Diophantine properties of linear recursive sequences I

A. Pethö*
Laboratory of Informatics
University of Medicine
Nagyerdei Krt. 98
H-4032 Debrecen, Hungary
e-mail: pethoe@peugeot.dote.hu

1 Introduction and notations

Let G_n be a k-th ($k \geq 2$) order linear recurrence sequence of integers defined by initial terms $G_0, \ldots, G_{k-1} \in \mathbb{Z}$ and by the relation

$$G_{n+k} = A_1 G_{n+k-1} + \ldots + A_k G_n$$

for $n \geq 0$, where $A_1, \ldots, A_k \in \mathbb{Z},\ A_k \neq 0$. We give in this note a survey on results concerning the mixed exponential-polynomial diophantine equation

$$G_n = P(x), \tag{1}$$

where $P(x) \in \mathbb{Z}[x]$ denotes a polynomial of degree $d \geq 2$. The ultimate goal is to find all integers n, x for which (1) holds. It is often the case that, with the currently available methods, we are unable to completely solve the problems, though we are usually able to at least obtain an upper bound for the number of solutions or to prove that the number of solutions is finite.

*This paper was written when the author was a visiting professor at the Mathematical Institute of the Technical University of Graz, Austria. Research partially supported by Hungarian National Foundation for Scientific Research Grant No 16741/95.

In the case $P(x) = 0$ there were proven recently very important, general finiteness theorems about (1) by Evertse [12] and by Schlickewei and van der Poorten [44], moreover Schlickewei [43] was able to give an upper bound for the number of solutions of (1). We mention also that Laurent [18, 19] and Schlickewei and Schmidt [45] characterized completely in which cases two linear recurrence sequences can have infinitely many common terms. As their method, which is based on the subspace theorem of W.M. Schmidt [46] seems not applicable if the degree of P is at least two, we do not go into details, but refer to the survey paper [13] and the book [47].

After this remark we introduce more notations. Let us denote $C_G(x) = x^k - A_1 x^{k-1} - \ldots - A_k$ the characteristic polynomial of G_n and $\alpha_1, \ldots, \alpha_h$ the distinct zeros of C_G with multiplicities $m_1, \ldots, m_h$ respectively. To exclude discussions of special cases we assume in the sequel that G_n is *non-degenerated*, i.e. if no quotients of distinct zeros of its characteristic polynomial are roots of unity.

We will distinguish some sequences which occur frequently in the paper with special notation. So F_n and L_n will denote the Fibonacci and Lucas sequences respectively. They are defined by the parameters: $k = 2, A_1 = A_2 = 1, F_0 = 0, F_1 = 1$ and $L_0 = 2, L_1 = 1$.

In this part of the paper we first show mathematical problems, which lead to equations of the form (1). Then the most frequently used elementary methods are discussed. In the second part [29] we are dealing with methods based on lower bounds for linear forms in logarithms of algebraic numbers.

2 Is (1) an organic problem?

In 1984 I gave a lecture in Cologne about perfect powers in second order linear recurrences after which C. Meyer asked me: 'Is this a generic problem? Are there mathematical problems which lead to this question?' I was not able to give him a satisfactory answer.

There are of course diophantine equations which can be transformed more or less directly to an equation of type (1). Consider for example

$$ax^{2q} + bx^q y + cy^2 = d, \tag{2}$$

with $a, b, c, d \in \mathbb{Z}$ and such that $b^2 - 4ac > 0$ and not a square. Then we have to deal with a generalized Pellian equation in unknowns x^q and y. It is well-known that the solutions of a Pellian equation can be given by terms of finitely many second order linear recurrence sequences and we get equations of the form (1). I will come back to (2) in [29]. I do not consider this example a generic one in the sence of C. Meyer.

As far as I know the classical question: 'Are the only squares in the Fibonacci sequence $0, 1$ and 144?' appeared at the first time in 1962 in the book of Ogilvy [25]. Unfortunately, neither he nor A.P. Rollett, the proposer of problem 5080 in the American Mathematical Monthly [42] write about its origin. J.H.E. Cohn[1] does not know earlier references. He heard the problem in a lecture of Mordell, but thinks that it was of considerable antiquity. The problem of Fibonacci squares is a natural, but not a generic one.

In the following I will present examples, which show that (1) is indeed a generic one. The first example is coming from the theory of elliptic curves. Let $\mathbb{K}$ denote an algebraic number field and consider the set $E(\mathbb{K})$ of those $x, y \in \mathbb{K}$ with $y^2 = x^3 + ax + b$, where $a, b \in \mathbb{K}$ together with the infinite point $\mathcal{O}$. One can define addition on $E(\mathbb{K})$, and we obtain by the Mordell-Weil's theorem a finitely generated Abelian group (see e.g. [49]). An often attacked problem in the theory of elliptic curves is for a given class of number fields the characterization of the possible torsion subgroups, i.e. for which integers n does there exist $P \in E(\mathbb{K})$ such that $[n]P = \mathcal{O}$. If $\mathbb{K}$ is a cubic number field and the j-invariant of $E(\mathbb{K})$ is an algebraic integer, then we proved with Weis and Zimmer [32, 28]

Theorem 2.1 *Let $\mathbb{K}$ be a cubic number field such that there exists over $\mathbb{K}$ an*

[1] e-mail from June 18, 1996

elliptic curve with integer j-invariant and with torsion group isomorphic to $\mathbb{Z}_5$. The field $\mathbb{K}$ has this property if and only if there exist $m, k \in \mathbb{Z}$, $m \geq 0, k \geq -1$ and $\varepsilon_2, \varepsilon_3 \in \{1, -1\}$ such that $\mathbb{K} = \mathbf{Q}(\eta)$, where η is a zero of the polynomial

$$P_3(z; k, m, \varepsilon_2, \varepsilon_3) = z^3 + (-12 + \varepsilon_2 5^k G_m)z^2 + (10 + \varepsilon_2\varepsilon_3 5^k G_{m-5\varepsilon_3})z + 1,$$

and $G_m = F_m$ or L_m, if $k \geq 0$ and F_{5m}, if $k = -1$.

From this theorem it follows that there exist infinitely many elliptic curves over cubic number fields, which have a torsion group isomorphic to the cyclic group of five elements. Restricting ourselves to cyclic cubic number fields the situation changes. In this case the discriminant of $P_3(z)$ has to be a square and we deal with the following diophantine equation:

$$D(\varepsilon_2 5^k G_m, \varepsilon_2\varepsilon_3 5^k G_{m-5\varepsilon_3}) = \Box \qquad (3)$$

where

$$\begin{aligned} D(u, w) \quad = \quad & 15125 + 1464w - 3948u - 462uw + 24w^2 \\ & -24uw^2 + 244u^2 + 20u^2w + u^2w^2 - 4u^3 - 4w^3. \end{aligned}$$

Thus, for fixed $k, \varepsilon_2, \varepsilon_3$, the left hand side of these equations are eighth order linear recurrence sequences, which are of course related to the Fibonacci and Lucas sequences. Using the methods of sections 3.1 and 3.2 we were able to solve these equations completely and proved

Theorem 2.2 *Let G_m be one of the sequences F_m, L_m, if $k \geq 0$ or F_{5m}, if $k = -1$. Then the diophantine equation (3) has in the integers $k \geq -1, m, y \geq 0$ and $\varepsilon_2, \varepsilon_3 \in \{-1, 1\}$ only the solutions*

F_m :	$(1, 0, 65, 1, 1)$	$(1, 4, 4075, 1, -1)$	$(0, 3, 163, -1, 1)$
L_m :	$(1, 1, 520, -1, 1)$	$(0, 2, 63, 1, 1)$	$(1, 2, 65, 1, 1)$
$F_{5m}/5$:	$(-1, 0, 117, 1, -1)$	$(-1, 5, 139, -1, 1)$.	

Remark that even the finiteness of the number of solutions of equations (3) does not follow from general results about diophantine equations.

The second example is coming from algebraic number theory. Let $\mathbb{K}$ be an algebraic number field of degree d and let us denote by $\mathbb{Z}_{\mathbb{K}}$ its ring of integers. It is well known that $\mathbb{Z}_{\mathbb{K}}$ admits always a $\mathbb{Z}$ basis $\omega_1 = 1, \omega_2, \dots, \omega_d$, but usually the $\omega's$ are not powers of a fixed element of $\mathbb{Z}_{\mathbb{K}}$, i.e. $\mathbb{Z}_{\mathbb{K}}$ does not have a power integer basis. For quartic number fields with Galois group D_4 we proved with Gaál and Pohst [15, 16] that in order to establish all power integer bases it is enough to find quadratic polynomial values in some second order linear recurrence sequences.

3 Elementary methods

From now on we shall concentrate on methods for the resolution of equation (1). To solve a concrete equation, elementary methods are the most frequently used ones. Relations between sequences, divisibility properties, etc. are often very useful, but we restrict ourselves here to dealing with two sieving procedures, which we consider the most powerful and specific elementary tools in this topic.

3.1 Wunderlich sieve

In order to prove that among the first one million Fibonacci numbers only $0, 1$ and 144 are squares, Wunderlich [58] used a sieving procedure. We describe his method in the more general situation, for equation (1).

We start with a common trick of the theory of diophantine equation: if $n, x \in \mathbb{Z}$ is a solution of (1) then

$$G_n \equiv P(x) \pmod{m}$$

holds for all $m \in \mathbb{Z}$. For the integer m let us fix a complete residue system. This consists usually of the absolute smallest or of the smallest positive residues. It is well known that the sequence $G_n \bmod m$ is periodic and if $(m, A_k) = 1$ then it is purely periodic. Let $r_G(m)$ denote the length of the minimal period of $G_n \bmod m$.

Choose integers $m_1, \dots, m_t > 0$ with $(m_i, A_k) = 1,\ i = 1, \dots, t$ and initialize an array $A[i,j] := 0,\ i = 1, \dots, t;\ j = 0, \dots, r_G(m_i) - 1$. Compute now for any $i = 1, \dots, t$ the numbers $G_n \bmod m_i$ for $n = 1, \dots, r_G(m_i) - 1$ and $P(x) \bmod m_i$ for $x = 0, \dots, m_i - 1$ and put $A[i,j] := 1$ if there exists a $0 \le x < m_i$ such that $G_j \equiv P(x) \pmod{m_i}$. The pair of integers n, x is a solution of (1) only if

$$A[i, n \bmod m_i] = 1$$

holds for all $i = 1, \dots, t$. By this simple procedure we are able to localize the possible solutions in n modulo the least common multiple R of $r_G(m_1), \dots r_G(m_t)$.

One can considerably increase the performance of the sieving procedure by computing first the period lengths for the elements of a large set of integers and choosing only those as sieving moduli for which the least common multiple of their period length is small compared to the individual period length. This method was implemented by Nemes [24].

If equation (1) has no solution, then one can prove this quickly by using the Wunderlich sieve. In [16] we reported about an extensive computation, where 13267 equations of type (1) were considered with G_n second order linear recurrence sequence and $P(x)$ quadratic polynomials. We got these by transforming index form equations of quartic number fields with Galois group D_4 and discriminants up to 10^6. The Wunderlich sieve found 6595 cases in which the equations were not solvable.

A typical application of the Wunderlich sieve is to prove, with an appropriate choice of the set $\mathcal{M} = \{m_1, \dots, m_t\}$, that all solutions of (1) in n belong to some residue classes mod R. Enlarging the set $\mathcal{M}$ we can prove the same result with respect to a larger range. But this process never yields a complete solution of (1) in the case when it admits a solution $n \in \mathbb{Z}$, because the elements of the residue class of $n \bmod R$ always solve (1). To completely solve (1) in such cases one needs either an upper bound for the possible solutions or one has to combine this method with Cohn's sieve. By combining the Wunderlich sieve with an upper bound for the possible solution, which was proved by using a lower bound for linear forms in logarithms of algebraic numbers I proved that only $0, 1$ and 8 are cubes [26] and only 0 and 1 are fifth power Fibonacci numbers [27]. You may find examples for the combination of the sieves Wunderlich and Cohn in [16] and [28, 33].

I finish this section with a problem:

Problem: *The sequence of tribonacci numbers is defined by* $T_0 = T_1 = 0, T_2 = 1$ *and* $T_{n+3} = T_{n+2} + T_{n+1} + T_n$ *for* $n \geq 0$*. Are the only squares* $T_0 = T_1 = 0, T_2 = T_3 = 1, T_5 = 4, T_{10} = 81, T_{16} = 3136 = 56^2$ *and* $T_{18} = 10609 = 103^2$ *in* T_n*?*

By using the sieving moduli $3, 7, 11, 13, 29, 41, 43, 53, 79, 101, 103, 131, 239, 397, 421, 911, 1021$ and 1123 one can show that this is true for $n \leq 2 \cdot 10^6$, but no known method seem to be applicable for the solution of this problem.

3.2 Cohn sieve

In this section $\Box$ will denote a square of an integer. The essential tools of J.E.H. Cohn [3] in solving the equations $F_n = \Box, 2\Box$ and $L_n = \Box, 2\Box$ were the following identities:

$$\begin{aligned} F_{n+\ell} &\equiv -F_\ell \pmod{L_{2^{t-1}m}}, \\ L_{n+\ell} &\equiv -L_\ell \pmod{L_{2^{t-1}m}}, \end{aligned}$$

provided that $n = 2^t m$ with $t \geq 2$ and $m \not\equiv 0 \pmod 3$. Several different generalizations were presented by himself [6, 7], by Ribenboim and McDaniel [34, 35, 36], by Gaál, Pethő and Pohst [16] and by Pethő and Zimmer [33]. We cite here a combination of Lemma 1 of [36] and Theorem 3.2 of [16].

In the rest of this section, $U_n = U_n(A_1, A_2), V_n = V_n(A_1, A_2)$ and $G_n = G_n(A_1, A_2)$ denote second order linear recurrence sequences satisfying the same recurrence relation with coefficients A_1, A_2 and with initial terms $U_0 = 0, U_1 = 1, V_0 = 2, V_1 = A_1$ and $G_0, G_1 \in \mathbb{Z}$ respectively. We assume further that $(A_1, A_2) = 1$ and $A_1^2 + 4A_2 > 0$. We will denote by $(a|m)$ the Jacobi symbol. The core of Cohn's sieve is the following theorem

Theorem 3.1 *Let A_1 be odd, $n = 2^t m$ with $t \geq 1$ and $m \geq 1$, odd. Then*

$$G_{2n+\ell} \equiv -(A_2)^n G_\ell \pmod{V_n} \tag{4}$$

for all $\ell \geq 0$.

This is a combination of Lemma 1 of [36] and Theorem 3.2 of [16]. Extending Cohn's idea Ribenboim and McDaniel used this theorem in the following way: If, for example, for given parameters A_1 and A_2, $U_n = \square$, then the residue class U_n modulo M is a square and therefore $(U_n|M) = 1$ for any odd M coprime to U_n. They were able to find, for most n, appropriate moduli $M_1, \ldots, M_t$ such that the product $(U_n|M_1) \cdots (U_n|M_t) = -1$, leading to contradiction. The remaining values of n were treated by using divisibility properties of U_n. They proved [36]

Theorem 3.2 *Let A_1 and A_2 be odd integers, then*

(a) If $V_n = \square$, then $n = 1, 3$ or 5.

(b) If $V_n = 2\square$, then $n = 0, 3$ or 6.

(c) If $U_n = \square$, then $n = 0, 1, 2, 3, 6$ or 12.

(d) If $U_n = 2\square$, then $n = 0, 3$ or 6.

Remark that in [36] the exceptional cases are completely described. Special cases of this theorem were proved in [3, 6, 7, 8, 59]. By using A. Baker's method Mignotte and Pethő [21] proved that if $U_n(A_1, -1) = d\square$, with $d = 1, 2, 3, 6$ then $n \leq 4$, moreover $U_4(A_1, -1) = d\square$ only if $A_1 = 338, U_4(338, -1) = (2 \cdot 13 \cdot 239)^2$. In this case A_1 is arbitrary. Another general result of this sort was found by Chen and Voutier [2]. By using hypergeometric polynomials they proved: Let

$d \geq 3$ and (u, v) be the fundamental solution of the Pell equation $X^2+1 = dY^2$. Then the equation $X^2 + 1 = dY^4$ has got at most one solution in positive integers. If this solution (x, y) exists, we have $v = y^2$. This result implies that if $U_{2t+1}(A_1, 1) = \square$ then $t = 0$, whenever $A_1 > 2$.

You can find several applications of variations of Theorem 3.1 in the literature. Williams [55] determined the Fibonacci numbers of the form $\square + 1$, Robbins [39] solved the equations $F_n, L_n = w^2 - 1, w^3 \pm 1$; Wall [52] determined the triangular Fibonacci numbers and Ribenboim and McDaniel [37, 34] the square classes in the Fibonacci and Lucas sequences and in their generalizations. I remark here that using linear forms in logarithms of algebraic numbers Kiss [17] generalized the latest mentioned result.

Theorem 3.1 can be used successfully to find quadratic polynomial values in second order linear recurrence sequences, and more generaly in polynomials of second order linear recurrence sequences as well. For this purpose the following theorem [33] is useful

Theorem 3.3 *Let $H(x) \in \mathbb{Z}[x], G_n$ an linear recurrence sequence with $|A_2| = 1$, $m_0 \in \mathbb{Z}$ and $\mathcal{P} = \{p_1, \ldots, p_t\}$ a set of primes with $p_i \geq 5, 1 \leq i \leq t$. Suppose that there exist positive integers $a, b_1, \ldots, b_t$ such that there exist for any $\alpha \geq a - 1$ integers $\beta_1, \ldots, \beta_t$ with $0 \leq \beta_i \leq b_i$ $(i = 1, \ldots, t)$ for which*

$$\left(H(-G_{m_0})|V_{2^\alpha p_1^{\beta_1}\cdots p_t^{\beta_t}}\right) = -1$$

holds. Then equation

$$H(G_n) = \square \qquad (5)$$

has at most one solution n satisfying

$$n \equiv m_0 \ (mod\, 2^{a+1}p_1^{b_1} \cdot p_t^{b_t}),$$

namely $n = m_0$.

This theorem implies the following process which we call Cohn's sieve. Put $M' = H(-G_{m_0})$ and let M be the square free part of M'. For simplicity we assume M to be odd. Let h be a positive odd integer, then

$$(M|V_{2^a h}) = \pm(V_{2^a h}|M)$$

holds by the reciprocity law of the Jacobi symbol.

Let now a run through the set of positive integers, then the sequence $\{V_{2^a h} \bmod M\}$ is periodic, thus $\{(V_{2^a h}|M)\}$ is periodic, too. Let denote $e(h, M)$ the length of its preperiod and $r(h, M)$ its period respectively. It is easy to see that $e(h, M) \leq e(1, M)$ holds for all odd h.

The sieving process is now the following: Choose primes $p_1, \ldots, p_t \geq 5$ and set

$$A[i, j] := (M|V_{2^j p_i})\ i = 1, \ldots, t,\ j = 1, \ldots, e(1, M) + r(p_i, M).$$

If there exists for any $j > e(1, M)$ an integer $1 \leq i \leq t$ such that $A[i, j] = -1$ then Theorem 3.3 can be applied and we conclude that the only solution of (5) with $n \equiv m_0 \pmod{2^{e(1,M)+1} p_1 \cdots p_t}$ is m_0. If, on the other hand, we are able to prove, for example by using the Wunderlich sieve, that (5) holds only if $n \equiv m_0 \pmod{2^{e(1,M)+1} p_1 \cdots p_t}$, then the equation is completely solved.

We illustrate the method by a simple example. Consider the equation

$$G_n = y^2 + 30,$$

where G_n denotes the sequence defined by $G_0 = 70, G_1 = 55, G_{n+2} = 3G_{n+1} - G_n$ for $n \geq 0$. It is clear that $(n, y) = (1, 5)$ is a solution, hence we have $m_0 = 1$ and $H(x) = x - 30$. Thus taking $M' = -G_1 - 30 = -85$, which is square-free and odd $M = M'$.

It is easy to see that the Lucas sequence $\{V_n(3, -1)\}$ associated to G_n has the property: $V_t \equiv -1 \pmod 4$ for every t, which is not divisible by 3. Let t be such an integer. Then

$$(M|V_t) = (-5 \cdot 17|V_t) = -(V_t|5)(V_t|17) = (V_t|17),$$

because $(V_t|5) = -1$ for all t. We also have

$$\begin{array}{cccccc} j & = 0 & 1 & 2 & 3 & 4 \\ (V_{2^j}|17) & = \text{-1} & \text{-1} & 1 & \text{-1} & \text{-1} \\ (V_{5\cdot 2^j}|17) & = 1 & \text{-1} & \text{-1} & 1 & \text{-1} \end{array}.$$

The period length of both sequences is three and by Theorem 3.3 we obtain $n = 1$ whenever $n \equiv 1 \pmod{20}$. On the other hand, $\{G_n - 30 \bmod 3\} = (1, 1, 2, 2)^\infty$ and $\{G_n - 30 \bmod 7\} = (5, 4, 2, 4)^\infty$, thus both sequences have period length 4 and as $(2|3) = (5|7) = -1$ we obtain $n \equiv 1 \pmod 4$, hence our equation has got the only solution $n = 1$.

Cohn's sieve was implemented at the Lajos Kossuth University by J. Sajtos. By using it we were able to solve 5919 of 7850 equations of type $G_n = \Box + D$, coming from index form equations over quartic number fields [16]. This was also the essential tool, using which we proved Theorem 2.2, see [33, 28].

Remark that Cohn's sieve does not work always; an example is presented in section 4, but the cases when it fails to work can be characterized. In [16] it is proved namely, that if there exist integers $e(1, M) < m_1, m_2 \le e(1, M)+r(1, M)$ such that $(V_{2^{m_1}}|M)(V_{2^{m_2}}|M) = -1$, then there exists an integer $a \le e(1, M) + r(1, M) + 1$ and primes $p_1, \ldots, p_t > 3$ such that equation (5) has got at most one solution $n \equiv m_0 \pmod{2^a p_1 \cdots p_t}$, namely $n = m_0$.

4 Tools from algebraic number theory

Elementary methods often fail in solving equation of type (1). In such cases we have to use much involved methods. Tools of the theory of algebraic numbers are often helpful to transform equations to more simple or more treatable ones. We illustrate this by an example, which is taken from de Weger [54].

Ray Steiner observed that the eleventh Fibonacci number 89 has the property

$$\frac{1}{89} = \sum_{k=0}^{\infty} \frac{F_t}{10^{t+1}}.$$

He asked de Weger, whether a similar phenomenon occurs for expansions in the base y number system of reciprocals of Fibonacci numbers for values of y other than 10. This is equivalent with the question: for which positive integers n, y does the identity

$$\frac{1}{F_n} = \sum_{k=0}^{\infty} \frac{F_t}{y^{t+1}}$$

hold? One can easily check, that *it happens also for* $(n, y) = (1, 2), (2, 2), (5, 3)$ *and* $(10, 8)$ *and de Weger [54] was able to prove that these are the only solutions.*

What does this problem have to do with diophantine equations? By observing that

$$\sum_{k=0}^{\infty} \frac{F_t}{y^{t+1}} = \frac{1}{y^2 - y - 1}$$

we see that to solve Steiner's problem it is enough to solve the equation

$$F_n = y^2 - y - 1. \tag{6}$$

Before continuing de Weger's argument we shall point out that for this equation Cohn's sieve fails to work because not only $(1, 2)$ but also $(-1, 1)$ is a solution of (6), hence we can not rule out $(1, 2)$ by the sieving procedure.

Using the well-known identity $L_n^2 - 5F_n^2 = \pm 4$ we transform (6) to the pair of equations

$$x^2 - 5(y^2 - y - 1)^2 = \pm 4. \tag{7}$$

Both of the equations (7) are quartic elliptic equations. It is well-known (see Mordell [23]) that all integer solutions can be obtained from integer solutions of finitely many quartic Thue equations. To find these Thue equations we have to work in algebraic number fields. De Weger followed essentially Mordell's argument, but made use of the special nature of the number fields appearing in the transformation.

After this remark consider first the case of minus sign in (7) and observe that

$$4 - 5(y^2 - y - 1)^2 = (2 - (y^2 - y - 1)\sqrt{5})(2 + (y^2 - y - 1)\sqrt{5}) = -x^2,$$

thus we have to work in the algebraic number field $\mathbf{Q}(\sqrt{5})$. It has got class number 1, a fundamental unit is $(1+\sqrt{5})/2$, and 2 remains prime. A common prime divisor of $(2+(y^2-y-1)\sqrt{5})$ and $(2-(y^2-y-1)\sqrt{5})$ can only be 2. Thus we obtain

$$2+(y^2-y-1)\sqrt{5} = (-1)^a 2^b \left(\frac{1+\sqrt{5}}{2}\right)^c \alpha^2,$$

where $a,b,c \in \{0,1\}$, and α is an integer in $\mathbf{Q}(\sqrt{5})$. Assuming $y \geq 2$ and since x has to be odd, this implies $a=b=0$. Finally, since the norm of $2+(y^2-y-1)\sqrt{5}$ is $(-1)^c N(\alpha)^2 = -x^2$, we have $c=1$. Writing $\alpha = (A+B\sqrt{5})/2$, where the integers A,B have the same parity we obtain

$$\begin{aligned} A^2+10AB+5B^2 &= 16 \\ A^2+2AB+5B^2 &= 8(y^2-y-1). \end{aligned} \tag{8}$$

Now five times the first equation plus eight times the second equation yields

$$13A^2+66AB+65B^2 = 16(2y-1)^2.$$

Observe that the polynomial staying on the left hand side factors over $\mathbf{Q}(\sqrt{61})$

$$(13A+33B+2B\sqrt{61})(13A+33B-2B\sqrt{61}) = 13\cdot 16(2y-1)^2.$$

The field $\mathbf{Q}(\sqrt{61})$ has got again class number 1, a fundamental unit is $(39+5\sqrt{61})/2$, the prime 2 remains prime, and 13 splits: $13 = -((3+\sqrt{61})/2)(3-\sqrt{61})/2))$. As a common prime divisor of the two factors of the left hand side of the last equation divides $2\cdot 13\cdot 61$, we obtain

$$13A+33B+2B\sqrt{61} = \pm 2^a \left(\frac{3+\sqrt{61}}{2}\right)^b \left(\frac{3-\sqrt{61}}{2}\right)^c (\sqrt{61})^d \left(\frac{39+5\sqrt{61}}{2}\right)^e \alpha^2,$$

where $a,b,c,d,|e| \in \{0,1\}$, and α is an integer in $\mathbf{Q}(\sqrt{61})$. Taking again norm we conclude that the only possibilities are $a=d=0$, $(b,c)=(0,1)$ or $(1,0)$ and

$e = \pm 1$. Thus, letting $\alpha = (u + v\sqrt{61})$ with integers u, v, we find

$$13A + 33B + 2B\sqrt{61} = (47 \pm 6\sqrt{61})(u + v\sqrt{61}). \tag{9}$$

Comparing the coefficients of 1 and $\sqrt{61}$ we can express A and B as quadratic forms in u, v. The negative sign in (9) which corresponds to the case $(b, c, e) = (0, 1, 1)$ leads to contradiction modulo 13. The positive sign can not be ruled out so easily. In that case we insert the expressions for A and B into (8) and using the transformation $E = v, F = (u + 7v)/2$ we find the Thue equation

$$E^4 + 2E^3F - 41E^2F^2 - 102EF^3 - 59F^4 = 1.$$

Similarly, considering the plus sign in (7) and working first in the field $\mathbf{Q}(\sqrt{-5})$ and then in the field $\mathbf{Q}(\sqrt{21})$ we obtain one more non trivial quartic Thue equation to solve, namely

$$9E^4 + 18E^3F + 31E^2F^2 + 2EF^3 - 11F^4 = 9.$$

De Weger finished the solution of Steiner's problem by solving these Thue equations.

Remark that for the solution of Thue equations there are very efficient methods available. We will not present them here, but refer to the papers [30, 50, 1]. We also mention that the method of [1] is implemented in the computational number theory package KANT, which was developed at the TU Berlin by M. Pohst and by his collaborators.

References

[1] Yu. Bilu and G. Hanrot, *Solving Thue equations of high degree* J. Number Theory, to appear.

[2] Chen Jian Hua and P.M. Voutier *Complete solution of the Diophantine equation $x^2 + 1 = dY^4$*, J. Number Theory, to appear.

[3] J.H.E. COHN, *On square Fibonacci numbers,* J. London Math. Soc. **39** (1964), 537–540.

[4] J.H.E. COHN, *Square Fibonacci numbers, etc.* Fibonacci Quart. **2** (1964), 109–113.

[5] J.H.E. COHN, *Lucas and Fibonacci numbers and some Diophantine equations,* Proc. Glasgow Math. Assoc. **7** (1965), 24–28.

[6] J.H.E. COHN, *Eight Diophantine equations,* Proc. London Math. Soc. **16** (1966), 153–166.

[7] J.H.E. COHN, *Five Diophantine equations,* Math. Scand. **21** (1967), 61–70.

[8] J.H.E. COHN, *Squares in some recurrent sequences,* Pacific J. Math. **41** (1972), 631–646.

[9] J.H.E. COHN, *The diophantine equation $x^2 + C = y^n$*, Acta Arith. **65** (1993), 367–381.

[10] J.H.E. COHN, *The Diophantine Equation $x^4 + 1 = Dy^2$*, Math. Comp., to appear.

[11] A. ESWARATHASAN, *On square pseudo-Lucas numbers,* Canad. Math. Bull. **21** (1978), 297–303.

[12] J.H. EVERTSE, *On sums of S-units and linear recurrences,* Comp. Math. **53** (1984), 225-244.

[13] J.-H. EVERTSE, K. GYŐRY, C. L. STEWART and R. TIDJEMAN, *$S-$unit equations and their applications* in: New Advances in Transcendence Theory, Ed: A. Baker, Camb. Univ. Press, Cambridge, 1988.

[14] R. FINKELSTEIN, *On Fibonacci numbers which are one more than a square,* J. reine angew. Math. **262-263** (1973), 171–178.

[15] I. Gaál, A. Pethő and M. Pohst *On the resolution of index form equations in biquadratic number fields* I. J. Number Theory **38** (1991), 18-34.

[16] I. Gaál, A. Pethő and M. Pohst *On the Resolution of Index Form Equations in Dihedral Quartic Number Fields,* Experimental Math. **3** (1994) 245–254.

[17] P. Kiss, *Pure powers and power classes in recurrence sequences*, Math. Slovaca **44** (1994) 525-529.

[18] M. Laurent, *Équations exponentielles polynômes et suites récurrentes linéaires* Asterisque **147-148**, (1987) 121–139.

[19] M. Laurent, *Équations exponentielles polynômes et suites récurrentes linéaires II* J. Number Theory **31** (1989) 24–53.

[20] H. London and R. Finkelstein, *On Fibonacci and Lucas numbers which are perfect powers,* Fibonacci Quart. **7** (1969), 476–481., errata bf 8 (1970), 248.

[21] M. Mignotte and A. Pethő, *Sur les carrés dans certaines suites de Lucas,* Journal de Théorie Nombres de Bordeaux **5** (1993), 333-341.

[22] M. Mignotte and N. Tzanakis, *Arithmetical study of recurrence sequences*, Acta Arith. **57** (1991). 357-364.

[23] L.J. Mordell, *Diophantine equations*, Academic Press, 1969.

[24] I. Nemes, *On the solution of the diophantine equation $G_n = P(x)$ with sieve method*, in Computational Number Theory, Walter de Gruyter, Berlin-New York, 1991, pp. 303-311.

[25] C.S. Ogilvy, *Tomorrow's math, unsolved problems for the amateur,* Oxford Univ. Press, 1962.

[26] A. Pethő, *Full Cubes in the Fibonacci Sequences,* Publ. Math. Debrecen **30** (1983), 117-127.

[27] A. Pethő, *Perfect Powers in Second Order Recurrences,* in: *Topics in Classical Number Theory*, Budapest, 1981, 1217-1227.

[28] A. Pethő, *Systems of norm equations over cubic number fields,* Grazer Math. Ber. **318** (1992), 111–120.

[29] A. Pethő, *Diophantine properties of linear recursive sequences II,* in preparation.

[30] A. Pethő und R. Schulenberg *Effektives Lösen von Thue Gleichungen,* Publ. Math. Debrecen **34** (1987) 189-196.

[31] A. Pethő and B.M.M. de Weger, *Product of Prime Powers in Binary Recurrence Sequences I.,* Math. Comp. **47** (1986), 713 -727.

[32] A. Pethő, Th. Weiss and H.G. Zimmer, *Torsion groups of elliptic curves with integral j-invariant over general cubic number fields,* Intern. J. Alg. Comp., to appear.

[33] A. Pethő and H.G. Zimmer, *On a system of norm-equations over cyclic cubic number fields,* in preparation.

[34] P. Ribenboim and W.L. McDaniel, *Square classes of Lucas sequences,* Port. Math. **48** (1991), 469–473.

[35] P. Ribenboim and W.L. McDaniel, *Squares and double-squares in Lucas sequences,* C.R. Math. Rep. Acad. Sci. Canada **14** (1992), 104–108.

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

[37] P. Ribenboim, *Square classes of Fibonacci and Lucas numbers,* Port. Math. **46** (1989), 159–175.

[38] N. Robbins, *On Fibonacci numbers which are powers,* Fibonacci Quart. **16** (1978), 515–517.

[39] N. Robbins, *Fibonacci and Lucas numbers of the form* $w^2 - 1, w^3 \pm 1$, Fibonacci Quart. **19** (1981), 369–373.

[40] N. Robbins, *On Fibonacci numbers of the form* px^2*, where* p *is a prime,* Fibonacci Quart. **21** (1983), 251–254.

[41] N. Robbins, *On Pell numbers of the form* PX^2*, where* P *is a prime,* Fibonacci Quart. **22** (1984), 340–348.

[42] A.P. Rollett, *Problem* 5080*,* Amer. Math. Monthly **70** (1963), 216.

[43] H.P. Schlickewei, *S-unit equations over number fields,* Invent. Math. **102** (1990), 95-107.

[44] H.P. Schlickewei and A.J. van der Poorten, *The growth conditions for recurrence sequences,* Macquarie Univ. Math. Rep. 82-0041. North Ryde, Australia.

[45] H. P. Schlickewei and W. M. Schmidt, *Linear Equations in Members of Recurrence Sequences* Ann. Scuola Norm. Sup. di Pisa (4) **20** (1993), 219–246

[46] W.M. Schmidt, *Norm form equations,* Annals of Math. **96** (1972), 526-551.

[47] W.M. Schmidt, *Diophantine Approximations and Diophantine Equations,* Lecture Notes in Mathematics Vol. 1467, Springer Verlag, 1991.

[48] T.N. Shorey and R. Tijdeman, *Exponential Diophantine Equations*, Cambridge Univ. Press 1986.

[49] J. Silverman, *The Arithmetic of Elliptic Curves,* Graduate Text in Math., Springer Verlag, 1985.

[50] N. Tzanakis and B.M.M. de Weger, *On the practical solution of the Thue equation*, J. Number Theory **31** (1989) 99-132.

[51] N.N. Vorobjev, *Fibonacci Numbers* (in Russian), sixth edition, Nauka Moskau, 1978.

[52] C.R. Wall, *On the triangular Fibonacci numbers,* Fibonacci Quart. **23** (1985), 77–79.

[53] B.M.M. de Weger, *Algorithms for diophantine equations*, CWI Tract Vol. 65. 1989.

[54] B.M.M. de Weger, *A curious property of the eleventh Fibonacci number,* Rocky Mountain J. of Math. **25** (1995), 977-994.

[55] H.C. Williams, *On the Fibonacci numbers of the form* k^2+1*, is a prime,* Fibonacci Quart. **13** (1975), 213-214.

[56] H.C. Williams and C.R. Zarnke *Computer solution of the Diophantine equation* $x^2-dy^4=-1$, Proceedings of the Second Manitoba Conference on Numerical Mathematics (Univ. Manitoba, Winnipeg, Man., 1972), pp. 405–416. Congressus Numeratium, No.VII, Utilitas Math., Winnipeg, Man., 1973.

[57] J. Wolfskill, *Bounding squares in second order recurrence sequences*, Acta Arith. **54** (1989) 127-145.

[58] M.C. Wunderlich, *On the existence of Fibonacci squares,* Math. Comp. **17** (1963), 455-457.

[59] O. Wyler, *Solution of Problem* 5080, Amer. Math. Monthly **71** (1964), 220-222.

[60] H. G. Zimmer, *Torsion Groups of Elliptic Curves over Cubic and Certain Biquadratic Number Fields.* Contemp. Math. **174** (1994), 203-220.

AMS Classification Numbers: 11B37, 11D61