Finding Rational Points on Bielliptic Genus 2 Curves

E. Victor Flynn*, Mathematical Institute, University of Oxford

Joseph L. Wetherell†, Department of Mathematics, University of Southern California

Abstract

We discuss a technique for trying to find all rational points on curves of the form $Y^2 = f_3X^6 + f_2X^4 + f_1X^2 + f_0$, where the sextic has nonzero discriminant. This is a bielliptic curve of genus 2. When the rank of the Jacobian is 0 or 1, Chabauty's Theorem may be applied. However, we shall concentrate on the situation when the rank is at least 2. In this case, we shall derive an associated family of elliptic curves, defined over a number field $\mathbb{Q}(\alpha)$. If each of these elliptic curves has rank less than the degree of $\mathbb{Q}(\alpha) : \mathbb{Q}$, then we shall describe a Chabauty-like technique which may be applied to try to find all the points (x, y) defined over $\mathbb{Q}(\alpha)$ on the elliptic curves, for which $x \in \mathbb{Q}$. This in turn allows us to find all $\mathbb{Q}$-rational points on the original genus 2 curve. We apply this to give a solution to a problem of Diophantus (where the sextic in X is irreducible over $\mathbb{Q}$), which simplifies the recent solution of Wetherell. We also present two examples where the sextic in X is reducible over $\mathbb{Q}$.

§0. Introduction

In Problem 17 of book VI of the Arabic manuscript of *Arithmetica* [8], Diophantus poses a problem equivalent to finding a non-trivial rational point on the genus 2 curve

$$\mathcal{C} : Y^2 = X^6 + X^2 + 1. \tag{0.1}$$

The related problem of finding all rational points has recently been solved by Wetherell [11], who showed that $\mathcal{C}(\mathbb{Q}) = \{\infty^+, \infty^-, (0, \pm 1), (\pm 1/2, \pm 9/8)\}$, where by ∞^+, ∞^- we

* The author thanks the Nuffield Foundation (Grant SCI/180/96/71/G) for financial support.

† The author thanks the National Science Foundataion (Grant DMS-9705959) for financial support.

mean the points on the non-singular curve that lie over the point at infinity on $\mathcal{C}$. We note that $\mathcal{C}$ covers two elliptic curves:

$$\begin{aligned} \mathcal{E}^a &: Y^2 = x^3 + x + 1, \\ \mathcal{E}^b &: \underline{Y}^2 = \underline{x}^3 + \underline{x}^2 + 1, \end{aligned} \tag{0.2}$$

with the maps $(X, Y) \mapsto (X^2, Y)$ from $\mathcal{C}$ to $\mathcal{E}^a$ and $(X, Y) \mapsto (1/X^2, Y/X^3)$ from $\mathcal{C}$ to $\mathcal{E}^b$. Both $\mathcal{E}^a(\mathbb{Q})$ and $\mathcal{E}^b(\mathbb{Q})$ have rank 1, and $A = \mathcal{E}^a \times \mathcal{E}^b$ is isogenous to J, the Jacobian of $\mathcal{C}$, so that $J(\mathbb{Q})$ has rank 2. This means that the explicit Chabauty techniques described in [3,7] cannot be directly applied, since they rely on the rank of $J(\mathbb{Q})$ being strictly less than the genus of $\mathcal{C}$. Wetherell uses pullbacks of the isogeny $\phi : A \to J$ to find a pair of genus 5 curves D_1, D_2 whose rational points cover the rational points on $\mathcal{C}$. The hyperelliptic involution on $\mathcal{C}$ lifts to an involution on each of the genus 5 curves, yielding genus 3 quotients F_1, F_2, respectively:

$$\begin{aligned} F_1 &: t^2 = (s^4 - 2s^2 - 8s + 1)(s^3 + s + 1), \\ F_2 &: \underline{t}^2 = (\underline{s}^4 - 8\underline{s} - 4)(\underline{s}^3 + \underline{s}^2 + 1). \end{aligned} \tag{0.3}$$

Wetherell [11] shows that, in order to compute $\mathcal{C}(\mathbb{Q})$, it is sufficient to find $F_1(\mathbb{Q})$ and $F_2(\mathbb{Q})$. It turns out that the Jacobians of F_1 and F_2 have ranks 1 and 0, respectively. Since these are both less than the genus, one can apply the explicit genus 3 Chabauty techniques in [11] to F_1, F_2. These determine $F_1(\mathbb{Q})$ and $F_2(\mathbb{Q})$ completely which in turn allows all of $\mathcal{C}(\mathbb{Q})$ to be found.

The above analysis can be generalised to any bielliptic genus 2 curve. Once we have obtained standard equations for the appropriate genus 3 curves, the genus 3 Chabauty arguments are fairly straightforward; however, the determination of equations for the genus 3 curves can be tricky. Our aim here is to demonstrate an approach which replaces each genus 3 curve over $\mathbb{Q}$ with an explicitly given elliptic curve over some number field $\mathbb{Q}(\alpha)$. Since we are trading genus for field degree, this approach is simultaneously simpler and more complicated. Nevertheless, the ease of obtaining equations for the elliptic curves makes the elliptic curve approach preferable in most circumstances.

In Section 1, we give models for these elliptic curves $\mathcal{E}_i$, and show that, if one can find all points $(x, y) \in \mathcal{E}_i(\mathbb{Q}(\alpha))$ with $x \in \mathbb{Q}$, then one can find $\mathcal{C}(\mathbb{Q})$. In Section 2 we give explicit Chabauty-style equations (using the elliptic curve formal group) which can be used to try to find all such (x, y) when the rank of each $\mathcal{E}_i(\mathbb{Q}(\alpha))$ is less than the degree of $\mathbb{Q}(\alpha) : \mathbb{Q}$. In Section 3, we apply the technique to three worked examples. The first example is a simplified reproof of the above Diophantus example in [11], where $\mathbb{Q}(\alpha)$ is cubic; we include (although we do not require it) a simpler derivation of the curves (0.3) than the derivation in [11]. In the second example $\mathbb{Q}(\alpha)$ is quadratic; in the third example $\mathbb{Q}(\alpha) = \mathbb{Q}$.

§1. Associated Elliptic Curves over a Number Field

Suppose we have a curve of genus 2

$$\mathcal{C} : Y^2 = f_3 X^6 + f_2 X^4 + f_1 X^2 + f_0, \tag{1.1}$$

where $f_0, \ldots, f_3 \in \mathbb{Z}$, and where the sextic has nonzero discriminant; we wish to find $\mathcal{C}(\mathbb{Q})$. We first observe that $(X, Y) \mapsto (X^2, Y)$ gives a map from $\mathcal{C}$ to the elliptic curve

$$\mathcal{E}^a : Y^2 = F^a(x) = f_3 x^3 + f_2 x^2 + f_1 x + f_0. \tag{1.2}$$

Finding $\mathcal{C}(\mathbb{Q})$ is equivalent to finding all points

$$(x, Y) \in \mathcal{E}^a(\mathbb{Q}) \text{ where } x = X^2, \text{ for some } X \in \mathbb{Q}. \tag{1.3}$$

We shall formally, with slight abuse of notation, write $(x, Y) = \infty$, when (x, Y) is the point at infinity, which we take to be the identity in $\mathcal{E}^a(\mathbb{Q})$. When $(x, Y) = \infty$, we shall say that (1.3) is satisfied if $f_3 \in (\mathbb{Q}^*)^2$. Suppose now that (x, Y) is such a point, so that $(x, Y) \in \mathcal{E}^a(\mathbb{Q})$ and $(X, Y) \in \mathcal{C}(\mathbb{Q})$. Suppose also that we have found $\mathcal{E}^a(\mathbb{Q})/2\mathcal{E}^a(\mathbb{Q})$ by performing a 2-descent, and that

$$\{(x_1, Y_1), \ldots, (x_m, Y_m)\} \text{ is a set of representatives for } \mathcal{E}^a(\mathbb{Q})/2\mathcal{E}^a(\mathbb{Q}). \tag{1.4}$$

For the moment we assume, for simplicity, that $F^a(x)$ is irreducible over $\mathbb{Q}$. Let

$$\alpha = \text{ root of } F^a(x) \tag{1.5}$$

and q denote the standard homomorphism, with kernel $2\mathcal{E}^a(\mathbb{Q})$, given by

$$q : \mathcal{E}^a(\mathbb{Q}) \longrightarrow \mathbb{Q}(\alpha)^*/(\mathbb{Q}(\alpha)^*)^2 : (x, Y) \mapsto f_3(x - \alpha), \tag{1.6}$$

where we define $x - \alpha = f_3$ when $(x, Y) = \infty$, so that $q(\infty) = 1$. From (1.4) we know that there is a unique choice of i such that $(x, Y) = (x_i, Y_i)$ in $\mathcal{E}^a(\mathbb{Q})/2\mathcal{E}^a(\mathbb{Q})$, which is equivalent to $(x, Y) + (x_i, Y_i) \in 2\mathcal{E}^a(\mathbb{Q})$. Using the homomorphism (1.6), we must have

$$(x_i - \alpha)(x - \alpha) \in \mathbb{Q}(\alpha)^2, \text{ for some } i = 1, \ldots m. \tag{1.7}$$

We also have, by pure algebra, that

$$F^a(x) = (x - \alpha)\big(f_3x^2 + (f_2 + \alpha f_3)x + (f_1 + \alpha f_2 + \alpha^2 f_3)\big) = Y^2 \in \mathbb{Q}^2 \subset \mathbb{Q}(\alpha)^2. \tag{1.8}$$

It follows from (1.7), (1.8) and $x = X^2 \in \mathbb{Q}^2 \subset \mathbb{Q}(\alpha)^2$ that

$$(x_i - \alpha)x\big(f_3x^2 + (\alpha f_3 + f_2)x + (\alpha^2 f_3 + \alpha f_2 + f_1)\big) \in \mathbb{Q}(\alpha)^2. \tag{1.9}$$

We may summarise the above discussion in the following Lemma.

Lemma 1.1(a). *Let $\mathcal{C}$ be the genus 2 curve, and $\mathcal{E}^a$ be the elliptic curve*

$$\mathcal{C} : Y^2 = f_3X^6 + f_2X^4 + f_1X^2 + f_0 \text{ and } \mathcal{E}^a : Y^2 = F^a(x) = f_3x^3 + f_2x^2 + f_1x + f_0,$$

where $f_0, \ldots f_3 \in \mathbb{Z}$ and $F^a(x)$ is irreducible over $\mathbb{Q}$. Let $\{(x_1, Y_1), \ldots, (x_m, Y_m)\}$ be a set of representatives for $\mathcal{E}^a(\mathbb{Q})/2\mathcal{E}^a(\mathbb{Q})$, and let $\alpha =$ root of $F^a(x)$. Suppose $(X, Y) \in \mathcal{C}(\mathbb{Q})$, and let $x = X^2$. Then there is a unique choice of i $(1 \leqslant i \leqslant m)$ such that x satisfies

$$\mathcal{E}^a_i : y^2 = (x_i - \alpha)x\big(f_3x^2 + (\alpha f_3 + f_2)x + (\alpha^2 f_3 + \alpha f_2 + f_1)\big), \tag{1.10}$$

for some $y \in \mathbb{Q}(\alpha)$, where $(x_i - \alpha)$ should be taken to be f_3 when $(x_i, Y_i) = \infty$. □

Of course, we could just as easily have used

$$\mathcal{E}^b : \underline{Y}^2 = f_0\underline{x}^3 + f_1\underline{x}^2 + f_2\underline{x} + f_3 \tag{1.11}$$

in place of $\mathcal{E}^a$ in all of the above discussion, with the adjustment that the map from $\mathcal{C}$ to $\mathcal{E}^b$ is $(X, Y) \mapsto (1/X^2, Y/X^3)$. This gives the following alternative version of the Lemma.

Lemma 1.1(b). *Let $\mathcal{C}$ be the genus 2 curve, and $\mathcal{E}^b$ be the elliptic curve*

$$\mathcal{C} : Y^2 = f_3X^6 + f_2X^4 + f_1X^2 + f_0 \text{ and } \mathcal{E}^b : \underline{Y}^2 = F^b(\underline{x}) = f_0\underline{x}^3 + f_1\underline{x}^2 + f_2\underline{x} + f_3,$$

where $f_0, \dots f_3 \in \mathbb{Z}$ and $F^b(\underline{x})$ is irreducible over $\mathbb{Q}$. Let $\{(\underline{x}_1, \underline{Y}_1), \dots, (\underline{x}_n, \underline{Y}_n)\}$ be a set of representatives for $\mathcal{E}^b(\mathbb{Q})/2\mathcal{E}^b(\mathbb{Q})$, and let $\underline{\alpha} =$ root of $F^b(\underline{x})$. Suppose $(X, Y) \in \mathcal{C}(\mathbb{Q})$, and let $\underline{x} = 1/X^2$. Then there is a unique choice of j $(1 \leqslant j \leqslant n)$ such that $\underline{x}$ satisfies

$$\mathcal{E}^b_j : \underline{y}^2 = (\underline{x}_j - \underline{\alpha})\underline{x}\big(f_0\underline{x}^2 + (\underline{\alpha}f_0 + f_1)\underline{x} + (\underline{\alpha}^2 f_0 + \underline{\alpha}f_1 + f_2)\big), \tag{1.12}$$

for some $\underline{y} \in \mathbb{Q}(\alpha)$, where $(\underline{x}_j - \underline{\alpha})$ should be taken to be f_0 when $(\underline{x}_j, \underline{Y}_j) = \infty$. □

Whichever version is used, this gives a strategy for trying to find $\mathcal{C}(\mathbb{Q})$. For example, suppose we have computed a complete set of representatives for $\mathcal{E}^a(\mathbb{Q})/2\mathcal{E}^a(\mathbb{Q})$. Then for each $i = 1, \dots, m$, we try to find all $(x, y) \in \mathcal{E}^a_i(\mathbb{Q}(\alpha))$ with $x \in \mathbb{Q}$. For each such (x, y), we then check whether $x \in \mathbb{Q}^2$ and $F^a(x) \in \mathbb{Q}^2$. By Lemma 1.1, all members of $\mathcal{C}(\mathbb{Q})$ must arise this way. An analogous strategy is available if we can compute a complete set of representatives for $\mathcal{E}^b(\mathbb{Q})/2\mathcal{E}^b(\mathbb{Q})$. Note that m does not necessarily equal n, so one of these strategies may be more efficient than the other.

On the other hand, if we can compute a complete set of representatives for both $\mathcal{E}^a(\mathbb{Q})/2\mathcal{E}^a(\mathbb{Q})$ and $\mathcal{E}^b(\mathbb{Q})/2\mathcal{E}^b(\mathbb{Q})$, then we can combine the results to cut down on the number of cases we must consider. This is due to the following observation. Suppose we fix a point $(X, Y) \in \mathcal{C}(\mathbb{Q})$ and apply both Lemma 1.1(a) and Lemma 1.1(b). (To be definite, in Lemma 1.1(b) we choose $\underline{\alpha} = 1/\alpha$.) This gives us values for i and j such that

$$(x_i - \alpha)(x - \alpha) \in \mathbb{Q}(\alpha)^2 \text{ and } (\underline{x}_j - \underline{\alpha})(\underline{x} - \underline{\alpha}) = (\underline{x}_j - \underline{\alpha})(\alpha - x)/(\alpha x) \in \mathbb{Q}(\alpha)^2. \tag{1.13}$$

Combining these two statements with the fact that $x = X^2$ we find that

$$c^2_{i,j} = \frac{-\alpha(\underline{x}_j - \underline{\alpha})}{(x_i - \alpha)} = \frac{(1 - \alpha\underline{x}_j)}{(x_i - \alpha)} \tag{1.14}$$

for some $c_{i,j} \in \mathbb{Q}(\alpha)$. The convention for computing $x_i - \alpha$ or $\underline{x}_j - \underline{\alpha}$ when $(x_i, Y_i) = \infty$ or $(\underline{x}_j, \underline{Y}_j) = \infty$, is the same as that described in Lemma 1.1. Note that for each choice of i there is at most one value of j which satisfies (1.14) and for each j there is at most one i; therefore we can view $c_{i,j}$ as depending merely on one of i or j.

This cuts down on the number of cases we need to consider when searching for rational points, since we only need to consider those values of i for which some value of j makes (1.14) true. Moreover, when i and j are related by (1.14) then the map $(x, y) \mapsto (1/x, c_{i,j}y/x^2)$ gives an isomorphism between $\mathcal{E}_i^a$ and $\mathcal{E}_j^b$ which is defined over $\mathbb{Q}(\alpha)$, and which preserves the $\mathbb{Q}$-rationality of the x-coordinate. In other words, when we restrict to the i-j pairs which satisfy (1.14), the search for points in $\mathcal{C}(\mathbb{Q})$ using Lemma 1.1(a) is exactly the same as the search using Lemma 1.1(b).

We now drop our assumption that $F^a(x)$ is irreducible over $\mathbb{Q}$, in which case a straightforward imitation of the above arguments proves the following.

Lemma 1.2(a). *Let $\mathcal{C}$, $\mathcal{E}^a$, $F^a(x)$, $(x_1, Y_1), \ldots, (x_m, Y_m)$ be as in Lemma 1.1(a), except that $F^a(x) = f_3(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$ might or might not be irreducible over $\mathbb{Q}$. Suppose $(X, Y) \in \mathcal{C}(\mathbb{Q})$, and let $x = X^2$. Then there is a choice of i $(1 \leqslant i \leqslant m)$ such that x satisfies*

$$\mathcal{E}_{i,k}^a : y_k^2 = (x_i - \alpha_k)xF^a(x)/(x - \alpha_k), \quad k = 1, 2, 3, \tag{1.15}$$

for some $y_k \in \mathbb{Q}(\alpha_k)$, where $(x_i - \alpha_k)$ should be taken to be f_3 when $(x_i, Y_i) = \infty$, and $f_3 \prod_{r \neq k}(x_i - \alpha_r)$ when $x_i = \alpha_k$. □

Lemma 1.2(b). *Let $\mathcal{C}$, $\mathcal{E}^b$, $F^b(\underline{x})$, $(\underline{x}_1, \underline{Y}_1), \ldots, (\underline{x}_n, \underline{Y}_n)$ be as in Lemma 1.1(b), except that $F^b(\underline{x}) = f_0(\underline{x}-\underline{\alpha}_1)(\underline{x}-\underline{\alpha}_2)(\underline{x}-\underline{\alpha}_3)$ might or might not be irreducible over $\mathbb{Q}$. Suppose $(X, Y) \in \mathcal{C}(\mathbb{Q})$, and let $\underline{x} = 1/X^2$. Then there is a choice of j $(1 \leqslant j \leqslant n)$ such that $\underline{x}$ satisfies*

$$\mathcal{E}_{j,k}^b : \underline{y}_k^2 = (\underline{x}_j - \underline{\alpha}_k)\underline{x}F^b(\underline{x})/(\underline{x} - \underline{\alpha}_k), \quad k = 1, 2, 3, \tag{1.16}$$

for some $\underline{y}_k \in \mathbb{Q}(\underline{\alpha}_k)$, where $(\underline{x}_j - \underline{\alpha}_k)$ should be taken to be f_0 when $(\underline{x}_j, \underline{Y}_j) = \infty$, and $f_0 \prod_{r \neq k}(\underline{x}_j - \underline{\alpha}_r)$ when $\underline{x}_j = \underline{\alpha}_k$. □

If F^a (or equivalently F^b) is irreducible over $\mathbb{Q}$, then Lemma 1.1 is derivable as a special case of Lemma 1.2, since the three elliptic curves $\mathcal{E}_{i,k}^a$ (respectively, $\mathcal{E}_{j,k}^b$), $k = 1, 2, 3$, are just the conjugates of $\mathcal{E}_i^a$ (respectively, $\mathcal{E}_i^b$) over $\mathbb{Q}$. When exactly one root of F^a (or equivalently F^b) is defined over $\mathbb{Q}$ and the other two are quadratic and conjugate, then exactly one elliptic curve is defined over $\mathbb{Q}$ and the other two are conjugate. Similarly, if all three roots of F^a (or equivalently F^b) are defined over $\mathbb{Q}$, then so are the three elliptic curves $\mathcal{E}^a_{i,k}$ (or $\mathcal{E}^b_{j,k}$), $k = 1, 2, 3$. In summary, the collection of three elliptic curves $\mathcal{E}^a_{i,k}$, for any given i (or $\mathcal{E}^b_{j,k}$, for any given j), has the same Galois structure as the collection of roots α_k of F^a.

As with Lemma 1.1 we can combine the results of Lemma 1.2(a) and Lemma 1.2(b). For example, if we are applying Lemma 1.2(a), we find that we only need to consider those choices of i such that, for some j, and for all three values $k = 1, 2, 3$,

$$c^2_{i,j,k} = \frac{-\alpha_k(\underline{x}_j - \underline{\alpha}_k)}{(x_i - \alpha_k)} = \frac{(1 - \alpha_k \underline{x}_j)}{(x_i - \alpha_k)} \tag{1.17}$$

for some $c_{i,j,k} \in \mathbb{Q}(\alpha_k)$, where we have chosen the roots $\underline{\alpha}_k$ of $F^b(\underline{x})$ to satisfy $\underline{\alpha}_k = 1/\alpha_k$ for $k = 1, 2, 3$. The convention for computing $x_i - \alpha_k$ or $\underline{x}_j - \underline{\alpha}_k$ when $(x_i, Y_i) = \infty, (\alpha_k, 0)$ or $(\underline{x}_j, \underline{Y}_j) = \infty, (\underline{\alpha}_k, 0)$, is the same as that described in Lemma 1.2. Computing all of the $(1 - \alpha_k \underline{x}_j)/(x_i - \alpha_k)$, for $1 \leqslant i \leqslant m$, $1 \leqslant j \leqslant n$ and $1 \leqslant k \leqslant 3$, is a useful initial task before embarking on an application of Lemma 1.2, since it can be used to eliminate some of the elliptic curve rank computations. When i and j are related by (1.17) then, for a fixed k, the map $(x, y) \mapsto (1/x, c_{i,j,k}y/x^2)$ gives an isomorphism between $\mathcal{E}^a_{i,k}$ and $\mathcal{E}^b_{j,k}$ which is defined over $\mathbb{Q}(\alpha_k)$, and which preserves the $\mathbb{Q}$-rationality of the x-coordinate. Note that (1.14) is a special case of (1.17) in the same way that Lemma 1.1 is a special case of Lemma 1.2.

What is still required is a method for taking an elliptic curve $\mathcal{E} : y^2 = g_3x^3 + \ldots + g_0$, defined over a number field $\mathbb{Q}(\alpha)$, and finding all $(x, y) \in \mathcal{E}(\mathbb{Q}(\alpha))$ for which $x \in \mathbb{Q}$. If we can do this for each of the above $\mathcal{E}^a_i$ (or if, for each i, we can do this for at least one $\mathcal{E}^a_{i,k}$), then we can find all of $\mathcal{C}(\mathbb{Q})$, as required. In Section 2, we shall discuss this problem in the case when $\mathcal{E}(\mathbb{Q}(\alpha))$ has rank less than the degree of $\mathbb{Q}(\alpha) : \mathbb{Q}$.

§2. Elliptic Curve Chabauty

In this section, we consider an elliptic curve

$$\mathcal{E} : y^2 = g_3x^3 + g_2x^2 + g_1x + g_0, \tag{2.1}$$

defined over the number field $\mathbb{Q}(\alpha)$ of degree d over $\mathbb{Q}$, and discuss how to try to find all

$$(x, y) \in \mathcal{E}(\mathbb{Q}(\alpha)) \text{ with } x \in \mathbb{Q}. \tag{2.2}$$

For the purposes of problem (0.1), only the cases $d = 1, 2, 3$ are relevant; however, the strategy in this section does not depend on d, and so we shall not place any restriction on d except (later in the section) that d is greater than the rank of $\mathcal{E}(\mathbb{Q}(\alpha))$. Imitating Chapter IV of [10], we introduce the variables z, w, defined by

$$z = -x/y, w = -1/y. \text{ Reverse transformation: } x = z/w, y = -1/w. \tag{2.3}$$

Then ∞ on $\mathcal{E}$ corresponds to $z = w = 0$, and z, w satisfy

$$w = g_3z^3 + g_2z^2w + g_1zw^2 + g_0w^3. \tag{2.4}$$

On recursive substitution, this gives w as a power series in z

$$\begin{aligned} w = w(z) &= g_3\big(z^3 + g_2z^5 + (g_1g_3 + g_2^2)z^7 + (g_0g_3^2 + g_2^3 + 3g_1g_2g_3)z^9 + O(z^{11})\big) \\ &\in \mathbb{Z}[g_0, g_1, g_2, g_3][[z]]. \end{aligned} \tag{2.5}$$

Of course $x(z) = z/w(z)$ and $y(z) = -1/w(z)$ are Laurent Series, not power series, but $1/x = w(z)/z$ is a power series, obtained by dividing (2.5) through by z:

$$\begin{aligned} \frac{1}{x} = \frac{1}{x(z)} &= g_3\big(z^2 + g_2z^4 + (g_1g_3 + g_2^2)z^6 + (g_0g_3^2 + g_2^3 + 3g_1g_2g_3)z^8 + O(z^{10})\big) \\ &\in \mathbb{Z}[g_0, g_1, g_2, g_3][[z]]. \end{aligned} \tag{2.6}$$

Furthermore, if (x_0, y_0) is another point on $\mathcal{E}$, then adding $(x_0, y_0) + (x, y)$ results in a point whose x-coordinate is as follows:

$$\begin{aligned} x\text{-coord of } (x_0, y_0) + (x, y) &= (((y - y_0)/(x - x_0))^2 - g_2)/g_3 - x - x_0 \\ &= \frac{w(1 + y_0w)^2 - (g_2w + g_3z + g_3x_0w)(z - x_0w)^2}{g_3w(z - x_0w)^2} \end{aligned} \tag{2.7}$$

where, as usual, $(x,y) = (z/w, -1/w)$. On replacing w by $w(z)$ of (2.5) in this last fraction, note that the z^3 terms cancel in the numerator, and that there is a common factor of $g_3 z^5$ in the numerator and denominator. On cancelling $g_3 z^5$, the denominator is of the form $1 + O(z)$, and so the fraction is a power series

$$\begin{aligned} x\text{-coord of } (x_0,y_0)+(x,y) &= x_0 + 2y_0 z + (3g_3x_0^2 + 2g_2x_0 + g_1)z^2 + (4g_3x_0y_0 + 2g_2y_0)z^3 \\ &+ (4g_3^2x_0^3 + 6g_2g_3x_0^2 + 2g_1g_3x_0 + 2g_2^2x_0 + g_0g_3 + g_3y_0^2 + g_1g_2)z^4 + O(z^5) \\ &\in \mathbb{Z}[g_0,g_1,g_2,g_3,x_0,y_0][[z]]. \end{aligned} \tag{2.8}$$

If $(z_1, w(z_1)), (z_2, w(z_2))$ are two points in z-w coordinates then the z-coordinate of the sum can be written as a power series, the *formal group*: $\mathcal{F}(z_1,z_2) \in \mathbb{Z}[g_0,g_1,g_2,g_3][[z_1,z_2]]$. Chapter IV of [10] can be imitated for deriving the terms of $\mathcal{F}(z_1,z_2)$ up to any desired degree. Letting $G(z_1,z_2) = \partial/\partial z_1 \mathcal{F}(z_1,z_2)$ and $\log(t) = \int G(0,t)^{-1}\mathrm{d}t$ gives

$$\begin{aligned} \log(t) &= t + \frac{1}{3}g_2t^3 + \frac{1}{5}(g_2^2 + 2g_1g_3)t^5 + \frac{1}{7}(g_2^3 + 6g_1g_2g_3 + 3g_0g_3^2)t^7 + O(t^9) \\ &\in \mathbb{Q}[g_0,g_1,g_2,g_3][[t]], \end{aligned} \tag{2.9}$$

which satisfies $\log(\mathcal{F}(z_1,z_2)) = \log(z_1) + \log(z_2)$. We can then solve for the function $\exp(t)$ defined by $\exp(\log(t)) = t$, giving

$$\begin{aligned} \exp(t) &= t - \frac{1}{3}g_2t^3 + \frac{1}{15}(2g_2^2 - 6g_1g_3)t^5 - \frac{1}{315}(17g_2^3 - 66g_1g_2g_3 + 135g_0g_3^2)t^7 + O(t^9) \\ &\in \mathbb{Q}[g_0,g_1,g_2,g_3][[t]], \end{aligned} \tag{2.10}$$

which satisfies $\mathcal{F}(\exp(z_1), \exp(z_2)) = \exp(z_1 + z_2)$. The denominators of the coefficents in both $\log(t)$ and $\exp(t)$ are restricted by the fact that

$$k!\big(\text{coeff of } t^k \text{ in } \log(t) \text{ or } \exp(t)\big) \in \mathbb{Z}[g_0,g_1,g_2,g_3]. \tag{2.11}$$

Suppose that we have performed a descent on $\mathcal{E}(\mathbb{Q}(\alpha))$ and have found the torsion group, the rank r and a set of generators for $\mathcal{E}(\mathbb{Q}(\alpha))$; the general principles for this can be found in Chapter X of [10], and there are now several articles in the literature explaining how to find generators of elliptic curves over number fields, such as [1,5,6,9]. If $r = 0$, then $\mathcal{E}(\mathbb{Q}(\alpha)) = \mathcal{E}(\mathbb{Q}(\alpha))_{tors}$, the torsion group of $\mathcal{E}(\mathbb{Q}(\alpha))$, which is finite. In this case, it is trivial to solve the problem given in equation (2.2), since we merely need to check all $(x, y) \in \mathcal{E}(\mathbb{Q}(\alpha))_{tors}$, and see which ones satisfy $x \in \mathbb{Q}$.

Suppose that the rank r of $\mathcal{E}(\mathbb{Q}(\alpha))$ is less than d, the degree of $\mathbb{Q}(\alpha) : \mathbb{Q}$, and that we have found generators for $\mathcal{E}(\mathbb{Q}(\alpha))$:

$$\mathcal{E}(\mathbb{Q}(\alpha)) = \langle \mathcal{E}(\mathbb{Q}(\alpha))_{tors}, P_1, \ldots, P_r \rangle. \tag{2.12}$$

Now, choose an odd prime p such that α is p-integral, and let $\tilde{\alpha}$ denote the image of α in $\mathcal{O}/p\mathcal{O}$, where $\mathcal{O}$ is the ring of integers in $\mathbb{Q}(\alpha)$. We shall assume that p satisfies

$$\begin{gathered}(\mathbf{1})\ [\mathbb{Q}_p(\alpha) : \mathbb{Q}_p] = [\mathbb{Q}(\alpha) : \mathbb{Q}] = d, \quad (\mathbf{2})\ \mathbb{Q}(\alpha) \text{ is unramified at } p, \\ (\mathbf{3})\ |\alpha|_p = 1, \quad (\mathbf{4})\ \mathbb{F}_p(\tilde{\alpha}) \text{ is the residue field of } \mathbb{Q}_p(\alpha), \\ (\mathbf{5})\ \mathcal{E} \text{ has good reduction at } p, \quad (\mathbf{6})\ |g_i|_p \leqslant 1, \text{ for } i = 0, \ldots 3.\end{gathered} \tag{2.13}$$

It may take a minute to digest these conditions. Condition **(1)** is the most striking; although it is always possible to satisfy **(1)** when $\mathbb{Q}(\alpha)$ has degree 2 or 3 over $\mathbb{Q}$, it is not possible if, for example, $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{a}, \sqrt{b})$. Without this condition we would need to study the ring $L = \mathbb{Q}(\alpha) \otimes \mathbb{Q}_p$ and the set of sections $\mathcal{E}(L)$. Note that $L \cong K_1 \times \cdots \times K_n$, where the K_i are p-adic fields, and $\mathcal{E}(L) \cong \mathcal{E}(K_1) \times \cdots \times \mathcal{E}(K_n)$. In what follows we would perform each step in parallel for each of the fields K_i. Since it will suffice to assume $\mathbb{Q}(\alpha)$ has degree 2 or 3, we have chosen to avoid these complications. The remaining conditions are fairly mild. Conditions **(2)**, **(5)**, and **(6)** are standard assumptions, while conditions **(3)** and **(4)** are imposed so that α (or its reduction) is a generator for all fields and rings we will consider.

Let $\widetilde{\mathcal{E}}$ denote the reduced curve

$$\widetilde{\mathcal{E}} : y^2 = \tilde{g}_3 x^3 + \tilde{g}_2 x^2 + \tilde{g}_1 x + \tilde{g}_0, \tag{2.14}$$

where each $\tilde{g}_i$ is the reduction of g_i mod p. This is an elliptic curve defined over $\mathbb{F}_p(\tilde{\alpha})$. We further let $\widetilde{P}_i$ denote the reduction mod p of P_i, and define m_i, Q_i by

$$m_i = \text{order of } \widetilde{P}_i \text{ in } \widetilde{\mathcal{E}}(\mathbb{F}_p(\tilde{\alpha})), \quad Q_i = m_i P_i \in \mathcal{E}(\mathbb{Q}(\alpha)), \text{ for } i = 1, \ldots, r, \tag{2.15}$$

so that each Q_i is in the kernel of the reduction map from $\mathcal{E}(\mathbb{Q}(\alpha))$ to $\widetilde{\mathcal{E}}(\mathbb{F}_p(\tilde{\alpha}))$. We now imitate the strategy developed in [7] (which applied to genus 2 curves over $\mathbb{Q}$) and let $\mathcal{S}$ be the finite set

$$\{T + k_1P_1 + \ldots + k_rP_r : T \in \mathcal{E}(\mathbb{Q}(\alpha))_{tors}, \lfloor -m_i/2 \rfloor + 1 \leqslant k_i \leqslant \lfloor m_i/2 \rfloor\} \tag{2.16}$$

so that every $P \in \mathcal{E}(\mathbb{Q}(\alpha))$ can be written uniquely in the form

$$P = S + n_1Q_1 + \ldots + n_rQ_r \tag{2.17}$$

for some $S \in \mathcal{S}$ and $n_1, \ldots n_r \in \mathbb{Z}$. Further, let

$$z_i = z\text{-coord of } Q_i, \text{ for } i = 1, \ldots, r, \tag{2.18}$$

so that $z_i = -x_i/y_i$ for each $Q_i = (x_i, y_i)$. Condition (6) of (2.13), the standard estimate $|k!|_p \geqslant p^{-(k-1)/(p-1)}$, and the fact that $|z_i| \leqslant p^{-1}$, give, on substitution into (2.9),(2.10), that

$$z\text{-coord of } n_1Q_1 + \ldots + n_rQ_r = \exp(n_1\log(z_1) + \ldots + n_r\log(z_r)) \in \mathbb{Z}_p[\alpha][[n_1, \ldots, n_r]], \tag{2.19}$$

and the coefficient of $n_1^{k_1} \ldots n_r^{k_r}$ must converge to 0 in $\mathbb{Z}_p[\alpha]$ as $k_1 + \ldots + k_r \to \infty$. Returning to our general P of (2.17), first suppose that $S = \infty$; then substitute (2.19) for z in (2.6) to define θ_∞ by

$$\theta_\infty(n_1, \ldots, n_r) = \frac{1}{x\text{-coord of } n_1Q_1 + \ldots + n_rQ_r} \in \mathbb{Z}_p[\alpha][[n_1, \ldots, n_r]]. \tag{2.20}$$

Now suppose that $S = (x_0, y_0) \neq \infty$. By the way $\mathcal{S}$ was constructed, S is not in the kernel of reduction mod p and so $|x_0|_p, |y_0|_p \leqslant 1$. Substitute (2.19) for z in (2.8) to define θ_S by

$$\theta_S(n_1, \ldots, n_r) = x\text{-coord of } S + n_1Q_1 + \ldots + n_rQ_r \in \mathbb{Z}_p[\alpha][[n_1, \ldots, n_r]]. \tag{2.21}$$

Whether $S = \infty$ or $S \neq \infty$, we now split θ_S into its components

$$\theta_S = \theta_S^{(0)} + \theta_S^{(1)}\alpha + \ldots + \theta_S^{(d-1)}\alpha^{d-1}, \text{ each } \theta_S^{(i)} = \theta_S^{(i)}(n_1, \ldots n_r) \in \mathbb{Z}_p[[n_1, \ldots, n_r]]. \tag{2.22}$$

It is clear that the coefficients of these power series tend to 0 in $\mathbb{Z}_p$, and that

$$(x\text{-coord of } P) \in \mathbb{Q} \Rightarrow \theta_S^{(1)} = \ldots = \theta_S^{(d-1)} = 0, \tag{2.23}$$

where P is as described in (2.17). But every $P \in \mathcal{E}(\mathbb{Q}(\alpha))$ can be written in the form (2.17). Hence, to solve our problem (2.2) as to which members of $\mathcal{E}(\mathbb{Q}(\alpha))$ have $\mathbb{Q}$-rational x-coordinate, it is sufficient, for each member S of the finite set $\mathcal{S}$, to determine which $n_1, \ldots, n_r$ satisfy all of $\theta_S^{(1)} = \ldots = \theta_S^{(d-1)} = 0$. At this point we should use the following standard result, proved on p. 62 of [2].

Theorem 2.1 (Strassman). *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 $\theta(x) = 0$.* □

There is now a clear strategy for attempting to solve our problem (2.2), as follows.

Step 1. Find a set of generators for $\mathcal{E}(\mathbb{Q}(\alpha))$.

Step 2. Choose an odd prime p satisfying the 6 conditions in (2.13). Compute the m_i, Q_i defined by (2.15) and the finite set $\mathcal{S}$ defined by (2.16), so that any $P \in \mathcal{E}(\mathbb{Q}(\alpha))$ can be written in the form given by (2.17).

Step 3. For each $S \in \mathcal{S}$ construct the power series $\theta_S^{(0)}, \theta_S^{(1)}, \ldots, \theta_S^{(d-1)}$ of (2.22), all defined over $\mathbb{Z}_p$ with coefficients converging to 0 in $\mathbb{Z}_p$. Then $(x\text{-coord of } P) \in \mathbb{Q} \Rightarrow \theta_S^{(1)} = \ldots = \theta_S^{(d-1)} = 0$. In the case of rank $\mathcal{E}(\mathbb{Q}(\alpha)) = 1$, each $\theta_S^{(i)} = \theta_S^{(i)}(n_1)$, a power series in one variable n_1. We compute the coefficients of the power series $\theta_S^{(1)}$, say, modulo a sufficiently high power of p so that the bound of Strassman's Theorem can be computed; this gives a bound on the number of $n_1 \in \mathbb{Z}_p$, and so on the number of $n_1 \in \mathbb{Z}$, for which $\theta_S^{(1)} = 0$. Alternatively any of $\theta_S^{(2)}, \ldots, \theta_S^{(d-1)}$ can be used in place of $\theta_S^{(1)}$. Indeed, when rank $\mathcal{E}(\mathbb{Q}(\alpha)) = 1$ and $d \geqslant 3$, then greatest common divisors have the potential to improve the bounds. For example, if $p \neq 2, 3$ and n_1 is a root of both $\theta_S^{(1)} \equiv 1 + 2n_1 + n_1^2 \pmod{p}$ and $\theta_S^{(2)} \equiv 1 + 3n_1 + 2n_1^2 \pmod{p}$, then the Strassman bound on the number of solutions is 2 for each power series considered separately; however, n_1 is also a root of $2\theta_S^{(1)} - \theta_S^{(2)} \equiv 1 + n_1 \pmod{p}$, for which the Strassman bound is 1.

At this stage, we have a bound on the number of $n_1 \in \mathbb{Z}$ for which $S + n_1 Q_1$ has $\mathbb{Q}$-rational x-coordinate. The sum of these bounds over all $S \in \mathcal{S}$ gives a bound on the total number of $P \in \mathcal{E}(\mathbb{Q}(\alpha))$ with $\mathbb{Q}$-rational x-coordinate, which we hope to be the same as the known number of such P.

In the case of rank $\mathcal{E}(\mathbb{Q}(\alpha)) \geqslant 2$, each $\theta_S^{(i)} = \theta_S^{(i)}(n_1, \ldots, n_r)$ for $i = 1, \ldots d-1$. For each i, we can try to apply the Weierstrass Preparation Theorem (see p. 108 of [2]) with respect to n_r, say, and find a polynomial in n_r (whose coefficients are power series in $n_1, \ldots n_{r-1}$), whose zero set is the same as $\theta_S^{(i)}$. Taking resultants with respect to n_r, one obtains $d-2$ power series in $n_1, \ldots n_{r-1}$. Continuing inductively, we can hope to obtain a single power series in n_1; then apply Strassman's Theorem as before. Note that our condition $r < d$ ensures that there are at least as many equations $\theta_S^{(1)}, \ldots, \theta_S^{(d-1)}$ as variables $n_1, \ldots, n_r$.

The reader may wonder why we have called this 'Elliptic Curve Chabauty'. This is due to the following classical result of Chabauty [4].

Theorem 2.2. *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.*

The problem described by (2.1),(2.2) can rephrased as follows. For simplicity, we suppose that $\mathbb{Q}(\alpha) : \mathbb{Q}$ is of degree 3, and we describe an associated curve given by the following 3 equations

$$y_i^2 = \sigma_i(g_3)x^3 + \sigma_i(g_2)x^2 + \sigma_i(g_1)x + \sigma_i(g_0), \ i = 1, 2, 3, \tag{2.24}$$

in the 4 variables x, y_1, y_2, y_3, where $\sigma_1, \sigma_2, \sigma_3$ are the 3 embeddings of $\mathbb{Q}(\alpha)$ into $\mathbb{C}$. The curve $\mathcal{C}$ given by this set of conjugate equations is genus 3 and can be defined over $\mathbb{Q}$. We view a point (x, y_1, y_2, y_3) on $\mathcal{C}$ to be $\mathbb{Q}$-rational if $x \in \mathbb{Q}$ and y_1, y_2, y_3 are a set of conjugates over $\mathbb{Q}$; it follows that the $\mathbb{Q}$-rational points on $\mathcal{C}$ come from points on $\mathcal{E}(\mathbb{Q}(\alpha))$ which have $\mathbb{Q}$-rational x-coordinate. Moreover, the rank of the Jacobian of $\mathcal{C}$ over $\mathbb{Q}$ is equal to the rank of $\mathcal{E}(\mathbb{Q}(\alpha))$. When the rank of $\mathcal{E}(\mathbb{Q}(\alpha))$ is $0, 1, 2$, the application of Chabauty's Theorem to $\mathcal{C}$ is equivalent to applying the methods of this section to $\mathcal{E}$.

§3. Worked Examples

In this section, we give a simplified and more accessible solution to the Diophantus Example (0.1), involving a cubic number field. We also present an example where the number field is quadratic, and an example where all $\mathcal{E}^a_{i,k}$ and $\mathcal{E}^b_{j,k}$ are defined over $\mathbb{Q}$.

Example 3.1. *Let* $\mathcal{C} : Y^2 = X^6+X^2+1$*. Then* $\mathcal{C}(\mathbb{Q}) = \{\infty^+, \infty^-, (0, \pm 1), (\pm 1/2, \pm 9/8)\}$.

Proof. The curves $\mathcal{E}^a : Y^2 = F^a(x) = x^3 + x + 1$ and $\mathcal{E}^b : \underline{Y}^2 = F^b(\underline{x}) = \underline{x}^3 + \underline{x}^2 + 1$ come with the usual maps $(X, Y) \mapsto (X^2, Y)$ from $\mathcal{C}$ to $\mathcal{E}^a$ and $(X, Y) \mapsto (1/X^2, Y/X^3)$ from $\mathcal{C}$ to $\mathcal{E}^b$. A standard descent shows that $\mathcal{E}^a(\mathbb{Q})$ has no torsion, has rank 1, and that $\{(x_1, Y_1), (x_2, Y_2)\} = \{\infty, (0, 1)\}$ is a set of representatives for $\mathcal{E}^a(\mathbb{Q})/2\mathcal{E}^a(\mathbb{Q})$. Similarly, $\mathcal{E}^b(\mathbb{Q})$ has no torsion, has rank 1, and $\{(\underline{x}_1, \underline{Y}_1), (\underline{x}_2, \underline{Y}_2)\} = \{\infty, (0, 1)\}$ is a set of representatives for $\mathcal{E}^b(\mathbb{Q})/2\mathcal{E}^b(\mathbb{Q})$. Let $\alpha =$ root of $F^a(x)$. Recall, from (1.14), that if $(X, Y) \in \mathcal{C}(\mathbb{Q})$ maps to $(x, Y) = (X^2, Y) = (x_i, Y_i) \in \mathcal{E}^a(\mathbb{Q})/2\mathcal{E}^a(\mathbb{Q})$ and maps to $(\underline{x}, \underline{Y}) = (1/X^2, Y/X^3) = (\underline{x}_j, \underline{Y}_j) \in \mathcal{E}^b(\mathbb{Q})/2\mathcal{E}^b(\mathbb{Q})$, then $(1 - \alpha\underline{x}_j)/(x_i - \alpha)$ is a square in $\mathbb{Q}(\alpha)$. We compute the matrix whose (i, j)th entry is $(1 - \alpha\underline{x}_j)/(x_i - \alpha)$ to get: $\left(\begin{smallmatrix} -\alpha & 1 \\ 1 & -\alpha \end{smallmatrix}\right)$. We see that 1 is a square, but $-\alpha$ is not (as can be seen from the fact that $\mathrm{Norm}(t^2 + \alpha) = t^6 + t^2 - 1$ is irreducible over $\mathbb{Q}$). This explicitly matches up the work involved in the $\mathcal{E}^a$ approach of Lemma 1.1(a) and the $\mathcal{E}^b$ approach of Lemma 1.1(b), with $\mathcal{E}^a_1, \mathcal{E}^a_2$ being $\mathbb{Q}(\alpha)$-birationally equivalent to $\mathcal{E}^b_2, \mathcal{E}^b_1$, respectively (where the birational transformations preserve the $\mathbb{Q}$-rationality of the x-coordinates). There are no entire rows or columns of non-squares in our 2×2 matrix, so the matrix does not save us from any rank computations, whether $\mathcal{E}^a$ or $\mathcal{E}^b$ is used.

We shall use $\mathcal{E}^a$; it is sufficient to show that $\infty, (0, \pm 1), (1/4, \pm 9/8)$ give all $(x, Y) \in \mathcal{E}^a(\mathbb{Q})$ for which x is a square in $\mathbb{Q}$. From Lemma 1.1(a), we derive the elliptic curves

$$\begin{aligned} \mathcal{E}^a_1 &: y^2 = x(x^2 + \alpha x + (\alpha^2 + 1)) \\ \mathcal{E}^a_2 &: y^2 = -\alpha x(x^2 + \alpha x + (\alpha^2 + 1)) \end{aligned} \tag{3.1}$$

corresponding to replacing (x_i, Y_i) in equation (1.12) by $\infty, (0, 1)$, respectively. It is sufficient, for each of $\mathcal{E}^a_1, \mathcal{E}^a_2$, to show that the only $(x, y) \in \mathcal{E}^a_i(\mathbb{Q}(\alpha))$ with $x \in \mathbb{Q}$ have

$x = 0, 1/4$ or ∞. A standard descent (as in [1,6,9,10]) shows that $\mathcal{E}_2^a(\mathbb{Q}(\alpha))$ has rank 0 and consists only of ∞ and $(0,0)$, so that $\mathcal{E}_2^a$ trivially satisfies our requirements.

A standard descent also shows that $\mathcal{E}_1^a(\mathbb{Q}(\alpha))$ has rank 1. A set of generators is given by $(0,0), (1/4, 1/8-\alpha/2+\alpha^2/4)$, where $(0,0)$ is of order 2 and $P_1 = (1/4, 1/8-\alpha/2+\alpha^2/4)$ is of infinite order. It is sufficient to show that these two points, together with ∞, are the only points in $\mathcal{E}_1^a(\mathbb{Q}(\alpha))$ with $\mathbb{Q}$-rational x-coordinate. Since $\mathcal{E}_1^a(\mathbb{Q}(\alpha))$ has rank 1, we can apply the strategy of Section 2, with $g_3 = 1, g_2 = \alpha, g_1 = \alpha^2 + 1, g_0 = 0$ in all of the equations of Section 2. We choose $p = 5$, which satisfies all 6 conditions of (2.13), and compute multiples of $\widetilde{P}_1$ in $\mathbb{F}_5(\tilde{\alpha})$. We find that the order of $\widetilde{P}_1$ is 7 and so we define, as in (2.15),(2,16):

$$\begin{aligned} &m_1 = 7, Q_1 = 7P_1, \text{ where } P_1 = (1/4, 1/8 - \alpha/2 + \alpha^2/4), \\ &\mathcal{S} = \{\infty, (0,0), \pm P_1, \pm 2P_1, \pm 3P_1, \pm P_1 + (0,0), \pm 2P_1 + (0,0), \pm 3P_1 + (0,0)\}, \end{aligned} \tag{3.2}$$

so that

$$\text{every } P \in \mathcal{E}_1^a(\mathbb{Q}(\alpha)) \text{ can be written as } P = S + n_1 Q_1, \text{ for some } S \in \mathcal{S}, n_1 \in \mathbb{Z}. \tag{3.3}$$

Since Q_1 is in the kernel of reduction mod p, $\widetilde{P} = \widetilde{S}$, and so if P has $\mathbb{Q}$-rational x-coordinate then $\widetilde{S}$ must have $\mathbb{F}_p$-rational x-coordinate. Computing the members of $\mathcal{S}$ mod p, we find that this is true only for $S = \infty, (0,0), \pm P_1$, and so these are the only $S \in \mathcal{S}$ we need to consider. We shall have solved our problem if we can prove the following four claims:

Claim k. *$n_1 = 0$ is the only $n_1 \in \mathbb{Z}$ for which $R_k + n_1 Q_1$ has $\mathbb{Q}$-rational x-coordinate,* where $k = 1, \ldots, 4$ and $R_1 = \infty$, $R_2 = (0,0)$, $R_3 = P_1$, $R_4 = -P_1$.

We first compute what is needed in all cases, namely the z-coordinate of $n_1 Q_1$ expressed as power series in n_1 over $\mathbb{Z}_5[\alpha]$. It will be sufficient to work mod 5^5 so that, in view of (2.11) and the standard estimate $|k!|_p \geqslant p^{-(k-1)/(p-1)}$, the $O(z^9)$ can be ignored in (2.9),(2.10). We first note that the z-coordinate of Q_1 (mod 5^5) is: $5(521+15\alpha+121\alpha^2)$. Substituting this for t in (2.9) gives log(z-coordinate of Q_1) (mod 5^5) as: $5(471 + 65\alpha + 321\alpha^2)$. We now substitute $5(471 + 65\alpha + 321\alpha^2)n_1$ for t in (2.10), and see that

$$\begin{aligned} &z\text{-coordinate of } n_1 Q_1 = \exp(n_1 \log(z\text{-coordinate of } Q_1)) = O(n_1) \in \mathbb{Z}_5[\alpha][[n_1]] \\ &\equiv 5(471 + 65\alpha + 321\alpha^2)n_1 + 5^3(22 + 13\alpha + 12\alpha^2)n_1^3 + 5^4(1 + 2\alpha + \alpha^2)n_1^5 \pmod{5^5}. \end{aligned} \tag{3.4}$$

Proof of Claim 1. We replace z by (3.4) in (2.6) to get:

$$\begin{aligned} &\phi_\infty(n_1) = 1/(x\text{-coordinate of } n_1Q_1) = O(n_1^2) \in \mathbb{Z}_5[\alpha][[n_1]], \\ &\phi_\infty(n_1) \equiv 5^2(111 + 84\alpha + 66\alpha^2)n_1^2 + 5^4(1 + 2\alpha + 3\alpha^2)n_1^4 \pmod{5^5}. \end{aligned} \tag{3.5}$$

We split up $\phi_\infty(n_1) = \phi_\infty^{(0)}(n_1) + \phi_\infty^{(1)}(n_1)\alpha + \phi_\infty^{(2)}(n_1)\alpha^2$, where each $\phi_\infty^{(i)}(n_1) \in \mathbb{Z}_5[[n_1]]$. If the x-coordinate of n_1Q_1 is $\mathbb{Q}$-rational, then $\phi_\infty^{(1)}(n_1) = \phi_\infty^{(2)}(n_1) = 0$. Separating $\phi_\infty^{(2)}(n_1)$ off from (3.5) gives

$$\begin{aligned} &\phi_\infty^{(2)}(n_1) = O(n_1^2) \in \mathbb{Z}_5[[n_1]], \\ &\phi_\infty^{(2)}(n_1) \equiv 5^2 \cdot 66 \cdot n_1^2 + 5^4 \cdot 3 \cdot n_1^4 \pmod{5^5}. \end{aligned} \tag{3.6}$$

This has a double root at 0, but $|5^2 \cdot 66|_5 = 5^{-2}$, which is strictly greater than the 5-adic norm of all subsequent coefficients. On applying Strassman's Theorem to $\phi_\infty^{(2)}(n_1)/n_1^2 \in \mathbb{Z}_5[[n_1]]$, we see that there are no other $n_1 \in \mathbb{Z}_5$ (and so no other $n_1 \in \mathbb{Z}$) satisfying $\phi_\infty^{(2)}(n_1) = 0$, proving Claim 1.

Proof of Claim 2. Replace (x_0, y_0) by $(0, 0)$ and z by (3.4) in (2.8) to give

$$\begin{aligned} &\phi_{(0,0)}(n_1) = x\text{-coordinate of } (0,0) + n_1Q_1 = O(n_1^2) \in \mathbb{Z}_5[\alpha][[n_1]] \\ &\equiv 5^2(27 + 59\alpha + 111\alpha^2)n_1^2 + 5^4(4 + 2\alpha + \alpha^2)n_1^4 \pmod{5^5}. \end{aligned} \tag{3.7}$$

This has a double root at 0, and an identical argument on $\phi_{(0,0)}^{(2)}(n_1)$ to that performed on $\phi_\infty^{(2)}(n_1)$ above, shows that $n_1 = 0$ is the only solution.

Proof of Claim 3. Replace (x_0, y_0) by $P_1 = (1/4, 1/8 - \alpha/2 + \alpha^2/4)$ and z by (3.4) in (2.8) to give

$$\begin{aligned} &\phi_{P_1}(n_1) = x\text{-coordinate of } P_1 + n_1Q_1 \in \mathbb{Z}_5[\alpha][[n_1]] \\ &\phi_{P_1}(n_1) \equiv 2344 + 5(250 + 142\alpha + 559\alpha^2)n_1 + 5^2(7 + 66\alpha + 56\alpha^2)n_1^2 \\ &\qquad + 5^3(14 + 21\alpha + 14\alpha^2)n_1^3 + 5^4(3 + 2\alpha + 3\alpha^2)n_1^4 \pmod{5^5}. \end{aligned} \tag{3.8}$$

Taking $\phi_{P_1}^{(2)}(n_1) \equiv 5 \cdot 559 \cdot n_1 + 5^2 \cdot 56 \cdot n_1^2 + 5^3 \cdot 14 \cdot n_1^3 + 5^4 \cdot 3 \cdot n_1^4 \pmod{5^5}$, and applying Strassman's Theorem to $\phi_{P_1}^{(2)}(n_1) = 0$ again gives that $n_1 = 0$ is the only solution.

Proof of Claim 4. Since $-P_1 + n_1Q_1 = -(P_1 - n_1Q_1)$, Claim 4 follows from Claim 3.

All four claims being proved, this completes the proof of Example 3.1. □

Although we do not require it here, it is interesting to see how the genus 3 curves F_1, F_2 over $\mathbb{Q}$ in (0.3) can be derived from our approach. As usual, let $(X, Y) \in \mathcal{C}(\mathbb{Q})$ so that $(X^2, Y) \in \mathcal{E}^a(\mathbb{Q})$ and $(1/X^2, Y/X^3) \in \mathcal{E}^b(\mathbb{Q})$, where $\mathcal{E}^a, \mathcal{E}^b$ are as in (0.2). We let, as usual, α denote a root of $x^3 + x + 1$ and $\underline{\alpha} = 1/\alpha$ denote a root of $x^3 + x^2 + 1$ so that, of course, $\mathbb{Q}(\alpha) = \mathbb{Q}(\underline{\alpha})$. Recall that, in the above example, $\mathcal{E}^a(\mathbb{Q})$ has no torsion, has rank 1, and $\{\infty, (0, 1)\}$ is a set of representatives for $\mathcal{E}^a(\mathbb{Q})/2\mathcal{E}^a(\mathbb{Q})$. It follows that $(X^2, Y) \in \mathcal{E}^a(\mathbb{Q})$ must satisfy either: $(X^2, Y) \in 2\mathcal{E}^a(\mathbb{Q})$ or $(X^2, Y) \in (0, 1) + 2\mathcal{E}^a(\mathbb{Q})$ (corresponding to $\mathcal{E}^a_1, \mathcal{E}^a_2$ of (3.1), respectively). In the second case, $(0-\alpha)(X^2-\alpha) \in \mathbb{Q}(\alpha)^2$, and so $1/X^2 - \underline{\alpha} = (0 - \alpha)(X^2 - \alpha)/(\alpha X)^2 \in \mathbb{Q}(\alpha)^2 = \mathbb{Q}(\underline{\alpha})^2$. This implies (using the homomorphism (1.6)) that $(1/X^2, Y/X^3) \in 2\mathcal{E}^b(\mathbb{Q})$. In summary:

$$(X, Y) \in \mathcal{C}(\mathbb{Q}) \Rightarrow (X^2, Y) \in 2\mathcal{E}^a(\mathbb{Q}) \text{ or } (1/X^2, Y/X^3) \in 2\mathcal{E}^b(\mathbb{Q}). \tag{3.9}$$

In the case of $(X^2, Y) \in 2\mathcal{E}^a(\mathbb{Q})$, say that $(X^2, Y) = 2R$, where $R \in \mathcal{E}^a(\mathbb{Q})$. Let s be the x-coordinate of R, and let $[2]_a$ denote the x-coordinate duplication map on $\mathcal{E}^a$. Then

$$X^2 = [2]_a(s) = (s^4 - 2s^2 - 8s + 1)/4(s^3 + s + 1). \tag{3.10}$$

Letting $t = 2(s^3 + s + 1)X$ gives the model F_1 in (0.3). Similary, in the case of $(1/X^2, Y/X^3) \in 2\mathcal{E}^b(\mathbb{Q})$, say that $(1/X^2, Y/X^3) = 2R$, where $R \in \mathcal{E}^b(\mathbb{Q})$. Let $\underline{s}$ be the $\underline{x}$-coordinate of R, and let $[2]_b$ denote the $\underline{x}$-coordinate duplication map on $\mathcal{E}^b$. Then

$$1/X^2 = [2]_b(\underline{s}) = (\underline{s}^4 - 8\underline{s} - 4)/4(\underline{s}^3 + \underline{s}^2 + 1). \tag{3.11}$$

Letting $\underline{t} = 2(\underline{s}^3 + \underline{s}^2 + 1)/X$ gives the model F_2 in (0.3). There is a trade off here in the methods for solving for $\mathcal{C}(\mathbb{Q})$. One can either, as we have done in the above worked example, find all members of $\mathcal{E}^a_1(\mathbb{Q}(\alpha)), \mathcal{E}^a_2(\mathbb{Q}(\alpha))$ (given in (3.1)) with $\mathbb{Q}$-rational x-coordinate; or, as in [11], one can find all members of $F_1(\mathbb{Q}), F_2(\mathbb{Q})$. That is, one can either work with elliptic curves over a cubic number field, or genus 3 curves over $\mathbb{Q}$. Both methods are essentially 'doing the same work', but the first is easier, as it avoids the machinery of genus 3 Jacobians. Furthermore, the approach to the general problem (2.1) of Section 2 is easily applicable whatever the degree of $d = \mathbb{Q}(\alpha) : \mathbb{Q}$; as d increases, the models for the corresponding high genus curves would become increasingly hard to derive, as would be the Chabauty techniques on their Jacobians.

We now give an example $Y^2 = F(X^2)$ in which the cubic $F(X)$ factors over $\mathbb{Q}$ as a linear times an irreducible quadratic, so that our Elliptic Curve Chabauty technique of Section 2 is applied to cases where $\mathbb{Q}(\alpha)$ is a quadratic number field. This is followed by an example where $F(X)$ factors completely over $\mathbb{Q}$ into 3 linear factors, so that all of the elliptic curves $\mathcal{E}^a_{i,k}$ in (1.15) are defined over $\mathbb{Q}$.

Example 3.2. *Let $\mathcal{C} : Y^2 = X^6 - 2X^4 - 2X^2 + 1 = (X^2+1)(X^4 - 3X^2 + 1)$. Then $\mathcal{C}(\mathbb{Q}) = \{\infty^+, \infty^-, (0, \pm 1), (\pm 2, \pm 5), (\pm 1/2, \pm 5/8)\}$.* □

Example 3.3. *Let $\mathcal{C} : Y^2 = (X^2+1)(X^2-3)(X^2+7)$. Then $\mathcal{C}$ has no $\mathbb{Q}$-rational affine points; that is, $\mathcal{C}(\mathbb{Q}) = \{\infty^+, \infty^-\}$.* □

The proofs for both of the above examples are available as a postscript file, at www.maths.ox.ac.uk/~flynn/genus2/local/ex2and3.ps (which includes the use of (1.17) to reduce the number of rank computations in Example 3.3).

We have done a small amount of rather unsystematic experimentation, in which 50 semi-random curves were tested. We found precisely one curve where the method failed, namely: $\mathcal{C} : Y^2 = (X^2+1)(X^2+3)(X^2+7)$. In this case, $\mathcal{E}^a(\mathbb{Q})$ and $\mathcal{E}^b(\mathbb{Q})$ both have rank 1; furthermore, there exists i (corresponding to $(x_i, Y_i) = (1, 8)$) for which each $\mathcal{E}^a_{i,k}(\mathbb{Q})$ has rank 1; similarly, there exists j (corresponding to $(\underline{x}_j, \underline{Y}_j) = (1, -8)$) for which each $\mathcal{E}^b_{j,k}(\mathbb{Q})$ has rank 1. Hence we cannot reduce our eligible $x = X^2$ down to a finite number of possibilities, and the method fails.

In performing our rank computations, we found helpful the public domain programs: the Mordell-Weil group program *mwrank* (John Cremona) and SIMATH (Horst Zimmer), which can be found, respectively, at

http://www.maths.nott.ac.uk/personal/jec/ftp/progs

http://emmy.math.uni-sb.de/~simath/

For anyone wishing to solve problems similar to those in this section, we have provided

www.maths.ox.ac.uk/~flynn/genus2/local/ell.curve.chab which contains the power series of Section 2, some to a higher degree in z; for example, the formal exponential and logarithm power series are up to terms of degree 9.

REFERENCES

[1] Bruin, N. *On Generalised Fermat Equations.* PhD Dissertation, Leiden, 1999.

[2] Cassels, J.W.S. *Local Fields.* London Mathematical Society Student Texts **3**. Cambridge University Press, 1986.

[3] Cassels, J.W.S. and Flynn, E.V. *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2.* Cambridge University Press, 1996.

[4] Chabauty C. *Sur les points rationnels des courbes algébriques de genre supérieur à l'unité.* Comptes Rendus, Paris **212** (1941), 882-885.

[5] Cremona, J.E. and Serf, P. *Computing the rank of elliptic curves over real quadratic number fields of class number 1.* To appear in Math. Comp.

[6] Djabri, Z., Schaefer, E.F. and Smart, N.P. *Computing the p-Selmer group of an elliptic curve.* To appear in Trans. A.M.S.

[7] Flynn, E.V. *A Flexible Method for Applying Chabauty's Theorem.* Compositio Mathematica. **105** (1997), 79–94.

[8] Sesiano, J. *Books IV to VII of Diophantus' Arithmetica in the Arabic Translation attributed to Qusta ibn Luqa.* Springer-Verlag, New York (1982).

[9] Siksek, S. *Infinite descent on elliptic curves.* Rocky Mountain Journal of Mathematics **25 No. 4** (1995), 1501–1538.

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

[11] Wetherell, J.L. *Bounding the Number of Rational Points on Certain Curves of High Rank*, PhD Dissertation (1997), University of California at Berkeley.

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

Joseph L. Wetherell, Department of Mathematics, University of Southern California,
1042 W.36th Place, Los Angeles, CA 90089-1113, U.S.A. jlwether@alum.mit.edu