ON INTEGRAL POINTS ON BIQUADRATIC CURVES AND NEAR MULTIPLES OF SQUARES IN LUCAS SEQUENCES

MAX A. ALEKSEYEV AND SZABOLCS TENGELY

Abstract. We describe algorithmic reduction of the search for integral points on a curve $y^2 = ax^4 + bx^2 + c$ with $ac(b^2 - 4ac) \neq 0$ to solving a finite number of Thue equations. While existence of such reduction is anticipated from arguments of algebraic number theory, our algorithm is elementary and to best of our knowledge is the first published algorithm of this kind. In combination with other methods and powered with existing software Thue equations solvers, it allows one to efficiently compute integral points on biquadratic curves.

We illustrate this approach with a particular application of finding near multiples of squares in Lucas sequences.

As an example, we establish that among Fibonacci numbers only 2 and 34 are of the form $2m^2 + 2$; only 1, 13, and 1597 are of the form $m^2 - 3$; and so on.

As an auxiliary result, we also give an algorithm for solving a Diophantine equation $k^2 = \frac{f(m,n)}{g(m,n)}$ in integers m, n, k, where f and g are homogeneous quadratic polynomials.

1. Introduction

Siegel [23] proved that any equation $y^2 = f(x)$ with irreducible polynomial $f \in \mathbb{Z}[x]$ of degree at least 3 has finitely many integral points. With the method of Baker [2, 3, 4], it became possible to bound the solutions and perform an exhaustive search. For third-degree curves, Baker's method was a subject to many practical improvements, and now there exists a number of software implementations for finding integral points on elliptic curves [6, 15, 24]. These procedures are based on a method developed by Stroeker and Tzanakis [26] and independently by Gebel, Pethő and Zimmer [14].

Thue equations of the form $g(x, y) = d$ where g is homogeneous irreducible polynomial of degree at least 3 were first studied by Thue [28], who proved that they have only a finite number of solutions. In computer era, Thue equations became a subject to developments of computational methods, resulting in at least two implementations: in computer algebra systems MAGMA [6] and PARI/GP [27]. For our practical computations, we chose SAGE [24], which adopts PARI/GP Thue equations solver based on Bilu and Hanrot's improvement [5] of Tzanakis and de Weger's method [29].

In the current work, we show how to reduce a search for integral points on a biquadratic curve

$$y^2 = ax^4 + bx^2 + c$$

with integer (or, more generally, rational) coefficients a, b, c with $ac(b^2 - 4ac) \neq 0$ firstly to a Diophantine equation $k^2 = \frac{f(m,n)}{g(m,n)}$ in coprime integers m, n with homogeneous quadratic polynomials f and g (Theorem 5), and then to a finite number of Thue equations (Theorem 4). While possibility of reduction to Thue equations was described by Mordell [17] based on arguments from algebraic number theory, to the best of our knowledge, there is no published algorithm applicable for the general case. Furthermore, in contrast to traditional treatment of this kind of problems with algebraic number theory [17, 25, 11, 18], our reduction method is elementary. It may be viewed as a generalization of the one of Steiner and Tzanakis [25] who reduced Ljunggren equation $y^2 = 2x^4 - 1$ to two Thue equations (in particular, we obtain the same Thue equations).

There are other methods which can be used in certain cases to determine all integral solutions of the equation $y^2 = ax^4 + bx^2 + c$. Poulakis [19] provided an elementary algorithm to solve Diophantine equations of the form $y^2 = f(x)$, where $f(x)$ is quartic monic polynomial with integer coefficients, based on Runge's method [21, 22, 30]. Here it is crucial that the leading coefficient of $f(x)$ is 1 (the idea also works if the leading coefficient is a perfect square). Using the theory of Pell equations, Kedlaya [16] described a method to solve the system of equations

$$\begin{cases} x^2 - a_1y^2 = b_1, \\ P(x, y) = z^2, \end{cases}$$

where P is a given integer polynomial, and implemented his algorithm in Mathematica (`http://math.ucsd.edu/~kedlaya/papers/pell.tar`). If we set $P(x, y) = c_1x + d_1$, then we obtain a quartic equation of the form $(a_1c_1y)^2 = a_1z^4 - 2a_1d_1z^2 - a_1b_1c_1^2$. There is also a simple reduction of the equation $y^2 = ax^4 + bx^2 + c$ to an elliptic equation: after multiplying the equation by a^2x^2, one obtains:

$$(xy)^2 = (ax^2)^3 + b(ax^2)^2 + ac(ax^2),$$

which can be further written as

$$Y^2 = X^3 + bX^2 + acX.$$

As we noted earlier to determine all integral points on a given elliptic curve one can follow a method developed by Stroeker and Tzanakis [26] and independently by Gebel, Pethő and Zimmer [14]. The disadvantage of this approach is that there is no known algorithm to determine the rank of the so-called Mordell-Weil group of an elliptic curve, which is necessary to determine all integral points on the curve.

For efficient computation of integral points on biquadratic curves, we implemented in SAGE a combination of the elliptic curve and reduction to Thue equations methods. By default we employ the elliptic curve method and if it fails, we fallback to our reduction to Thue equations. The SAGE code can be downloaded from `http://www.math.unideb.hu/~tengely/biquadratic.sage`.

Our approach also allows one to efficiently compute solutions to a system of Diophantine equations (Theorem 6):

$$\begin{cases} a_1x^2 + c_1z = d_1, \\ b_2y^2 + c_2z^2 = d_2. \end{cases}$$

From this perspective, it continues earlier work [1], where the first author described an algorithm for computing solutions to a system of Diophantine equations:

$$\begin{cases} a_1x^2 + b_1y^2 + c_1z^2 = d_1, \\ a_2x^2 + b_2y^2 + c_2z^2 = d_2, \end{cases}$$

and demonstrated applications for finding common terms of distinct Lucas sequences of the form $U(P, \pm 1)$ or $V(P, \pm 1)$, which include Fibonacci, Lucas, Pell, and Lucas-Pell numbers. The current method also has applications for such Lucas sequences, allowing one to find all terms of the form $a \cdot m^2 + b$ for any fixed integers a, b. While the question of finding multiples of squares (i.e., with $b = 0$) in Lucas sequences has been widely studied, starting with the works of Cohn [9] and Wyler [31] (we refer to Bremner and Tzanakis [7] for an extensive review of the literature), finding *near* multiples of squares (i.e., with $b \neq 0$) has got so far only a limited attention [12, 13, 20]. In the current work, we present an unified computational approach for solving this problem. As an example, we establish that among Fibonacci numbers only 2 and 34 are of the form $2m^2 + 2$; only 1, 13, and 1597 are of the form $m^2 - 3$; and so on.

The paper is organized as follows. In Section 2, we develop our machinery for homogeneous quadratic polynomials with integer coefficients. In Section 3, we prove our method for finding integral points on biquadratic curves and illustrate its workflow on Ljunggren equation. In Section 4, we further demonstrate how our method can be used for finding near multiples of squares in Lucas sequences and list some results of this kind.

2. Homogeneous quadratic polynomials

We start with studying properties of quadratic homogeneous polynomials with integer coefficients in two and three variables. We do not distinguish between homogeneous polynomials in two variables from their univariate counterparts (i.e., $f(x, y) = ax^2+bxy+cy^2$ and $\tilde{f}(z) = az^2 + bz + c$) that allows us to define resultant (Res) and discriminant (Disc) on them.

Theorem 1 (Theorem 5 in [1][1])**.** *Let A, B, C be non-zero integers and let (x_0, y_0, z_0) with $z_0 \neq 0$ be a particular non-trivial integer solution to the Diophantine equation $Ax^2 + By^2 + Cz^2 = 0$. Then its general integer solution is given by*

$$(x, y, z) = \frac{p}{q} \left(P_x(m, n),\ P_y(m, n),\ P_z(m, n)\right) \tag{1}$$

where m, n as well as p, q are coprime integers with $q > 0$ dividing $2\,\mathrm{lcm}(A, B)Cz_0^2$, and

$$\begin{aligned} P_x(m, n) &= x_0Am^2 + 2y_0Bmn - x_0Bn^2, \\ P_y(m, n) &= -y_0Am^2 + 2x_0Amn + y_0Bn^2, \\ P_z(m, n) &= z_0Am^2 + z_0Bn^2. \end{aligned}$$

We refer to [8, 10] for general methods of finding a particular solution to a quadratic homogeneous equation in three variables.[2]

Theorem 2. *Let $P_1(x, y)$ and $P_2(x, y)$ be homogeneous quadratic polynomials with integer coefficients and $R = \mathrm{Res}(P_1, P_2) \neq 0$. Let G be the largest element in the Smith normal form of the resultant matrix of P_1 and P_2.[3] Then for any coprime integers m, n, $\gcd(P_1(m, n), P_2(m, n))$ divides G.*

[1] This theorem corrects an error in Corollary 6.3.8 of [8].

[2] In PARI/GP, a particular solution can be computed with the function *bnfisnorm*.

[3] While $G = R$ would also satisfy the theorem statement, we want G as small as possible. The resultant R is often much larger than G defined in the theorem.

Proof. Let $P_1(x,y) = a_1x^2+b_1xy+c_1y^2$ and $P_2(x,y) = a_2x^2+b_2xy+c_2y^2$ where a_1,b_1,c_1,a_2,b_2,c_2 are integer. Consider polynomials $x\cdot P_1(x,y)$, $y\cdot P_1(x,y)$, $x\cdot P_2(x,y)$, $y\cdot P_2(x,y)$ as linear combinations with integer coefficients of the basis terms x^3, x^2y, xy^2, y^3. Our goal is to find two linear combinations of these polynomials: one equal an integer multiple of x^3 and the other equal an integer multiple of y^3. This corresponds to the following two systems of linear equations with the same resultant matrix:

$$\text{(2)}\qquad \begin{matrix} x^3: \\ x^2y: \\ xy^2: \\ y^3: \end{matrix} \quad \begin{bmatrix} a_1 & 0 & a_2 & 0 \\ b_1 & a_1 & b_2 & a_2 \\ c_1 & b_1 & c_2 & b_2 \\ 0 & c_1 & 0 & c_2 \end{bmatrix} \cdot \begin{bmatrix} t_1 \\ t_2 \\ t_3 \\ t_4 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \text{ or } \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

with respect to rational numbers t_1,t_2,t_3,t_4. Since the matrix determinant equals the resultant $R \neq 0$, the systems have unique solutions of the form:

$$(t_1,t_2,t_3,t_4) = \frac{1}{R}(\Delta_1,\Delta_2,\Delta_3,\Delta_4) = \frac{1}{G}\left(\frac{\Delta_1}{d_3},\frac{\Delta_2}{d_3},\frac{\Delta_3}{d_3},\frac{\Delta_4}{d_3}\right)$$

where Δ_i are determinant of certain 3×3 minors of the resultant matrix and d_3 is its third determinant divisor. Here we used the fact that $\frac{R}{d_3} = G$ is the fourth elementary divisor of the resultant matrix (and the largest element of its Smith normal form). It is important to notice that all vector components $\frac{\Delta_i}{d_3}$ are integer.

So we have two linear combinations of $x\cdot P_1(x,y)$, $y\cdot P_1(x,y)$, $x\cdot P_2(x,y)$, $y\cdot P_2(x,y)$ with integer coefficients $\frac{\Delta_1}{d_3}$, $\frac{\Delta_2}{d_3}$, $\frac{\Delta_3}{d_3}$, $\frac{\Delta_4}{d_3}$ equal $G\cdot x^3$ and $G\cdot y^3$, respectively. For $(x,y) = (m,n)$ where m,n are coprime integers, these linear combinations imply that $\gcd(P_1(m,n),P_2(m,n))$ divides both $G\cdot m^3$ and $G\cdot n^3$. Therefore, $\gcd(P_1(m,n),P_2(m,n))$ divides $\gcd(G\cdot m^3, G\cdot n^3) = G\cdot \gcd(m^3,n^3) = G$. □

We remark that in practice to compute G, we do not need to compute Smith normal form of the resultant matrix. Instead, we simply solve the two linear systems (2) and define G as the least common multiple of all denominators in both solutions (t_1,t_2,t_3,t_4).

Theorem 3. *Any homogeneous quadratic polynomial with integer coefficients and non-zero discriminant can be represented as a linear combination with non-zero rational coefficients of squares of two homogeneous linear polynomials. Moreover, these polynomials are linearly independent.*

Proof. Let $ax^2+bxy+cy^2$ be a homogeneous quadratic polynomial with integer coefficients and non-zero discriminant, i.e., $b^2-4ac \neq 0$. If $b=0$ then $ac \neq 0$ and the statement is trivial.

Suppose that $b \neq 0$. If $a \neq 0$, then we have

$$ax^2+bxy+cy^2 = \frac{1}{4a}\cdot\left((2ax+by)^2 + (4ac-b^2)y^2\right).$$

Similarly, if $c \neq 0$, then we have

$$ax^2+bxy+cy^2 = \frac{1}{4c}\cdot\left((4ac-b^2)x^2 + (bx+2cy)^2\right).$$

Finally, if $a=c=0$, then

$$bxy = \frac{b}{4}\cdot\left((x+y)^2 - (x-y)^2\right).$$

It is easy to see that in all cases, the linear polynomials are linearly independent. □

Theorem 4. *Let $P_1(x,y)$ and $P_2(x,y)$ be homogeneous quadratic polynomials with integer coefficients such that* $\mathrm{Disc}(P_1) \neq 0$, $\mathrm{Disc}(P_2) \neq 0$, *and* $\mathrm{Res}(P_1, P_2) \neq 0$. *Then the equation*

$$z^2 = \frac{P_1(x,y)}{P_2(x,y)} \tag{3}$$

has a finite number of integer solutions $(x,y,z) = (m,n,k)$ *with* $\gcd(m,n) = 1$.

Proof. Suppose that $(x,y,z) = (m,n,k)$ with $\gcd(m,n) = 1$ satisfies the equation (3). Then by Theorem 2, $\gcd(P_1(m,n), P_2(m,n)) = P_2(m,n)$ divides certain integer G. Then for some divisor[4] g of G, we have $P_2(m,n) = g$ and $P_1(m,n) = gk^2$. So $(x,y,z) = (m,n,k)$ represents a solution to the following system of equations:

$$\begin{cases} P_1(x,y) = g \cdot z^2, \\ P_2(x,y) = g. \end{cases} \tag{4}$$

Therefore, to find all solutions to (3), we need to solve the systems (4) for g ranging over the divisors of G. Each such system is solved as follows.

We start with using Theorem 3 to represent $P_1(x,y)$ as a linear combination with rational coefficients of squares of two linearly independent polynomials, say, $P_1(x,y) = a \cdot Q_1(x,y)^2 + b \cdot Q_2(x,y)^2$. Substituting this representation into the first equation of (4), we get the following equation:

$$a \cdot Q_1(x,y)^2 + b \cdot Q_2(x,y)^2 - g \cdot z^2 = 0. \tag{5}$$

We solve this equation using Theorem 1 to obtain $Q_1(x,y) = \frac{p}{q} \cdot R_1(m,n)$ and $Q_2(x,y) = \frac{p}{q} \cdot R_2(m,n)$, where q ranges over the positive divisors of a certain integer and integer p is coprime to q. We solve these linear equations with respect to x, y to obtain

$$(x,y) = \frac{p}{q} \cdot \left(S_x(m,n),\ S_y(m,n) \right),$$

where $S_x(m,n)$ and $S_y(m,n)$ are linear homogeneous polynomials with rational coefficients (which depend only on g but not p, q). Plugging this into the second equation of (4), we get the following quartic equations with integer coefficients w.r.t. m, n:

$$\ell_g \cdot P_2(S_x(m,n), S_y(m,n)) = q^2 \cdot \frac{g \cdot \ell_g}{p^2}. \tag{6}$$

where ℓ_g is the least common multiple of the coefficients denominators of $P_2(S_x(m,n), S_y(m,n))$ (notice that ℓ_g depends only on g but not p, q). Here p^2 must divide $g\ell$ and thus there is a finite number of such equations. By Theorem 3 in [1], each such equation has a finite number of solutions, unless $P_2(S_x(m,n), S_y(m,n)) = c \cdot T(m,n)^2$ for some polynomial $T(x,y)$, which is not the case since $\mathrm{Disc}(P_2) \neq 0$. □

From practical perspective, we remark that different choices of values for g, p, q may result in the same equation (6). In particular, if $g' = g \cdot d^2$ for some integer d, then we can represent equation (5) for g' in the form $a \cdot Q_1(x,y)^2 + b \cdot Q_2(x,y)^2 - g \cdot (d \cdot z)^2 = 0$ so that it has the same solutions w.r.t. $Q_1(x,y)$ and $Q_2(x,y)$. Then the equation (6) for g' has the same left hand side as the one for g (with $\ell_{g'} = \ell_g$), while the former has an extra factor d^2 in the right hand side. Therefore, to reduce the number of equations, we can restrict g

[4] Unless specified otherwise, the divisors of an integer include both positive and negative divisors.

to the square-free divisors of G: for each such g, we compute the left hand side of (6) and iterate over all *distinct* integer right hand sides of the form $q^2 \cdot \frac{g \cdot \ell_g \cdot d^2}{p^2}$, where d^2 divides $\frac{G}{g}$.

3. Finding integral points on biquadratic curves

Now we are ready to prove our main result:

Theorem 5. *Finding integral points on a biquadratic curve*

$$y^2 = a \cdot x^4 + b \cdot x^2 + c \tag{7}$$

with integer coefficients a, b, c, $ac(b^2 - 4ac) \neq 0$, reduces to solving a finite number of quartic Thue equations.

Proof. Multiplying the equation (7) by $4c$, we can rewrite it as a linear combination of three squares with non-zero integer coefficients:[5]

$$(b^2 - 4ac)(x^2)^2 + 4cy^2 - (bx^2 + 2c)^2 = 0.$$

Denoting $X = x^2$, $Y = y$, $Z = bx^2 + 2c$, $A = b^2 - 4ac$, $B = 4c$, $C = -1$, we get a Diophantine equation :

$$A \cdot X^2 + B \cdot Y^2 + C \cdot Z^2 = 0. \tag{8}$$

If this equation is solvable with a particular solution $(X, Y, Z) = (X_0, Y_0, Z_0)$, $Z_0 \neq 0$, then by Theorem 1 its general solution is given by:

$$(X, Y, Z) = r \cdot \left(P_x(m, n),\ P_y(m, n),\ P_z(m, n)\right),$$

where $P_i(m, n)$ are polynomials defined by (2), m, n are coprime integers, and r is a rational number. In our case, this solution should additionally satisfy the relation:

$$2c = Z - bX = r \cdot (P_z(m, n) - b \cdot P_x(m, n)),$$

implying that

$$r = \frac{2c}{P_z(m, n) - b \cdot P_x(m, n)}.$$

So we get a constraining Diophantine equation:

$$x^2 = \frac{2c \cdot P_x(m, n)}{P_z(m, n) - b \cdot P_x(m, n)}, \tag{9}$$

which reduces to a finite number of Thue equations by Theorem 4, unless $\text{Res}(P_x, P_z - b \cdot P_x) = 0$ or $\text{Disc}(P_z - b \cdot P_x) = 0$.

The case of $\text{Res}(P_x, P_z - b \cdot P_x) = \text{Res}(P_x, P_z) = 0$ is impossible since by direct computation we have $\text{Res}(P_x, P_z) = -4AB^2CZ_0^4 \neq 0$.

In the case of $\text{Disc}(P_z - b \cdot P_x) = 0$, we have $\text{Disc}(P_z - b \cdot P_x) = 4b^2B^2Y_0^2 - 4AB(Z_0^2 - b^2X_0^2) = 0$ and thus $b^2BY_0^2 = A(Z_0^2 - b^2X_0^2)$. Since $BY_0^2 = -AX_0^2 - CZ_0^2$, we further get $b^2(-AX_0^2 - CZ_0^2) = A(Z_0^2 - b^2X_0^2)$, which reduces to $A + b^2C = 0$. However this is impossible since $A + b^2C = -4ac \neq 0$.

Therefore, Theorem 4 is applicable. ∎

[5]Alternatively, we can multiply (7) by $4a$ and obtain another linear combination of three squares: $(2ax^2 + b)^2 + (4ac - b^2) \cdot 1^2 - 4ay^2 = 0$, which has smaller coefficients and thus may be preferrable when $c \gg a$.

As a corollary we get:

Theorem 6. *The following system of Diophantine equations:*

$$\begin{cases} z = ax^2 + d_1, \\ z^2 = by^2 + d_2, \end{cases}$$

where a, b, d_1, d_2 are rational numbers with $abd_2(d_1^2 - d_2) \neq 0$ reduces to a finite number of Thue equations.

Proof. The system implies that $(ax^2 + d_1)^2 = by^2 + d_2$ or $(by)^2 = a^2bx^4 + 2abd_1x^2 + b(d_1^2 - d_2)$. Since $(2d_1ab)^2 - 4a^2b^2(d_1^2 - d_2) = 4a^2b^2d_2 \neq 0$, Theorem 5 applies. □

Example: Ljunggren equation. We illustrate our method on Ljunggren equation $y^2 = 2x^4 - 1$ whose reduction to Thue equations was first obtained in [25]. Here we have $(a, b, c) = (2, 0, -1)$. First we compute $A = b^2 - 4ac = 8$, $B = 4c = -4$, and $C = -1$ and consider equation (8). Its particular solution is $(1, 1, 2)$ yields by Theorem 1 a general solution:

$$(X, Y, Z) = \frac{p}{q}\,(P_x(m, n),\ P_y(m, n),\ P_z(m, n))$$

with

$$\begin{aligned} P_x(m, n) &= 8m^2 - 8mn + 4n^2, \\ P_y(m, n) &= -8m^2 + 16mn - 4n^2, \\ P_z(m, n) &= 16m^2 - 8n^2. \end{aligned}$$

Now we consider equation (9):

$$x^2 = \frac{2cP_x(m, n)}{P_z(m, n) - b \cdot P_x(m, n)} = \frac{-2(8m^2 - 8mn + 4n^2)}{16m^2 - 8n^2} = \frac{-2m^2 + 2mn - n^2}{2m^2 - n^2}$$

and use Theorem 4 to solve it. We take the resultant matrix of $P_1(x, y) = -2x^2 + 2xy - y^2$ and $P_2(x, y) = 2x^2 - y^2$ and solve the two linear systems (2) to obtain $(t_1, t_2, t_3, t_4) = \frac{1}{4}(-2, -1, 0, 1)$ and $(t_1, t_2, t_3, t_4) = (-1, -1, -1, 0)$. So we get $G = 4$. Let g range over the divisors of G, i.e., $g \in \{-4, -2, -1, 1, 2, 4\}$.

We use Theorem 3 to represent $P_1(x, y)$ as a linear combination of squares:

$$P_1(x, y) = -2x^2 + 2xy - y^2 = -\frac{1}{8}\left((-4x + 2y)^2 + 4y^2\right) = -\frac{1}{2}\left((-2x + y)^2 + y^2\right)$$

and obtain the equation (5) (multiplied by -2):

$$(-2x + y)^2 + y^2 + 2gz^2 = 0.$$

Clearly, it may have non-trivial solutions only for $g < 0$ and only when -1 is a square modulo $2g$, which leaves us the only suitable value $g = -1$. The corresponding equation has a particular solution $(1, 1, 1)$ and by Theorem 1 its general solution is:

$$(-2x + y, y, z) = \frac{p}{q} \cdot \left(m^2 + 2mn - n^2, -m^2 + 2mn + n^2, m^2 + n^2\right)$$

where $(p, q) = 1$ and $q > 0$ divides 4.

From this solution we express $x = \frac{p}{q} \cdot (-m^2 + n^2)$ and $y = \frac{p}{q} \cdot (-m^2 + 2mn + n^2)$ and plug them into the equation $P_2(x, y) = g$ to obtain the following quartic equations:

$$m^4 + 4m^3n - 6m^2n^2 - 4mn^3 + n^4 = q^2 \cdot \frac{-1}{p^2}$$

and conclude that $p^2 = 1$. Since the left hand side is irreducible, these are Thue equations.

We used PARI/GP to solve the resulting three Thue equations (for $q = 1, 2, 4$) and found that only the one with $q = 2$ has solutions, which are $(m, n) = \pm(5, -1), \pm(1, 5), (\pm 1, \pm 1)$. The corresponding solutions to $\frac{P_1(m,n)}{P_2(m,n)} = x^2$ are $(m, n) = \pm(12, 17)$ and $\pm(0, 1)$, giving respectively $x = \pm 13$ and ± 1.

4. Near multiples of squares in Lucas sequences

The pair of Lucas sequences $U(P, Q)$ and $V(P, Q)$ are defined by the same linear recurrent relation with the coefficient $P, Q \in \mathbb{Z}$ but different initial terms:

$$\begin{aligned} &U_0(P, Q) = 0, \quad U_1(P, Q) = 1, \quad U_{n+1}(P, Q) = P \cdot U_n(P, Q) - Q \cdot U_{n-1}(P, Q),\ n \geq 1; \\ &V_0(P, Q) = 2, \quad V_1(P, Q) = P, \quad V_{n+1}(P, Q) = P \cdot V_n(P, Q) - Q \cdot V_{n-1}(P, Q),\ n \geq 1. \end{aligned}$$

Some Lucas sequences have their own names:

Sequence	Name	Initial terms
$U(1, -1)$	Fibonacci numbers	$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, \ldots$
$V(1, -1)$	Lucas numbers	$2, 1, 3, 4, 7, 11, 18, 29, 47, 76, 123, \ldots$
$U(2, -1)$	Pell numbers	$0, 1, 2, 5, 12, 29, 70, 169, 408, 985, \ldots$
$V(2, -1)$	Pell-Lucas numbers	$2, 2, 6, 14, 34, 82, 198, 478, 1154, \ldots$

Other examples include Jacobsthal numbers $U(1, -2)$, Mersenne numbers $U(3, 2)$ etc.

The characteristic polynomial of Lucas sequences $U(P, Q)$ and $V(P, Q)$ is $\lambda^2 - P\lambda + Q$ with the discriminant $D = P^2 - 4Q$. For non-degenerate sequences, the discriminant D is a positive non-square integer.

Terms of Lucas sequences satisfy the following identity:

$$V_n(P, Q)^2 - D \cdot U_n(P, Q)^2 = 4Q^n. \tag{10}$$

In the current paper, we focus on the case of $Q = 1$ or $Q = -1$, implying that the pairs $(V_n(P, Q), U_n(P, Q))$ satisfy the equation:[6]

$$x^2 - Dy^2 = \pm 4. \tag{11}$$

The converse statement can be used to prove that given positive integers belong to $V(P, Q)$ or $U(P, Q)$ respectively:

Theorem 7 (Theorem 1 in [1]). *Let P, Q be integers such that $P > 0$, $|Q| = 1$, $(P, Q) \neq (3, 1)$, and $D = P^2 - 4Q > 0$. If positive integers u and v are such that*

$$v^2 - Du^2 = \pm 4,$$

then $u = U_n(P, Q)$ and $v = V_n(P, Q)$ for some integer $n \geq 0$.

[6]Here and everywhere below $\pm$ in the r.h.s. of an equation means that we accept both signs as solutions.

Theorem 8. *For fixed integers $a \neq 0$ and b, finding terms of the form $am^2 + b$ in nondegenerate Lucas sequences $U(P, Q)$ or $V(P, Q)$ with $Q = \pm 1$ reduces to a finite number of Thue equations, unless this sequence is $V(P, Q)$ and $b = \pm 2$. Thus there are only a finite number of such terms in these Lucas sequences.*

Proof. Let $ax^2 + b$ be a term of $U(P, \pm 1)$. By Theorem 7 we have $y^2 = D(ax^2 + b)^2 \pm 4 = Da^2x^4 + 2Dabx^2 + (Db^2 \pm 4)$. Theorem 5 applies, since $Db^2 \pm 4 \neq 0$ (notice that $D \neq \pm 1$) and $(2Dab)^2 - 4Da^2(Db^2 \pm 4) = \mp 16Da^2 \neq 0$.

Now let $ax^2 + b$ be a term of $V(P, \pm 1)$. By Theorem 7 we have $(Dy)^2 = D((ax^2 + b)^2 \mp 4) = Da^2x^4 + 2Dabx^2 + D(b^2 \mp 4)$. We have $(2Dab)^2 - 4D^2a^2(b^2 \mp 4) = \pm 16D^2a^2 \neq 0$. Theorem 5 applies here as soon as $b^2 \mp 4 \neq 0$ (i.e., $b \neq \pm 2$). □

We remark that for $b = \pm 2$, the sequence $V(P, Q)$ may have an infinite number of terms of the form $am^2 + b$. In particular, Lucas sequence $V(1, -1)$ (Lucas numbers) has infinitely many terms of the forms $m^2 + 2$ and $m^2 - 2$ since $V_{4n}(1, -1) = V_{2n}(1, -1)^2 - 2$ and $V_{4n+2}(1, -1) = V_{2n+1}(1, -1)^2 + 2$. The following theorem allows to find all terms solutions of the form $am^2 \pm 2$ in $V(P, \pm 1)$.

Theorem 9. *For fixed integers $a \neq 0$ and $b = \pm 2$, finding terms of the form $am^2 + b$ in nondegenerate Lucas sequence $V(P, Q)$ with $Q = \pm 1$ reduces to a finite number of Thue equations and a Pell-Fermat equation, which may or may not have infinitely many solutions.*

Proof. Let $ax^2 + b$ with $b = \pm 2$ be a term of $V(P, \pm 1)$. By Theorem 7, we have the following equations:

$$(Dy)^2 = D((ax^2 + b)^2 + 4) = Da^2x^4 + 2Dabx^2 + 8D$$

and

$$(Dy)^2 = D((ax^2 + b)^2 - 4) = Da^2x^4 + 2Dabx^2.$$

The former equation is addressed by Theorem 5, while the latter equation always has solution $x = 0$ (corresponding to the term $V_0 = 2$) and for $x \neq 0$ is equivalent to the Pell-Fermat equation:

$$\left(\frac{Dy}{x}\right)^2 - Da^2x^2 = 2Dab.$$

For solution of this equation, we refer to Section 6.3.5 in [8]. □

In the table below we list all the terms of the form $am^2 + b$ for $1 \leq a \leq 3$ and $-3 \leq b \leq 3$ in Fibonacci, Lucas, Pell, and Pell-Lucas numbers:

Form	Fibonacci numbers	Lucas numbers	Pell numbers	Pell-Lucas numbers
m^2	$0, 1, 144$	$1, 4$	$0, 1, 169$	none
$m^2 + 1$	$1, 2, 5$	$1, 2$	$1, 2, 5$	$2, 82$
$m^2 - 1$	$0, 3, 8$	3	0	none
$m^2 + 2$	$2, 3$	$2, 11$, and V_{4n+2}	2	2 and V_{4n+2}
$m^2 - 2$	$2, 34$	V_{4n}	2	14 and V_{4n}
$m^2 + 3$	3	$3, 4, 7, 199$	12	none
$m^2 - 3$	$1, 13, 1597$	1	1	6
$2m^2$	$0, 2, 8$	$2, 18$	$0, 2$	2
$2m^2 + 1$	$1, 3$	$1, 3$	1	none
$2m^2 - 1$	1	$1, 7, 199$	1	none
$2m^2 + 2$	$2, 34$	$2, 4$	2	2 and V_{4n}
$2m^2 - 2$	0	none	$0, 70$	V_{4n+2}
$2m^2 + 3$	$3, 5, 21$	$3, 11$	5	none
$2m^2 - 3$	5	$29, 47, 64079$	$5, 29$	none
$3m^2$	$0, 3$	3	$0, 12$	none
$3m^2 + 1$	$1, 13$	$1, 4, 76$	1	none
$3m^2 - 1$	2	$2, 11, 47$	2	2
$3m^2 + 2$	$2, 5$	$2, 29$	$2, 5, 29$	$2, 14$
$3m^2 - 2$	1	1	1	none
$3m^2 + 3$	3	3	none	6
$3m^2 - 3$	$0, 144$	none	0	none

Acknowledgements

We thank Dr. John Cremona, Dr. Nikos Tzanakis, and Dr. Noam Elkies for a number of helpful suggestions and discussions.

The first author was supported by the National Science Foundation under Grant No. IIS-1253614. The second author was partially supported by the European Union and the European Social Fund through project Supercomputer, the national virtual lab (grant no.: TÁMOP-4.2.2.C-11/1/KONV-2012-0010).

References

[1] M. A. Alekseyev. On the intersections of Fibonacci, Pell, and Lucas numbers. *INTEGERS*, 11(3):239–259, 2011.

[2] A. Baker. Linear forms in the logarithms of algebraic numbers. *Mathematika*, 13(02):204–216, 1966.

[3] A. Baker. Linear forms in the logarithms of algebraic numbers (ii). *Mathematika*, 14(01):102–107, 1967.

[4] A. Baker. Linear forms in the logarithms of algebraic numbers (iii). *Mathematika*, 14(02):220–228, 1967.

[5] Y. Bilu and G. Hanrot. Solving Thue equations of high degree. *Journal of Number Theory*, 60(2):373–392, 1996.

[6] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997.

[7] A. Bremner and N. Tzanakis. Lucas sequences whose n-th term is a square or an almost square. *Acta Arithm.*, 126(3):261–280, 2007.

[8] H. Cohen. *Number Theory: Tools and Diophantine equations*, volume I. Springer, 2007.

[9] J. H. E. Cohn. On Square Fibonacci Numbers. *J. London Math. Soc.*, s1-39:537–540, 1964.

[10] J. E. Cremona and D. Rusin. Efficient solution of rational conics. *Mathematics of Computation*, 72:1417–1441, 2003.

[11] B. M. M. de Weger. A curious property of the eleventh Fibonacci number. *Rocky Mountain J. of Math.*, 25:977–994, 1995.

[12] R. Finkelstein. On Fibonacci numbers which are one more than a square. *J. reine angew. Math.*, 262/263:171–178, 1973.

[13] R. Finkelstein. On Lucas numbers which are one more than a square. *Fibonacci Quart.*, 13:340–342, 1975.
[14] J. Gebel, A. Pethő, and H.G. Zimmer. Computing integral points on elliptic curves. *Acta Arith.*, 68(2):171–192, 1994.
[15] J. E. Cremona. *eclib, version* 2013-01-01. University of Warwick, U.K., 2013. http://homepages.warwick.ac.uk/staff/J.E.Cremona/mwrank/.
[16] K. S. Kedlaya. Solving constrained Pell equations. *Math. Comput.*, 67(222):833–842, 1998.
[17] L. J. Mordell. *Diophantine equations*. Academic Press, 1969.
[18] A. Pethő. Diophantine properties of linear recursive sequences I. *Applications of Fibonacci Numbers*, 7:295–309, 1998.
[19] D. Poulakis. A simple method for solving the Diophantine equation $Y^2 = X^4 + aX^3 + bX^2 + cX + d$. *Elem. Math.*, 54(1):32–36, 1999.
[20] N. Robbins. Fibonacci and Lucas numbers of the form $w^2 - 1$ and $w^3 \pm 1$. *Fibonacci Quart.*, 19:369–373, 1981.
[21] C. Runge. Über ganzzahlige Lösungen von Gleichungen zwischen zwei Veränderlichen. *J. Reine Angew. Math.*, 100:425–435, 1887.
[22] A. Schinzel. An improvement of Runge's theorem on Diophantine equations. *Comment. Pontificia Acad. Sci.*, 2(20):1–9, 1969.
[23] C. L. Siegel. Über einige Anwendungen Diophantischer Approximationen. *Abh. Preuss. Akad. Wiss. Phys. Math. Kl.*, 1:41–69, 1929.
[24] W. A. Stein et al. *Sage Mathematics Software, version* 5.11. The Sage Development Team, 2013. http://www.sagemath.org.
[25] R. Steiner and N. Tzanakis. Simplifying the solution of Ljunggren's equation $X^2 + 1 = 2Y^4$. *Journal of Number Theory*, 37(2):123–132, 1991.
[26] R. J. Stroeker and N. Tzanakis. Solving elliptic diophantine equations by estimating linear forms in elliptic logarithms. *Acta Arith.*, 67(2):177–196, 1994.
[27] The PARI Group, Bordeaux. *PARI/GP, version* 2.6.0, 2013. http://pari.math.u-bordeaux.fr.
[28] A. Thue. Über Annäherungswerte algebraischer Zahlen. *Journal für die reine und angewandte Mathematik*, 135:284–305, 1909.
[29] N. Tzanakis and B. M. M. de Weger. On the practical solution of the Thue equation. *Journal of Number Theory*, 31(2):99–132, 1989.
[30] P. G. Walsh. A quantitative version of Runge's theorem on Diophantine equations. *Acta Arith.*, 62(2):157–172, 1992.
[31] O. Wyler. In the Fibonacci series $F_1 = 1$, $F_2 = 1$, $F_{n+1} = F_n + F_{n-1}$ the first, second and twelfth terms are squares. *Amer. Math. Monthly*, 71:221–222, 1964.

Max A. Alekseyev
University of South Carolina, Columbia, SC, USA
E-mail address: maxal@cse.sc.edu

Szabolcs Tengely
Mathematical Institute, University of Debrecen, Hungary
E-mail address: tengely@science.unideb.hu