t divides a.

The following result is perhaps more whimsical than useful. In order to state it precisely, we need a definition. We shall say that a class of curves satisfies an effective version of Mordell's conjecture if, for every curve C of genus g in that class, defined over a number field k by equations whose coefficients have absolute height bounded by H, there exists an effectively computable constant $c = c(k, g, H)$ such that every point in $C(k)$ has height bounded by c.

COROLLARY 2.2. *Suppose that the class of curves of genus* 2 *satisfies an effective version of Mordell's conjecture. Then the class of hyperelliptic curves also satisfies an effective version of Mordell's conjecture.*

Proof. Let the curve be defined by $y^2 = f(x)$. By adjoining roots of $f(x)$, we may assume that we are in the situation of the proposition. Doing this replaces k by an explicit finite extension. But then the computation of points on this curve of genus g is determined by the computation of points on a finite, effectively computable list of hyperelliptic curves of genus $g-1$. The result follows by induction.

Certain standard facts about the arithmetic of hyperelliptic curves of genus g will be used in the sequel. Any such curve has a model either in the form $y^2 = f(x)$, where $f(x)$ is a monic polynomial of degree $2g+1$, or in the form $dy^2 = f(x)$, where $f(x)$ is a monic polynomial of degree $2g+2$. These models are singular at infinity. In the former case, the corresponding non-singular model has a single point at infinity, which is rational. In the latter case, the corresponding non-singular model has a pair of points at infinity, which are rational if and only if d is a square. Finally, if k is a number field, then we may assume that d and the coefficients of $f(x)$ lie in the ring of integers of k.

3. *Double covers of genus* 2 *curves*

Consider the curve C of genus 2 defined by

$$y^2 = x^5 + px,$$

where p is a positive prime number. By Proposition 2.1, every rational point on C is the image of a rational point on one of four heterogeneous spaces

$$D_t: tu^2 = t^4x^8 + p,$$

where $t \in \{\pm 1, \pm p\}$. Setting $w = tx^2$, we find that each D_t covers a curve of genus 1 defined by

$$E_t: tu^2 = w^4 + p.$$

If t is negative, then E_t has no real points. If $t = 1$, then E_t is a principal homogeneous space for the elliptic curve [**14**]

$$F_1: y^2 = x^3 - 4px.$$

Since E_1 has rational points at infinity, it is a trivial homogeneous space. Thus, E_1 is isomorphic to F_1. Similarly, if $t = p$, then E_t is a trivial homogeneous space for the elliptic curve

$$F_p: y^2 = x^3 - 4p^3x.$$

So, E_p and F_p are isomorphic.

The curves F_1 and F_p are of the type studied extensively in [**14**]. Indeed, it is shown there that

(1) $F_1(\mathbb{Q})_{\text{tor}} \simeq \mathbb{Z}/2\mathbb{Z}$,
(2) F_1 is isogenous to $G_1: y^2 = x^3 + px$, and
(3) $\text{rank}_{\mathbb{Z}}(G_1(\mathbb{Q})) = 0$ if $p \equiv 7, 11 \bmod 16$.

The Mordell–Weil rank of G_1 is calculated by a descent carried out via a degree-two isogeny [**14**]. A similar calculation shows that

(1) $F_p(\mathbb{Q})_{\text{tor}} \simeq \mathbb{Z}/2\mathbb{Z}$,
(2) F_p is isogenous to $G_p: y^2 = x^3 + p^3x$, and
(3) $\text{rank}_{\mathbb{Z}}(G_p(\mathbb{Q})) = 0$ if $p^3 \equiv 7, 11 \bmod 16$.

THEOREM 3.1. *If p is a positive prime, $p \equiv 7 \bmod 16$, then the $\mathbb{Q}$-rational points on*

$$y^2 = x^5 + px$$

are precisely the point at infinity and the point $(0, 0)$.

Proof. When $p \equiv 7 \bmod 16$, so is p^3. So E_1 has two $\mathbb{Q}$-rational points, both at infinity. Hence, the only rational points on D_1 are the two points at infinity. Also, the only rational points on E_p are $(w, u) = (0, \pm 1)$, and thus D_p has only the rational points $(x, u) = (0, \pm 1)$. Since these four points map onto the rational points of C, the only rational points on C are the point at infinity and the point $(x, y) = (0, 0)$.

COROLLARY 3.2. *If $p \equiv 7 \bmod 16$, then the $\mathbb{Q}$-rational points on*

$$y^2 = x^{4n+1} + px$$

are precisely the point at infinity and the point $(0, 0)$.

Proof. The associated heterogeneous spaces cover the same elliptic curves as in the proof of the theorem.

The careful reader will have already noticed that the Jacobian of the curve C in Theorem 3.1 has complex multiplication by the eighth roots of unity. Since a biquadratic field has no simple CM-types [**9**], C must cover a pair of elliptic curves. It might appear that the rational points on C could have been more easily computed by studying this pair of elliptic curves. But these curves are only defined over a field containing a fourth root of p—precisely the kinds of fields which our method is designed to avoid.

For those who, nevertheless, would think it always preferable to descend from a curve of genus 2 to an elliptic curve, we provide the following example. Consider the curve

$$C: y^2 = x^5 + 4x^3 + x.$$

Over $\mathbb{Q}$, the curve C covers the elliptic curves

$$E_1: w^2 = v^3 + 4v^2 + 6v$$

and

$$E_2: w^2 = v^3 - 4v^2 + 6v.$$

A descent via a two-isogeny shows that each elliptic curve has Mordell–Weil rank at most 1. The points $(v, w) = (2, 6)$ on E_1, and $(v, w) = (2, 2)$ on E_2, are easily seen to be non-torsion. Thus, since both curves have rank 1, they cannot be used directly to find the rational points on C. Since they are not isomorphic over $\mathbb{Q}$, neither can the method of Dem'janenko [4] be used.

However, by Proposition 2.1, all the rational points on C lie in the image of rational points on the heterogeneous spaces

$$D_1: u^2 = x^8 + 4x^4 + 1$$

and

$$D_{-1}: -u^2 = x^8 + 4x^4 + 1.$$

The latter has no real points, and the former covers the elliptic curve

$$E: u^2 = w^4 + 4w^2 + 1.$$

Putting E into Weierstrass form shows that it has rational two-torsion, and a two-descent shows that it has rank zero. The torsion on E is easily seen to consist of the two points at infinity and the points $(w, u) = (0, \pm 1)$. Tracing these points up to D_1 and down to C, one finds that the only rational points on C are the point at infinity and the point $(x, y) = (0, 0)$.

4. *Double covers of genus* 3 *curves*

Consider the hyperelliptic curve C of genus 3 defined over $\mathbb{Q}$ by the equation

$$y^2 = x^7 + px.$$

Here we assume that p is a positive prime. This curve has complex multiplication by the 12th roots of unity. Over some extension field, it covers curves of lower genus. But it is not easy to see how to use this fact to compute the rational points on C. Nevertheless, Proposition 2.1 can be used to construct heterogeneous spaces. Let $t \in \{\pm 1, \pm p\}$. The heterogeneous spaces D_t cover the genus 2 curves E_t defined by

$$tu^2 = x^6 + p.$$

If t is negative, then E_t clearly has no real points, and thus no rational points. So, there are only two heterogeneous spaces to consider.

By setting $w = x^2$, we can view E_t as a cover of the elliptic curve

$$tu^2 = w^3 + p.$$

Multiplying this equation by t^3 and making a scale change on the variables, this elliptic quotient can be written in Weierstrass form as

$$u^2 = w^3 + pt^3.$$

When $t = p$, this curve has a rational three-torsion point at $(0, p^2)$.

On the other hand, we can also set $w = x^2$ and $z = ux$ to get a different elliptic curve covered by E_t:

$$tz^2 = w^4 + pw.$$

By setting $y = pz/w^2$, $x = p/w$, this elliptic quotient becomes isomorphic to the curve defined by

$$ty^2 = x^3 + p^2.$$

When $t = 1$, this elliptic curve also has a rational three-torsion point, at $(0, p)$.

In summary, the problem of finding rational points on C has been reduced to the problem of finding rational points on a pair of elliptic curves. Each elliptic curve has a rational three-torsion point, and hence has a three-isogeny defined over $\mathbb{Q}$. The structure of the group of rational points can be assessed by carrying out a three-descent. Satgé [**11**, **12**] has worked out the equations for a three-descent in a special case which would be adequate for our purposes. However, we do not know a good reference for the equations necessary to carry out a general three-descent, so they are included here.

LEMMA 4.1. *The general elliptic curve with a rational three-torsion point is defined by*

$$y^2+axy+by = x^3.$$

Proof. After writing the equation in Weierstrass form, move the three-torsion point to $(0,0)$ and choose coordinates so the tangent line is defined by $y = 0$. Also notice that the discriminant of this curve is $b^3(a^3-27b)$.

LEMMA 4.2. *Let E be an elliptic curve with a rational three-torsion point, as in the previous lemma. The three-isogenous elliptic curve $\hat{E}$ is defined by*

$$v^2-auv+9bv = u^3-b(27b+a^3).$$

Proof. See also [**16**]. Introduce a homogenizing variable z. In projective coordinates, the automorphism defined by adding the three-torsion point to a general point is

$$(0:0:1)+(x:y:z) = (x:bz:-(ax+y+bz)/b).$$

It is easiest to see the next step by introducing new coordinates

$$X = y, \qquad Y = bz, \qquad Z = -ax-y-bz.$$

In these coordinates, adding the three-torsion point is a cyclic permutation, while the curve itself is defined by

$$(*) \qquad a^3XYZ = b(X+Y+Z)^3.$$

The map to the isogenous curve must be given by cyclically invariant cubics. The cyclically invariant cubics

$$q = X^3+Y^3+Z^3, \qquad r = XYZ,$$
$$s = X^2Y+Y^2Z+Z^2X, \qquad t = XY^2+YZ^2+ZX^2$$

define a cubic surface

$$stq-3r^2q-rq^2 = s^3+t^3-6rst+9r^3$$

in $\mathbb{P}^3$. Equation $(*)$ defines the isogenous elliptic curve as the hyperplane section

$$a^3r = b(q+3(s+t)+6r).$$

This curve can be identified with the projectivization of the one in the statement of the lemma by setting

$$u = b(X+Y+Z)(XY+XZ+YZ),$$
$$v = ab(XY^2+YZ^2+ZX^2+6XYZ), \qquad w = -aXYZ.$$

An interesting facet of this proof is that the intermediate change of variables does not make sense when $a = 0$. Nevertheless, the composite

$$u = x(axy + abxz + y^2 + byz + b^2z^2),$$
$$v = a^2bx^2z - axy^2 - 4abxyz + 2ab^2xz^2 - y^3 - 6by^2z - 3b^2yz^2 + b^3z^3,$$
$$w = yz(ax + y + bz)$$

is well defined and identifies the isogenous curve correctly even in this case.

To carry out a three-descent completely, we must be able to twist both the isogeny $\phi: E \to \hat{E}$ and its dual $\hat{\phi}: \hat{E} \to E$. These will necessarily differ in character. Because $\mathrm{Ker}[\phi] = \mathbb{Z}/3\mathbb{Z}$, the Galois invariance of the Weil pairing [**8**] implies that $\mathrm{Ker}[\hat{\phi}] = \mu_3$. These are different Galois modules if the cube roots of unity do not lie in the ground field. This difference shows up arithmetically in that $H^1(G, \mathbb{Z}/3\mathbb{Z})$ classifies cyclic cubic field extensions, but $H^1(G, \mu_3)$ classifies radical cubic extensions.

As remarked in [**13**], it is easy to see that every cyclic cubic extension is defined by an irreducible polynomial of the form

$$X^3 - 3jX^2 + 3(j-1)X + 1,$$

where $j \in k$ is not a sixth root of unity. The fundamental fact underlying this observation is that the roots can be normalized to have the form

$$r, \qquad \frac{1}{1-r}, \qquad \frac{r-1}{r}.$$

LEMMA 4.3. *Let $j \in k$ determine a cyclic cubic extension. The twisted form of E corresponding to this cyclic cubic field as an element of $H^1(G, \mathbb{Z}/3\mathbb{Z})$ is defined by*

$$\frac{a^3 - 27b}{9(j^2 - j + 1)} X^3 = aX(Z^2 - ZY + Y^2) - (Z^3 - 3jZ^2Y + 3(j-1)ZY^2 + Y^3).$$

Proof. Begin by writing each of the variables x, y, z in the general form of an element of the cyclic extension. For instance,

$$x = x_0 + x_1 r + x_2 r^2.$$

Let σ denote the generator of the Galois group which acts on the root r by $\sigma(r) = 1/(1-r)$. One gets a system of linear equations in the subscripted variables by setting

$$\sigma(x:y:z) = (x:bz:-(ax+y+bz)/b),$$

and equating corresponding coefficients of powers of r. Solving this system of equations leads to the twisted form of the curve, by setting

$$x = 3bX,$$
$$y = b[(-aX + (2-3j)Y + 2Z) + ((3j+1)Y + (3j-2)Z)r - (Y+Z)r^2],$$
$$z = (-aX + 2Y + (3j-4)Z) + ((3j-2)Y + (1-6j)Z)r - (Y-2Z)r^2.$$

LEMMA 4.4. *For each $t \in k$, the twist of $\hat{E}$ corresponding to the radical cubic extension $k(\sqrt[3]{t})$ is defined by*

$$bU^3 + tW^3 + t^2V^3 = atUVW.$$

Proof. To obtain this result, first adjoin a cube root of unity ω to the ground field. Now there is a three-torsion point

$$\left(-\frac{a^2}{3}, -\frac{27b(3-\sqrt{3})+a^3(3+\sqrt{3})}{18}\right)$$

on the isogenous curve. Rewrite the isogenous curve in the standard form of Lemma 4.1 and twist it by a cyclic cubic extension as in Lemma 4.3. In order to ensure that this twist is by a radical cubic extension of the original ground field, it is enough to take $j = -\omega(t-\omega)/(t-1)$. Finally, rewrite the twisted curve to remove extraneous roots of unity. The result is the curve described above, obtained by setting

$$u = 9bU + a^2W\theta + a^2V\theta^2, \qquad v = 9abU + a^3W\theta + 27bV\theta^2,$$
$$w = -aU - 3W\theta - 3V\theta^2,$$

where $\theta = t^{\frac{1}{3}}$.

THEOREM 4.5. *Let $p \equiv 2 \bmod 3$ be a positive rational prime such that 2 is not a cube modulo p. Then the only rational points on the curve*

$$y^2 = x^7 + px$$

are the point at infinity and the point $(0,0)$.

Proof. As noted above, we must find all points on the heterogeneous spaces D_1 and D_p, each of which covers an elliptic curve with a three-torsion point. These are the only rational torsion points on the curves; the result will follow if we can show that each curve has Mordell–Weil rank zero. The elliptic curves can be written in the form

$$E_\alpha : y^2 = x^3 + p^{2\alpha},$$

where $\alpha = 1, 2$. These curves can be rewritten in the form of Lemma 4.1 with $a = 0$ and $b = 2p^\alpha$. Thus the set of places where ramification can occur is

$$S = \{2, 3, p, \infty\}.$$

Since $p \equiv 2 \bmod 3$, the only cyclic cubic extension which is unramified outside S is the maximal real subfield of the extension generated by the ninth roots of unity, which corresponds to $j = 0$ in Lemma 4.3. So, the only twist of E_α which must be looked at is

$$6p^\alpha x^3 = z^3 - 3zy^2 + y^3.$$

Because of the congruence condition which we assumed to hold on p, adjoining the ninth roots of unity is an extension of $\mathbb{Z}/p\mathbb{Z}$ of full degree. Since the roots of $z^3 - 3z + 1$ generate the maximal real subfield of $\mathbb{Q}(\mu_9)$, this curve cannot have p-adic points.

We must now consider the twists

$$2p^\alpha U^3 + tW^3 + t^2V^3 = 0$$

of the isogenous curve

$$v^2 - 18p^\alpha v + 108p^{2\alpha} = u^3,$$

by elements $t \in \mathbb{Q}^*/\mathbb{Q}^{*3}$ supported at the primes 2, 3, and p. We must show that the set of twists having rational points is isomorphic to a copy of $\mathbb{Z}/3\mathbb{Z}$.

When the 3-adic valuation of t is equal to 1, the twist cannot have any 3-adic points. This follows because the three terms in the equation have distinct valuations modulo 3, so can never cancel. The same argument applies when the 3-adic valuation of t is equal to 2.

We have shown so far that the set of twists with rational points is contained inside the copy of $(\mathbb{Z}/3\mathbb{Z})^2$ generated by 2 and p. It suffices to show that one of the remaining twists does not have any rational points. When $t = p^\alpha$, the twist becomes

$$2U^3 + W^3 + p^\alpha V^3 = 0.$$

Since we have assumed that 2 is not a cube modulo p, the result follows.

5. *Triple covers of genus 2 curves*

Let A be an abelian variety over a perfect field k of characteristic different from three. Geometrically irreducible, unramified, abelian covers of degree three of A over $\bar{k}$ are classified by $H^1(A, \mathbb{Z}/3\mathbb{Z})$. The Galois invariants of this group are given by $\hat{A}[3]^{\chi_3}$, where χ_3 is the character giving the action of $\mathrm{Gal}(\bar{k}/k)$ on μ_3. If $\mu_3 \notin k$, then such covers over k are determined by three-torsion points on the dual abelian variety which are rational over $k(\mu_3)$, but not over k.

Let C be a hyperelliptic curve of genus 2 defined by $y^2 = f(x)$, where $f(x)$ is a sextic polynomial with coefficients in k. Since the Jacobian J of C is self-dual, heterogeneous spaces of degree three over C can only arise from three-torsion points on J which are rational over $k(\mu_3)$, but not over k.

Let ∞_1 and ∞_2 denote the two points at infinity on C. Every point on J other than the origin can be uniquely represented by a divisor

$$P_1 + P_2 - \infty_1 - \infty_2,$$

where $P_1, P_2 \in C$. If a divisor defines a non-zero three-torsion point, then it is easy to verify that neither P_1 nor P_2 can be a point at infinity.

Hence, non-trivial three-torsion on the Jacobian comes from a function on C with a pole of order three at each point at infinity, and zeros of order three at a pair of points. All such functions must be of the form $y - c(x)$, where $c(x)$ is a cubic polynomial in x. The condition that $y - c(x)$ have triple-order zeros implies that

$$f(x) - (c(x))^2 = d(q(x))^3,$$

where $q(x)$ is a quadratic polynomial in x, and d is a constant. Finally, the three-torsion point will have the appropriate rationality if $c(x)$, $q(x)$ and d are defined over $k(\mu_3)$, but at least one of these is not defined over k.

It would be a computational nightmare to write out the equations defining the degree-three isogeny onto the Jacobian corresponding to this three-torsion. So we shall be content to build a degree-three cover D of C defined over k, which is unramified and abelian over k. By Proposition 1.3, we shall know that D is a heterogeneous space associated to some isogeny of the Jacobian. Then all heterogeneous spaces are obtained by twisting this cover over the cubic number fields classified by $H^1(\mathrm{Gal}(\bar{k}/k), \mathbb{Z}/3\mathbb{Z})$; that is, over cyclic cubic extensions of k.

In practice, it is easier to build abelian three-covers of C and their twists over $k(\mu_3)$. We use the fact that heterogeneous spaces defined over k can be identified with heterogeneous spaces defined over $k(\mu_3)$ which descend to k.

One such cover is

$$u^3 = y - c(x), \qquad dv^3 = y + c(x), \qquad uv = q(x).$$

All cyclic cubic extensions of $k(\mu_3)$ are of the form $k(\mu_3, t^{\frac{1}{3}})$ for some $t \in k$. It follows as in the proof of Lemma 4.3 that each twist over $k(\mu_3, t^{\frac{1}{3}})$ is isomorphic to

$$u^3 = t(y - c(x)), \qquad dv^3 = t^2(y + c(x)), \qquad uv = tq(x).$$

As an example, we take $k = \mathbb{Q}$, $q(x) = x^2$, $c(x) = 18\sqrt{-3}$, and $d = 1$.

PROPOSITION 5.1. *Let C be the curve defined by*

$$y^2 = x^6 - 972.$$

The only $\mathbb{Q}$-rational points on C are the two points at infinity.

Proof. The curve C has bad reduction at 2 and at 3. Thus, we need only consider twists over cyclic cubic extensions of $\mathbb{Q}$ ramified over 2 and 3. The only such extension is the maximal real subfield of $\mathbb{Q}(\mu_9)$. Hence the only heterogeneous spaces over $\mathbb{Q}(\mu_3)$ that we must consider are the ones where $t = \omega^i$, for $\omega = \frac{1}{2}(-1 + \sqrt{-3})$ and $i = 0$, 1 or 2.

Write $G = \mathrm{Gal}(\mathbb{Q}(\mu_3)/\mathbb{Q})$. The descended curves are found by writing u, v, x and y in terms of the basis $1, \sqrt{-3}$ of the vector space of $\mathbb{Q}(\mu_3)$-functions on D_t over the G-invariant functions, and then equating G-isotypical parts. For the cover to be defined over $\mathbb{Q}$, both x and y must be G-invariant. Since t^2 is the conjugate of t, we see that v differs from the conjugate of u by a cube root of unity. Write $u = \alpha + \beta\sqrt{-3}$, and $v = w\omega^i$. Then $uw = x^2$, so $w = (\alpha - \beta\sqrt{-3})$. Equating G-isotypical parts when $t = \omega$ yields

$$x^2 = \alpha^2 + 3\beta^2, \qquad 36 = \alpha^2 - 9\alpha\beta^2 + 3\alpha^2\beta - 3\beta^3.$$

It is easy to see this curve has no 3-adic points. When $t = \omega^2$, we get a curve isomorphic to the one above, which again has no 3-adic points.

When $t = 1$, equating G-isotypical parts yields

$$x^2 = \alpha^2 + 3\beta^2, \qquad \alpha^2\beta = \beta^3 - 6.$$

This covers the elliptic curve

$$\beta x^2 = 4\beta^3 - 6.$$

Setting $m = 6x/\beta$, $e = -6/\beta$ gives the isomorphic curve

$$m^2 = e^3 + 144.$$

This is isogenous to the curve $D = 3$ on Stephens's table [15], which has Mordell–Weil rank zero. It is easy to see that the elliptic curve has just three torsion points, $(e, m) = (0, \pm 12)$, and the point at infinity. Tracing these upward, we see that the only rational points on D_1 are points at infinity, hence the only rational points on C are the two points at infinity.

References

1. C. CHABOUTY, 'Démonstration de quelques lemmes de rehaussement', *C. R. Acad. Sci. Paris* 217 (1943) 413–415.
2. C. CHEVALLEY and A. WEIL, 'Un théorème d'arithmétique sur les courbes algébriques', *C. R. Acad. Sci. Paris* 195 (1930) 570–572.

3. J. L. COLLIOT-THÉLÈNE, J. J. SANSUC and H. P. F. SWINNERTON-DYER, 'Intersections of two quadrics and Châtelet surfaces, I', *J. Reine Angew. Math.* 373 (1987) 37–107.
4. V. DEM'JANENKO, 'Rational points of a class of algebraic curves', *Amer. Math. Soc. Translations* 66 (1968) 246–272.
5. G. FALTINGS, 'Endlichkeitsätze für abelsche Varietäten über Zahlkörpern', *Invent. Math.* 73 (1983) 349–366.
6. A. GROTHENDIECK, *Séminaire de géométrie algébrique du Bois-Marie*, 1, Lecture Notes in Mathematics 224 (Springer, Berlin, 1971).
7. D. KUBERT and S. LANG, 'Units in the modular function field, I', *Math. Ann.* (1975) 67–96.
8. S. LANG, *Abelian varieties*, 2nd edition (Springer, New York, 1983).
9. S. LANG, *Complex multiplication* (Springer, New York, 1983).
10. D. MUMFORD, *Introduction to algebraic geometry* (Harvard University, Cambridge, Mass., 1967).
11. P. SATGÉ, 'Une généralisation du calcul de Selmer', *Séminaire de théorie des nombres de Paris*, 1981–1982 (Birkhäuser, Boston, 1983) 245–265.
12. P. SATGÉ, 'Groupes de selmer et corps cubiques', *J. Number Theory* 23 (1986) 294–317.
13. J. P. SERRE, *Groupes algébriques et corps de classes* (Hermann, Paris, 1975).
14. J. H. SILVERMAN, *The arithmetic of elliptic curves* (Springer, New York, 1986).
15. N. M. STEPHENS, 'The diophantine equation $x^3+y^3=dz^3$ and the conjectures of Birch and Swinnerton-Dyer', *J. Reine Angew. Math.* 231 (1968) 121–162.
16. J. VÉLU, 'Isogénies entre courbes ellipiques', *C. R. Acad. Sci. Paris* 273 (1971) 238–241.
17. P. VOJTA, 'A higher dimensional Mordell conjecture', *Arithmetic geometry* (eds. G. Cornell and J. H. Silverman, Springer, New York, 1986) 341–353.

Department of Mathematics
University of Michigan
Ann Arbor
Michigan 48109
USA