On squares in Lucas sequences

A. Bremner* N. Tzanakis†

July 5, 2006

Abstract

Let P and Q be non-zero integers. The Lucas sequence $\{U_n(P,Q)\}$ is defined by $U_0 = 0, \quad U_1 = 1, \quad U_n = PU_{n-1} - QU_{n-2} \quad (n \geq 2)$. The question of when $U_n(P,Q)$ can be a perfect square has generated interest in the literature. We show that for $n = 2, ..., 7$, U_n is a square for infinitely many pairs (P,Q) with $\gcd(P,Q) = 1$; further, for $n = 8, ..., 12$, the only non-degenerate sequences where $\gcd(P,Q) = 1$ and $U_n(P,Q) = \square$, are given by $U_8(1,-4) = 21^2$, $U_8(4,-17) = 620^2$, and $U_{12}(1,-1) = 12^2$.

Keywords: Lucas sequence, squares, genus two curves

1 Introduction

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

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

The sequence $\{U_n(1,-1)\}$ is the familiar Fibonacci sequence, and it was proved by Cohn [6] 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? In what follows, we shall assume that we are not dealing with the degenerate sequences corresponding to $(P,Q) = (\pm 1, 1)$, where U_n is periodic with period 3, and we also assume $(P,Q) \neq (-2,1)$ (in which case $U_n = \square$ precisely when n is an odd square) and $(P,Q) \neq (2,1)$ (when $U_n = \square$ precisely when n is square). Ribenboim and McDaniel [10] 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

[*] Department of Mathematics, Arizona State University, Tempe AZ, USA, e-mail: bremner@asu.edu, http://˜andrew/bremner.html

[†] Department of Mathematics, University of Crete, Iraklion, Greece, e-mail: tzanakis@math.uoc.gr , http://www.math.uoc.gr/˜tzanakis

for which U_n can be square. They characterize fully the instances when $U_n = \Box$, for $n = 2, 3, 6$. Bremner & Tzanakis [1] extend these results by determining all Lucas sequences $\{U_n(P,Q)\}$ with $U_{12} = \Box$, subject only to the restriction that $\gcd(P,Q) = 1$ (it turns out that the Fibonacci sequence provides the only example). Under the same hypothesis, all Lucas sequences with $\{U_n(P,Q)\}$ with $U_9 = \Box$ are determined. There seems little mention in the literature of when under general hypotheses $U_n(P,Q)$ can be a perfect square. It is straightforward to see from Theorem 1 of Darmon and Granville [7] that for n sufficiently large ($n \geq 11$ certainly suffices), the equation $U_n(P,Q) = \Box$ can have only finitely many solutions for coprime P, Q. Note that for $n \geq 1$, $U_n(kP, k^2Q) = k^{n-1}U_n(P,Q)$, and so for fixed P, Q, and *even* n, appropriate choice of k gives a sequence with $U_n(kP, k^2Q)$ a perfect square. The restriction to $\gcd(P,Q) = 1$ is therefore a sensible one, and we shall assume this from now on. Rather curiously, a small computer search reveals sequences with $U_n(P,Q)$ a perfect square only for $n = 0, \ldots, 8$, and $n = 12$. In this paper, we shall dispose of this range of n. Bremner & Tzanakis [1] have addressed the cases $n = 9, 12$. Section 2 of this paper addresses the case $U_n(P,Q) = \Box$, $n \leq 7$, which can be treated entirely elementarily. Section 3 addresses the cases $U_n(P,Q) = \Box$, $8 \leq n \leq 11$. In these instances, we deduce a finite collection of curves, whose rational points cover all required solutions. In turn, this reduces to a number of problems of similar type, namely, finding all points on an elliptic curve defined over a number field K subject to a "$\mathbb{Q}$-rationality" condition on the X-coordinate. Nils Bruin has powerful techniques for addressing this type of problem, and [2], [3], [4], [5] provide details and examples. See in particular §4 of [5] for development of the underlying mathematics. The latest release of Magma [9] now contains Bruin's routines and so we only set up the appropriate computation here, with details of the Magma programs available on request.

The results of Sections 2, 3, when combined with the results of Bremner & Tzanakis [1] give the following theorem:

Theorem 1. *Let P, Q be non-zero coprime integers such that if $Q = 1$ then $P \neq \pm 1, \pm 2$ (that is, P, Q determine a non-degenerate Lucas sequence). Then (i) for $n = 2, ..., 7$, $U_n(P,Q)$ is a square for infinitely many such pairs (P,Q), and (ii) for $n = 8, ..., 12$, the only solutions of $U_n(P,Q) = \Box$ are given by $U_8(1,-4) = 21^2$, $U_8(4,-17) = 620^2$, and $U_{12}(1,-1) = 12^2$.*

2 Solution of $U_n(P,Q) = \Box$, $n \leq 7$

Certainly $U_2(P,Q) = \Box$ if and only if $P = a^2$, and $U_3(P,Q) = \Box$ if and only if $P^2 - Q = a^2$.

Now $U_4(P,Q) = \Box$ if and only if $P(P^2 - 2Q) = \Box$, so if and only if either $P = \delta a^2, Q = \frac{1}{2}(a^4 - \delta b^2)$, or $P = 2\delta a^2, Q = 2a^4 - \delta b^2$, with $\delta = \pm 1$ (where, in

the first instance, ab is odd and in the second instance b is odd).
The demand that $U_5(P,Q)$ be square is that $P^4 - 3P^2Q + Q^2 = \Box$, equivalently, that $1 - 3x + x^2 = \Box$, where $x = Q/P^2$. Parametrizing the quadric, $Q/P^2 = (5\lambda^2 + 6\lambda\mu + \mu^2)/(4\lambda\mu)$, where, without loss of generality, $(\lambda,\mu) = 1$, $\lambda > 0$, and $\mu \not\equiv 0 \pmod 5$. Necessarily $(\lambda,\mu) = (a^2, \pm b^2)$, giving $(P,Q) = (2ab, 5a^4 + 6a^2b^2 + b^4)$ or $(2ab, -5a^4 + 6a^2b^2 - b^4)$ if a and b are of opposite parity, and $(P,Q) = (ab, \frac{1}{4}(5a^4 + 6a^2b^2 + b^4))$ or $(ab, \frac{1}{4}(-5a^4 + 6a^2b^2 - b^4))$, if a and b are both odd.
The demand that $U_6(P,Q)$ be square is that $P(P^2 - Q)(P^2 - 3Q) = \Box$, which leads to one of seven cases: $P = a^2$, $P^2 - Q = b^2$, with $-2a^4 + 3b^2 = \Box$; $P = a^2$, $P^2 - Q = -2b^2$, with $a^4 + 3b^2 = \Box$; $P = -a^2$, $P^2 - Q = 2b^2$, with $a^4 - 3b^2 = \Box$; and $P = 3a^2$, $P^2 - Q = \delta b^2$, $(\delta = \pm 1, \pm 2)$, with $-\frac{6}{\delta}a^4 + b^2 = \Box$. So finitely many parametrizations result (which can easily be obtained if we wish to do so).
The demand that $U_7(P,Q)$ be square is that $P^6 - 5P^4Q + 6P^2Q^2 - Q^3 = \Box$, equivalently, that $1 + 5x + 6x^2 + x^3 = y^2$, where $x = -Q/P^2$. This latter elliptic curve has rank 1, with generator $P_0 = (-1,1)$, and trivial torsion. Accordingly, sequences with $U_7(P,Q) = \Box$ are parametrized by the multiples of P_0 on the above elliptic curve, corresponding to $(\pm P, Q) = (1,1)$, $(1,5)$, $(2,-1)$, $(5,21)$, $(1,-104)$, $(21,545)$, $(52,415)$,...

3 Solution of $U_n(P,Q) = \Box$, $n = 8, 10, 11$

Here we shall show the following result:

Theorem. *The only non-degenerate sequences where* $\gcd(P,Q) = 1$ *and* $U_n(P,Q) = \Box$*,* $8 \le n \le 11$*, are given by* $U_8(1,-4) = 21^2$ *and* $U_8(4,-17) = 620^2$*.*

For each $n \in \{8, 10, 11\}$ we reduce the solution of our problem to a number of questions, all having the following general shape:

Problem 1. *Let*

$$\mathcal{E} : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6 \tag{2}$$

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* $d \ge 2$*, and let* $\beta, \gamma \in \mathbb{Q}(\alpha)$ *be algebraic integers. Find all points* $(X,Y) \in \mathcal{E}(\mathbb{Q}(\alpha))$ *for which* $\beta X + \gamma$ *is a* rational number.

As mentioned in the Introduction, problems of this type may be attacked with the Magma routines of Nils Bruin, in particular the routine "Chabauty" using output from "PseudoMordellWeilGroup". It is not *a priori* guaranteed that these routines will be successful, particularly over number fields of high degree, but for our purposes and the computations encountered in this paper, no difficulties arose.

3.1 $n = 8$

The demand that $U_8(P,Q)$ be square is that $P(P^2-2Q)(P^4-4P^2Q+2Q^2) = \square$. In the case P is odd, it follows that $(P, P^2-2Q, P^4-4P^2Q+2Q^2) = (a^2, b^2, c^2)$, $(a^2, -b^2, -c^2)$, $(-a^2, b^2, -c^2)$, or $(-a^2, -b^2, c^2)$, where a, b, c are positive integers with ab odd. The latter two possibilities are impossible modulo 4, and the first two possibilities lead respectively to:

$$\begin{aligned} -a^8 + 2a^4b^2 + b^4 &= 2c^2 && (3) \\ -a^8 - 2a^4b^2 + b^4 &= -2c^2. && (4) \end{aligned}$$

We shall see that the only positive solutions to the above equations are $(a,b) = (1,1), (1,3)$ and $(1,1)$ respectively, leading to $(P,Q) = (1,0), (1,-4)$ and $(1,1)$, from which we reject the first one. The last gives a degenerate sequence. In the case that P is even, then Q is odd, and 2 exactly divides both $P^4-4P^2Q+2Q^2$ and P^2-2Q, forcing $P \equiv 0 \pmod 4$. Put $P = 4p$, so that $U_8 = \square$ if and only if $p(8p^2-Q)(128p^4-32p^2Q+Q^2) = \square$, with $\gcd(p,Q) = 1$. It follows that $(p, 8p^2-Q, 128p^4-32p^2Q+Q^2) = (a^2, b^2, c^2)$, $(a^2, -b^2, -c^2)$, $(-a^2, b^2, -c^2)$, or $(-a^2, -b^2, c^2)$, where a, b, c are positive integers, $(a,b) = 1$ and bc is odd. The middle two possibilities are impossible modulo 4, and the remaining two possibilities lead respectively to:

$$\begin{aligned} -64a^8 + 16a^4b^2 + b^4 &= c^2 && (5) \\ -64a^8 - 16a^4b^2 + b^4 &= c^2. && (6) \end{aligned}$$

We shall see that the only positive solution which leads to a desired pair (P,Q) is from the first equation when $(a,b) = (1,5)$, leading to $(P,Q) = (4,-17)$.

We shall work in the number field $K = \mathbb{Q}(\phi)$ where ϕ is a root of $f_\phi(x) = x^4 + 2x^2 - 1$. The class number of K is 1, the maximal order $\mathcal{O}$ of K is $\mathbb{Z}[\phi]$, and fundamental units of $\mathcal{O}$ are $\eta_1 = \phi$, $\eta_2 = 2 - 3\phi + \phi^2 - \phi^3$. The factorization of 2 is $2 = \eta_1^{-4}\eta_2^2(1+\phi)^4$.

3.1.1 Equation (3)

The factorization of (3) over K is

$$(b - \phi a^2)(b + \phi a^2)(b^2 + (2+\phi^2)a^4) = 2\square,$$

and it is easy to see that each of the first two factors is exactly divisible by $1+\phi$ and the third factor is exactly divisible by $(1+\phi)^2$. Thus the gcd of any two (ideal) terms on the left hand side is equal to $(1+\phi)$, and

$$b + \phi a^2 = \pm\eta_1^{i_1}\eta_2^{i_2}(1+\phi)\square, \qquad b^2 + (2+\phi^2)a^4 = \pm\eta_1^{j_1}\eta_2^{j_2}(1+\phi)^2\square, \qquad (7)$$

where the exponents of the units are 0,1. Specializing ϕ at the real root 0.643594... of $f_\phi(x)$, and using $b > 0$, then necessarily the sign on the right hand side must be positive. Taking norms in the first equation gives $2c^2 = (-1)^{i_1} 2\Box$, so that $i_1 = 0$. Applying the automorphism of K defined by $\phi \to -\phi$, it follows that $b - \phi a^2 = \eta_2^{-i_2}(1-\phi)\Box = \eta_2^{-i_2+1}(1+\phi)\Box$. Multiplying this equation by the two displayed equations at (7) gives $\eta_1^{j_1}\eta_2^{j_2+1}\Box = 2c^2 = \Box$, so that $j_1 = 0$, $j_2 = 1$. We now have

$$(b + \phi a^2)(b^2 + (2+\phi^2)a^4) = \eta_2^j (1+\phi)\Box,$$

with $j = 0, 1$. Putting $b/a^2 = \delta^{-1}x/(1+\phi)$, where $\delta \in \{1, \eta_2\}$, our problem reduces to finding all K-points (x, y) on the curves

$$(x + \phi(1+\phi)\delta)(x^2 + (2+\phi^2)(1+\phi)^2\delta^2) = y^2,$$

subject to $\delta^{-1}x/(1+\phi) \in \mathbb{Q}$. For both curves, the Magma routines of Bruin show that solutions to (3) occur only for $(\pm a, \pm b) = (1, 1), (1, 3)$.

3.1.2 Equation (4)

As above, (4) leads to equations

$$b + \phi^{-1}a^2 = \eta_1^{i_1}\eta_2^{i_2}(1+\phi)\Box, \qquad b^2 + (-2+\phi^{-2})a^4 = \eta_1^{j_1}\eta_2^{j_2}(1+\phi)^2\Box,$$

with exponents 0, 1. Taking norms in the first equation gives $-2c^2 = (-1)^{i_1}2\Box$, so that $i_1 = 1$; and specializing ϕ at the real root $-0.643594...$ of $f_\phi(x)$ in the second equation gives $j_1 = 0$. We thus obtain

$$(b + \phi^{-1}a^2)(b^2 + (-2+\phi^{-2})a^4) = \eta_1\eta_2^j(1+\phi)\Box,$$

with $j = 0, 1$. Putting $b/a^2 = \delta^{-1}x/(1+\phi)$, where $\delta = \eta_1\eta_2^j$, we thus have to find all K-points (x, y) on the curves

$$(x + \frac{1+\phi}{\phi}\delta)(x^2 + (-2 + \frac{1}{\phi^2})(1+\phi)^2\delta^2) = y^2,$$

such that $\delta^{-1}\frac{x}{1+\phi} \in \mathbb{Q}$, for $\delta = \eta_1$, $\eta_1\eta_2$. The Magma routines show that solutions to (4) occur only for $(\pm a, \pm b) = (1, 1)$.

3.1.3 Equation (5)

As above, (5) leads to equations

$$b + 2(\phi^3 + \phi)a^2 = \eta_1^{i_1}\eta_2^{i_2}\Box, \qquad b^2 + 8(2+\phi^2)a^4 = \eta_1^{j_1}\eta_2^{j_2}\Box,$$

with exponents 0, 1. Arguing just as for equation (3), we deduce $i_1 = 0$, and $j_1 = 0$, $j_2 = 0$. Thus

$$(b + 2(\phi^3 + \phi)a^2)(b^2 + 8(2+\phi^2)a^4) = \eta_2^j\Box,$$

with $j = 0, 1$. For $a \neq 0$, put $b/a^2 = \delta^{-1}x$, where $\delta = \eta_2^j$, which leads to seeking all K-points (x, y) on the curves

$$(x + 2(\phi^3 + \phi)\delta)(x^2 + 8(\phi^2 + 2)\delta^2) = y^2,$$

subject to $\delta^{-1}x \in \mathbb{Q}$, with $\delta = 1$, η_2. Magma routines show the only solutions of (5) are given by $(\pm a, \pm b) = (0, 1), (1, 2), (1, 5)$, of which only the third provides a desired pair (P, Q).

3.1.4 Equation (6)

Arguing as in previous cases, we deduce an equation

$$(b + 2(\phi^3 + 3\phi)a^2)(b^2 + 8\phi^2 a^4) = \eta_2^j \Box,$$

with $j = 0, 1$. For $a \neq 0$, put $b/a^2 = \delta^{-1}x$, where $\delta = \eta_2^j$. This leads to finding all K-points (x, y) on the curves

$$(x + 2(\phi^3 + 3\phi)\delta)(x^2 + 8\phi^2\delta^2) = \Box,$$

with $\delta^{-1}x \in \mathbb{Q}$, and $\delta = 1$, η_2. Magma routines show the only solution of (6) occurs for $a = 0$, with no solution for (P, Q).

3.2 $n = 10$

The equation $U_{10} = \Box$ is given by

$$P(P^4 - 3P^2Q + Q^2)(P^4 - 5P^2Q + 5Q^2) = \Box. \tag{8}$$

Our aim is to show that the only integer solutions are given by $(P, Q) = (1, 0)$, $(0, 1)$, $(-1, 1)$. The assumption $\gcd(P, Q) = 1$ implies that P is coprime to the second factor on the left at (8), and may only have the divisor 5 in common with the third factor. Further, the second and third factors can only have common divisor 2, impossible for $\gcd(P, Q) = 1$. Putting $(x, y) = (P^2, Q)$, then factorization over $\mathbb{Z}$ implies

$$x^2 - 3xy + y^2 = d_1 z^2, \qquad x^2 - 5xy + 5y^2 = d_2 w^2,$$

with $d_1 = \pm 1$, $d_2 = \pm 1, \pm 5$, giving 8 curves of genus 1. Most of the possibilities for (d_1, d_2) are readily eliminated, either by local consideration, or by leading to rank 0 elliptic curves; the case $(d_1, d_2) = (-1, -5)$ however resists elementary treatment, apparently leading to a curve of genus 3 with Jacobian of rank 4. We have found it preferable to invoke factorization of (8) over $K = \mathbb{Q}(\sqrt{5})$, when (8) becomes

$$P(P^2 - \epsilon^2 Q)(P^2 - \epsilon^{-2} Q)(P^2 - \sqrt{5}\epsilon Q)(P^2 - \sqrt{5}\epsilon^{-1} Q) = \Box, \tag{9}$$

where $\epsilon = (1+\sqrt{5})/2$ is a fundamental unit of the ring of integers $\mathcal{O}_K$ of K, of class number 1. Denote with a bar conjugation under $\sqrt{5} \to -\sqrt{5}$, so that $\bar{\epsilon} = -\epsilon^{-1}$. We have two cases to consider: (1) $(P,5)=1$, and (2) $(P,5)=5$.

Case (1): $(P,5)=1$. It follows that $P = \pm p^2$, and

$$\begin{array}{rclcrcl} p^4 - \epsilon^2 Q & = & \lambda_1 \alpha_1^2, & \qquad & p^4 - \epsilon\sqrt{5}Q & = & \lambda_2\alpha_2^2, \\ p^4 - \epsilon^{-2} Q & = & \bar{\lambda_1}\bar{\alpha_1}^2, & & p^4 - \epsilon^{-1}\sqrt{5}Q & = & \bar{\lambda_2}\bar{\alpha_2}^2 \end{array}$$

where λ_i, $\alpha_i \in \mathcal{O}_K$, with λ_i units. Equivalently, since $p \neq 0$,

$$\begin{array}{rcl} 1-\epsilon^2 q = \lambda_1\beta_1^2, & \qquad & 1-\epsilon\sqrt{5}q = \lambda_2\beta_2^2, \\ 1-\epsilon^{-2} q = \bar{\lambda_1}\bar{\beta_1}^2, & & 1-\epsilon^{-1}\sqrt{5}q = \bar{\lambda_2}\bar{\beta_2}^2, \end{array} \tag{10}$$

where $q = Q/p^4 \in \mathbf{Q}$, $\beta_i \in K$, and without loss of generality, $\lambda_i \in \{\pm 1, \pm\epsilon\}$. From the first three of these equations,

$$(q-\epsilon^{-2})(q-\epsilon^2)(q-\frac{\epsilon^{-1}}{\sqrt{5}}) = -\lambda_1\bar{\lambda_1}\lambda_2\frac{\epsilon^{-1}}{\sqrt{5}}\square = v\frac{\epsilon^{-1}}{\sqrt{5}}\square,$$

where $v = -\lambda_1\bar{\lambda_1}\lambda_2 = \pm\lambda_2$. Putting

$$x = \delta q, \quad \delta = v\epsilon\sqrt{5}, \qquad \text{where} \quad \delta^{-1}x \in \mathbb{Q},$$

then

$$(x - v\epsilon^{-1}\sqrt{5})(x - v\epsilon^3\sqrt{5})(x-v) = \square.$$

If $v = \pm\lambda_2 = \pm 1$, then one of the following equations holds:

$$y^2 = (x-(3-\epsilon))(x-(3+4\epsilon))(x-1) \tag{11}$$

$$y^2 = (x+(3-\epsilon))(x+(3+4\epsilon))(x+1) \tag{12}$$

under the condition $\frac{\epsilon^{-1}}{\sqrt{5}}x \in \mathbb{Q}$. Equation (11) defines an elliptic curve of K-rank 0, with no corresponding value of Q; equation (12) defines an elliptic curve of positive K-rank, and the Magma routines show that the only points satisfying the rationality condition are $(x, \pm y) = (0, \epsilon\sqrt{5})$, $(-2-\epsilon, 1+3\epsilon)$, corresponding to $Q=0$ and $Q=1$.
If $\lambda_2 = \pm\epsilon$, then one of the following equations holds:

$$\begin{array}{rcl} y^2 & = & (x-\sqrt{5})(x-\epsilon^4\sqrt{5}))(x-\epsilon) \\ y^2 & = & (x+\sqrt{5})(x+\epsilon^4\sqrt{5}))(x+\epsilon) \end{array}$$

under the condition $\frac{\epsilon^{-2}}{\sqrt{5}}x \in \mathbb{Q}$. Both these curves have K-rank 0, and no solution to our problem arises.

Case (2): $(P,5)=5$. We have $P=\pm 5p^2$, and

$$(25p^4-\epsilon^2 Q)(25p^4-\epsilon^{-2}Q)(5\sqrt{5}p^4-\epsilon Q)(5\sqrt{5}p^4-\epsilon^{-1}Q)=\pm\Box,$$

so that either $p=0$ (returning the solution $(P,Q)=(0,1)$ to (8)), or

$$\begin{aligned} 5-\epsilon^2 r &= \mu_1\gamma_1^2, & \sqrt{5}-\epsilon r &= \mu_2\gamma_2^2, \\ 5-\epsilon^{-2} r &= \bar{\mu_1}\bar{\gamma_1}^2, & \sqrt{5}-\epsilon^{-1} r &= -\bar{\mu_2}\bar{\gamma_2}^2, \end{aligned} \tag{13}$$

where $r=Q/(5p^4)\in\mathbf{Q}$, $\gamma_i\in K$, and μ_i units of $\mathcal{O}_K$, without loss of generality in the set $\{\pm 1,\pm\epsilon\}$. From the first three of these equations,

$$(r-5\epsilon^{-2})(r-5\epsilon^2)(r-\sqrt{5}\epsilon^{-1})=-\mu_1\bar{\mu_1}\mu_2\epsilon^{-1}\Box=w\epsilon^{-1}\Box,$$

where $w=-\mu_1\bar{\mu_1}\mu_2=\pm\mu_2$. Putting

$$x=\eta r,\quad \eta=w\epsilon,\qquad \text{where}\quad \eta^{-1}x\in\mathbb{Q},$$

then

$$(x-5w\epsilon^{-1})(x-5w\epsilon^3)(x-w\sqrt{5})=\Box.$$

If $w=\pm\mu_2=\pm 1$, then one of the following equations holds:

$$y^2 = (x-5\epsilon^{-1})(x-5\epsilon^3)(x-\sqrt{5}) \tag{14}$$

$$y^2 = (x+5\epsilon^{-1})(x+5\epsilon^3)(x+\sqrt{5}) \tag{15}$$

under the condition $\epsilon^{-1}x\in\mathbb{Q}$.
If $w=\pm\epsilon$, then one of the following equations holds:

$$y^2 = (x-5)(x-5\epsilon^4)(x-\epsilon\sqrt{5}) \tag{16}$$

$$y^2 = (x+5)(x+5\epsilon^4)(x+\epsilon\sqrt{5}) \tag{17}$$

under the condition $\epsilon^{-2}x\in\mathbb{Q}$. These last four equations define elliptic curves, the first three of which have positive K-rank, the fourth having K-rank 0 (giving no solution to our problem). Magma computations show that no solutions arise from the first three curves. (Computations do disclose the point $(x,y)=(-2\epsilon,\epsilon)$ on (15) satisfying the rationality condition, but this point leads to $(P,Q)=(5,10)$, disallowed for our original problem).

3.3 $n=11$

The equation $U_{11}=\Box$ is given by

$$U_{11}(P,Q)=P^{10}-9P^8Q+28P^6Q^2-35P^4Q^3+15P^2Q^4-Q^5=M^2. \tag{18}$$

There is the trivial solution given by $(P, Q) = (0, -1)$, and henceforth we assume $P \neq 0$. Our aim is to show that when $\gcd(P, Q) = 1$, the only integer solution of (18) is given by $(P^2, Q) = (1, 0)$. On putting $x = Q/P^2$, $y = M/P^5$, equation (18) becomes that of a genus 2 curve

$$C : y^2 = -x^5 + 15x^4 - 35x^3 + 28x^2 - 9x + 1,$$

and Magma computations show that the Jacobian J of C has rank 1, so that a Chabauty argument can be applied to determine all rational points of C. A generator is found to be $\{\big((3+\sqrt{5})/2, (11+5\sqrt{5})/2\big) - \infty\}$ (where ∞ is the unique point at infinity on C), and Magma tells us that there is at most one pair of rational points on C, which is accordingly $(0, \pm 1)$ as required. Full details of such an argument may be found in Flynn, Poonen, Schaefer [8]. For greater transparency, we outline the method that reduces as in previous cases to finding points on elliptic curves over a number field under a certain rationality condition. We shall be working over a Galois field, and this approach requires only application of the formal group of an elliptic curve, conceptually more straightforward than invoking the formal group of a curve of genus 2. It is easy to see that

$$M^2 = u_{11}(P, Q) = \prod_{j=1}^{j=5}((\zeta^{j/2} + \zeta^{-j/2})^{-2}P^2 - Q), \tag{19}$$

and thus $U_{11}(P, Q)$ splits completely over the real subfield of the cyclotomic field $\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta_{11})$. Let $\theta = \zeta + \zeta^{-1}$, so that

$$f_\theta(\theta) = \theta^5 + \theta^4 - 4\theta^3 - 3\theta^2 + 3\theta + 1 = 0,$$

and work in the number field $K = \mathbb{Q}(\theta)$, with ring of integers $\mathcal{O}_K = \mathbb{Z}[\theta]$, discriminant 11^4, and class-number 1. The unit group is of rank 4, and generators may be taken as:

$$\epsilon_1 = -\theta, \quad \epsilon_2 = -\theta^2 + 2, \quad \epsilon_3 = -\theta^4 + 4\theta^2 - 2, \quad \epsilon_4 = -\theta^3 + 3\theta,$$

with norms all equal +1. Rewrite (19) in the form

$$M^2 = \prod_{j=1}^{j=5} L_j(P, Q), \tag{20}$$

where $L_j(P, Q) = \theta_j P^2 - Q$, with $\theta_j = (\zeta^{j/2} + \zeta^{-j/2})^{-2}$. The Galois group of $\mathbb{Q}(\theta)/\mathbb{Q}$ is cyclic, generated by the automorphism $\sigma : \theta \to \theta^2 - 2$, which acts cyclically on the θ_i, and satisfies $\epsilon_i^\sigma = \epsilon_{i+1}$ for $i = 1, 2, 3$, $\epsilon_4^\sigma = \epsilon_1^{-1}\epsilon_2^{-1}\epsilon_3^{-1}\epsilon_4^{-1}$. Since $U_{11}(x, 1) \equiv 0 \bmod 11^2$ has no solution, $M \not\equiv 0 \bmod 11$; so each factor $L_j(P, Q)$ is prime to 11 in $\mathcal{O}_K$. Further, for $j \neq k$, the $K/\mathbb{Q}$ norm of $\theta_j - \theta_k$ is

±11, and it follows that the factors $L_j(P,Q)$ for $j=1,...,5$ are coprime in $\mathcal{O}_K$. Accordingly,

$$L_1(P,Q)=(\theta^4-\theta^3-2\theta^2+\theta+1)P^2-Q=(-1)^{i_0}\epsilon_1^{i_1}\epsilon_2^{i_2}\epsilon_3^{i_3}\epsilon_4^{i_4}\square, \qquad (21)$$

where $i_0,i_1,...,i_4\in\{0,1\}$. Since the norm of $L_1(P,Q)$ equals M^2, we must have $i_0=0$. Now let $^*:\mathbb{Q}(\theta)\hookrightarrow\mathbb{R}$ be the embedding that sends θ to the smallest real root $-1.9189859...$ of $f_\theta(x)$. It is straightforward to check that $\theta_1^*>\theta_4^*>\theta_5^*>\theta_3^*>\theta_2^*$, whence

$$L_1^*>L_4^*>L_5^*>L_3^*>L_2^*. \qquad (22)$$

Since (20) implies that the exact number of the L_j^* that are negative must be even, then (22) gives $L_1^*>0$. But $\epsilon_1^*>0$, $\epsilon_2^*<0$, $\epsilon_3^*<0$, $\epsilon_4^*>0$, and so necessarily i_2+i_3 is even.

By applying σ repeatedly to (21) we obtain:

$$\operatorname{sgn}(L_2^*)=(-1)^{i_1+i_2},\ \operatorname{sgn}(L_3^*)=(-1)^{i_1},\ \operatorname{sgn}(L_4^*)=(-1)^{i_4},\ \operatorname{sgn}(L_5^*)=(-1)^{i_3+i_4}.$$

Listing the 8 possibilities for (i_1,i_2,i_3,i_4), together with the corresponding signs of the L_i, the only ones that respect the linear ordering (22) are $(0,0,0,0)$, $(1,0,0,0)$, and $(1,0,0,1)$. The conclusion is that

$$L_1(P,Q)=\theta_1P^2-Q=\eta\square, \qquad \eta\in\{1,\ \ \epsilon_1,\ \ \epsilon_1\epsilon_4\}.$$

Certainly

$$L_1=\eta\square,\ \ L_2=\eta^\sigma\square,\ \ L_3=\eta^{\sigma^2}\square,\ \ L_4=\eta^{\sigma^3}\square,\ \ L_5=\eta^{\sigma^4}\square,$$

and we have various possibilities for producing an elliptic curve cover of our original equation. When $\eta=1$, then

$$(\theta_1P^2-Q)(\theta_2P^2-Q)(\theta_3P^2-Q)=\square,$$

so that $x=-Q/P^2$ is the x-coordinate of a K-rational point on the elliptic curve

$$(x+\theta_1)(x+\theta_2)(x+\theta_3)=y^2,$$

with $x\in\mathbb{Q}$. Magma computations show that the only such points on this curve are at infinity (corresponding to $P=0$), and $(x,y)=(0,\epsilon_3\epsilon_4)$, corresponding to $(P^2,Q)=(1,0)$.

When $\eta=\epsilon_1$ or $\epsilon_1\epsilon_4$, then

$$(\theta_1P^2-Q)(\theta_2P^2-Q)(\theta_3P^2-Q)=\delta\square,$$

with $\delta=\epsilon_1\epsilon_2\epsilon_3$ or ϵ_1, respectively; and $x=-\delta Q/P^2$ is the x-coordinate of a K-rational point on the elliptic curve

$$(x+\delta\theta_1)(x+\delta\theta_2)(x+\delta\theta_3)=y^2,$$

satisfying $\delta^{-1}x \in \mathbb{Q}$. These two curves both have positive K-rank, and by the Magma routines lead to no non-trivial solutions for P, Q.

Acknowledgement: We thank the anonymous referee for several useful comments.

References

[1] A. Bremner and N. Tzanakis, *Lucas sequences whose 12th or 9th term is a square*, J. Number Theory, **107** (2004), 215-227.

[2] N. Bruin, *The primitive solutions to* $x^3 + y^9 = z^2$, J. Number Theory, **111** (2005), 179-189.

[3] N. Bruin and N.D. Elkies, *Trinomials* ax^7+bx+c *and* ax^8+bx+c *with Galois Groups of Order 168 and* $8 * 168$, Algorithmic Number Theory, 5th International Symposium, ANTS-V, (Claus Fieker, David R. Kohel Eds.), Lecture Notes in Computer Science **2369** Springer (2002), 172-188.

[4] N. Bruin, *Chabauty methods and covering techniques applied to generalized Fermat equations*, CWI Tract, vol. 133, Stichtung Mathematisch Centrum Centrum voor Wiskunde en Informatica, Amsterdam (2002), Dissertation, University of Leiden, Leiden (1999).

[5] N. Bruin, *Chabauty methods using elliptic curves*, J. reine angew. Math., **562** (2003), 27-49.

[6] J.H.E. Cohn, *On square Fibonacci numbers*, J. London Math. Soc. **39** (1964), 537-541.

[7] On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$, Bull. London Math. Soc. **27** (1995), 513-543.

[8] E.V. Flynn, B. Poonen, and E. Schaefer, *Cycles of quadratic polynomials and rational points on a genus-2 curve*, Duke Math. J., **90** (1997), no. 3, 435-463.

[9] Magma, <http://magma.maths.usyd.edu.au/>

[10] P. Ribenboim and W.L. McDaniel, *The square terms in Lucas sequences*, J. Number Theory, **58**, 1996, 104-123.