

Lucas sequences whose 12th or 9th term is a square

A. Bremner* N. Tzanakis†

1 Introduction

Let P and Q be non-zero relatively prime integers. The Lucas sequence $\{U_n(P, Q)\}$ is defined by

$$U_0 = 0, \quad U_1 = 1, \quad U_n = PU_{n-1} - QU_{n-2} \quad (n \geq 2). \quad (1)$$

The sequence $\{U_n(1, -1)\}$ is the familiar Fibonacci sequence, and it was proved by Cohn [11] in 1964 that the only perfect square greater than 1 in this sequence is $U_{12} = 144$. The question arises, for which parameters P, Q , can $U_n(P, Q)$ be a perfect square? This has been studied by several authors: see for example Cohn [12] [13] [14], Ljunggren [21], and Robbins [24]. Using Baker's method on linear forms in logarithms, work of Shorey & Tijdeman [25] implies that there can only be finitely many squares in the sequence $\{U_n(P, Q)\}$. Ribenboim and McDaniel [22] with only elementary methods show that when P and Q are *odd*, and $P^2 - 4Q > 0$, then U_n can be square only for $n = 0, 1, 2, 3, 6$ or 12 ; and that there are at most two indices greater than 1 for which U_n can be square. They characterize fully the instances when $U_n = \square$, for $n = 2, 3, 6$, and observe that $U_{12} = \square$ if and only if there is a solution to the Diophantine system

$$P = \square, P^2 - Q = 2\square, P^2 - 2Q = 3\square, P^2 - 3Q = \square, (P^2 - 2Q)^2 - 3Q^2 = 6\square. \quad (2)$$

When P is even, a later paper of Ribenboim and McDaniel [23] proves that if $Q \equiv 1 \pmod{4}$, then $U_n(P, Q) = \square$ for $n > 0$ only if n is a square or twice a square, and all prime factors of n divide $P^2 - 4Q$. Further, if $p^{2t} | n$ for a prime p , then $U_{p^{2u}}$ is square for $u = 1, \dots, t$. In addition, if n is even, then $U_n = \square$ only if P is a square or twice a square. A remark is made that no example is known

*Department of Mathematics, Arizona State University, Tempe AZ, USA, e-mail: bremner@asu.edu, <http://math.la.asu.edu/~andrew/bremner.html>

†Department of Mathematics, University of Crete, Iraklion, Greece, e-mail: tzanakis@math.uoc.gr, <http://www.math.uoc.gr/~tzanakis>

of an integer pair P, Q , and an odd prime p , such that $U_{p^2} = \square$ (note none can exist for P, Q odd, $P^2 - 4Q > 0$).

In this paper, we complete the results of Ribenboim and MacDaniel [22] by determining all Lucas sequences $\{U_n(P, Q)\}$ with $U_{12} = \square$ (in fact, the result is extended, because we do not need the restrictions that P, Q be odd, and $P^2 - 4Q > 0$): it turns out that the Fibonacci sequence provides the only example. Moreover, we also determine all Lucas sequences $\{U_n(P, Q)\}$ with $U_9 = \square$, subject only to the restriction that $(P, Q) = 1$. Throughout this paper the symbol \square means square of a *non-zero* rational number.

Theorem 1. *Let (P, Q) be any pair of relatively prime non-zero integers. Then,*

- $U_{12}(P, Q) = \square$ iff $(P, Q) = (1, -1)$ (corresponding to the Fibonacci sequence).
- $U_9(P, Q) = \square$ iff $(P, Q) = (\pm 2, 1)$ (corresponding to the sequences $U_n = n$ and $U_n = (-1)^{n+1}n$).

The remainder of the paper is devoted mainly to the proof of this theorem. Theorems 3 and 6 of [22] combined with the first statement of Theorem 1 imply the following.

Theorem 2. *Let P, Q be relatively prime odd integers, such that $P^2 - 4Q > 0$. Then the n th term, $n > 1$, of the Lucas sequence $U_n = U_n(P, Q)$ can be a square only if $n = 2, 3, 6$ or 12 . More precisely¹:*

- $U_2 = \square$ iff $P = a^2$.
- $U_3 = \square$ iff $P = a, Q = a^2 - b^2$.
- $U_6 = \square$ iff $P = 3a^2b^2, Q = \frac{-a^8 + 12a^4b^4 - 9b^8}{2}$.
- $U_{12} = \square$ iff $(P, Q) = (1, -1)$. Moreover, this result is also valid even if we remove all restrictions on P, Q except for $\gcd(P, Q) = 1$.

The proof of Theorem 1 hinges, in both cases, upon finding all rational points on a curve of genus 2. When the rank of the Jacobian of such a curve is less than 2, then methods of Chabauty [10], as expounded subsequently by Coleman [15], Cassels and Flynn [9] and Flynn [16] may be used to determine the (finitely many) rational points on the curve. When the rank of the Jacobian is at least 2, as is the case here, a direct application of these methods fails. In order to deal with such situations, very interesting methods have been developed recently by a number of authors; see chapter 1 of Wetherell's Ph.D. thesis [31], Bruin [1, 2, 3], Bruin and Flynn [4, 5], Flynn [17], and Flynn & Wetherell [18, 19]. For the purpose of this paper, the method of [17] or [18] is sufficient.

¹Below it is understood that parameters a, b are in every case chosen so that P, Q are odd, relatively prime and $P^2 - 4Q > 0$.

2 The Diophantine equations

2.1 The case U_{12}

For $U_{12}(P, Q)$ to be square, we have from (1)

$$U_{12}(P, Q) = P(P^2 - 3Q)(P^2 - 2Q)(P^2 - Q)(P^4 - 4P^2Q + Q^2) = \square. \quad (3)$$

Now $(P(P^2 - 3Q)(P^2 - Q), (P^2 - Q)(P^4 - 4P^2Q + Q^2))$ divides 2, so that $U_{12} = \square$ implies

$$P(P^2 - 3Q)(P^2 - Q) = \delta\square, \quad (P^2 - 2Q)(P^4 - 4P^2Q + Q^2) = \delta\square,$$

where $\delta = \pm 1, \pm 2$. With $x = Q/P^2$, we deduce

$$(1 - 2x)(1 - 4x + x^2) = \delta\square,$$

and of these four elliptic curves, only the curve with $\delta = 2$ has positive rational rank. Torsion points on the three other curves do not provide any solutions for P, Q . We are thus reduced to considering the equations

$$P(P^2 - 3Q)(P^2 - Q) = 2\square, \quad (P^2 - 2Q)(P^4 - 4P^2Q + Q^2) = 2\square.$$

From the first equation,

$$P(P^2 - 3Q) = \pm 2\square, P^2 - Q = \pm\square, \quad \text{or} \quad P(P^2 - 3Q) = \pm\square, P^2 - Q = \pm 2\square.$$

The former case implies one of

$$\begin{aligned} P = \delta\square \quad P^2 - 3Q = 2\delta\square \quad P^2 - Q = \square \\ P = \delta\square \quad P^2 - 3Q = -2\delta\square \quad P^2 - Q = -\square \\ P = 2\delta\square \quad P^2 - 3Q = \delta\square \quad P^2 - Q = \square \\ P = 2\delta\square \quad P^2 - 3Q = -\delta\square \quad P^2 - Q = -\square \end{aligned} \quad (4)$$

where $\delta = \pm 1, \pm 3$.

The latter case implies one of

$$\begin{aligned} P = \delta\square \quad P^2 - 3Q = \delta\square \quad P^2 - Q = 2\square \\ P = \delta\square \quad P^2 - 3Q = -\delta\square \quad P^2 - Q = -2\square \end{aligned} \quad (5)$$

where $\delta = \pm 1, \pm 3$.

Solvability in \mathbb{R} or elementary congruences shows impossibility of the above equations (4), (5), except in the following instances:

$$\begin{aligned} P = -\square, \quad P^2 - 3Q = -2\square, \quad P^2 - Q = \square \\ P = -3\square, \quad P^2 - 3Q = -6\square, \quad P^2 - Q = \square \\ P = 6\square, \quad P^2 - 3Q = 3\square, \quad P^2 - Q = \square \\ P = \square, \quad P^2 - 3Q = -2\square, \quad P^2 - Q = -\square \\ P = 6\square, \quad P^2 - 3Q = -3\square, \quad P^2 - Q = -\square \\ P = \square, \quad P^2 - 3Q = \square, \quad P^2 - Q = 2\square \\ P = -3\square, \quad P^2 - 3Q = -3\square, \quad P^2 - Q = 2\square. \end{aligned} \quad (6)$$

Recall now that

$$(P^2 - 2Q)(P^4 - 4P^2Q + Q^2) = 2\Box,$$

from which

$$P^2 - 2Q = \eta\Box, P^4 - 4P^2Q + Q^2 = 2\eta\Box \quad \text{or} \quad P^2 - 2Q = 2\eta\Box, P^4 - 4P^2Q + Q^2 = \eta\Box,$$

where $\eta = \pm 1, \pm 3$. The only locally solvable equations are

$$\begin{aligned} P^2 - 2Q &= -\Box, & P^4 - 4P^2Q + Q^2 &= -2\Box \\ P^2 - 2Q &= 3\Box, & P^4 - 4P^2Q + Q^2 &= 6\Box \\ P^2 - 2Q &= 2\Box, & P^4 - 4P^2Q + Q^2 &= \Box \end{aligned} \tag{7}$$

It is straightforward by elementary congruences to deduce from (6), (7), that we must have one of the following:

P	$P^2 - 3Q$	$P^2 - Q$	$P^2 - 2Q$	$P^4 - 4P^2Q + Q^2$
$-\Box$	$-2\Box$	\Box	$-\Box$	$-2\Box$
$6\Box$	$3\Box$	\Box	$2\Box$	\Box
\Box	$-2\Box$	$-\Box$	$-\Box$	$-2\Box$
\Box	\Box	$2\Box$	$3\Box$	$6\Box$

Now the rational ranks of the following elliptic curves are 0:

$$(-x+1)(x^2-4x+1) = -2\Box, \quad (-3x+1)(x^2-4x+1) = 3\Box, \quad (-x+1)(x^2-4x+1) = 2\Box,$$

and consequently the rational points on the curves corresponding to the first three rows of the above table are straightforward to determine: they are $(P, Q) = (-1, 1), (0, -1),$ and $(1, 1)$ respectively. These lead to degenerate Lucas sequences with $U_{12} = 0$.

It remains only to find all rational points on the following curve:

$$P = \Box, P^2 - 3Q = \Box, P^2 - Q = 2\Box, P^2 - 2Q = 3\Box, P^4 - 4P^2Q + Q^2 = 6\Box,$$

satisfying $(P, Q) = 1$. Note that this is the curve (2), though we have removed the restriction that P and Q be odd, and $P^2 - 4Q > 0$.

Put $Q/P^2 = 1 - 2u^2$, so that

$$3u^2 - 1 = 2\Box, \quad 4u^2 - 1 = 3\Box, \quad 2u^4 + 2u^2 - 1 = 3\Box. \tag{8}$$

The equations (8) define a curve of genus 9, with certainly only finitely many points. We restrict attention to the curve of genus 2 defined by

$$4u^2 - 1 = 3\Box, \quad 2u^4 + 2u^2 - 1 = 3\Box.$$

Define $K = \mathbb{Q}(\sqrt{3})$, with ring of integers $\mathcal{O}_K = \mathbb{Z}[\sqrt{3}]$, and fundamental unit $2 + \sqrt{3}$. Observe that $(u^2 - 1)^2 - 3u^4 = -3\Box$ implies

$$u^2 - 1 + u^2\sqrt{3} = \epsilon\sqrt{3}\gamma^2,$$

for ϵ a unit of \mathcal{O}_K of norm $+1$, and $\gamma \in \mathcal{O}_K$. If $\epsilon = 2 + \sqrt{3}$, the resulting equation is locally unsolvable above 3 , and so without loss of generality, $\epsilon = 1$. Consider now

$$u^2(4u^2 - 1)(u^2(1 + \sqrt{3}) - 1) = 3\sqrt{3}V^2, \quad V \in K.$$

In consequence, $(x, y) = ((12 + 4\sqrt{3})u^2, (36 + 12\sqrt{3})V)$ is a point defined over K on the elliptic curve

$$E_1 : y^2 = x(x - (3 + \sqrt{3}))(x - 4\sqrt{3}) \quad (9)$$

satisfying $\frac{(3-\sqrt{3})}{24}x \in \mathbb{Q}^2$. We shall see that the K -rank of E_1 is equal to 1 , with generator of infinite order $P = (\sqrt{3}, 3\sqrt{3})$.

2.2 The case U_9

For $U_9(P, Q)$ to be square, we have from (1)

$$U_9(P, Q) = (P^2 - Q)(P^6 - 6P^4Q + 9P^2Q^2 - Q^3) = \Box. \quad (10)$$

So

$$P^2 - Q = \delta\Box, \quad P^6 - 6P^4Q + 9P^2Q^2 - Q^3 = \delta\Box,$$

where $\pm\delta = 1, 3$. Put $Q = P^2 - \delta R^2$. Then

$$\frac{3}{\delta}P^6 - 9P^4R^2 + 6\delta P^2R^4 + \delta^2R^6 = \Box, \quad (11)$$

with covering elliptic curves

$$\frac{3}{\delta} - 9x + 6\delta x^2 + \delta^2 x^3 = \Box, \quad \frac{3}{\delta}x^3 - 9x^2 + 6\delta x + \delta^2 = \Box. \quad (12)$$

For $\delta = \pm 1$, the first curve has rational rank 0 , and torsion points do not lead to non-zero solutions for P, Q . For $\delta = \pm 3$, both curves at (12) have rational rank 1 , so that the rank of the Jacobian of (11) equals 2 . To solve the equation $U_9(P, Q) = \Box$, it is necessary to determine all integer points on the two curves

$$P^6 - 9P^4R^2 + 18P^2R^4 + 9R^6 = \Box, \quad (13)$$

and

$$-P^6 - 9P^4R^2 - 18P^2R^4 + 9R^6 = \Box. \quad (14)$$

To this end, let $L = \mathbb{Q}(\alpha)$ be the number field defined by $\alpha^3 - 3\alpha - 1 = 0$. $\text{Gal}(L/\mathbb{Q})$ is cyclic of order 3 , generated by σ , say, where $\alpha^\sigma = -1/(1 + \alpha) = -2 - \alpha + \alpha^2$. The ring of integers \mathcal{O}_L has basis $\{1, \alpha, \alpha^2\}$, and class number 1 . Generators for the group of units in \mathcal{O}_L are $\epsilon_1 = \alpha, \epsilon_2 = 1 + \alpha$, with norms $\text{Norm}(\epsilon_1) = 1, \text{Norm}(\epsilon_2) = -1$. The discriminant of L/\mathbb{Q} is 81 , and the ideal (3) factors in \mathcal{O}_L as $(-1 + \alpha)^3$.

2.2.1

Equation (13) may be written in the form

$$\text{Norm}_{L/\mathbb{Q}}(P^2 + (-5 + \alpha + \alpha^2)R^2) = S^2, \text{ say,}$$

and it follows that

$$P^2 + (-5 + \alpha + \alpha^2)R^2 = \lambda U^2, \quad (15)$$

with $\lambda \in \mathcal{O}_L$ squarefree and of norm $+1$ modulo L^{*2} .

Applying σ ,

$$P^2 + (-5 - 2\alpha + \alpha^2)R^2 = \lambda^\sigma V^2. \quad (16)$$

Suppose \mathcal{P} is a first degree prime ideal of \mathcal{O}_L dividing (λ) . Then for the norm of λ to be a square, λ must also be divisible by one of the conjugate prime ideals of \mathcal{P} . It follows that \mathcal{P} , or one of its conjugates, divides both λ and λ^σ . Then this prime will divide $((-5 + \alpha + \alpha^2) - (-5 - 2\alpha + \alpha^2)) = (3\alpha) = (1 - \alpha)^3$. So \mathcal{P} has to be $(1 - \alpha)$, with $(1 - \alpha)^2$ dividing λ , contradicting λ squarefree. If the residual degree of \mathcal{P} is 3, then the norm of λ cannot be square. Finally, the residual degree of \mathcal{P} cannot be 2, otherwise $\theta = 5 - \alpha - \alpha^2 \equiv m \pmod{\mathcal{P}}$, for some rational integer m , so that $\alpha = 1 - 2\theta + \frac{1}{3}\theta^2$ is congruent to a rational integer modulo \mathcal{P} , impossible. In consequence, λ is forced to be a unit, of norm $+1$. Without loss of generality, the only possibilities are $\lambda = 1, \epsilon_1, -\epsilon_2, -\epsilon_1\epsilon_2$. However, specializing the left hand side of (15) at the root $\alpha_0 = 1.8793852415\dots$ of $x^3 - 3x - 1 = 0$ shows that $P^2 + 0.4114\dots R^2 = \lambda(\alpha_0)U(\alpha_0)^2$, so that $\lambda(\alpha_0) > 0$, giving unsolvability of (15) for $\lambda = -\epsilon_2, -\epsilon_1\epsilon_2$. There remain the two cases $\lambda = 1$, with solution $(P, R, U) = (1, 0, 1)$, and $\lambda = \epsilon_1$, with solution $(P, R, U) = (0, 1, 4 - \alpha^2)$. From (15) and (16) we now have

$$P^2(P^2 + (-5 + \alpha + \alpha^2)R^2)(P^2 + (-5 - 2\alpha + \alpha^2)R^2) = \mu W^2,$$

with $\mu = \lambda\lambda^\sigma = 1$ or $1 + \alpha - \alpha^2$. Accordingly, $X = P^2/R^2$ gives a point on the elliptic curve:

$$X(X + (-5 + \alpha + \alpha^2))(X + (-5 - 2\alpha + \alpha^2)) = \mu Y^2. \quad (17)$$

Now when $\mu = 1$, a relatively straightforward 2-descent argument shows that the $\mathbb{Q}(\alpha)$ -rank of (17) is equal to 0 (we also checked this result using the Pari-GP software of Denis Simon [30]). The torsion group is of order 4, and no non-zero P, Q arise.

When $\mu = 1 + \alpha - \alpha^2$, then $(x, y) = (\frac{\mu}{(1-\alpha)^2} \frac{P^2}{R^2}, \frac{\mu^2}{(1-\alpha)^3} \frac{W}{R^3})$ is a point on the elliptic curve E_2 over $\mathbb{Q}(\alpha)$, where

$$E_2 : y^2 = x(x + (-2 - \alpha + \alpha^2))(x + (-1 + \alpha + \alpha^2)), \quad (18)$$

satisfying $\frac{(1-\alpha)^2}{\mu} x = (4 + \alpha - 2\alpha^2)x \in \mathbb{Q}^2$.

We shall see that the $\mathbb{Q}(\alpha)$ -rank of E_2 is 1, with generator of infinite order equal to $(1, \alpha)$.

2.2.2

Equation (14) may be written in the form

$$\text{Norm}_{L/\mathbb{Q}}(-P^2 + (-5 + \alpha + \alpha^2)R^2) = S^2, \text{ say,}$$

so that

$$-P^2 + (-5 + \alpha + \alpha^2)R^2 = \lambda U^2, \quad (19)$$

with $\lambda \in \mathcal{O}_L$ squarefree and of norm $+1$ modulo L^{*2} . Arguing as in the previous case, λ must be a squarefree unit of norm $+1$, so without loss of generality equal to $1, \epsilon_1, -\epsilon_2, -\epsilon_1\epsilon_2$. Only when $\lambda = \epsilon_1$ is (19) solvable at all the infinite places. Thus

$$-P^2 + (-5 + \alpha + \alpha^2)R^2 = \alpha U^2, \quad -P^2 + (-5 - 2\alpha + \alpha^2)R^2 = (-2 - \alpha + \alpha^2)V^2,$$

and $x = \frac{(1+\alpha-\alpha^2)P^2}{(1-\alpha)^2 R^2}$ is the x -coordinate of a point on the elliptic curve

$$y^2 = x(x + (2 + \alpha - \alpha^2))(x + (1 - \alpha - \alpha^2)). \quad (20)$$

satisfying $\frac{(1-\alpha)^2}{(1+\alpha-\alpha^2)}x = (4 + \alpha - 2\alpha^2)x \in \mathbb{Q}^2$. However, a straightforward calculation shows that the $\mathbb{Q}(\alpha)$ -rank of (20) is equal to 0, with torsion group the obvious group of order 4. There are no corresponding solutions for P, Q .

3 The Mordell-Weil basis

Here we justify our assertions about the elliptic curves E_1 at (9) and E_2 at (18).

3.1 The case U_{12}

First, consider the curve (9). Because $K = \mathbb{Q}(\sqrt{3})$ has unique factorization, and E_1 has K -rational 2-torsion, a two-descent over K works analogously to the standard two-descent over \mathbb{Q} for an elliptic curve with rational two-torsion.

Recall the generalities.

For

$$E : y^2 = x(x^2 + ax + b) \text{ with } a, b \in \mathcal{O}_K,$$

there is the 2-isogenous curve

$$E' : Y^2 = X(X^2 + a'X + b')$$

with $a' = -2a, b' = a^2 - 4b$. A 2-isogeny $\theta : E \rightarrow E'$ is given explicitly by

$$(x, y) \rightarrow \left(\frac{y^2}{x^2}, y \frac{x^2 - b}{x^2} \right),$$

with kernel $\{\mathbf{O}, (0, 0)\}$. The 2-descent homomorphism $\phi : E(K) \rightarrow K^*/K^{*2}$ is defined by

$$\begin{aligned}\phi(\mathbf{O}) &= 1 \bmod K^{*2} \\ \phi((0, 0)) &= b \bmod K^{*2} \\ \phi((x, y)) &= x \bmod K^{*2}, \text{ if } (x, y) \neq \mathbf{O}, (0, 0)\end{aligned}$$

Analogously, define $\phi' : E'(K) \rightarrow K^*/K^{*2}$. Then the rank $r_E = \text{rank}(E(K))$ satisfies

$$2^{r_E} = \frac{|\phi(E(K))| \cdot |\phi'(E'(K))|}{2^2}.$$

Moreover, to compute the order $|\phi(E(K))|$, we have the following: let $S = \{d_1 \in \mathcal{O}_K : b = d_1 d_2, \text{ and } w^2 = d_1 u^4 + a u^2 v^2 + d_2 v^4 \text{ has a non-zero solution } (u, v, w) \in \mathcal{O}_K^3, (u, v) = 1\}$. Then $\phi(E(K))$ is the group generated by the elements of S modulo K^{*2} .

Specific details of the computation for our curve (9) do not present intrinsic difficulty, and full details are available upon request from the authors. The result is that $|\phi(E_1(K))| = 2^2$ and $|\phi(E'_1(K))| = 2$, with final deduction that $\text{rank}(E_1(K)) = 1$.

To prove that $P = (\sqrt{3}, 3\sqrt{3})$ is a generator for the Mordell-Weil group $E_1(K)$ requires several steps. First, we need to compute the canonical height $\hat{h}(P)$, which is done by summing the contributions of the local heights (note that there is disparity in the literature as to definition of local components of heights: we take as definition that of Silverman [27]. Siksek [26] adjusts by a local component of the discriminant). Since $x(P)$ lies in the ring of integers $\mathcal{O}_K = \mathbf{Z}[\sqrt{3}]$ of K , the only valuations of \mathcal{O}_K contributing to $\hat{h}(P)$ are the two Archimedean valuations $|x|_{\infty_1} = |x|$ (ordinary absolute value); $|x|_{\infty_2} = |\bar{x}|$ (absolute value of the conjugate of x); and the non-Archimedean valuations corresponding to the primes above 2 and 3, namely $(1 + \sqrt{3})_2$ and $(\sqrt{3})_3$. The computations are relatively straightforward, with result that $\hat{h}(P) = 0.3507058805\dots$ We checked this computation using the TECC calculator of Kida [20]. As second step, we remark that the descent argument shows that P up to torsion cannot be divisible by 2 in $E_1(K)$. So if P is not a generator, then $P = nQ$, for some point $Q \in E_1(K)$, and $n \geq 3$. Since P has K -integral coordinates, so does Q . Then

$$\hat{h}(Q) = \frac{1}{n^2} \hat{h}(P) \leq \frac{1}{9} \hat{h}(P) < 0.0389673200\dots \quad (21)$$

We can now use standard estimates for the difference between the canonical height $\hat{h}(P)$ and the logarithmic height $h(P)$: using the Silverman [29] bounds we obtain for all $R \in E_1(K)$

$$-7.8324020052\dots \leq 2\hat{h}(R) - h(R) \leq 8.3495215394\dots$$

so that using (21)

$$h(Q) \leq 2\hat{h}(Q) + 7.8324020053 < 7.911.$$

Thus the naive height $H(Q)$ satisfies $H(Q) < \exp(7.911) < 2728$. If $x(Q) \in \mathbf{Z}$ then $|x(Q)| < 2728$; if $x(Q) \notin \mathbf{Z}$, then suppose $x(Q)$ satisfies the minimal polynomial $X^2 + a_1X + a_2$, with $a_1, a_2 \in \mathbf{Z}$. Silverman [28] shows $\max(|a_1|, |a_2|) \leq 2H(Q)^2 < 14883968$. This however determines too large a search area. Instead we have to use the refinements of Siksek [26]. He shows

$$h(P) - 2\hat{h}(P) \leq \frac{1}{[K : \mathbf{Q}]} \left(\sum_{\nu} \mu_{\nu} n_{\nu} \log(\epsilon_{\nu}) \right),$$

with sum over all valuations ν of \mathcal{O}_K . Here, $n_{\nu} = [K_{\nu} : \mathbb{Q}_{\nu}]$ is the local index, μ_{ν} are constants depending upon the reduction type of E_1 at ν (in our example, $\mu_{\nu} = 0$ except for $\mu_{(1+\sqrt{3})} = \mu_{(\sqrt{3})} = \frac{1}{4}$, and $\mu_{\infty_1} = \mu_{\infty_2} = \frac{1}{3}$); and

$$\epsilon_{\nu}^{-1} = \inf_{(X,Y) \in E_1(K_{\nu})} \frac{\max(|f(X)|_{\nu}, |g(X)|_{\nu})}{\max(1, |X|_{\nu})^4}$$

with

$$f(X) = 4X(X - (3 + \sqrt{3}))(X - 4\sqrt{3}), \quad g(X) = (X^2 - 12(1 + \sqrt{3}))^2.$$

(Another discrepancy in notation should be noted, in that Siksek's canonical height is twice the canonical height of Silverman used in this paper). Siksek gives a method for computing the ϵ_{ν} , and putting all the computations together finally shows that

$$h(Q) \leq 2\hat{h}(Q) + 1.7987046450.. < 1.876639286$$

giving

$$H(Q) < 6.53151738.$$

Now we have to test all polynomials of types $x + a$ with $|a| \leq 6$, and $x^2 + a_1x + a_2$ with $\max(|a_1|, |a_2|) < 2 \times 6.53151738^2 \leq 85$; and for those roots x lying in \mathcal{O}_K , determine whether x can be the x -coordinate of $Q \in E_1(K)$. A search finds the following points $(x, \pm y)$, and we observe that each point is generated by $P = (\sqrt{3}, 3\sqrt{3})$, up to torsion:

$$\begin{aligned} (0, 0) &= T_1 \\ (3 + \sqrt{3}, 0) &= T_2 \\ (4\sqrt{3}, 0) &= T_1 + T_2 \\ (\sqrt{3}, 3\sqrt{3}) &= P \\ (3 + 3\sqrt{3}, 6) &= P + T_2 \\ (4, 4 - 4\sqrt{3}) &= P + T_1 + T_2 \\ (12 + 4\sqrt{3}, 36 + 12\sqrt{3}) &= -P - T_1 \end{aligned}$$

In particular, none has height satisfying (21); and so Q cannot exist. Thus $P = (\sqrt{3}, 3\sqrt{3})$ is indeed a generator for $E_1(K)$.

3.2 The case U_9

The computations for the curve (18) are rather similar. Recall $L = \mathbb{Q}(\alpha)$, with ring of integers $\mathcal{O}_L = \mathbb{Z}[\alpha]$. Then with same notation as above, a descent argument shows that $|\phi(E_2(L))| = 2^2$ and $|\phi'(E_2(L))| = 2$, so that $\text{rank}(E_2(L)) = 1$. With $P = (1, \alpha)$, the only valuations of \mathcal{O}_L needing to be considered in determining $\hat{h}(P)$ are at the non-Archimedean valuations (2) and $(1 - \alpha)$, and the three Archimedean valuations corresponding to the three conjugations. We find

$$\hat{h}(P) = 0.1579573296\dots$$

As before, P up to torsion is not divisible by 2; so if P is not a generator, then $P = nQ$, for some point $Q \in E_2(L)$, and $n \geq 3$. Since P has L -integral coordinates, so does Q . Then

$$\hat{h}(Q) = \frac{1}{n^2} \hat{h}(P) \leq \frac{1}{9} \hat{h}(P) < 0.0175508144\dots \quad (22)$$

Again, the Silverman estimates for the difference between canonical and logarithmic height are too weak for our purpose, so we resort to the Siksek estimates. These produce

$$h(Q) \leq 2\hat{h}(Q) + 0.8640466498 < 0.899148279$$

giving

$$H(Q) < 2.45750911.$$

Now we have to test all polynomials of types $x + a$ with $|a| \leq 2$, and $x^3 + a_1x^2 + a_2x + a_3$ with $\max(|a_1|, |a_2|, |a_3|) < 4 \times 2.45751^3 \leq 59$; and for those roots x lying in \mathcal{O}_L , determine whether x can be the x -coordinate of $Q \in E_2(L)$. A search finds the following points $(x, \pm y)$, and we observe that each point is generated by $P = (1, \alpha)$, up to torsion:

$$\begin{aligned} (2 + \alpha - \alpha^2, 0) &= T_1 \\ (1 - \alpha - \alpha^2, 0) &= T_2 \\ (0, 0) &= T_3 \\ (1, \alpha) &= P \\ (1 + \alpha, -2\alpha - \alpha^2) &= P + T_1 \\ (3 - \alpha^2, -3 - \alpha + \alpha^2) &= P + T_2 \\ (2 - \alpha^2, 1 + \alpha) &= P + T_3 \\ (-7 - 17\alpha + 11\alpha^2, -50 - 116\alpha + 76\alpha^2) &= 2P + T_2 \end{aligned}$$

In particular, none has height satisfying (22); and so Q cannot exist. Hence P is the required generator.

4 The formal group method

The problems to which we were led in section 2 are of the following shape.

Problem: Let

$$\mathcal{E} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 , \quad (23)$$

be an elliptic curve defined over $\mathbb{Q}(\alpha)$, where α is a root of a polynomial $f(X) \in \mathbb{Z}[X]$, irreducible over \mathbb{Q} , of degree $d \geq 2$ and $\beta \in \mathbb{Q}(\alpha)$ an algebraic integer. Find all points $(x, y) \in \mathcal{E}(\mathbb{Q}(\alpha))$ for which βx is the square of a *rational number*.

For the solution of this type of problem we assume the existence of a rational prime p with the following properties:

- $f(X)$ is irreducible in $\mathbb{Q}_p[X]$. This implies that p is a prime divisor of the number field $\mathbb{Q}(\alpha)$ and there is only one discrete (normalized) valuation v defined on $\mathbb{Q}(\alpha)$ with $v(p) = 1$. Moreover, the completion of $\mathbb{Q}(\alpha)$ with respect to v is $\mathbb{Q}_p(\alpha)$ and, according to our assumptions, $[\mathbb{Q}_p(\alpha) : \mathbb{Q}_p] = [\mathbb{Q}(\alpha) : \mathbb{Q}] = d$.
- The coefficients of (23) are in $\mathbb{Z}_p[\alpha]$.
- Equation (23) is a *minimal Weierstrass equation* for $\mathcal{E}/\mathbb{Q}_p(\alpha)$ at v .
- $\beta \in \mathbb{Q}_p(\alpha)$ is a p -adic unit.

We use the following notation and facts:

- The ring of integers of $\mathbb{Q}_p(\alpha)$, i.e. the ring $\{x \in \mathbb{Q}_p(\alpha) : v(x) \geq 0\}$, is $\mathbb{Z}_p[\alpha]$.
- The maximal ideal of $\mathbb{Z}_p[\alpha]$ is $p\mathbb{Z}_p[\alpha]$; for simplicity we denote this ideal by \mathcal{M} .
- The natural homomorphism $\mathbb{Z}_p[\alpha] \rightarrow \mathbb{Z}_p[\alpha]/\mathcal{M}$ is denoted by $t \rightarrow \tilde{t}$. The residue field $\mathbb{Z}_p[\alpha]/\mathcal{M}$ is isomorphic to $\mathbb{F}_p(\tilde{\alpha})$.

The curve $\tilde{\mathcal{E}}/\mathbb{F}_p(\tilde{\alpha})$ defined by $y^2 + \tilde{a}_1xy + \tilde{a}_3y = x^3 + \tilde{a}_2x^2 + \tilde{a}_4x + \tilde{a}_6$ is *the reduction of $\mathcal{E} \bmod p$* , possibly a singular curve. Any point $P \in \mathcal{E}(\mathbb{Q}_p(\alpha))$ can be written in projective coordinates $[X_0, Y_0, Z_0]$ with all three coordinates in $\mathbb{Z}_p[\alpha]$ and not all zero. Then $\tilde{P} = [\tilde{X}_0, \tilde{Y}_0, \tilde{Z}_0]$ is a point belonging to $\tilde{\mathcal{E}}(\mathbb{F}_p(\tilde{\alpha}))$. Thus, there is a *reduction map*

$$\mathcal{E}(\mathbb{Q}_p(\alpha)) \ni P \mapsto \tilde{P} \in \tilde{\mathcal{E}}(\mathbb{F}_p(\tilde{\alpha})) .$$

- We set $\mathcal{E}_1(\mathbb{Q}_p(\alpha)) = \{P \in \mathcal{E}(\mathbb{Q}_p(\alpha)) : \tilde{P} = \tilde{O}\}$. This is a subgroup of $\mathcal{E}(\mathbb{Q}_p(\alpha))$.

We work with the *formal group* $\hat{\mathcal{E}}/\mathbb{Z}_p[\alpha]$ associated to $\mathcal{E}/\mathbb{Q}_p(\alpha)$. For this, we need the following model of our elliptic curve

$$w = z^3 + a_1zw + a_2z^2w + a_3w^2 + a_4zw^2 + a_6w^3. \quad (24)$$

The birational transformation between (23) and (24) is

$$\begin{aligned} (x, y) &\mapsto (z, w) = \left(-\frac{x}{y}, -\frac{1}{y}\right) \\ (z, w) &\mapsto (x, y) = \left(\frac{z}{w}, -\frac{1}{w}\right) \end{aligned}$$

With a few obvious exceptions, any point Q of our elliptic curve can be viewed either as a pair $(x(Q), y(Q))$ satisfying equation (23) or as pair $(z(Q), w(Q))$ satisfying equation (24), with the two pairs related by the above birational transformation. We characterize $z(Q)$ as “the z -coordinate of Q ”.

For $z_1, z_2 \in \mathcal{M}$, a “sum” $\mathcal{F}(z_1, z_2)$ is defined² by means of a p -adically convergent power series $\mathcal{F}(z_1, z_2) \in \mathbb{Z}[\alpha][[z_1, z_2]]$ and this operation $(z_1, z_2) \mapsto \mathcal{F}(z_1, z_2)$ makes \mathcal{M} a group denoted $\hat{\mathcal{E}}(\mathcal{M})$. For every integer $r \geq 1$, $\hat{\mathcal{E}}(\mathcal{M}^r)$ is the subgroup of $\hat{\mathcal{E}}(\mathcal{M})$ consisting of the elements of \mathcal{M}^r . There is a group isomorphism³

$$\hat{\mathcal{E}}(\mathcal{M}) \rightarrow \mathcal{E}_1(\mathbb{Q}_p(\alpha)), \quad \text{given by } z \mapsto \begin{cases} \left(\frac{z}{w(z)}, -\frac{1}{w(z)}\right) & \text{if } z \neq 0 \\ \mathcal{O} & \text{if } z = 0 \end{cases} \quad (25)$$

where $w(z)$ is a convergent (in the p -adic sense) power series, formally obtained as follows⁴: Denote the right-hand side of (24) by $F(z, w)$ and define recursively

$$F_1(z, w) = F(z, w), \quad F_{m+1}(z, w) = F_m(z, F(z, w)) \quad \text{for } m \geq 1.$$

Then $w(z) = \lim_{m \rightarrow \infty} F_m(z, 0)$. The inverse map of (25) is⁵ the “ z -coordinate” function restricted to $\mathcal{E}_1(\mathbb{Q}_p(\alpha))$:

$$\mathcal{E}_1(\mathbb{Q}_p(\alpha)) \ni Q \mapsto z(Q) \in \hat{\mathcal{E}}(\mathcal{M}), \quad \text{where } z(Q) = \begin{cases} -\frac{x(Q)}{y(Q)} & \text{if } Q \neq \mathcal{O} \\ 0 & \text{if } Q = \mathcal{O} \end{cases}. \quad (26)$$

The remarkable property of the formal group is

$$z(Q_1 + Q_2) = \mathcal{F}(z(Q_1), z(Q_2)) \quad \text{for any points } Q_1, Q_2 \in \mathcal{E}_1(\mathbb{Q}_p(\alpha)). \quad (27)$$

²See § 1, Chapter IV of [28] for the definition of \mathcal{F} .

³Proposition 2.2, Chapter VII of [28].

⁴See § 1, Chapter IV of [28].

⁵See the proof of Proposition 2.2, Chapter VII of [28].

A *logarithmic* and an *exponential* function are related to the formal group:

The *logarithm* of $\hat{\mathcal{E}}$ is formally defined⁶ by

$$\log t = \int G(0, t)^{-1} dt, \quad \text{where} \quad G(z_1, z_2) = \frac{\partial \mathcal{F}(z_1, z_2)}{\partial z_1}.$$

This is a series of the form⁷ $t + \sum_{k=2}^{\infty} \frac{\lambda_k}{k} t^k$, with $\lambda_k \in \mathbb{Z}_p[\alpha]$ for every k , hence⁸ it converges p -adically for $t \in \mathcal{M} = p\mathbb{Z}_p[\alpha]$.

The *exponential* of $\hat{\mathcal{E}}$ is formally defined⁹ as the unique power series $\exp t \in \mathbb{Q}_p(\alpha)[[t]]$ which satisfies $\log(\exp t) = \exp(\log t) = t$. It is a series of the form¹⁰,

$$\exp t = t + \sum_{k=2}^{\infty} \frac{\epsilon_k}{k!} t^k, \quad (28)$$

with $\epsilon_k \in \mathbb{Z}_p[\alpha]$ for every k , hence¹¹ it converges p -adically for $t \in p^r\mathbb{Z}_p[\alpha]$, with $r = 1$ if $p > 2$ and $r = 2$ if $p = 2$.

Let $\hat{\mathbb{G}}_a(\mathcal{M}^r)$ be the formal additive group, so that, by its definition, “addition” in $\hat{\mathbb{G}}_a(\mathcal{M}^r)$ means usual addition in \mathcal{M}^r . An important fact¹² is that, for $r = 1$ if $p > 2$ and $r = 2$ if $p = 2$, the function

$$\log : \hat{\mathcal{E}}(\mathcal{M}^r) \rightarrow \hat{\mathbb{G}}_a(\mathcal{M}^r) \quad (29)$$

is a group isomorphism, the inverse isomorphism being the function \exp . This means in practice that, if $z_1, z_2 \in p^r\mathbb{Z}_p[\alpha]$, then

$$\log \mathcal{F}(z_1, z_2) = \log z_1 + \log z_2 \quad \text{and} \quad \exp(z_1 + z_2) = \mathcal{F}(\exp z_1, \exp z_2),$$

which, in combination with (27) easily implies the following important fact:

If $z(Q_1), \dots, z(Q_k) \in \hat{\mathcal{E}}(\mathcal{M}^r)$, where $r = 1$ if $p > 2$ and $r = 2$ if $p = 2$, and n_1, \dots, n_k are any integers, then

$$z(n_1 Q_1 + \dots + n_k Q_k) = \exp(n_1 \log z(Q_1) + \dots + n_k \log z(Q_k)). \quad (30)$$

Until the end of this section, the meaning of r will be as above. Suppose that we know a point $Q \in \mathcal{E}(\mathbb{Q}(\alpha)) \cap \mathcal{E}_1(\mathbb{Q}_p(\alpha))$. Then, by (26), $z(Q) \in \hat{\mathcal{E}}(\mathcal{M})$. If $p = 2$,

⁶See § 5 and Proposition 4.2, Chapter IV of [28].

⁷Proposition 5.5, Chapter IV, of [28]

⁸Lemma 6.3(a), Chapter IV of [28]

⁹See § 5, Chapter IV of [28].

¹⁰Proposition 5.5, Chapter IV, of [28]

¹¹Lemma 6.3(b), Chapter IV of [28]

¹²Theorem 6.4, Chapter IV of [28].

suppose something more about Q , namely, that $z(Q) \in \hat{\mathcal{E}}(\mathcal{M}^2)$. Further, assume that, for a certain point $P \in \mathbb{Q}(\alpha) \cap \mathcal{E}(\mathbb{Z}_p[\alpha])$, or for $P = \mathcal{O}$, we want to find all $n \in \mathbb{Z}$ for which $\beta x(P + nQ)$ is a rational number.

(i) Let P be a finite point with coordinates (x_0, y_0) in the model (23). Following § 2 of Flynn & Wetherell [18], we first express the x -coordinate $x(P + R)$, where R is the generic finite point, as a power series in $\mathbb{Z}[\alpha, x_0, y_0][[z(R)]]$:

$$x(P + R) = \xi_0 + \xi_1 z(R) + \xi_2 z(R)^2 + \xi_3 z(R)^3 + \cdots, \quad \xi_i \in \mathbb{Z}[\alpha, x_0, y_0]. \quad (31)$$

Next, by (30), $z(nQ) = \exp(n \log z(Q))$ and by (29), $\log z(Q) \in \mathcal{M}^r$. Write temporarily $\log z(Q) = p^r \lambda$, $\lambda \in \mathbb{Z}_p[\alpha]$ and use (28) to expand $z(nQ)$ as a power series in n :

$$z(nQ) = \exp(n \log z(Q)) = \exp(np^r \lambda) = \lambda p^r n + \sum_{k=2}^{\infty} \frac{\epsilon_k \lambda^k}{k!} p^{rk} n^k.$$

In view of the estimation $v(k!) < k/(p-1)$, we easily see that the above series has the following property:

$$v(\text{coefficient of } n^k) \geq \begin{cases} \left\lfloor \frac{(p-2)k}{p-1} \right\rfloor + 1 & \text{if } p \geq 3 \\ k + 1 & \text{if } p = 2 \end{cases} \quad (32)$$

Therefore, if we write $z(nQ) = Z_0(n) + Z_1(n)\alpha + \cdots + Z_{d-1}(n)\alpha^{d-1}$, where $Z_i(n) \in \mathbb{Z}[\alpha, x_0, y_0][[n]]$ for $i = 0, 1, \dots, d-1$, then every series $Z_i(n)$ also has property (32). Consequently, if we substitute in (31) the above expression of $z(nQ)$ for $z(R)$ and multiply by the p -adic unit β , we immediately see that we can write

$$\beta x(P + nQ) = \theta_0(n) + \theta_1(n)\alpha + \cdots + \theta_{d-1}(n)\alpha^{d-1}, \quad (33)$$

where each series $\theta_i(n)$ is a power series in n with coefficients in \mathbb{Z}_p having also the property (32). Since we have assumed that the left-hand side is a rational number, we must have $\theta_i(n) = 0$ for $i = 1, \dots, d-1$. At this point we use the following useful result¹³:

Theorem 4.1. (Strassman) *Let $\theta(Z) = c_0 + c_1 Z + c_2 Z^2 + \cdots \in \mathbb{Z}_p[[Z]]$ with $\lim_{k \rightarrow +\infty} v(c_k) \rightarrow +\infty$ and let $k_0 \geq 0$ be the unique index such that $v(c_{k_0}) < v(c_k)$ for every $k > k_0$ and $v(c_{k_0}) \leq v(c_k)$ for every $k \geq 0$. Then there are at most k_0 elements $z \in \mathbb{Z}_p$ satisfying $\theta(z) = 0$.*

Provided that the assumptions of Strassman's Theorem are satisfied, we have at our disposal a tool to restrict all possible n for which $\beta x(P + nQ) \in \mathbb{Q}$.

¹³Theorem 4.1, in [8].

(ii) Next, let $P = \mathcal{O}$. Now, we want to find all $n \in \mathbb{Z}$, such that $\beta x(nQ) \in \mathbb{Q}$. Following section 2 of Flynn & Wetherell [18], instead of $\beta x(nQ)$, we rather consider $1/(\beta x(nQ))$, simply because

$$\frac{1}{x(nQ)} = \frac{w(z(nQ))}{z(nQ)},$$

(see immediately after (25) for the definition of $w(z)$). Now $w(z)/z$ is a power-series in $\mathbb{Z}[a_1, a_2, a_3, a_4, a_6][[z]]$ and, actually,

$$\frac{w(z)}{z} = \zeta_2 z^2 + \zeta_4 z^4 + \zeta_6 z^6 + \dots, \quad \zeta_{2i} \in \mathbb{Z}[\alpha]. \quad (34)$$

On the other hand, as we saw in case (i) above, $z(nQ) = Z_0(n) + Z_1(n)\alpha + \dots + Z_{d-1}(n)\alpha^{d-1}$, where $Z_i(n) \in \mathbb{Z}[\alpha, x_0, y_0][[n]]$ for $i = 0, 1, \dots, d-1$ and every series $Z_i(n)$ has property (32). Substituting $z(nQ)$ for z in (34) we obtain, exactly as in (i),

$$\frac{1}{\beta x(nQ)} = \theta_0(n) + \theta_1(n)\alpha + \dots + \theta_{d-1}(n)\alpha^{d-1}, \quad (35)$$

where each series $\theta_i(n)$ is a power series in n with coefficients in \mathbb{Z}_p (remember that β is a p -adic unit), having property (32). Again, if the assumptions of Strassman's Theorem are fulfilled, we can restrict the possible values of n for which the left-hand side is a rational number.

Two remarks on Strassman's Theorem. (i) If we *actually know* k_0 distinct solutions $z \in \mathbb{Z}_p$ of $\theta(z) = 0$, then we know *all solutions* of $\theta(z) = 0$ in p -adic integers.

(ii) Two trivial, but useful and often occurring, instances of Strassman's Theorem are the following: (a) $k_0 = 0$, $v(c_0) = 0$ and $v(c_k) > 0$ for every $k \geq 1$. Obviously, in this case, $\theta(z) = 0$ has no solution in p -adic integers. (b) $c_k = 0$ for $k = 0, \dots, k_0 - 1$ and $v(c_k) > v(c_{k_0})$ for $k > k_0$. In this case, one obvious solution is $z = 0$. Dividing out both sides of $\theta(z) = 0$ by z^{k_0} reduces the equation to one falling in case (a), hence insoluble. Thus, in case (b), $z = 0$ is the only solution of $\theta(z) = 0$ in p -adic integers.

5 The solution of the genus 2 equations

5.1 Genus 2 equation resulting from $U_{12} = \square$

For this section, let $\alpha = \sqrt{3}$. According to the discussion in section 2.1, it suffices to find all points (x, y) in $\mathcal{E}(\mathbb{Q}(\alpha))$, where

$$\mathcal{E} : y^2 = x^3 - (3 + 5\alpha)x^2 + 12(1 + \alpha)x, \quad (36)$$

such that $\beta x = u^2 \in \mathbb{Q}^2$, where $\beta = (3 - \alpha)/24$.

We shall work p -adically with $p = 7$, specializing accordingly the notation, assumptions and results of section 4. All assumptions of section 4 before equation (24) are fulfilled. According to section 3.1, any point on $\mathcal{E}(\mathbb{Q}(\alpha))$ is of the form $n_1 P_1 + T$, where

$$P_1 = (\alpha, 3\alpha) \text{ and } T \in \{\mathcal{O}, (0, 0), (4\alpha, 0), (3 + \alpha, 0)\}. \quad (37)$$

The point $Q = 11P_1$ belongs to $\mathcal{E}_1(\mathbb{Q}_7(\alpha))$ and

$$z(Q) = 7 \cdot 37864420 + 7 \cdot 34884700\alpha + O(7^{12}) \in \mathcal{M}.$$

Any point of $\mathcal{E}(\mathbb{Q}(\alpha))$ can therefore be written in the form

$$n_1 P_1 + T = (11n + r)P_1 + T = nQ + P, \quad (38)$$

with $P = rP_1 + T$, $-5 \leq r \leq 5$ and T a torsion point as in (37).

The ‘‘addition law’’ $\mathcal{F}(z_1, z_2)$ is given by

$$\begin{aligned} \mathcal{F}(z_1, z_2) = & z_1 + z_2 + (3 + 5\alpha)z_1 z_2^2 + (3 + 5\alpha)z_1^2 z_2 - 24(1 + \alpha)z_1 z_2^4 \\ & + 18(2 - \alpha)z_1^2 z_2^3 + 18(2 - \alpha)z_1^3 z_2^2 - 24(1 + \alpha)z_1^4 z_2 + \dots \end{aligned}$$

and the series $w(z)$ mentioned immediately after (25) is

$$w(z) = z^3 - (3 + 5\alpha)z^5 + (96 + 42\alpha)z^7 - (1350 + 798\alpha)z^9 + O(z^{11}).$$

The logarithmic and exponential series are

$$\begin{aligned} \log t = & t - (1 + \frac{5}{3}\alpha)t^3 + (\frac{108}{5} + \frac{54}{5}\alpha)t^5 \\ & - (\frac{1998}{7} + \frac{1086}{7}\alpha)t^7 + (4252 + 2576\alpha)t^9 + O(t^{11}) \\ \exp t = & t + (1 + \frac{5}{3}\alpha)t^3 + (\frac{32}{5} - \frac{4}{5}\alpha)t^5 \\ & + (-\frac{258}{35} + \frac{778}{105}\alpha)t^7 + (\frac{1351436}{315} + \frac{806272}{315}\alpha)t^9 + O(t^{11}) \end{aligned}$$

For any finite points $P = (x_0, y_0)$ and R , following section 2 of Flynn & Wetherell [18], we express $x(P + R)$ as a power series of $z(R)$ with coefficients in $\mathbb{Z}[\alpha, x_0, y_0]$, as follows:

$$\begin{aligned} x(P + R) = & x_0 + 2y_0 z(R) + (12 - 6x_0 + 3x_0^2 + 12\alpha - 10x_0\alpha)z(R)^2 \\ & + (-6y_0 + 4x_0y_0 - 10y_0\alpha)z(R)^3 \\ & + (4x_0^3 - 18x_0^2 + 192x_0y_0^2 - 216 - 30\alpha x_0^2 + 84x_0\alpha - 96\alpha)z(R)^4 \\ & + (-24y_0x_0 + 6y_0x_0^2 + 192y_0 + 84y_0\alpha - 40y_0x_0\alpha)z(R)^5 + O(z(R)^6) \end{aligned} \quad (39)$$

Again following section 2 of Flynn & Wetherell [18], we also express $1/x(R)$ as a power series of $z(R)$ with coefficients in $\mathbb{Z}[\alpha, x_0, y_0]$, as follows:

$$\begin{aligned} \frac{1}{x(R)} = & z(R)^2 - (3 + 5\alpha)z(R)^4 + (96 + 42\alpha)z(R)^6 - (1350 + 798\alpha)z(R)^8 \\ & + (23436 + 13824\alpha)z(R)^{10} + O(z^{12}). \end{aligned} \quad (40)$$

We have the 7-adic expansion

$$\log z(Q) = 7 \cdot 35764917 + 7 \cdot 10549438\alpha + O(7^{10})$$

and, for any integer n ,

$$\begin{aligned} z(nQ) = & 7 \cdot 35764917n + 7^4 \cdot 72313n^3 + 7^5 \cdot 1380n^5 + 7^6 \cdot 1931n^7 + 7^8 \cdot 27n^9 + \dots \\ & + (7 \cdot 10549438n + 7^3 \cdot 134528n^3 + 7^5 \cdot 8706n^5 + 7^6 \cdot 57n^7 + 7^8 \cdot 44n^9 + \dots)\alpha \\ & + O(7^{10}) \end{aligned} \quad (41)$$

We refer now to (38). There are 44 possibilities for P , one of which is $P = \mathcal{O}$.

(i) Consider first the case when $P = (x_0, y_0)$ is one out of the 43 possible finite points. In (39) we substitute $z(R)$ by $z(nQ)$ given in (41) and multiply both sides by β . This gives an expression for $\beta x(P + nQ)$, as in (33). In 35 out of the 43 cases, it turns out that $\theta_1(0) \not\equiv 0 \pmod{7}$, which, in particular, implies that $\theta_1(n) \neq 0$, hence $\beta x(P + nQ) = \theta_0(n) + \theta_1(n)\alpha$ cannot be rational. The only cases that are not excluded in this way correspond to

$$P \in \{\pm 4P_1 + (0, 0), \pm 3P_1 + (0, 0), \pm P_1 + (0, 0), (0, 0), (3 + \alpha, 0)\}.$$

We deal with these cases as follows, always remembering that the power series $\theta_0(n)$ and $\theta_1(n)$ satisfy property (32), hence, in particular, $\theta_i(n) \equiv \theta_i(0) \pmod{7}$: If $P = \pm 4P_1 + (0, 0)$, then $\theta_0(0) = 5$, a quadratic non-residue of 7; therefore, whatever n may be, $\beta x(P + nQ) = \theta_0(n) + \theta_1(n)\alpha$ cannot be the square of a rational number. In a completely analogous manner we exclude $P = \pm 3P_1 + (0, 0)$, since, in this case, $\theta_0(0) = 6$.

Next, consider $P = \pm P_1 + (0, 0) = (12 + 4\alpha, \pm(36 + 12\alpha))$. With the plus sign we compute $\theta_1(n) = 7 \cdot 94n + 7^2 \cdot 40n^2 + 7^3 \cdot 6n^3 + \dots$, and with the minus sign, $\theta_1(n) = 7 \cdot 249n + 7^2 \cdot 40n^2 + 7^3 n^3 + \dots$. In both cases, if $n \neq 0$, then dividing out by $7n$ we are led to an impossible relation mod 7; hence $n = 0$ and $x = x(P + nQ) = x(P) = 12 + 4\alpha$, which gives $u^2 = \beta(12 + 4\alpha) = 1$ and $u = 1$. If $P = (0, 0)$, then we compute $\theta_1(n) = 7^3 \cdot 6889n^2 + 7^4 \cdot 1733n^4 + 7^7 \cdot 2n^6 + 7^7 \cdot 5n^8 + \dots$ and if $n \neq 0$ we divide out by $7^3 n$ and we are led to an impossible relation mod 7. Thus, $n = 0$, which leads to $x = 0$ and $u = 0$. Finally, if $P = (3 + \alpha, 0)$, then $\theta_1(n) = 7^2 \cdot 288n^2 + 7^4 n^4 + \dots$, forcing again $n = 0$. Thus, $x = 3 + \alpha$ and $u^2 = \beta(3 + \alpha) = 1/4$, hence $u = 1/2$.

(ii) Assume now that $P = \mathcal{O}$. For $R = nQ$, we obtain by means of (40) and (41) a power series of the form (35), in which $\theta_1(n) = 7^2 \cdot 244n^2 + 7^4 \cdot 2n^4 + \dots$.

Since we are interested in finite points $(x, y) = nQ$, n must be non-zero. Moreover, $\theta_1(n)$ has property (32) and must be zero. Therefore, dividing out $\theta_1(n) = 0$ by $7^2 n^2$ we obtain an impossible equality.

Conclusion. The only points on (9) satisfying $\beta x = u^2 \in \mathbb{Q}^2$ are those with $x = 12 + 4\alpha, 3 + \alpha, 0$, corresponding to $u = 1, \frac{1}{2}, 0$. Only the first leads to a solution of (8) and this leads to the solution $(P, Q) = (1, -1)$ of (3) with $U_{12}(1, -1) = 12^2$.

5.2 Genus 2 equation resulting from $U_9 = \square$

According to the discussion in section 2.2.1, it suffices to find all points (x, y) in $\mathcal{E}(\mathbb{Q}(\alpha))$, where

$$\mathcal{E} : y^2 = x^3 + (-3 + 2\alpha^2)x^2 + (2 - \alpha^2)x, \quad (42)$$

such that $\beta x \in \mathbb{Q}^2$, where $\beta = 4 + \alpha - 2\alpha^2$. We shall work p -adically with $p = 2$, specializing accordingly the notation, assumptions and results of section 4. All assumptions of section 4 before equation (24) are fulfilled. According to section 3.2, any point on $\mathcal{E}(\mathbb{Q}(\alpha))$ is of the form $n_1 P_1 + T$, where

$$P_1 = (1, \alpha) \text{ and } T \in \{\mathcal{O}, (1 - \alpha - \alpha^2, 0), (0, 0), (2 + \alpha - \alpha^2, 0)\}. \quad (43)$$

The point

$$Q = 4P_1 = \left(\frac{73}{48} - \frac{47}{16}\alpha + \frac{49}{24}\alpha^2, -\frac{97}{32} - \frac{2323}{192}\alpha + \frac{29}{3}\alpha^2 \right)$$

belongs to $\mathcal{E}_1(\mathbb{Q}_2(\alpha))$ and

$$z(Q) = -\frac{3592928}{2800223} - \frac{404928}{2800223}\alpha + \frac{928628}{2800223}\alpha^2 \in \mathcal{M}^2.$$

Any point of $\mathcal{E}(\mathbb{Q}(\alpha))$ can therefore be written in the form

$$n_1 P_1 + T = (4n + r)P_1 + T = nQ + P, \quad (44)$$

with $P = rP_1 + T$, $r \in \{-1, 0, 1, 2\}$ and T a torsion point as in (43).

The ‘‘addition law’’ $\mathcal{F}(z_1, z_2)$ is given by

$$\begin{aligned} \mathcal{F}(z_1, z_2) = & z_1 + z_2 + (3 - 2\alpha^2)z_1 z_2^2 + (3 - 2\alpha^2)z_1^2 z_2 \\ & (-4 + 2\alpha^2)z_1 z_2^4 + (1 + 4\alpha + 4\alpha^2)z_1^2 z_2^3 \\ & + (1 + 4\alpha + 4\alpha^2)z_1^3 z_2^2 + (-4 + 2\alpha^2)z_1^4 z_2 + \dots \end{aligned}$$

and the series $w(z)$ mentioned immediately after (25) is

$$w(z) = z^3 + (-3 + 2\alpha^2)z^5 + (11 + 4\alpha - \alpha^2)z^7 + (-37 + 6\alpha + 21\alpha^2)z^9 + O(z^{11}).$$

The logarithmic and exponential series are

$$\begin{aligned}\log t &= t + \left(-1 + \frac{2}{3}\alpha^2\right)t^3 + \left(\frac{13}{5} + \frac{4}{5}\alpha - \frac{2}{5}\alpha^2\right)t^5 \\ &\quad + \left(-\frac{55}{7} + \frac{24}{7}\alpha^2\right)t^7 + \left(\frac{91}{3} + \frac{10}{3}\alpha - \frac{98}{9}\alpha^2\right)t^9 + O(t^{11}) \\ \exp t &= t + \left(1 - \frac{2}{3}\alpha^2\right)t^3 + \left(\frac{2}{5} + \frac{8}{15}\alpha + \frac{2}{5}\alpha^2\right)t^5 \\ &\quad + \left(-\frac{73}{315} - \frac{16}{15}\alpha - \frac{16}{21}\alpha^2\right)t^7 + \left(\frac{9749}{315} + \frac{116}{21}\alpha - \frac{27178}{2835}\alpha^2\right)t^9 + O(t^{11})\end{aligned}$$

For any finite points $P = (x_0, y_0)$ and R , following section 2 of [18], we express $x(P + R)$ as a power series in $z(R)$ with coefficients in $\mathbb{Z}[\alpha, x_0, y_0]$, as follows:

$$\begin{aligned}x(P + R) &= x_0 + 2y_0z(R) + [3x_0^2 - 6x_0 + 2 + (4x_0 - 1)\alpha^2]z(R)^2 \\ &\quad + (4y_0x_0 - 6y_0 + 4y_0\alpha^2)z(R)^3 \\ &\quad + [(4x_0^3 - 18x_0^2 + 22x_0 - 6 + y_0^2) + (8x_0 - 2)\alpha + (12x_0^2 - 2x_0 + 1)\alpha^2]z(R)^4 \\ &\quad + [(6y_0x_0^2 - 24y_0x_0 + 22y_0) + 8y_0\alpha + (16y_0x_0 - 2y_0)\alpha^2]z(R)^5 + O(z(R)^6)\end{aligned}\tag{45}$$

Again following section 2 of [18], we also express $1/x(R)$ as a power series of $z(R)$ with coefficients in $\mathbb{Z}[\alpha, x_0, y_0]$, as follows:

$$\begin{aligned}\frac{1}{x(R)} &= z^2 + (-3 + 2\alpha^2)z^4 + (11 + 4\alpha - \alpha^2)z^6 \\ &\quad + (-37 + 6\alpha + 21\alpha^2)z^8 + (173 + 50\alpha - 40\alpha^2)z^{10} + O(z^{12}).\end{aligned}\tag{46}$$

We have the 2-adic expansion

$$\log z(Q) = 3872 + 1216\alpha + 3148\alpha^2 + O(2^{12})$$

and, for any integer n ,

$$\begin{aligned}z(nQ) &= \exp(n \log z(Q)) \\ &= (2^5 \cdot 121n + 2^6 \cdot 31n^3 + \dots) + (2^6 \cdot 19n + 2^8 n^3 + \dots)\alpha \\ &\quad + (2^2 \cdot 787n + 2^6 \cdot 51n^3 + 2^{11}n^5 + \dots)\alpha^2 + O(2^{12}).\end{aligned}\tag{47}$$

We refer now to (44). There are 16 possibilities for P , one of which is $P = \mathcal{O}$.

(i) Consider first the case when $P = (x_0, y_0)$ is one out of the 15 possible finite points. In (45) we substitute $z(R)$ by $z(nQ)$ given in (47) and multiply both sides by β . This gives an expression for $\beta x(P + nQ)$, as in (33). In most cases, it can be easily seen that the right-hand side of such an expression cannot be rational. Take, for example, $P = -P_1 + T$, with $T = (1 - \alpha - \alpha^2, 0)$. Then $(x_0, y_0) = (3 - \alpha^2, 3 + \alpha - \alpha^2)$. We compute $\theta_1(n) \equiv 2 + 2^3 \cdot 7n + \dots \pmod{2^3\mathbb{Z}[[n]]}$. Since every series $\theta_i(n)$ has the property (32), we see that $\theta_1(n) \equiv 2 \pmod{8}$ and, therefore, by remark

(ii.a) after Theorem 4.1, cannot be zero. An example of a more “difficult” instance is $P = (0, 0)$. Now we need a somewhat higher 2-adic precision. We compute $\theta_1(n) \equiv 2^6 \cdot 5n^2 + 0 \cdot n^3 + 0 \cdot n^4 + 0 \cdot n^5 + \dots \pmod{2^7\mathbb{Z}[[n]]}$, and the remaining terms are divisible at least by 2^7 , in view of the fact that $\theta_1(n)$ has property (32). Hence, by remark (ii.b) after Theorem 4.1, the only possible solution is $n = 0$, implying the actual solution $(x, y) = (0, 0)$. A third characteristic example is $P = 2P_1 + T$, with $T = (0, 0)$. Then $(x_0, y_0) = (\frac{4}{3}(1 - \alpha^2), -\frac{2}{3}(\alpha + \alpha^2))$ and we compute $\theta_1(n) \equiv 2^6 \cdot 7n + 2^6 \cdot 3n^2 + 0 \cdot n^3 + 0 \cdot n^4 + 0 \cdot n^5 + \dots \pmod{2^7\mathbb{Z}[[n]]}$ and, as always, property (32) holds. In the notation of Strassman’s Theorem, $k_0 = 2$, so that there are at most two solutions. On the other hand, a straightforward computation shows that $\beta x(P + 0 \cdot Q) = 4 = \beta x(P - Q)$, which implies, in particular, that $\theta_1(0) = 0 = \theta_1(-1)$; hence, by remark (i) after Theorem 4.1, $n = 0, -1$ are the only solutions obtained for the above specific value of (x_0, y_0) . Testing in a similar way one by one the 15 possible finite points (x_0, y_0) , we obtain only the solutions $(x, y) = (0, 0), (\frac{4}{3}(1 - \alpha^2), \pm\frac{2}{3}(\alpha + \alpha^2))$ for (42) with the property $\beta x \in \mathbb{Q}^2$. These solutions imply, respectively, $P^2/R^2 = 0, 4$, hence $R = 1$ and $P = 0$ or ± 2 .

(ii) Assume now that $P = \mathcal{O}$. For $R = nQ$, we obtain by means of (46) and (47) a power series of the form (35), in which $\theta_1(n) = 2^4n^2 + 0 \cdot n^4 + \dots \pmod{2^6\mathbb{Z}[[n]]}$. Since we are interested in finite points $(x, y) = nQ$, n must be non-zero. Moreover, $\theta_1(n)$ has property (32) and must be zero. Therefore, dividing out $\theta_1(n) = 0$ by 2^4n^2 we obtain an impossible relation.

Conclusion. The only points on (18) satisfying $\beta x \in \mathbb{Q}^2$ are those with $x = 0$ (leading to $P = 0$), and $x = \frac{4}{3}(1 - \alpha^2)$ giving successively (in the notation of section 2.2.1) $\frac{P^2}{R^2} = 4$ and $(P, Q) = (\pm 2, 1)$, corresponding to degenerate Lucas sequences.

References

- [1] N. BRUIN, *Chabauty methods and covering techniques applied to generalized Fermat equations*, CWI Tract, vol. 133, Stichting Mathematisch Centrum voor Wiskunde en Informatica, Amsterdam, 2002, Dissertation, University of Leiden, Leiden 1999.
- [2] N. BRUIN, The diophantine equations $x^2 \pm y^4 = \pm z^6$ and $x^2 + y^8 = z^3$, *Compositio Math.* **118** (1999), 305-321.
- [3] N. BRUIN, Chabauty methods using elliptic curves, *J. reine angew. Math.* **562** (2003), 27-49.
- [4] N. BRUIN and E.V. FLYNN, Towers of 2-covers of hyperelliptic curves, *Pacific Institute Math. Sci.*, preprint PIMS-01-12 (2001).

- [5] N. BRUIN and E.V. FLYNN, N -covers of hyperelliptic curves, *Math. Proc. Camb. Phil. Soc.* **134** (2003), 397-405.
- [6] N. BRUIN, <http://www.cecm.sfu.ca/~bruin/ell.shar>
- [7] N. BRUIN, <http://www.cecm.sfu.ca/~bruin/malgaie.tgz>
- [8] J.W.S. CASSELS, *Local Fields*, LMS Student Texts **3**, Cambridge University Press, Cambridge and London 1986.
- [9] J.W.S. CASSELS and E.V. FLYNN, *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2* LMS Lecture Note Series **230**, Cambridge University Press, Cambridge 1996.
- [10] C. CHABAUTY, Sur les points rationnels des courbes algébriques de genre supérieur à l'unité, *C. R. Acad. Sci. Paris* **212** (1941), 882-885.
- [11] J.H.E. COHN, On square Fibonacci numbers, *J. London Math. Soc.* **39** (1964), 537-541.
- [12] J.H.E. COHN, Eight Diophantine equations, *Proc. London Math. Soc.* **16** (1966), 153-166.
- [13] J.H.E. COHN, Five Diophantine equations, *Math. Scand.* **21** (1967), 61-70.
- [14] J.H.E. COHN, Squares in some recurrent sequences, *Pacific J. Math.* **41** (1972), 631-646.
- [15] R.F. COLEMAN, Effective Chabauty, *Duke Math. J.* **52** (1985), 765-770 .
- [16] E.V. FLYNN, A flexible method for applying Chabauty's Theorem, *Compositio Math.* **105** (1997), 79-94.
- [17] E.V. FLYNN, On Q -Derived Polynomials, *Proc. Edinburgh Math. Soc.* **44** (2001), 103-110.
- [18] E.V. FLYNN and J.L. WETHERELL, Finding rational points on bielliptic genus 2 curves, *Manuscripta Math.* **100** (1999), 519-533.
- [19] E.V. FLYNN and J.L. WETHERELL, Covering Collections and a Challenge Problem of Serre, *Acta Arithm.* **98** (2001), 197-205.
- [20] M. KIDA, *TECC manual version 2.4*, The University of Electro-Communications, September 2000.
- [21] W. LJUNGGREN, *New propositions about the indeterminate equation $(x^n - 1)/(x - 1) = y^q$* , *Norske Mat. Tidsskrift*, **25**, 1943, 17-20.

- [22] P. RIBENBOIM and W.L. MCDANIEL, *The square terms in Lucas sequences*, J. Number Theory, **58**, 1996, 104-123.
- [23] P. RIBENBOIM and W.L. MCDANIEL, *Squares in Lucas sequences having an even first parameter*, Colloq. Math., **78**, 1998, 29-34.
- [24] N. ROBBINS, *On Pell numbers of the form PX^2 , where P is prime*, Fibonacci Quart. (4), 1984, 340-348.
- [25] T.N. SHOREY and R. TIJDEMAN, *Exponential Diophantine Equations*, Cambridge Univ. Press, Cambridge, 1986.
- [26] S. SIKSEK, *Infinite descent on elliptic curves*, Rocky Mountain J. Math., Vol. 25, No. 4, 1995, 1501-1538
- [27] J.H. SILVERMAN, *Computing heights on elliptic curves*, Math. Comp. 51 (1988), no. 183, 339-358.
- [28] J.H. SILVERMAN, *The Arithmetic of Elliptic Curves*, Graduate Texts in Math., vol. 106, Springer-Verlag, Berlin and New York, 1986.
- [29] J.H. SILVERMAN, *The difference between the Weil height and the canonical height on elliptic curves*, Math. Comp. 55 (1990), no. 192, 723-743.
- [30] D. SIMON, <http://www.math.unicaen.fr/~simon/ell.gp>
- [31] J.L. WETHERELL, *Bounding the number of rational points on certain curves of high rank*, Ph.D. Dissertation, University of California at Berkeley, 1997.