Coverings of Curves of Genus 2

E.V. Flynn

Mathematical Institute, University of Oxford
Oxford OX1 3LB, United Kingdom
flynn@maths.ox.ac.uk

Abstract. We shall discuss the idea of finding all rational points on a curve $\mathcal{C}$ by first finding an associated collection of curves whose rational points cover those of $\mathcal{C}$. This classical technique has recently been given a new lease of life by being combined with descent techniques on Jacobians of curves, Chabauty techniques, and the increased power of software to perform algebraic number theory. We shall survey recent applications during the last 5 years which have used Chabauty techniques and covering collections of curves of genus 2 obtained from pullbacks along isogenies on their Jacobians.

1 Introduction

We consider a general curve of genus 2 defined over an number field K

$$\mathcal{C}: \ Y^2 = F(X) = f_6X^6 + f_5X^5 + \ldots + f_0 = F_1(X)\ldots F_k(X), \qquad (1)$$

where $F_1(X), \ldots, F_k(X)$ are the irreducible factors of $F(X)$ over K; we assume that $F(X)$ has no repeated roots and that $f_6 \neq 0$ or $f_5 \neq 0$. The intention is to describe, in a way accessible to a non-specialist, recent developments in Chabauty and covering techniques. These techniques all use essentially the same idea; we first find an Abelian variety A which maps to $\mathcal{J}$, the Jacobian of $\mathcal{C}$, under an isogeny ϕ. The pullbacks under ϕ of a suitably chosen set of embeddings of $\mathcal{C}$ in $\mathcal{J}$, give a collection of curves lying on A whose rational points cover those of $\mathcal{C}$. Despite this rather geometric description, the mechanics of this, in the cases we shall consider, do not in fact require any difficult geometry. Provided the reader is prepared to take on faith a few standard results, the equations for the covering collections of curves can be obtained directly from that of $\mathcal{C}$.

In Section 2, we shall define the Jacobian of a curve of genus 2, and outline a few standard techniques for trying to find its rank. In Section 3, we describe Chabauty's Theorem and, in particular, how it can be applied to the problem of finding the K-rational points on a curve of genus 2 defined over K; similar ideas can also be applied to an elliptic curve $\mathcal{E}$ defined over a number field K, when one wants to find all points in $\mathcal{E}(K)$ subject to some arithmetic condition, such as the $\mathbb{Q}$-rationality of the x-coordinate. In Sections 4,5, we describe the covering collections associated to various choices of isogeny, and give applications. Finally, in Section 6, we compare these techniques with a more classical approach using

resultants. We shall try, in all sections, to provide sufficient detail that the non-specialist reader gains an impression of the techniques and difficulties involved.

We shall have in mind several motivating examples. The first of these concerns cycles of quadratic polynomials. Given a quadratic polynomial $az^2 + bz + c$, with $a, b, c \in \mathbb{Q}$ and $a \neq 0$, we say that $z \in \mathbb{Q}$ is a point *of exact period* N if $g^N(z) = z$ and $g^n(z) \neq z$ for all $n < N$. For example, $z = 0$ is a point of exact period 2 for $z^2 - 1$. It is easy to find such examples for $N = 1, 2, 3$, and it was shown in [19] that none exist for $N = 4$. We shall later summarise the proof in [14] of the fact that none exist for $N = 5$ also. It remains an unsolved problem whether any examples exist for $N \geq 6$. Applying a linear transformation on z, we can assume that our quadratic is monic and has no linear term; that is, it is of the form $g(z) = z^2 + c$ for some $c \in \mathbb{Q}$. Suppose that z is a point of exact period 5; then z, c must satisfy the curve $(g^5(z) - z)/(g(z) - z) = 0$. This curve in z, c is of degree 30 and genus 14, but it has a quotient $\mathcal{C}_1$ of genus 2, derived in [14], given by

$$\mathcal{C}_1 : Y^2 = X^6 + 8X^5 + 22X^4 + 22X^3 + 5X^2 + 6X + 1. \tag{2}$$

There are six obvious points $\infty^{\pm}, (0, \pm 1), (-3, \pm 1)$, where ∞^+, ∞^- denote the points on the non-singular curve that lie over the singular point at infinity on $\mathcal{C}$ (for any curve (1) with $f_6 \neq 0$ both ∞^+ and ∞^- are in $\mathcal{C}(K)$ when $f_6 \in (K^*)^2$). These six points do not have preimages corresponding to $z, c \in \mathbb{Q}$ with z a point of exact period 5, and so the following Lemma gives a way of resolving the case $N = 5$.

Lemma 1 *Let $\mathcal{C}_1$ be as in (2). If $\mathcal{C}_1(\mathbb{Q}) = \{\infty^{\pm}, (0, \pm 1), (-3, \pm 1)\}$ then there is no quadratic polynomial in $\mathbb{Q}[z]$ with a rational point of exact period 5.*

Another application is to the equation

$$a^2 + b^2 = c^2, \quad a^3 + b^3 + c^3 = d^3, \quad a, b, c, d \in \mathbb{Z}. \tag{3}$$

There are the obvious solutions $(3, 4, 5, 6), (4, 3, 5, 6), (1, 0, -1, 0), (0, 1, -1, 0)$, and we would like to show that these are all of them up to scalar multiplication. The first solution, the so-called "Nuptial Number of Plato", is thought (see [29]) to be mentioned indirectly in Plato's *Republic*, as being a special relationship between the 3-4-5 triangle (viewed at the time as the marriage triangle between the "male" number 3 and "female" number 4) and the first perfect number 6. It is shown in [29] that there are no other solutions, using 15 pages of lengthy but elementary resultant and congruence arguments. We shall give a different proof here, using the ideas of the next two sections. For the moment, we merely observe that, on dividing through by c, we get equations in the three affine variables $A = a/c, B = b/c, D = d/c$. Furthermore, the solutions to $A^2 + B^2 = 1$ can be parametrised as $A = (1 - s^2)/(1 + s^2), B = 2s/(1 + s^2)$. We substitute these into $A^3 + B^3 + 1 = D^3$, multiply though by $(1 + s^2)^3$, and replace D by $t = D(1 + s^2)$ to give the curve

$$t^3 = 6s^4 + 8s^3 + 2, \tag{4}$$

which is a plane quartic with a double point at $s = -1, t = 0$, and no other singularities, and so is of genus 2. Using a standard trick (see p.4 of [7]) which involves mapping the double point to $(0,0)$ and then completing a square, we can birationally change variable to $X = t/(1+s), Y = 12s - 4 - t^3/(1+s)^3$, which gives the equation $Y^2 = X^6 + 32X^3 - 32$, with our four known solutions to (3) corresponding to $\infty^{\pm}, (1, \pm 1)$.

Lemma 2 *Let $\mathcal{C}_2 : Y^2 = X^6 + 32X^3 - 32$. If $\mathcal{C}_2(\mathbb{Q}) = \{\infty^{\pm}, (1, \pm 1)\}$ then the only solutions to (3) are $(3, 4, 5, 6)$, $(4, 3, 5, 6)$, $(1, 0, -1, 0)$, $(0, 1, -1, 0)$ up to scalar multiples.*

Also of historical interest is Problem 17 of book VI of the Arabic manuscript of *Arithmetica* [22]. Diophantus poses a problem equivalent to finding a non-trivial rational point on the genus 2 curve

$$\mathcal{C}_3 : Y^2 = X^6 + X^2 + 1. \tag{5}$$

The related problem of finding all rational points has recently been solved by Wetherell [28], who showed that $\mathcal{C}_3(\mathbb{Q}) = \{\infty^{\pm}, (0, \pm 1), (\pm 1/2, \pm 9/8)\}$ using Jacobians and covering techniques. We shall later give a sketch of the proof. This appears to be the only curve considered by Diophantus which has genus > 1.

Another application, close to the heart of anyone who wants to construct exercises for a calculus class, is that of $\mathbb{Q}$-*derived* polynomials; that is, polynomials defined over $\mathbb{Q}$, with all derivatives having all of their roots in $\mathbb{Q}$. An example is $f(x) = x(x-1)(x-8/3), f'(x) = (3x - 4/3)(x-2), f''(x) = 6x - 22/3$. We say that a polynomial is of type $p_{m_1,\ldots,m_r}$ if it has r distinct roots, and each m_i is the multiplicity of the i-th root. Two $\mathbb{Q}$-derived polynomials $q_1(x)$ and $q_2(x)$ are *equivalent* if $q_2(x) = rq_1(sx+t)$, for some constants $r, s, t \in \mathbb{Q}$, with $r, s \neq 0$. The problem of classifying all $\mathbb{Q}$-derived polynomials has been reduced in [5] to showing the following two conjectures.

Conjecture 1 *No polynomial of type $p_{1,1,1,1}$ is $\mathbb{Q}$-derived.*

Conjecture 2 *No polynomial of type $p_{3,1,1}$ is $\mathbb{Q}$-derived.*

Indeed, the following is shown in [5].

Theorem 1 *If Conjectures 1 and 2 are true then all $\mathbb{Q}$-derived polynomials are equivalent to one of*

$$x^n,\ x^{n-1}(x-1),\ x(x-1)\big(x - \frac{v(v-2)}{v^2-1}\big),\ x^2(x-1)\big(x - \frac{9(2w+z-12)(w+2)}{(z-w-18)(8w+z)}\big),$$

for some $n \in \mathbb{Z}^+$, $v \in \mathbb{Q}$, $(w, z) \in \mathcal{E}_0(\mathbb{Q})$, where $\mathcal{E}_0 : z^2 = w(w-6)(w+18)$ is an elliptic curve of rank 1.

For Conjecture 2, we let $q(x)$ be a $\mathbb{Q}$-derived polynomial of type $p_{3,1,1}$, which we may take to be in the form $q(x) = x^3(x-1)(x-a)$, for some $a \in \mathbb{Q}$ with $a \neq 0, 1$. The discriminants of the quadratics $q'''(x)$, $q''(x)/x$ and $q'(x)/x^2$, must

all be rational squares, and so must be their product. This implies that a satisfies $(4a^2 - 7a + 4)(9a^2 - 12a + 9)(4a^2 - 2a + 4) = b^2$, for some $b \in \mathbb{Q}$. Using the transformation $a = (X - 3)/(X + 3), b = 6Y/(X + 3)^3$ gives the genus 2 curve

$$\mathcal{C}_4 : Y^2 = (X^2 + 15)(X^2 + 45)(X^2 + 135). \tag{6}$$

The obvious points $\infty^{\pm}, (\pm 3, \pm 432)$ correspond to the illegal values $a = 0, 1, \infty$, and so it is sufficient to show there are no others.

Lemma 3 *Let $\mathcal{C}_4$ be as in (6). If $\mathcal{C}_4(\mathbb{Q}) = \{\infty^{\pm}, (\pm 3, \pm 432)\}$ then Conjecture 2 is true.*

In Section 4, we shall sketch the proof in [16] that this is indeed all of $\mathcal{C}_4(\mathbb{Q})$, and so now only Conjecture 1 (a surface) remains unsolved.

A very recent result has been the solution in [17] of the "Serre curve"

$$\mathcal{D} : x^4 + y^4 = 17. \tag{7}$$

Serre asks (p.67 of [21]) whether $(x, y) = (\pm 1, \pm 2), (\pm 2, \pm 1)$ are the only $x, y \in \mathbb{Q}$ satisfying (7). This curve is the only Fermat quartic of the type $x^4 + y^4 = c$, with $c \leq 81$, which cannot trivially be solved by local methods or by a map onto an elliptic curve of rank 0. It has gained some notoriety as being resistant to various methods of attack, but has finally succumbed to the general method we shall briefly mention in Section 5.

The work of Bruin develops related ideas, which have been applied with great success to equations of the type $x^p + y^q = z^r$. We shall mention two of these, and give an indication of the approach used.

2 Preliminary Definitions

At the risk of insulting the reader's intelligence, we shall briefly summarise a few standard facts about elliptic curves. Consider the elliptic curve defined over K

$$\mathcal{E} : \ y^2 = G(x) = g_3x^3 + g_2x^2 + g_1x + g_0 = G_1(x) \dots G_k(x), \tag{8}$$

where $G(x)$ has no repeated roots, $g_3 \neq 0$, and $G_1(x), \dots, G_k(x)$ are the irreducible factors of $G(x)$ over K. Let ∞ denote the point at infinity, which we take to be the identity in the group $\mathcal{E}(K)$ of K-rational points on $\mathcal{E}$. The rules $-(x, y) = (x, -y)$ and $P+Q+R = \infty \iff P, Q, R$ are collinear, are sufficient to compute the group law on $\mathcal{E}(K)$, and the points of order 2 are of the form $(x, 0)$, where $x \in K$ is a root of $G(x)$. The Mordell-Weil Theorem gives that $\mathcal{E}(K)$ is isomorphic to $\mathcal{E}(K)_{\text{tor}} \times \mathbb{Z}^r$, where $\mathcal{E}(K)_{\text{tor}}$ is the subgroup of $\mathcal{E}(K)$ consisting of points of finite order, and r is the *rank* of $\mathcal{E}(K)$. The finite group $\mathcal{E}(K)_{\text{tor}}$ is normally found by using reduction maps modulo primes of good reduction. For each $i \in \{1, \dots, k\}$ let α_i be a root of $G_i(x)$ and let $L_i = K(\alpha_i)$.

Define the homomorphism

$$\mu : \mathcal{E}(K) \to L_1^*/(L_1^*)^2 \times \dots \times L_k^*/(L_k^*)^2, \ \ (x, y) \mapsto [g_3(x-\alpha_1), \dots, g_3(x-\alpha_k)], \tag{9}$$

which has kernel $2\mathcal{E}(K)$. Here, $g_3(x-\alpha_j)$ is taken to be 1 when $(x,y)=\infty$, and $\prod_{i\neq j}(x-\alpha_i)$ when $x=\alpha_j$. If we let $S=\{2,p_1,\ldots,p_m\}$, where $p_1,\ldots,p_m$ are the rational primes of bad reduction, then the image of q is contained inside the finite group M, consisting of those $[d_1,\ldots,d_k]$ such that all of the field extensions $L_1(\sqrt{d_1}):L_1,\ldots,L_k(\sqrt{d_k}):L_k$ are unramified outside of primes lying over primes of S. Once M is determined, one eliminates members of M as potential members of $\mathrm{im}(q)$ by local (congruence) arguments. What remains is the *2-Selmer group*, and one hopes that this is enough to determine the 2-rank of $\mathrm{im}(q)$, and hence that of $\mathcal{E}(K)/2\mathcal{E}(K)$. If so, then one will have performed a successful complete 2-descent. On subtracting the 2-rank of $\mathcal{E}(K)_{\mathrm{tor}}/2\mathcal{E}(K)_{\mathrm{tor}}$, the remainder is the rank of $\mathcal{E}(K)$. A benefit of recent developments in algebraic number theory software, such as PARI/GP [1] and KASH [10], is that the above approach has become possible for elliptic curves defined over increasingly complicated number fields. Some of the methodology is described in [11],[20],[23],[24]; see also the program [4]. We mention here two such computations in the literature ([15], [16], respectively) which will be relevant to later sections.

Example 1 *Let α satisfy $\alpha^3+\alpha+1=0$, and define over $\mathbb{Q}(\alpha)$ the elliptic curves $\mathcal{E}_1: y^2=x(x^2+\alpha x+(\alpha^2+1))$ and $\mathcal{E}_2: y^2=-\alpha x(x^2+\alpha x+(\alpha^2+1))$. Then $\mathcal{E}_1(\mathbb{Q}(\alpha))$ has rank 1, with generators given by $(0,0),(-\alpha,1)$, where $(0,0)$ is of order 2 and $(-\alpha,1)$ is of infinite order. Also, $\mathcal{E}_2(\mathbb{Q}(\alpha))$ has rank 0 and consists only of ∞ and $(0,0)$.*

Example 2 *Let $\beta=\sqrt{-15}$ and let $\mathcal{E}_3: y^2=6(54+6\beta)(-45x^2+1)(\beta x+1)$ and $\mathcal{E}_4: y^2=6(9+\beta)(-45x^2+1)(\beta x+1)$. Then $\mathcal{E}_3(\mathbb{Q}(\beta))$ has rank 1 and is generated by the 2-torsion point $(-1/\beta,0)$ and the point $(1/6+\beta/30,24)$ of infinite order. Similarly, $\mathcal{E}_4(\mathbb{Q}(\beta))$ has rank 1 and is generated by the 2-torsion point $(-1/\beta,0)$ and the point $(-1/6+\beta/30,9+\beta)$ of infinite order.*

Given a curve $\mathcal{C}$ of genus 2, as in (1) with $f_6\neq 0$, we use ∞^+,∞^- as described after (2). When $f_6=0$ (and so $f_5\neq 0$), we let ∞ denote the point at infinity, which is always in $\mathcal{C}(K)$. Following Chapter 1 of [7], any member of $\mathcal{J}(K)$, the K-rational points on the Jacobian, may be represented by a divisor of the form $P_1+P_2-\infty^+-\infty^-$, where P_1,P_2 are points on $\mathcal{C}$ and either P_1,P_2 are both K-rational or P_1,P_2 are quadratic over K and conjugate. We shall abbreviate such a divisor by: $\{P_1,P_2\}$. This representation gives a 1-1 correspondence with members of $\mathcal{J}(K)$, except that everything of the form $\{(X,Y),(X,-Y)\}$ must be identified into a single equivalence class $\mathcal{O}$, which serves as the group identity in $\mathcal{J}(K)$. Note that $-\{(x_1,y_1),(x_2,y_2)\}=\{(x_1,-y_1),(x_2,-y_2)\}$; furthermore $\{P_1,P_2\}+\{Q_1,Q_2\}+\{R_1,R_2\}=\mathcal{O}$ if and only if there exists $\Upsilon(X)$ of degree ≤ 3 such that $Y=\Upsilon(X)$ meets $\mathcal{C}$ at P_1,P_2,Q_1,Q_2,R_1,R_2. These two rules are sufficient for computing the group law on $\mathcal{J}(K)$. Clearly, an element of order 2 in $\mathcal{J}(K)$ is given by $\{(X_1,0),(X_2,0)\}$, where X_1,X_2 are the roots of quadratic $Q(X)$ defined over K, satisfying $Q(X)|F(X)$. The Mordell-Weil Theorem gives that $\mathcal{J}(K)$ is isomorphic to $\mathcal{J}(K)_{\mathrm{tor}}\times\mathbb{Z}^r$, where $\mathcal{J}(K)_{\mathrm{tor}}$ is the subgroup of $\mathcal{J}(K)$ consisting of points of finite order, and r is the *rank* of $\mathcal{J}(K)$.

The finite group $\mathcal{J}(K)_{\rm tor}$ is normally found by using reduction maps modulo primes of good reduction. For each $i \in \{1, \ldots, k\}$ let α_i be a root of $F_i(x)$ and let $L_i = K(\alpha_i)$. When $f_6 \neq 0$, we define the homomorphism

$$\begin{array}{c} \mu: \quad \mathcal{J}(K) \to \Big(L_1^*/(L_1^*)^2 \times \ldots \times L_k^*/(L_k^*)^2\Big)/\sim, \\ : \{(X_1, Y_1), (X_2, Y_2)\} \mapsto [(X_1 - \alpha_1)(X_2 - \alpha_2), \ldots, (X_1 - \alpha_k)(X_2 - \alpha_k)], \end{array} \tag{10}$$

where the equivalence relation $\sim$ is defined by

$$[a_1, \ldots, a_k] \sim [b_1, \ldots, b_k] \iff a_1 = wb_1, \ldots, a_k = wb_k, \text{ for some } w \in K^*. \tag{11}$$

The interpretations of $X_i - \alpha_j$ in special cases where (X_i, Y_i) is a point at infinity, or $X_i = \alpha_j$, are as described immediately after (9). Either $2\mathcal{J}(K)$ is the kernel of q or it has index 2 in the kernel of q (see [14]). The image of q is contained inside a finite group M, which is as described above for elliptic curves. Once M is determined, one proceeds in a similar manner to the complete 2-descent for elliptic curves described above, and hopes to find [26] the 2-rank of $\mathcal{J}(K)/2\mathcal{J}(K)$. There is some extra finesse here in determining the whether or not the kernel of q is $2\mathcal{J}(K)$, and in the interpretation of the local information; there is also the potential for difficult computations in number fields of higher degree over the ground field than for elliptic curves. When $f_6 = 0$, the relation $\sim$ can be removed, and the mechanics become more similar to that of complete 2-descent on an elliptic curve. As with elliptic curves, the final step is to subtract the 2-rank of $\mathcal{J}(K)_{\rm tor}/2\mathcal{J}(K)_{\rm tor}$ from that of $\mathcal{J}(K)/2\mathcal{J}(K)$ to obtain the rank of $\mathcal{J}(K)$. Recent developments in canonical heights and infinite descent ([13],[25],[27]) also allow actual generators for $\mathcal{J}(K)$ to be computed in many cases. We mention here three ranks computed in the literature ([14], [28], [16], respectively), which we shall require later. Only the first of these is a genuine genus 2 computation, the other three ranks being computable via maps to elliptic curves.

Example 3 *Let $\mathcal{C}_1 : Y^2 = X^6 + 8X^5 + 22X^4 + 22X^3 + 5X^2 + 6X + 1$, as in (2), with Jacobian $\mathcal{J}_1$. Then $\mathcal{J}_1(\mathbb{Q})_{\rm tor} = \{\mathcal{O}\}$; the rank of $\mathcal{J}_1(\mathbb{Q})$ is 1, and it is generated by $\{\infty^+, \infty^+\}$.*

Example 4 *Let $\mathcal{C}_2 : Y^2 = X^6 + 32X^3 - 32$, as in Lemma 2, with Jacobian $\mathcal{J}_2$. Then $\mathcal{J}_2(\mathbb{Q})_{\rm tor} = \{\mathcal{O}, \{\infty^+, \infty^+\}, \{\infty^-, \infty^-\}\}$; the rank of $\mathcal{J}_2(\mathbb{Q})$ is 1, and it is generated by $\mathcal{J}_2(\mathbb{Q})_{\rm tor}$ and $\{(1, 1), \infty^+\}$.*

Example 5 *Let $\mathcal{C}_3 : Y^2 = X^6 + X^2 + 1$, with Jacobian $\mathcal{J}_3$. Then $\mathcal{J}_3(\mathbb{Q})_{\rm tor} = \{\mathcal{O}\}$; the rank of $\mathcal{J}_3(\mathbb{Q})$ is 2, and it is generated by $\{(0, 1), (0, 1)\}$ and $\{(0, 1), \infty^+\}$.*

Example 6 *Let $\mathcal{C}_4 : Y^2 = F_1(X)F_2(X)F_3(X)$, with Jacobian $\mathcal{J}_4$, where:*
$$F_1(X) = X^2 + 15,\ F_2(X) = X^2 + 45,\ F_3(X) = X^2 + 135,$$
and let α_i, β_i be the roots of $G_i(X)$ for $1 \leq i \leq 3$. Then
$$\mathcal{J}_4(\mathbb{Q})_{\rm tor} = \{\mathcal{O}, \{(\alpha_1, 0), (\beta_1, 0)\}, \{(\alpha_2, 0), (\beta_2, 0)\}, \{(\alpha_3, 0), (\beta_3, 0)\}\};$$
the rank of $\mathcal{J}_4(\mathbb{Q})$ is 2, and it is generated by the 2-torsion above, together with $\{\infty^+, \infty^+\}$ and $\{(3, 432), \infty^+\}$.

3 Chabauty's Theorem

Let $\mathcal{E}$ be an elliptic curve, as in (8), defined over a number field $K = \mathbb{Q}(\alpha)$ of degree d. We shall consider the problem of trying to find all

$$(x, y) \in \mathcal{E}(\mathbb{Q}(\alpha)) \text{ with } x \in \mathbb{Q}. \tag{12}$$

Imitating Chapter IV of [24] (with the difference that our equations include g_3, the coefficient of x^3), we introduce the variables $s = -x/y, w = -1/y$. Then $w = g_3 s^3 + g_2 s^2 w + g_1 s w^2 + g_0 w^3$, and recursive substitution gives $w = w(s)$, a power series in the local parameter s, with initial term $g_3 s^3$. Then $1/x = w(s)/s$ is a power series

$$\frac{1}{x}(s) = g_3\big(s^2 + g_2 s^4 + (g_1 g_3 + g_2^2)s^6 + O(s^8)\big) \in \mathbb{Z}[g_0, g_1, g_2, g_3][[s]]. \tag{13}$$

If (x_0, y_0) is another point on $\mathcal{E}$, then the x-coordinate of $(x_0, y_0) + (x, y)$ is a power series

$$\begin{aligned} x\text{-coord of } \big(\,(x_0, y_0) + (x, y)\big) &= x_0 + 2y_0 s + (3g_3 x_0^2 + 2g_2 x_0 + g_1)s^2 + O(s^3) \\ &\in \mathbb{Z}[g_0, g_1, g_2, g_3, x_0, y_0][[s]]. \end{aligned} \tag{14}$$

If $(s, w(s)), (t, w(t))$ are two points in s-w coordinates then the s-coordinate of the sum can be written as $\mathcal{F}(s, t) \in \mathbb{Z}[g_0, g_1, g_2, g_3][[s, t]]$, the *formal group*. There are then power series

$$\log(t) = t + \frac{1}{3}g_2 t^3 + \frac{1}{5}(g_2^2 + 2g_1 g_3)t^5 + O(t^7) \in \mathbb{Q}[g_0, g_1, g_2, g_3][[t]], \tag{15}$$

$$\exp(t) = t - \frac{1}{3}g_2 t^3 + \frac{1}{15}(2g_2^2 - 6g_1 g_3)t^5 + O(t^7) \in \mathbb{Q}[g_0, g_1, g_2, g_3][[t]], \tag{16}$$

satisfying $\log(\mathcal{F}(s, t)) = \log(s) + \log(t)$, $\mathcal{F}(\exp(s), \exp(t)) = \exp(s + t)$. In either power series, the denominator of the coefficient of t^k divides $k!$.

We now suppose that the rank r of $\mathcal{E}(\mathbb{Q}(\alpha))$ is less than $d = [\mathbb{Q}(\alpha) : \mathbb{Q}]$, and that we have found generators for $\mathcal{E}(\mathbb{Q}(\alpha))$:

$$\mathcal{E}(\mathbb{Q}(\alpha)) = \langle \mathcal{E}(\mathbb{Q}(\alpha))_{\text{tor}}, P_1, \ldots, P_r \rangle. \tag{17}$$

Suppose that p is an odd prime such that $|\alpha|_p = 1$, $\mathbb{Q}(\alpha)$ is unramified at p, $\mathcal{E}$ has good reduction at p, $[\mathbb{Q}_p(\alpha) : \mathbb{Q}_p] = [\mathbb{Q}(\alpha) : \mathbb{Q}] = d$, and $|g_i|_p \le 1$, for $i = 1, \ldots, 3$. These restrictions on p (which cannot be satisfied for some choices of α) are only for the sake of simplifying the exposition. Let $\tilde{\alpha}$, $\widetilde{\mathcal{E}}$, $\widetilde{P}_1, \ldots, \widetilde{P}_r$ represent, respectively, the reductions mod p of $\alpha, \mathcal{E}, P_1, \ldots, P_r$. Further define $m_i, Q_i, x_i, y_i, s^{(i)}$ by

$$m_i = \text{order of } \widetilde{P}_i \text{ in } \widetilde{\mathcal{E}}(\mathbb{F}_p(\tilde{\alpha})), \quad Q_i = m_i P_i = (x_i, y_i), \quad s^{(i)} = -x_i/y_i, \tag{18}$$

so that each $Q_i \in \mathcal{E}(\mathbb{Q}(\alpha))$ is in the kernel of the reduction map from $\mathcal{E}(\mathbb{Q}(\alpha))$ to $\widetilde{\mathcal{E}}(\mathbb{F}_p(\tilde{\alpha}))$, giving $|s^{(i)}|_p \le p^{-1}$. Now, let $\mathcal{S}$ be a set (which must be finite) of

representatives of $\mathcal{E}(\mathbb{Q}(\alpha))$ modulo $\langle Q_1, \ldots, Q_r \rangle$, so that every $P \in \mathcal{E}(\mathbb{Q}(\alpha))$ can be written uniquely in the form

$$P = S + n_1 Q_1 + \ldots + n_r Q_r, \tag{19}$$

for some $S \in \mathcal{S}$ and $n_1, \ldots n_r \in \mathbb{Z}$. We can now express the s-coordinate of $n_1 Q_1 + \ldots + n_r Q_r$, using (15),(16), as: $\exp(n_1 \log(s^{(1)}) + \ldots + n_r \log(s^{(r)}))$, which is a power series in $n_1, \ldots, n_r$. Substituting this power series for s in (13) when $S = \infty$, and in (14) when $S = (x_0, y_0) \neq \infty$ gives

$$\theta_S(n_1, \ldots, n_r) = x_S(S + n_1 Q_1 + \ldots + n_r Q_r) \in \mathbb{Z}_p[\alpha][[n_1, \ldots, n_r]], \tag{20}$$

where x_S means x-coordinate, when $S \neq \infty$, and $1/x$-coordinate when $S = \infty$. It is clear, from the standard estimate $|k!|_p \geq p^{-(k-1)/(p-1)}$, that the coefficient of $n_1^{k_1} \ldots n_r^{k_r}$ is in $\mathbb{Z}_p[\alpha]$, and converges to 0 as $k_1 + \ldots + k_r \to \infty$. Splitting θ_S into its components

$$\theta_S = \theta_S^{(0)} + \theta_S^{(1)} \alpha + \ldots + \theta_S^{(d-1)} \alpha^{d-1}, \text{ each } \theta_S^{(i)}(n_1, \ldots n_r) \in \mathbb{Z}_p[[n_1, \ldots, n_r]], \tag{21}$$

we obtain power series satisfying

$$(x\text{-coord of } P) \in \mathbb{Q} \Rightarrow \theta_S^{(1)} = \ldots = \theta_S^{(d-1)} = 0. \tag{22}$$

We now make use of the following theorem (p.62 of [6]).

Theorem 2 (Strassmann). *Let $\theta(X) = c_0 + c_1 X + \ldots \in \mathbb{Z}_p[[X]]$ satisfy $c_j \to 0$ in $\mathbb{Z}_p$. Define ℓ uniquely by: $|c_\ell|_p \geqslant |c_j|_p$ for all $j \geqslant 0$, and $|c_\ell|_p > |c_j|_p$ for all $j > \ell$. Then there are at most ℓ values of $x \in \mathbb{Z}_p$ such that $\theta(x) = 0$.*

When r, the rank of $\mathcal{E}(\mathbb{Q}(\alpha))$, is 1 (as will be the case in the following examples), and $d = [\mathbb{Q}(\alpha) : \mathbb{Q}] > 1$, then we can apply Strassmann's Theorem to bound, for example, the number of roots of $\theta_S^{(1)}(n_1)$. In view of (22), summing these bounds over all $S \in \mathcal{S}$ gives an upper bound on the total number of (x, y) satisfying (12), which we hope to be the number of known such (x, y). When $r > 1$ and $r < d$, we can in principle try to perform repeated applications if the Weierstrass Preparation Theorem (see p.108 of [6]) and resultant computations to derive univariate power series from d power series in r variables.

Example 7 *Let $\alpha, \mathcal{E}_1, \mathcal{E}_2$ be as in Example 1. Then the only $(x, y) \in \mathcal{E}_1(\mathbb{Q}(\alpha))$ with $x \in \mathbb{Q}$ are $\infty, (0, 0), \pm(1/4, 1/8 - \alpha/2 + \alpha^2/4)$. The only $(x, y) \in \mathcal{E}_2(\mathbb{Q}(\alpha))$ with $x \in \mathbb{Q}$ are $\infty, (0, 0)$.*

Proof (see [15] for details): The result on $\mathcal{E}_2(\mathbb{Q}(\alpha))$ follows immediately from Example 1, since the rank is 0, and $\infty, (0, 0)$ are the only members of $\mathcal{E}_2(\mathbb{Q}(\alpha))$.

For $\mathcal{E}_1(\mathbb{Q}(\alpha))$, let $P_1 = (-\alpha, 1)$, $p = 5$, $m_1 = 28$; then $28P_1$ is in the kernel of reduction mod 5, but it is more efficient to take $Q_1 = 14P_1 + (0, 0)$, which is also in the kernel of reduction mod 5. Let

$$\mathcal{S} = \{kP_1 : -6 \leq k \leq 7\} \cup \{(0, 0) + kP_1 : -6 \leq k \leq 7\}, \tag{23}$$

so that any $P \in \mathcal{E}_1(\mathbb{Q}(\alpha))$ can be written as $S + n_1 Q_1$, for some $S \in \mathcal{S}, n_1 \in \mathbb{Z}$. Let us first consider $S = -2P_1 = (1/4, 1/8 - \alpha/2 + \alpha^2/4)$. Applying (15),(16), gives the s-coordinate of $n_1 Q_1$ as:

$$\exp(n_1 \log(s\text{-coordinate of } Q_1)) \equiv 5(21 + 15\alpha + 21\alpha^2)n_1 \pmod{5^3}. \quad (24)$$

Replacing (x_0, y_0) by $(1/4, 1/8 - \alpha/2 + \alpha^2/4)$ and s by (24) in (14) gives the x-coordinate of $-2P_1 + n_1 Q_1$ as:

$$\theta_{-2P_1}(n_1) \equiv 94 + 5(17\alpha + 9\alpha^2)n_1 + 5^2(2 + \alpha + \alpha^2)n_1^2 \pmod{5^3}. \quad (25)$$

We may consider either $\theta^{(1)}_{-2P_1}$ or $\theta^{(2)}_{-2P_1}$, due to the fact that the rank of $\mathcal{E}(\mathbb{Q}(\alpha))$ is two less than $[\mathbb{Q}(\alpha) : \mathbb{Q}]$. Taking $\theta^{(2)}_{-2P_1}(n_1) \equiv 5 \cdot 9 \cdot n_1 + 5^2 \cdot n_1^2 \pmod{5^3}$, and applying Strassmann's Theorem, gives that there is at most one root; but we know that $n_1 = 0$ is a root, since $-2P_1 + 0 \cdot Q_1$ has x-coordinate $= 1/4 \in \mathbb{Q}$. Hence $n_1 = 0$ is the only solution. Similarly, for $S = \infty, (0,0), 2P_1$ we can show that $n_1 = 0$ is the value of n_1 for which $S + n_1 Q_1$ can have $\mathbb{Q}$-rational x-coordinate. For the remaining ten values of $S \in \mathcal{S}$, we find that $\theta^{(2)}_S(n_1)$ has constant term of 5-adic norm strictly greater than all subsequent coeffients; hence there are no roots in these cases. In summary, we have shown that $\infty, (0,0), \pm P_1$ are the only members of $\mathcal{E}(\mathbb{Q}(\alpha))$ with $\mathbb{Q}$-rational x-coordinate, as required. $\square$

A similar argument (see [16]), working mod 11^3, shows the following.

Example 8 *Let $\beta, \mathcal{E}_3, \mathcal{E}_4$ be as in Example 2. Then the only $(x, y) \in \mathcal{E}_3(\mathbb{Q}(\beta))$ with $x \in \mathbb{Q}$ are $\infty, \pm(-1/3, 12 + 12\beta), \pm(1/9, 12 + 4\beta/3)$. Similarly, the only $(x, y) \in \mathcal{E}_4(\mathbb{Q}(\beta))$ with $x \in \mathbb{Q}$ are $\infty, \pm(1/3, 12 - 4\beta), \pm(-1/9, 16/3)$.*

Now, consider a curve (1) of genus 2; suppose that it is defined over $\mathbb{Q}$ and that $\mathcal{J}(\mathbb{Q})$ has rank 1. Given $D = \{(X_1, Y_1), (X_2, Y_2)\} \in \mathcal{J}(\mathbb{Q})$, it is possible to describe a local parameter $\mathbf{s} = (s_1, s_2)$ given by

$$\begin{aligned} s_1 &= (\mathcal{G}_1(X_1, X_2)Y_1 - \mathcal{G}_1(X_2, X_1)Y_2)(X_1 - X_2)/(\mathcal{F}_0(X_1, X_2) - 2Y_1Y_2)^2, \\ s_2 &= (\mathcal{G}_0(X_1, X_2)Y_1 - \mathcal{G}_0(X_2, X_1)Y_2)(X_1 - X_2)/(\mathcal{F}_0(X_1, X_2) - 2Y_1Y_2)^2, \end{aligned} \quad (26)$$

where

$$\begin{aligned} \mathcal{F}_0(X_1, X_2) &= 2f_0 + f_1(X_1 + X_2) + 2f_2(X_1X_2) + f_3(X_1X_2)(X_1 + X_2) \\ &\quad + 2f_4(X_1X_2)^2 + f_5(X_1X_2)^2(X_1 + X_2) + 2f_6(X_1X_2)^3, \\ \mathcal{G}_1(X_1, X_2) &= 2f_0(X_1 + X_2) + f_1X_2(3X_1 + X_2) + 4f_2(X_1X_2^2) \\ &\quad + f_3(X_1^2X_2^2 + 3X_1X_2^3) + f_4(2X_1^2X_2^3 + 2X_1X_2^4) \\ &\quad + f_5(3X_1^2X_2^4 + X_1X_2^5) + 4f_6(X_1^2X_2^5), \\ \mathcal{G}_0(X_1, X_2) &= 4f_0 + f_1(X_1 + 3X_2) + f_2(2X_1X_2 + 2X_2^2) + f_3(3X_1X_2^2 + X_2^3) \\ &\quad + 4f_4(X_1X_2^3) + f_5(X_1^2X_2^3 + 3X_1X_2^4) + f_6(2X_1^2X_2^4 + 2X_1X_2^5). \end{aligned}$$

The derivations of the above definitions are given in Chapter 7 of [7]. The reader can at least observe that s_1, s_2 will both be small when D is close to $\mathcal{O}$. It is sufficient, in what follows, to accept on faith that $\mathbf{s} = (s_1, s_2)$ performs the

same role on $\mathcal{J}(\mathbb{Q})$ as $s = -x/y$ does on an elliptic curve. Let $D_0, D \in \mathcal{J}(\mathbb{Q})$, with $\mathbf{s} = \mathbf{s}(D) = (s_1(D), s_2(D))$ being the local parameter for D, and let $D_0 + D = \{(X_1', Y_1'), (X_2', Y_2')\}$. Then the group law on $\mathcal{J}(\mathbb{Q})$ can be applied to find $\psi^{(1)}_{D_0}(\mathbf{s}), \psi^{(2)}_{D_0}(\mathbf{s}), \psi^{(3)}_{D_0}(\mathbf{s})$, power series in $\mathbf{s}$, such that

$$(1 : X_1' + X_2' : X_1'X_2') = (\psi^{(1)}_{D_0}(\mathbf{s}) : \psi^{(2)}_{D_0}(\mathbf{s}) : \psi^{(3)}_{D_0}(\mathbf{s})), \tag{27}$$

where both sides should be viewed as projective triples. Associated to our local parameter is $\mathcal{F}(\mathbf{s}, \mathbf{t})$, the two-parameter formal group of $\mathcal{J}(\mathbb{Q})$, the formal logarithm $L = (L_1, L_2)$ and exponential map $E = (E_1, E_2)$, given by

$$\begin{array}{ll} L_1(\mathbf{s}) = s_1 + \frac{1}{3}(-2f_4 s_1^3 + f_1 s_2^3) + \ldots & E_1(\mathbf{s}) = s_1 + \frac{1}{3}(2f_4 s_1^3 - f_1 s_2^3) + \ldots \\ L_2(\mathbf{s}) = s_2 + \frac{1}{3}(-2f_2 s_2^3 + f_5 s_1^3) + \ldots & E_2(\mathbf{s}) = s_2 + \frac{1}{3}(2f_2 s_2^3 - f_5 s_1^3) + \ldots \end{array} \tag{28}$$

These satisfy $L(\mathcal{F}(\mathbf{s}, \mathbf{t})) = L(\mathbf{s}) + L(\mathbf{t})$ and $E(\mathbf{s} + \mathbf{t}) = \mathcal{F}(E(\mathbf{s}), E(\mathbf{t}))$. Now, suppose that $\mathcal{J}(\mathbb{Q}) = \langle J(\mathbb{Q})_{\mathrm{tor}}, D_1 \rangle$, and let p be a prime of good reduction. Let $\widetilde{\mathcal{J}}$ and $\widetilde{D}_1$ represent, respectively, the reductions mod p of J and D_1. Further define $m_1, E_1, \mathbf{s}^{(1)}$ by

$$m_1 = \text{order of } \widetilde{D}_1 \text{ in } \widetilde{\mathcal{J}}(\mathbb{F}_p), \quad E_1 = m_1 D_1, \quad \mathbf{s}^{(1)} = \mathbf{s}(D_1), \tag{29}$$

so that $E_1 \in \mathcal{J}(\mathbb{Q})$ is in the kernel of the reduction map from $\mathcal{J}(\mathbb{Q})$ to $\widetilde{\mathcal{J}}(\mathbb{F}_p)$, giving $|s_1^{(1)}|_p, |s_2^{(1)}|_p \leq p^{-1}$. Now, let $\mathcal{S}$ be a set (which must be finite) of representatives of $\mathcal{J}(\mathbb{Q})$ modulo $\langle E_1 \rangle$, so that every $D \in \mathcal{J}(\mathbb{Q})$ can be written uniquely in the form

$$D = S + n_1 E_1, \tag{30}$$

for some $S \in \mathcal{S}$ and $n_1 \in \mathbb{Z}$. Now express $\mathbf{s}(D)$, using (28), as: $\exp(n_1 \log(\mathbf{s}^{(1)}))$, which is a power series in n_1. Substitute this power series for $\mathbf{s}$ in (27) and take $D_0 = S$ to obtain

$$\theta_S^{(i)}(n_1) = \psi_S^{(i)}(\exp(n_1 \log(\mathbf{s}^{(1)}))) \in \mathbb{Z}_p[[n_1]], \quad \text{for } i = 1, 2, 3. \tag{31}$$

As with elliptic curves, the standard estimate $|k!|_p \geq p^{-(k-1)/(p-1)}$, can be used to show that the coefficient of n_1^k is in $\mathbb{Z}_p$, and converges to 0 as $k \to \infty$.

So far, what we have achieved is to find a finite set of triples of power series, namely $(\theta_S^{(1)}(n_1), \theta_S^{(2)}(n_1), \theta_S^{(3)}(n_1))$ for $S \in \mathcal{S}$, such that any $D \in \mathcal{J}(\mathbb{Q})$ has $(1 : X_1 + X_2 : X_1 X_2)$ equal to one of them. Now recall our original purpose, to find all of $\mathcal{C}(\mathbb{Q})$. The strategy is to embed the curve $\mathcal{C}$ into its Jacobian; we shall choose the map $P \mapsto \{P, P\}$, for any $P \in \mathcal{C}(\mathbb{Q})$. This is not quite an injection, since any $(X, 0) \mapsto \mathcal{O}$; however, it is straightforward to find all $\mathbb{Q}$-rational roots of the sextic $F(X)$, and so all points $(X, 0) \in \mathcal{C}(\mathbb{Q})$. Therefore, we can set these aside and concentrate on $P = (X, Y)$ with $Y \neq 0$, where $P \mapsto \{P, P\}$ is injective. It is sufficient, then, to find all $D \in \mathcal{J}(\mathbb{Q})$ of the form $D = \{P, P\}$. Note that this implies $X_1 = X_2$, and so $(X_1 + X_2)^2 - 4X_1X_2 = 0$, giving

$$\theta_S^{(2)}(n_1)^2 - 4\theta_S^{(1)}(n_1)\theta_S^{(3)}(n_1) = 0, \tag{32}$$

for some $S \in \mathcal{S}$ – namely the $S \in \mathcal{S}$ such that $D = S \bmod \langle E_1 \rangle$. Our strategy, then, is to compute the power series in (32) and use Strassmann's Theorem to find an upper bound on the number of possible n_1. Adding these bounds together gives an upper bound on the number of $(X, Y) \in \mathcal{C}(\mathbb{Q})$ with $Y \neq 0$, which we hope to be the same as the number of known points. We illustrate this with the following example from [14].

Example 9 *Let $\mathcal{C}_1$ be as in Example 3. Then $\mathcal{C}_1(\mathbb{Q}) = \{\infty^{\pm}, (0, \pm 1), (-3, \pm 1)\}$.*

Proof: We already know from Example 3 that $\mathcal{J}_1(\mathbb{Q})$ has no nontrivial torsion and has rank 1, with $\mathcal{J}_1(\mathbb{Q}) = \langle D_1 \rangle$, where $D_1 = \{\infty^+, \infty^+\}$. Let $p = 3$, which is a prime of good reduction, since the discriminant of the sextic is $2^{12} \cdot 3701$. Let $\widetilde{D}_1 \in \widetilde{\mathcal{J}}(\mathbb{F}_3)$ denote the reduction of D_1 mod 3. The following lists the first few multiples of D_1 and $\widetilde{D}_1$. In the table, which is reproduced from [14], $P_0 = (-2 + \frac{1}{3}\sqrt{33}, -\frac{17}{3} + \frac{10}{9}\sqrt{33})$ and $Q_0 = (-\frac{1}{2} + \frac{1}{6}\sqrt{-87}, \frac{22}{3} + \frac{5}{9}\sqrt{-87})$, and $\overline{P}_0$ and $\overline{Q}_0$ are their conjugates over $\mathbb{Q}$.

n	nD_1	$n\widetilde{D}_1$
0	$\mathcal{O}$	$\mathcal{O}$
1	$\{\infty^+, \infty^+\}$	$\{\infty^+, \infty^+\}$
2	$\{(0,1), (-3,1)\}$	$\{(0,1), (0,1)\}$
3	$\{(0,-1), \infty^-\}$	$\{(0,-1), \infty^-\}$
4	$\{(0,-1), \infty^+\}$	$\{(0,-1), \infty^+\}$
5	$\{(-3,1), \infty^-\}$	$\{(0,1), \infty^-\}$
6	$\{(-3,1), \infty^+\}$	$\{(0,1), \infty^+\}$
7	$\{(0,-1), (0,-1)\}$	$\{(0,-1), (0,-1)\}$
8	$\{P, \overline{P}\}$	$\{\infty^-, \infty^-\}$
9	$\{(0,-1), (-3,1)\}$	$\mathcal{O}$
10	$\{Q, \overline{Q}\}$	$\{\infty^+, \infty^+\}$
11	$\{(-3,1), (-3,1)\}$	$\{(0,1), (0,1)\}$

Table 1. The first 11 multiples of D_1 and $\widetilde{D}_1$.

It is apparent that $\pm D_1, \pm 7D_1, \pm 11D_1$ are all of the form $\{P, P\}$, and it is sufficient to show that no other member of $\mathcal{J}_1(\mathbb{Q})$ is of this form. Let $E_1 = 9D_1$, which is in the kernel of reduction mod 3 since $9\widetilde{D}_1 = \mathcal{O}$, with corresponding local parameter $(-9/14, 426/49)$. Applying equation (28) we find that the local parameter of $n_1 E_1$ is $(36n_1, 3n_1 + 9n_1^3) \bmod 3^3$. Any $D \in \mathcal{J}_1(\mathbb{Q})$ can be written as $D = S + n_1 E_1$, for some $S \in \mathcal{S} = \{\mathcal{O}, D_1, 2D_1 \ldots, 8D_1\}$. Consider, for example, $S = 2D_1$. Using the group law to compute (27) mod 3^3 at $D_0 = S = 2D_1$, and then substituting $(36n_1, 3n_1 + 9n_1^3)$ for (s_1, s_2) gives (31) as

$$\begin{aligned} \theta^{(1)}_{2D_1}(n_1) &\equiv 25 + 15n_1 + 18n_1^2 + 18n_1^3 \pmod{3^3}, \\ \theta^{(2)}_{2D_1}(n_1) &\equiv 6 + 24n_1 + 9n_1^2 + 18n_1^2 \pmod{3^3}, \\ \theta^{(3)}_{2D_1}(n_1) &\equiv 18n_1 + 18n_1^2 \pmod{3^3}, \end{aligned} \tag{33}$$

and so $\theta^{(2)}_{2D_1}(n_1)^2 - 4\theta^{(1)}_{2D_1}(n_1)\theta^{(3)}_{2D_1}(n_1) \equiv 9 + 18n_1^2 \pmod{3^3}$. Strassmann's Theorem tells us that there are at most two roots. In fact we know that $n_1 = \pm 1$ are solutions, since $2D_1 + E_1 = 11D_1 = \{(-3,1),(-3,1)\}$ and $2D_1 - E_1 = -7D_1 = \{(0,1),(0,1)\}$ are both of the form $\{P,P\}$. Therefore, $n_1 = \pm 1$ are the only $n_1 \in \mathbb{Z}$ such that $2D_1 + n_1E_1$ is of the form $\{P,P\}$. Similar arguments show that: the only $n_1 \in \mathbb{Z}$ such that $D_1 + n_1E_1$ is of the form $\{P,P\}$ is $n_1 = 0$; the only $n_1 \in \mathbb{Z}$ such that $7D_1 + n_1E_1$ is of the form $\{P,P\}$ are $n_1 = 0, -2$; the only $n_1 \in \mathbb{Z}$ such that $8D_1 + n_1E_1$ is of the form $\{P,P\}$ is $n_1 = -1$. For the remaining five $S \in \mathcal{S}$, Strassmann's Theorem shows that $S + n_1E_1$ is never of this form. Hence the upper bound on the order of $\mathcal{C}_1(\mathbb{Q})$ is six, and so $\infty^{\pm}, (0,\pm 1), (-3,\pm 1)$ must give all of $\mathcal{C}_1(\mathbb{Q})$. □

Combining Lemma 1 and Example 9 gives us the result shown in [14]

Theorem 3 *There is no quadratic polynomial in $\mathbb{Q}[z]$ with a rational point of exact period 5.*

A similar argument, but using the prime $p = 43$, shows that $\mathcal{C}_2(\mathbb{Q}) = \{\infty^{\pm}, (1,\pm 1)\}$, where $\mathcal{C}_2$ is as in (3) and Example 4 (which showed that $\mathcal{J}_2(\mathbb{Q})$ has rank 1). In view of Lemma 2, this gives a new proof of the result originally shown in [29] by an elaborate set of resultant and congruence arguments.

Theorem 4 *The only integer solutions to $a^2 + b^2 = c^2,\ a^3 + b^3 + c^3 = d^3$ are $(3,4,5,6), (4,3,5,6), (1,0,-1,0), (0,1,-1,0)$ up to scalar multiplies.*

Both of the above examples are special cases of the following theorem of Chabauty [8].

Theorem 5 *Let $\mathcal{C}$ be a curve of genus g defined over a number field K, whose Jacobian has Mordell-Weil rank $\leqslant g - 1$. Then $\mathcal{C}$ has only finitely many K-rational points.*

Apparent from the above examples is the similarity between the strategy for finding all $(x,y) \in \mathcal{E}(K)$ with $x \in \mathbb{Q}$, where $\mathcal{E}$ is an elliptic curve, $[K:\mathbb{Q}] = 2$, and $\mathcal{E}(K)$ has rank 1 (sometimes called "Elliptic Curve Chabauty"), and that for finding $\mathcal{C}(\mathbb{Q})$, where $\mathcal{C}$ is a curve of genus 2 and $\mathcal{J}(\mathbb{Q})$ has rank 1. In each case, $\mathcal{E}(K)$ or $\mathcal{J}(\mathbb{Q})$, the group law is locally described by a 2-parameter system over $\mathbb{Q}$, and an arithmetic condition, $x \in \mathbb{Q}$ or $X_1 = X_2$, gives a power series in one variable n_1. In general the local methods for finding all $(x,y) \in \mathcal{E}(K)$ with $x \in \mathbb{Q}$, where $\mathcal{E}$ is an elliptic curve, $[K:\mathbb{Q}] = g$, and $\mathcal{E}(K)$ has rank less than g, will be similar to those for finding $\mathcal{C}(\mathbb{Q})$, where $\mathcal{C}$ is a curve of genus g and $\mathcal{J}(\mathbb{Q})$ has rank less than g. Sometimes one can even choose between either of these to solve the same problem. The work done in Example 1 turns out to be equivalent to showing $\mathcal{F}_1(\mathbb{Q}) = \{\infty, (0,\pm 1)\}$ and $\mathcal{F}_2(\mathbb{Q}) = \{\infty\}$, where

$$\begin{aligned} \mathcal{F}_1 &: t^2 = (s^4 - 2s^2 - 8s + 1)(s^3 + s + 1), \\ \mathcal{F}_2 &: \underline{t}^2 = (\underline{s}^4 - 8\underline{s} - 4)(\underline{s}^3 + \underline{s}^2 + 1), \end{aligned} \tag{34}$$

both of genus 3. The derivation of $\mathcal{F}_1, \mathcal{F}_2$ will be made clear in the next section.

We conclude this section with the result in [2], which also makes use of Chabauty's Theorem.

Theorem 6 *The only $x, y, z \in \mathbb{Z}$ with $(x, y, z) = 1$, satisfying $x^2 + y^8 = z^3$ are $(\pm 1, 0, 1), (0, \pm 1, 1)$ and $(\pm 1549034, \pm 33, 15613)$.*

The proof uses a parametrisation of $x^2 + v^4 = z^3$ to obtain a covering of the solutions by the $\mathbb{Q}$-rational points on five curves of genus 2. Two of these can be resolved by maps to elliptic curves. The remaining three all have $\mathcal{J}(\mathbb{Q})$ of rank 1, and an argument similar to that used in the above examples can be used to find the rational points on each of them.

We should also mention that it is also possible to use differentials instead of the formal group as way of applying Chabauty's Theorem. This approach is described, for example, in [28]. For other work on Chabauty's Theorem, see also [9], [12], [18].

4 Coverings of Bielliptic Curves

We shall suppose, in this section, that our curve of genus 2 is defined over $\mathbb{Q}$ and has a $\mathbb{Q}$-rational point, which has been mapped to infinity. Suppose also that there are only quadratic terms in X.

$$\mathcal{C} : Y^2 = G(X^2), \text{ where } G(x) = (x - e_1)(x - e_2)(x - e_3). \tag{35}$$

The map $X \mapsto -X$ swaps roots of the sextic of (35) in pairs, and the function $x = X^2$ is invariant under this map. There are then maps $(X, Y) \mapsto (X^2, Y)$ and $(X, Y) \mapsto (1/X^2, Y/X^3)$ from $\mathcal{C}$ to the elliptic curves

$$\begin{array}{l} \mathcal{E}^a : Y^2 = G(x) = (x - e_1)(x - e_2)(x - e_3), \\ \mathcal{E}^b : \underline{Y}^2 = \underline{x}^3 G(1/\underline{x}) = (-e_1\underline{x} + 1)(-e_1\underline{x} + 1)(-e_3\underline{x} + 1), \end{array} \tag{36}$$

respectively. As in [28], these induce isogenies $\phi_1 : A_1 \to J$ and $\phi_1' : J \to A_1$, where $A_1 = \mathcal{E}^a \times \mathcal{E}^b$.

$$\begin{array}{l} \phi_1 : [(x, Y), (\underline{x}, \underline{Y})] \mapsto \{(\sqrt{x}, Y), (-\sqrt{x}, Y)\} + \{(\frac{1}{\sqrt{\underline{x}}}, \frac{\underline{Y}}{\underline{x}\sqrt{\underline{x}}}), (-\frac{1}{\sqrt{\underline{x}}}, -\frac{\underline{Y}}{\underline{x}\sqrt{\underline{x}}})\}, \\ \phi_1' : \{(X_1, Y_1), (X_2, Y_2)\} \mapsto [(X_1^2, Y_1) + (X_2^2, Y_2), (\frac{1}{X_1^2}, \frac{Y_1}{X_1^3}) + (\frac{1}{X_2^2}, \frac{Y_2}{X_2^3})]. \end{array} \tag{37}$$

Both of ϕ_1, ϕ_1' have kernels of order 4, and $\phi_1' \circ \phi_1$, $\phi_1 \circ \phi_1'$ both give multiplication by 2 maps. There is furthermore an injective homomorphism (a special case of [20]):

$$\begin{array}{l} \mu_1 : J(\mathbb{Q})/\phi_1\big(A_1(\mathbb{Q})\big) \longrightarrow L_1^*/(L_1^*)^2 \times L_2^*/(L_2^*)^2 \times L_3^*/(L_3^*)^2 \\ \quad : D \mapsto [\mu_1^{(1)}(D), \mu_1^{(2)}(D), \mu_1^{(3)}(D)], \\ \quad \text{where } \mu_1^{(j)} : \{(X_1, Y_1), (X_2, Y_2)\} \mapsto (X_1^2 - e_j)(X_2^2 - e_j), \text{ for } j = 1, 2, 3, \end{array} \tag{38}$$

and where $L_i = \mathbb{Q}(e_i)$ for $i = 1, 2, 3$. This map is analogous to the map $(x, y) \mapsto x$ used to perform descent via 2-isogeny on an elliptic curve $y^2 = x(x^2 + ax + b)$ (see p.302 of [24]).

Suppose that, after performing a descent, we have determined the set

$$J(\mathbb{Q})/\phi_1\big(A_1(\mathbb{Q})\big) = \{D_1, \ldots, D_m\}. \tag{39}$$

Let $(X,Y) \in \mathcal{C}(\mathbb{Q})$. Then $\{(X,Y),\infty^+\} = D_i$ in $J(\mathbb{Q})/\phi_1\big(A_1(\mathbb{Q})\big)$, for some $1 \le i \le m$, and so $\mu_1^{(j)}(\{(X,Y),\infty^+\} = \mu^{(j)}(D_i)$ for $j = 1,2,3$, which is the same as $(X^2 - e_j) = \mu^{(j)}(D_i)$ in $L_j^*/(L_j^*)^2$ for $j = 1,2,3$. Since also $G(X^2)$ is a square by (35), we have

$$Y_{i,j}^2 = \mu^{(j)}(D_i)G(X^2)/(X^2 - e_j), \tag{40}$$

which is a curve of genus 1 defined over L_j (note that the right hand side is a quartic polynomial in X, after cancelling $X^2 - e_j$). Multiplying both sides by X^2, we see that the variables $y_{i,j} = XY_{i,j}$ and $x = X^2$ satisfy

$$y_{i,j}^2 = \mu^{(j)}(D_i)xG(x)/(x - e_j), \tag{41}$$

an elliptic curve isogenous to the Jacobian of (40). We now have a strategy for trying to find the $\mathbb{Q}$-rational points on the curve $\mathcal{C}$ in (35), even when $\mathcal{J}(\mathbb{Q})$ has rank at least 2. Namely, for each i, one tries to find all $(x, y_{i,j})$ on (41) using the techniques at the beginning of Section 3. The following was proved first in [28] and then [15]. The proof we sketch here is a blend of those two proofs.

Theorem 7 *Let $\mathcal{C}_3 : Y^2 = X^6 + X^2 + 1$, the Diophantus curve of (5) and Example 5. Then $\mathcal{C}_3(\mathbb{Q}) = \{\infty^{\pm}, (0,\pm 1), (\pm 1/2, \pm 9/8)\}$.*

Proof We take $e_1 = \alpha$ where $\alpha^3 + \alpha + 1 = 0$, and note that $G(x) = x^3 + x + 1 = (x - \alpha)(x^2 + \alpha x + (\alpha^2 + 1))$. From Example 5 we know that $\mathcal{J}_3(\mathbb{Q})$ has rank 2 and is generated by $\{(0,1),(0,1)\}$ and $\{(0,1),\infty^+\}$. We first note that $\{(0,1),(0,1)\}$ is trivial in $J_3(\mathbb{Q})/\phi_1\big(A_1(\mathbb{Q})\big)$, as can be seen either by applying (37) to get $\{(0,1),(0,1)\} = \phi_1([(0,1),\infty])$, or by applying (38) to get $\mu_1(\{(0,1),(0,1)\}) = [1,1,1]$. Applying (38) also gives that $\{(0,1),\infty^+\} \ne \mathcal{O}$ in $J_3(\mathbb{Q})/\phi_1\big(A_1(\mathbb{Q})\big)$. We conclude that $J_3(\mathbb{Q})/\phi_1\big(A_1(\mathbb{Q})\big)$ has exactly two members: $D_1 = \mathcal{O}$ and $D_2 = \{(0,1),\infty^+\}$.

Let $(X,Y) \in \mathcal{C}_3(\mathbb{Q})$. Then $\{(X,Y),\infty^+\} = D_1$ or D_2 in $J_3(\mathbb{Q})/\phi_1\big(A_1(\mathbb{Q})\big)$. Applying (41) gives that $x = X^2 \in \mathbb{Q}$ satisfies one of the equations

$$\begin{aligned} y_{1,1}^2 &= x(x^2 + \alpha x + (\alpha^2 + 1)), \\ y_{2,1}^2 &= -\alpha x(x^2 + \alpha x + (\alpha^2 + 1)). \end{aligned} \tag{42}$$

We know from Example 7 that the only possible $x \in \mathbb{Q}$ are $x = \infty, 0, 1/4$, and so any $(X,Y) \in \mathcal{C}_3(\mathbb{Q})$ must satisfy $X = \infty, 0, \pm 1/2$, as required. □

As an alternative, note that if $\{(X,Y),\infty^+\} = D_1 = \mathcal{O}$ in $J_3(\mathbb{Q})/\phi_1\big(A_1(\mathbb{Q})\big)$ then $\{(X,Y),\infty^+\} = \phi_1([R_a,R_b])$ for some $R_a \in \mathcal{E}^a(\mathbb{Q})$, $R_b \in \mathcal{E}^b(\mathbb{Q})$. Taking ϕ_1' of both sides gives $[(X^2,Y) + \infty, (1/X^2, Y/X^3) + (0,1)] = [2R_a, 2R_b]$. Let s be the x-coordinate of R_a, and let $[2]_a$ denote the x-coordinate duplication map on $\mathcal{E}^a$. Then

$$X^2 = [2]_a(s) = (s^4 - 2s^2 - 8s + 1)/4(s^3 + s + 1). \tag{43}$$

Letting $t = 2(s^3 + s + 1)X$ gives the model $\mathcal{F}_1$ in (34).

Similarly, if $\{(X,Y),\infty^+\} = D_2 = \{(0,1),\infty^+\}$ in $J_3(\mathbb{Q})/\phi_1\big(A_1(\mathbb{Q})\big)$ then $\{(X,Y),\infty^+\} - D_2 = \{(X,Y),(0,-1)\} = \mathcal{O}$ in $J_3(\mathbb{Q})/\phi_1\big(A_1(\mathbb{Q})\big)$, so that $\{(X,Y),(0,-1)\} = \phi_1([S_a,S_b])$ for some $S_a \in \mathcal{E}^a(\mathbb{Q})$, $S_b \in \mathcal{E}^b(\mathbb{Q})$. Taking ϕ_1' of both sides gives $[(X^2,Y)+(0,-1),(1/X^2,Y/X^3)+\infty] = [2S_a,2S_b]$. Let $\underline{s}$ be the x-coordinate of S_b, and let $[2]_b$ denote the x-coordinate duplication map on $\mathcal{E}^b$. Then

$$1/X^2 = [2]_b(\underline{s}) = (\underline{s}^4 - 8\underline{s} - 4)/4(\underline{s}^3 + \underline{s}^2 + 1). \tag{44}$$

Letting $\underline{t} = 2(\underline{s}^3 + \underline{s}^2 + 1)/X$ gives the model F_2 in (34). One can either, as we have done above, find all points the curves (42) with $\mathbb{Q}$-rational x-coordinate; or, as in [28], one can find all members of $F_1(\mathbb{Q}), F_2(\mathbb{Q})$.

The underlying geometry is described in [28]. Each D_i corresponds to an embedding of $\mathcal{C}$ into its Jacobian, given by $P \mapsto \{P,\infty^+\} - D_i$. If the D_i give a complete set of representatives for $J(\mathbb{Q})/\phi_1\big(A_1(\mathbb{Q})\big)$, then every member of $\mathcal{C}(\mathbb{Q})$ will be 'hit' by $\phi_1(A(\mathbb{Q}))$ via one of these embeddings. It is therefore sufficient to find each $\mathcal{D}_i(\mathbb{Q})$, where $\mathcal{D}_i$ is the pullback of the embedded curve. Each $\mathcal{D}_i$ is a curve of genus 5 lying on A. and it has a hyperelliptic genus 3 quotient $\mathcal{F}_i$. In our example, these are the $\mathcal{F}_1, \mathcal{F}_2$ of (34). Furthermore, the Jacobians of $\mathcal{F}_1, \mathcal{F}_2$ are isogenous to the Weil restriction of scalars from $\mathbb{Q}(\alpha)$ to $\mathbb{Q}$ of the curves in (42).

If we try solve $\mathcal{C}_4 : Y^2 = (X^2+15)(X^2+45)(X^2+135)$ of (6) by the same technique, a problem arises. Here, $e_1 = -15, e_2 = -45, e_3 = -135$, and every elliptic curve given by (41) is defined over $\mathbb{Q}$. This means that, if the method is to work, for every i at least one curve (41) for $j = 1, 2$ or 3 has to have rank 0. Applying (38) to the generators of $\mathcal{J}_4(\mathbb{Q})$ given in Example 6, we find that the torsion group and $\{\infty^+,\infty^+\}$ are all trivial in $J_4(\mathbb{Q})/\phi_1\big(A_1(\mathbb{Q})\big)$. Hence $J_4(\mathbb{Q})/\phi_1\big(A_1(\mathbb{Q})\big)$ just consists of the two elements $\mathcal{O}$ and $\{(3,432),\infty^+\}$. Let $(X,Y) \in \mathcal{C}_4(\mathbb{Q})$. Then $\{(X,Y),\infty^+\}$ is equal to either $D_1 = \mathcal{O}$ or $D_2 = \{(3,432),\infty^+\}$ in $J_4(\mathbb{Q})/\phi_1\big(A_1(\mathbb{Q})\big)$. Consider first the case $\{(X,Y),\infty^+\} = D_1 = \mathcal{O}$ in $J_4(\mathbb{Q})/\phi_1\big(A_1(\mathbb{Q})\big)$. Then, using (41), we know that $x = X^2$ satisfies $y_{1,1}^2 = x(x+45)(x+135)$, for some $y_{1,1} \in \mathbb{Q}$. This is an elliptic curve of rank 0 over $\mathbb{Q}$, which has only the 2-torsion points with $x = \infty, 0, -45, -135$. None of $0, -45, -135$ are rational squares and so they do not correspond to points $(X,Y) \in \mathcal{C}(\mathbb{Q})$.

The case $\{(X,Y),\infty^+\} = D_2 = \{(3,432),\infty^+\}$ is more troublesome. Using (41), we know that $x = X^2$ satisfies $y_{2,1}^2 = 24x(x+45)(x+135), y_{2,2}^2 = 54x(x+15)(x+135)$ and $y_{2,3}^2 = 144x(x+15)(x+45)$, for some $y_{2,1}, y_{2,2}, y_{2,3} \in \mathbb{Q}$. These are elliptic curves of ranks 2,1,1, respectively, over $\mathbb{Q}$, and so they do not restrict x to a finite number of choices. At this point, we have not determined $\mathcal{C}_4(\mathbb{Q})$, but we have shown

$$(X,Y) \in \mathcal{C}_4(\mathbb{Q}) \Rightarrow \{(X,Y),\infty^+\} = \{(3,432),\infty^+\} \text{ in } J_4(\mathbb{Q})/\phi_1\big(A_1(\mathbb{Q})\big). \tag{45}$$

For the curve $\mathcal{C}_4$, the map $X \mapsto -X$ is not the only way of permuting the roots of the sextic. The curve is a special case of

$$Y^2 = (X^2 - k)(X^2 - rk)(X^2 - r^2k),\ r, k \in \mathbb{Q}, \tag{46}$$

which has the involution $(X, Y) \mapsto (-rk/X,\ rk\sqrt{-rk}\ Y/X^3)$. The functions $U = (X+\sqrt{-rk})/(-X+\sqrt{-rk})$ and $V = (8\sqrt{-rk}\ Y)/(X-\sqrt{-rk})^3$ are invariant, and $(X, Y) \mapsto (U^2, V)$, $(X, Y) \mapsto (1/U^2, V/U^3)$ are maps from (46) to the quotient

$$v^2 = -2k\big(u + 1\big)\big((r + 1)^2u^2 - 2(r^2 - 6r + 1)u + (r + 1)^2\big), \tag{47}$$

defined over $\mathbb{Q}$. Viewing (47) as being defined over $\mathbb{Q}(\sqrt{-rk})$, let A_2 be its Weil-restriction over $\mathbb{Q}$. The maps $(X, Y) \mapsto (U^2, V)$, $(X, Y) \mapsto (1/U^2, V/U^3)$ induce isogenies $\phi_2 : A_2 \to J$ and $\phi_2' : J \to A_2$, analogous to ϕ_1 of (37), where here J is the Jacobian of (46). There is also an injective homomorphism

$$\begin{aligned}
\mu_2 &: J(\mathbb{Q})/\phi_2\big(A_2(\mathbb{Q})\big) \longrightarrow \mathbb{Q}^*/(\mathbb{Q}^*)^2 \times K^*/(K^*)^2, : D \mapsto [\mu_2^{(1)}(D), \mu_2^{(2)}(D)],\\
\mu_2^{(1)} &: \{(X_1, Y_1), (X_2, Y_2)\} \mapsto (X_1^2 - rk)(X_2^2 - rk),\\
\mu_2^{(2)} &: \{(X_1, Y_1), (X_2, Y_2)\} \mapsto (X_1 - \sqrt{k})(X_1 + r\sqrt{k})(X_2 - \sqrt{k})(X_2 + r\sqrt{k}),
\end{aligned} \tag{48}$$

where $K = \mathbb{Q}(\sqrt{k})$. Suppose that, after performing a descent, we have determined the set

$$J(\mathbb{Q})/\phi_2\big(A_2(\mathbb{Q})\big) = \{D_1', \ldots, D_n'\}. \tag{49}$$

Let $(X, Y) \in \mathbb{Q}$. Then $\{(X, Y), \infty^+\} = D_i$ in $J(\mathbb{Q})/\phi_1\big(A_1(\mathbb{Q})\big)$, for some $1 \le i \le n$, and so $\mu_2^{(j)}(\{(X, Y), \infty^+\} = \mu^{(j)}(D_i')$ for $j = 1, 2$. By a similar argument to that used for (41), we can show (see [16] for details) that $u = 2X/(X^2 - rk)$ satisfies

$$y_i^2 = \mu_2^{(1)}(D_i')\mu_2^{(2)}(D_i')(rku^2 + 1)((r - 1)\sqrt{k}\ u/2 + 1), \tag{50}$$

for some $y_i \in K$. If this is an elliptic curve of rank 1, then we can try to apply the Elliptic Curve Chabauty techniques described at the beginning of Section 3. For our curve $\mathcal{C}_4$ of (6), a special case of (46) with $r = 3, k = -15$, we apply (38) to the generators of $\mathcal{J}_4(\mathbb{Q})$ given in Example 6, and find that $\{\infty^+, \infty^+\}$ is trivial in $J_4(\mathbb{Q})/\phi_2\big(A_2(\mathbb{Q})\big)$. Hence $J_4(\mathbb{Q})/\phi_2\big(A_2(\mathbb{Q})\big)$ just consists of the eight elements generated by the 2-torsion and $\{(3, 432), \infty^+\}$, that is: $D_1' = \mathcal{O}, D_2' = \{(\beta, 0), (-\beta, 0)\}, D_3' = \{(\sqrt{-45}, 0), (-\sqrt{-45}, 0)\}, D_4' = \{(3\beta, 0), (-3\beta, 0)\}, D_5' = \{(3, 432), \infty^+\}, D_6' = D_5'+D_2', D_7' = D_5'+D_3', D_8' = D_5'+D_4'$. Let $(X, Y) \in \mathcal{C}_4(\mathbb{Q})$. Then $\{(X, Y), \infty^+\} = D_i'$ in $J_4(\mathbb{Q})/\phi_2\big(A_2(\mathbb{Q})\big)$ for some $1 \le i \le 8$. Now, for $i = 1, \ldots, 4$, $D_i' = \mathcal{O}$ in $J_4(\mathbb{Q})/\phi_1\big(A_1(\mathbb{Q})\big)$, which has already been discounted by (45). For $i = 6, 7$, one can use a straightforward 5-adic argument (see [16]) to show the nonexistence of $u \in \mathbb{Q}_5$, $y_i \in \mathbb{Q}_5(\beta)$, and hence the nonexistence of $u \in \mathbb{Q}, y_i \in \mathbb{Q}(\beta)$, satisfying (50).

In summary, if $(X, Y) \in \mathcal{C}_4(Q)$, where $\mathcal{C}_4$ is as in (6), then $\{(X, Y), \infty^+\} = D_i'$ in $J_4(\mathbb{Q})/\phi_2\big(A_2(\mathbb{Q})\big)$ for $i = 5$ or $i = 8$. Therefore $u = 2X/(X^2-rk) = 2X/(X^2+45) \in \mathbb{Q}$ satisfies (50) for $i = 5$ or $i = 8$ (with $r = 3, k = -15$); that is, it satisfies

one of the two equations

$$\begin{array}{l} y_5^2 = 6(54+6\beta)(-45u^2+1)(\beta u+1), \\ y_8^2 = 6(9+\beta)(-45u^2+1)(\beta u+1), \end{array} \tag{51}$$

for some y_5 or y_8 in $K = \mathbb{Q}(\beta) = \mathbb{Q}(\sqrt{-15})$. We have already seen, in Example 8, that the only $u \in \mathbb{Q}$ on either curve are $u = \infty, \pm 1/3, \pm 1/9$. For $u = \infty, \pm 1/3$, there are no $X \in \mathbb{Q}$ satisfying $u = 2X/(X^2+45)$. For $u = \pm 1/9$, there are $X = \pm 3, \pm 15$; however, substituting $X = \pm 15$ into $(X^2+15)(X^2+45)(X^2+135)$ gives 23328000, which is nonsquare, and so there is no $(X,Y) \in \mathcal{C}(\mathbb{Q})$ with $X = \pm 15$. This leaves $X = \pm 3$ as the only possible X-coordinates of an affine $(X,Y) \in \mathcal{C}(\mathbb{Q})$. This proves that $\mathcal{C}(\mathbb{Q}) = \{\infty^{\pm}, (\pm 3, 432)\}$. In view of Lemma 3 this proves Conjecture 2, as in [16].

Theorem 8 *No polynomial of type $p_{3,1,1}$ is $\mathbb{Q}$-derived.*

A feature of the above proof is that covers via both ϕ_1 and ϕ_2 were required; neither the ϕ_1 nor the ϕ_2 information on its own is sufficient to determine $\mathcal{C}_4(\mathbb{Q})$.

5 Coverings of a General Curve of Genus 2

The next two sections use ideas of Nils Bruin, as in [2],[3], and variations by Flynn and Wetherell, as in [15],[17]. Let $\mathcal{C} : Y^2 = F(X) = F_1(X) \dots F_k(X)$ be a curve of genus 2, as in (1). We shall not assume that $\mathcal{C}$ is of any of the special types in the last section, although we shall continue to assume that $\mathcal{C}$ has a $\mathbb{Q}$-rational point that has been mapped to infinity. Let μ be the map on $\mathcal{J}(K)$ defined in (10), and suppose, as usual, that we have found $J(K)/2J(K)$. It is then straightforward to deduce $J(K)/\ker(\mu)$, which we list as

$$J(K)/\ker(\mu) = \{D_1, \dots, D_n\}. \tag{52}$$

Let $P = (X,Y) \in \mathcal{C}(K)$ so that $\{P, \infty^+\} \in J(K)$. Then, for some $i \in \{1, \dots, n\}$, we must have $\mu(\{(X,Y), \infty^+\}) = \mu(D_i)$. Let $G(X)$ be any polynomial of even degree such that $G(x)|F(x)$. Then there is an induced map

$$\mu_{_G} : J(K) \to L_{_G}^*/(L_{_G}^*)^2 : [\sum_{j=1}^{\ell} n_j(x_j, y_j)] \mapsto \prod_{j=1}^{\ell} G(x_j)^{n_j}, \tag{53}$$

where $L_{_G}$ denotes the smallest field containing K over which $G(x)$ is defined. Is follows that

$$q_{_G}(D_i)G(x) \in (L_{_G}^*)^2 \text{ for all } G(x)|F(x) \text{ with } 2|\deg(G(x)). \tag{54}$$

Each choice of G therefore gives a hyperelliptic curve $v_{i,G}^2 = q_{_G}(D_i)G(x)$, defined over $L_{_G}$, on which there must be an $L_{_G}$-rational point with K-rational x-coordinate. When $G(x)$ has degree 4, it may be that this is an elliptic curve whose rank over $L_{_G}$ is less that $[L_{_G} : K]$. In such cases, the Elliptic Curve

Chabauty techniques at the beginning of Section 3 can be applied. This idea has recently been applied in [17] to $\mathcal{D} : x^4 + y^4 = 17$, the "Serre curve", as in (7). This is a curve of genus 3 whose Jacobian has rank 6. It is shown on pp.187–189 of [7] that the rearrangement

$$\big(17 + (5x^2 - 4xy + 5y^2)\big)\big(17 - (5x^2 - 4xy + 5y^2)\big) = -2(2x^2 - 5xy + 2y^2)^2 \quad (55)$$

can be used, together with a resultant argument, to show that it is sufficient to find all $\mathbb{Q}$-rational points on the curve of genus 2

$$\mathcal{C}_5 : Y^2 = (9X^2 - 28X + 18)(X^2 + 12X + 2)(X^2 - 2). \quad (56)$$

Specifically, if $\mathcal{C}_5(\mathbb{Q})$ has no affine points, then $\mathcal{D}(\mathbb{Q})$ has only the affine points $(\pm 1, \pm 2), (\pm 2, \pm 1)$. Equations (7) and (56) have stubbornly resisted the techniques described in the last two sections, as well as the method of Dem'yanenko (see [21], p.67). However, [17] finally showed, using the ideas sketched above, that it is sufficient to find all points on an elliptic curve over $\mathbb{Q}(\sqrt{2}, \sqrt{17})$ with $\mathbb{Q}$-rational x-coordinate. This elliptic curve, which we do not reproduce here (see [17]) has rank 1 over $\mathbb{Q}(\sqrt{2}, \sqrt{17})$; the Elliptic Curve Chabauty techniques at the beginning of Section 3 can be applied to show that indeed $\mathcal{C}_5(\mathbb{Q})$ has no affine points, from which $\mathcal{D}(\mathbb{Q})$ can be deduced, as in [17].

Theorem 9 *The only $x, y \in \mathbb{Q}$ satisfying $x^4 + y^4 = 17$ are $(\pm 1, \pm 2), (\pm 2, \pm 1)$.*

The technique to obtain the genus 2 cover (56) generalises to other Fermat quartics $x^4 + y^4 = c$, and so the methods of [17] are potentially applicable to other nontrivial values of c; that is, to the cases where $x^4 + y^4 = c$ cannot be trivially solved by a direct local argument or a map to a rank 0 elliptic curve. There are only four such cases with $c \leq 300$, namely: $c = 17, 82, 97, 257$.

6 A Classical Approach via Resultants

Given a curve such as

$$\mathcal{C}_6 : Y^2 = (X^2 + 1)(X^4 + 1), \quad (57)$$

one could, if desired, apply the techniques described above. Here, $\mathcal{J}_6(\mathbb{Q})$ has rank 2, and one can find $\mathcal{J}_6(\mathbb{Q})/2\mathcal{J}_6(\mathbb{Q})$, followed by a set of coverings curves as described in the last two sections. However, it is worth bearing in mind that more than enough techniques were available to deal with such a curve long before recent methods for finding $\mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q})$. Letting $X = a/b$, where $a, b \in \mathbb{Z}$ and $\gcd(a, b) = 1$, and multiplying through by b^6, we have that fg is an integer square, where $f = a^2 + b^2$ and $g = a^4 + b^4$. Now, if $d = \gcd(f, g)$ then d divides $g - (a^2 - b^2)f = 2b^4$ and $g + (a^2 - b^2)f = 2a^4$. Since $\gcd(a, b) = 1$, this means that $d|2$ and so $d = \pm 1, \pm 2$. Combining this with the fact that fg is an integer square gives that, for some choice of $d = \pm 1, \pm 2$, both of df and dg are integer squares. Dividing dg through by b^4 we have, in particular that $d(X^4 + 1)$ is a $\mathbb{Q}$-rational

square, for some choice of $d = \pm 1, \pm 2$. The negative values of d give no such $X \in \mathbb{R}$ and so no $X \in \mathbb{Q}$. This means that $(X, Y) \in \mathcal{C}_6(\mathbb{Q})$ satisfies $Y_1^2 = X^4 + 1$ for some $Y_1 \in \mathbb{Q}$ or $Y_2^2 = 2(X^4+1)$ for some $Y_2 \in \mathbb{Q}$. Both of these are rank 0 elliptic curves over $\mathbb{Q}$, the first having only the points $\infty^{\pm}, (0, \pm 1)$ and the second having only the points $(\pm 1, \pm 2)$, defined over $\mathbb{Q}$. We can therefore say that $\mathcal{C}_6(\mathbb{Q}) = \{\infty^{\pm}, (0, \pm 1), (\pm 1, \pm 2)\}$, without having done anything sophisticated.

In principle, this idea can be attempted even when $F(X)$ is written as a product of factors not defined over the ground field. When $F(X)$ is written as $F(X) = Q_1(X)Q_2(X)$, where $Q_1(X)$ is a quadratic and $Q_2(X)$ is a quartic, then resultant arguments (similar to those above) give a finite number of curves of genus 1 of the form: $y^2 = dQ_2(X)$, defined over an extension field, which need to be considered. One can then hope to apply Elliptic Curve Chabauty to each of these, and solve for $\mathcal{C}(\mathbb{Q})$ without ever having been required to compute $\mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q})$. In [3], this strategy is used to solve the following Diophantine problem.

Theorem 10 *The only $x, y, z \in \mathbb{Z}$ with $(x, y, z) = 1$ and $xyz \neq 0$, satisfying $x^8 + y^3 = z^2$ are $(x, y, z) = (\pm 1, 2, \pm 3), (\pm 43, 96222, \pm 3004207)$.*

In the proof of this result, ten associated curves of genus 2 are found, as in Theorem 6. Of these, there are three difficult cases which required the technique outlined in this section, together with the Elliptic Curve Chabauty technique at the beginning of Section 3. It would also be possible to solve these three cases using the strategy in Section 5. It is, to some extent, a matter of taste. The resultant method in [3] bypasses the need to find $\mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q})$. On the other hand, an initial computation of $\mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q})$ is often a straightforward and efficient way of removing many of the curves $y^2 = dQ_2(X)$ from consideration.

The author thanks Nils Bruin, Bjorn Poonen and Michael Stoll for their helpful comments on an earlier draft of this manuscript.

References

1. C. Batut, K. Belabas, D. Bernardi, H. Cohen, and M. Olivier. PARI-GP. Available from `ftp://megrez.math.u-bordeaux.fr/pub/pari`.
2. Nils Bruin. The Diophantine equations $x^2 \pm y^4 = \pm z^6$ and $x^2 + y^8 = z^3$. *Compositio Math.*, 118:305–321, 1999.
3. Nils Bruin. Chabauty methods using covers on curves of genus 2. Report MI 1999-15, Leiden. http://www.math.leidenuniv.nl/reports/1999-15.shtml
4. Nils Bruin. KASH-based program for performing 2-descent on elliptic curves over number fields. http://www.math.uu.nl/people/bruin/ell.shar
5. R.H. Buchholz and J.A. MacDougall. When Newton met Diophantus: A study of rational-derived polynomials and their extension to quadratic fields. To appear in J. Number Theory.
6. J.W.S. Cassels. *Local Fields.* LMS–ST 3. Cambridge University Press, Cambridge, 1986.
7. J.W.S. Cassels and E.V. Flynn. *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2.* LMS–LNS 230. Cambridge University Press, Cambridge, 1996.

8. Claude Chabauty. Sur les points rationnels des variétés algébriques dont l'irrégularité est supérieure à la dimension. *C. R. Acad. Sci. Paris*, 212:1022–1024, 1941.
9. R.F. Coleman. Effective Chabauty, *Duke Math. J.*, 52:765–780, 1985.
10. M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner, M. Schörnig, and K. Wildanger. KANT V4. *J. Symbolic Comput.*, 24(3-4):267–283, 1997. Available from `ftp://ftp.math.tu-berlin.de/pub/algebra/Kant/Kash`.
11. Z. Djabri, E.F. Schaefer, and N.P. Smart. Computing the p-Selmer group of an elliptic curve. Manuscript (1999). To appear in *Trans. Amer. Math. Soc.*
12. E.V. Flynn. A flexible method for applying chabauty's theorem. *Compositio Mathematica*, 105:79–94, 1997.
13. E.V. Flynn and N.P. Smart. Canonical heights on the Jacobians of curves of genus 2 and the infinite descent. *Acta Arith.*, 79:333–352, 1997.
14. E.V. Flynn, B. Poonen and E.F. Schaefer. Cycles of quadratic polynomials and rational points on a genus-two curve. *Duke Math. J.*, 90:435–463, 1997.
15. E.V. Flynn and J.L. Wetherell. Finding Rational Points on Bielliptic Genus 2 Curves. *Manuscripta Math.*, 100:519–533, 1999.
16. E.V. Flynn. On Q-Derived Polynomials. *Proc. Edinburgh Math. Soc.* 44:103–110, 2001.
17. E.V. Flynn and J.L. Wetherell. Covering Collections and a Challenge Problem of Serre. *Acta Arithmetica* XCVIII.2:197–205, 2001.
18. W. McCallum. On the method of Coleman and Chabauty. *Math. Ann.* 299(3): 565–596, 1994.
19. P. Morton. Arithmetic properties of periodic points of quadratic maps, II. *Acta Arith.* 87(2):89–102, 1998.
20. E.F. Schaefer. Computing a Selmer group of a Jacobian using functions on the curve. *Math. Ann.*, 310(3):447–471, 1998.
21. J.-P. Serre. *Lectures on the Mordell-Weil Theorem* Transl. and ed. by Martin Brown. From notes by Michel Waldschmidt. Wiesbaden; Braunschweig: Vieweg, 1989.
22. J. Sesiano. *Books IV to VII of Diophantus' Arithmetica in the Arabic Translation attributed to Qusta ibn Luqa.* Springer-Verlag, New York, 1982.
23. S. Siksek. Infinite descent on elliptic curves. *Rocky Mountain J. Math.*, 25(4):1501–1538, 1995.
24. J.H. Silverman. *The Arithmetic of Elliptic Curves.* GTM 106. Springer-Verlag, 1986.
25. M. Stoll. On the height constant for curves of genus two. *Acta Arith.* 90(2):183–201, 1999.
26. M. Stoll. Implementing 2-descent for Jacobians of hyperelliptic curves, preprint, 1999.
27. M. Stoll. On the height constant for curves of genus two, II. Manuscript (2000).
28. J.L. Wetherell. Bounding the Number of Rational Points on Certain Curves of High Rank. PhD Dissertation, University of California at Berkeley, 1997.
29. G.C. Young. On the Solution of a Pair of Simultaneous Diophantine Equations Connected with the Nuptial Numbers of Plato. *Proc. London Math. Soc.*, 23(2):27–44, 1924.