involve
a journal of mathematics

A nonextendable Diophantine quadruple arising from a triple of Lucas numbers

A. M. S. Ramasamy and D. Saraswathy

msp

2012 vol. 5, no. 3

INVOLVE 5:3 (2012)
dx.doi.org/10.2140/involve.2012.5.257

A nonextendable Diophantine quadruple arising from a triple of Lucas numbers

A. M. S. Ramasamy and D. Saraswathy

(Communicated by Filip Saidak)

We establish that the only positive integral solutions common to the two Pell's equations $U^2 - 18V^2 = -119$ and $Z^2 - 29V^2 = -196$ are $U = 41$, $V = 10$ and $Z = 52$.

1. Introduction

Let n be a nonzero integer. We say that two integers α and β have the Diophantine property $D(n)$ if $\alpha\beta + n$ is a prefect square. A set of numbers has the property $D(n)$ if every pair of distinct elements of the set has this property. A Diophantine set S with property $D(n)$ is said to be extendable if, for some integer d, with d not belonging to S, the set $S \cup \{d\}$ is also a Diophantine set with property $D(n)$.

Sets consisting of Fibonacci numbers $\{F_m\}$ and Lucas numbers $\{L_m\}$ with the Diophantine property $D(n)$ have attracted the attention of many number theorists recently. A. Baker and H. Davenport [1969] dealt with the quadruple $\{1, 3, 8, 120\}$ with property $D(1)$ in which the first three terms are F_2, F_4 and F_6. They proved that the set cannot be extended further. V. E. Hoggatt and G. E. Bergum [1977] proved that the four numbers F_{2k}, F_{2k+2}, F_{2k+4} and $d = 4F_{2k+1}F_{2k+2}F_{2k+3}$, for $k \geq 1$, have the Diophantine property $D(1)$ and conjectured that no other integer can replace d here. The result of Baker and Davenport [1969] was an assertion of the conjecture for $k = 1$. A. Dujella [1999] proved the Hoggatt-Bergum conjecture for all positive integral values of k.

Dujella [1995] also considered Diophantine quadruples for squares of Fibonacci and Lucas numbers. In this paper we consider the Lucas numbers L_n, which are defined by $L_0 = 2$, $L_1 = 1$, $L_{n+2} = L_{n+1} + L_n$. The three Lucas numbers L_1, L_6 and L_7 have the property $D(7)$. The aim of this paper is to determine whether this set $\{1, 18, 29\}$ is extendable.

MSC2010: primary 11B39; secondary 11D09, 11B37.

Keywords: Lucas numbers, Diophantine property, recurrence relation, simultaneous Pell's equations, characteristic number, factorization, Jacobi symbol.

2. Formulation of the problem

Suppose the natural number x extends the set $S = \{1, 18, 29\}$. Then we have

$$x + 7 = V^2, \tag{1}$$

$$18x + 7 = U^2, \tag{2}$$

$$29x + 7 = Z^2, \tag{3}$$

for some integers U, V, Z. Solving (1), (2) and (3) is equivalent to solving simultaneously the two Pell's equations

$$U^2 - 18V^2 = -119, \tag{4}$$

$$Z^2 - 29V^2 = -196. \tag{5}$$

We prove that there is essentially a unique solution, so the set S can be extended by exactly one element:

Theorem. *The only positive integral solutions common to the two Pell's equations* $U^2 - 18V^2 = -119$ *and* $Z^2 - 29V^2 = -196$ *are* $U = 41$, $V = 10$ *and* $Z = 52$.

Using these values in (1) yields $x = 93$. Therefore:

Corollary. *The triple* $\{1, 18, 29\}$ *of Lucas numbers is extendable*; *the quadruple* $\{1, 18, 29, 93\}$ *has the Diophantine property* $D(7)$ *and cannot be extended further.*

3. Methodology

For the determination of the common solutions of the system of Pell's equations $3x^2 - 2 = y^2$ and $8x^2 - 7 = z^2$, Baker and Davenport [1969] gave a method based on the linear forms of logarithms of algebraic numbers. P. Kanagasabapathy and T. Ponnudurai [1975] applied quadratic reciprocity to the same system. S. P. Mohanty and A. M. S. Ramasamy [1985] introduced the concept of the characteristic number of two simultaneous Pell's equations and solved the system $U^2 - 5V^2 = -4$ and $Z^2 - 12V^2 = -11$. N. Tzanakis [2002] gave a method in for solving a system of Pell's equations using elliptic logarithms, and earlier [1993] described various methods available in the literature for finding out the common solutions of a system of Pell's equations. (For a history of numbers with the Diophantine property, one may refer to [Ramasamy 2007].)

When applying congruence methods to solve a given system of Pell's equations, the traditional approach is to work with a modulus of the form $2^\tau \cdot 3 \cdot 5$ ($\tau \geq 1$) in the final stage of computation; see, e.g., [Kangasabapathy and Ponnudurai 1975] and [Mohanty and Ramasamy 1985]. This modulus involves only two specific odd primes, namely 3 and 5. Because of the inadequacy of such a restricted modulus for handling several problems, a method involving a general modulus was established in [Ramasamy 2006]. The present problem involves computational complexities and a new method is devised to overcome the computational difficulty by employing a result in this same reference. Taking D as a fixed natural number, one may refer to [Nagell 1951, pp. 204–212] for a theory of the general Pell's equation

$$U^2 - DV^2 = N. \tag{6}$$

We follow the conventional notations in the literature. An interesting property of Equation (6) is that its solutions may be partitioned into a certain number of disjoint classes. If m and n are two distinct integers, $U_n + V_n\sqrt{D}$ and $U_m + V_m\sqrt{D}$ belong to the same class of solutions of (6) if

$$U_n + V_n\sqrt{D} = (u + v\sqrt{D})(a + b\sqrt{D})^n, \tag{7}$$

$$U_m + V_m\sqrt{D} = (u + v\sqrt{D})(a + b\sqrt{D})^m, \tag{8}$$

where $a + b\sqrt{D}$ is the fundamental solution of Pell's equation

$$A^2 - DB^2 = 1 \tag{9}$$

and $u + v\sqrt{D}$ is the fundamental solution of (6) in the particular class. Otherwise, $U_n + V_n\sqrt{D}$ and $U_m + V_m\sqrt{D}$ belong to different classes of solutions, which are referred to as nonassociated classes (see [Nagell 1951, pp. 204–205], for example). Let $U_n + V_n\sqrt{D}$ ($n = 0, 1, 2, \dots$) constitute a class of solutions of (6), so that we have

$$U_n + V_n\sqrt{D} = (u + v\sqrt{D})(a + b\sqrt{D})^n.$$

All the solutions of (9) with positive A and B are obtained from the formula

$$A_n + B_n\sqrt{D} = (a + b\sqrt{D})^n, \tag{10}$$

where $n = 1, 2, 3, \dots$. We have the following relations from [Mohanty and Ramasamy 1985, pp. 204–205]:

$$U_n = uA_n + DvB_n, \tag{11}$$

$$V_n = vA_n + uB_n, \tag{12}$$

$$U_{n+s} = A_sU_n + DB_sV_n, \tag{13}$$

$$V_{n+s} = B_sU_n + A_sV_n. \tag{14}$$

The sequences U_n and V_n satisfy the following recurrence relations:

$$U_{n+2} = 2aU_{n+1} - U_n, \tag{15}$$

$$V_{n+2} = 2aV_{n+1} - V_n, \tag{16}$$

$$U_{n+2s} \equiv -U_n \pmod{A_s}, \tag{17}$$

$$U_{n+2s} \equiv U_n \pmod{B_s}, \tag{18}$$

$$V_{n+2s} \equiv -V_n \pmod{A_s}, \tag{19}$$

$$V_{n+2s} \equiv V_n \pmod{B_s}. \tag{20}$$

Equations (7) and (10) imply that U_n and V_n depend on the values of A_n and B_n. In our present problem, we have $D = 18$ from (4) and therefore we have to consider the Pell equation

$$A^2 - 18B^2 = 1. \tag{21}$$

Equation (21) has the fundamental solution $A_1 = 17$, $B_1 = 4$. We check that $-67 + 16\sqrt{18}$, $-13 + 4\sqrt{18}$, $-23 + 6\sqrt{18}$ and $-41 + 10\sqrt{18}$ are the fundamental solutions of (4). Employing the condition stated for (7), we see that (4) has four nonassociated classes of solutions. Hence the general solution of (4) is given by

$$U_n + \sqrt{18}\, V_n = (-67 + 16\sqrt{18})(17 + 4\sqrt{18})^n, \tag{22}$$

$$U_n + \sqrt{18}\, V_n = (-13 + 4\sqrt{18})(17 + 4\sqrt{18})^n, \tag{23}$$

$$U_n + \sqrt{18}\, V_n = (-23 + 6\sqrt{18})(17 + 4\sqrt{18})^n, \tag{24}$$

$$U_n + \sqrt{18}\, V_n = (-41 + 10\sqrt{18})(17 + 4\sqrt{18})^n. \tag{25}$$

The solutions of (21) are provided by

$$A_0 = 1, \quad A_1 = 17, \quad A_{n+2} = 34A_{n+1} - A_n,$$
$$B_0 = 0, \quad B_1 = 4, \quad B_{n+2} = 34B_{n+1} - B_n.$$

4. Solutions of the form (22)

Now, we consider the solutions of (4) given by (22), namely

$$U_0 = -67, \quad U_1 = 13, \quad U_{n+2} = 34U_{n+1} - U_n,$$
$$V_0 = 16, \quad V_1 = 4, \quad V_{n+2} = 34V_{n+1} - V_n.$$

We repeatedly use the relation (19) and reason by cases.

(a) From (19) we have $V_{n+2s} \equiv -V_n \pmod{A_s}$. From this we obtain $V_{n+2} \equiv -V_n \pmod{A_1} \equiv -V_n \pmod{17}$. The sequence $V_n \pmod{17}$ is periodic with period 4. By quadratic reciprocity, we see that $n \not\equiv 0, 2 \pmod 4$. So, we are left with odd values of n only.

(b) We have $V_{n+4} \equiv -V_n \pmod{A_2} \equiv -V_n \pmod{577}$. The sequence V_n (mod 577) is periodic with period 8. We obtain $n \not\equiv 1, 3, 5, 7 \pmod 8$. Hence no solution of (4) having the form (22) satisfies (5).

5. Solutions of the form (23)

Next we consider the solutions of (4) of the form (23), namely

$$U_0 = -13, \quad U_1 = 67, \quad U_{n+2} = 34U_{n+1} - U_n,$$
$$V_0 = 4, \quad V_1 = 16, \quad V_{n+2} = 34V_{n+1} - V_n.$$

As in the previous case, one can check that no such solution can satisfy (5).

6. Solutions of the form (24)

Next we consider the solutions of (4) of the form (24), namely

$$U_0 = -23, \quad U_1 = 41, \quad U_{n+2} = 34U_{n+1} - U_n,$$
$$V_0 = 6, \quad V_1 = 10, \quad V_{n+2} = 34V_{n+1} - V_n.$$

(a) We see that $V_{n+4} \equiv -V_n \pmod{A_2} \equiv -V_n \pmod{577}$. The sequence $V_n \pmod{577}$ has period 8. By evaluating the Jacobi symbol

$$\left(\frac{V_n}{577}\right),$$

we check that $n \not\equiv 2, 3, 6, 7 \pmod 8$.

(b) We have $V_{n+6} \equiv -V_n \pmod{A_3} \equiv -V_n \pmod{1153}$. The sequence $V_n \pmod{1153}$ has period 12. It is ascertained that $n \not\equiv 8, 9 \pmod{12}$.

(c) We get $V_{n+12} \equiv -V_n \pmod{A_6} \equiv -V_n \pmod{768398401}$. On factoring, we get $768398401 = 97 \cdot 577 \cdot 13729$. Therefore $V_{n+12} \equiv -V_n \pmod{97}$. The sequence $V_n \pmod{97}$ has period 24. We see that $n \not\equiv 4, 5, 16, 17 \pmod{24}$. Also, we have $V_{n+12} \equiv -V_n \pmod{13729}$. The sequence $V_n \pmod{13729}$ has period 24. It is seen that $n \not\equiv 0, 12 \pmod{24}$.

So far we have excluded all possibilities other than $n \equiv 1 \pmod{12}$.

(d) We obtain $V_{n+16} \equiv -V_n \pmod{A_8} \equiv -V_n \pmod{886731088897}$. We see that $886731088897 = 257 \cdot 1409 \cdot 2448769$. Therefore $V_{n+16} \equiv -V_n \pmod{257}$. The sequence $V_n \pmod{257}$ has a period of 32. We check that $n \not\equiv 5, 9, 13, 21, 25, 29 \pmod{32}$. So we are left with $n \equiv 1 \pmod{16}$.

(e) We have $V_{n+10} \equiv -V_n \pmod{A_5} \equiv -V_n \pmod{22619537}$. We see that $22619537 = 17 \cdot 241 \cdot 5521$. Therefore $V_{n+10} \equiv -V_n \pmod{241}$. The sequence $V_n \pmod{241}$ has period 20. We check that $n \not\equiv 5, 17 \pmod{20}$. Also $V_{n+10} \equiv -V_n \pmod{5521}$ and the sequence $V_n \pmod{5521}$ has period 20. It is seen that $n \not\equiv 9 \pmod{20}$.

(f) We get $V_{n+20} \equiv -V_n \pmod{A_{10}} \equiv -V_n \pmod{1023286908188737}$. We see that $1023286908188737 = 577 \cdot 188801 \cdot 9393281$. Therefore $V_{n+10} \equiv -V_n$ (mod

9393281). The sequence V_n (mod 9393281) has a period of 40. We verify that $n \not\equiv 13, 33 \pmod{40}$.

The last three steps leave only the possibility $n \equiv 1 \pmod{20}$.

(g) We obtain $V_{n+14} \equiv -V_n \pmod{A_7} \equiv -V_n \pmod{26102926067}$. We see that 26102926067 = 17·1535466241. Therefore $V_{n+14} \equiv -V_n \pmod{1535466241}$. The sequence V_n (mod 1535466241) has period 28. We check that $n \not\equiv 5$, 13, 17, 21 (mod 28).

(h) We have $V_{n+28} \equiv -V_n (\mathrm{mod}\ A_{14}) \equiv -V_n \pmod{136272550150887306817}$. We see that 136272550150887306817 = 577·209441·11276410240481. Therefore $V_{n+28} \equiv -V_n \pmod{209441}$. The sequence V_n (mod 209441) has period 56. We obtain $n \not\equiv 9, 25 \pmod{56}$.

Steps (d), (g) and (h) leave only the possibility $n \equiv 1 \pmod{28}$.

(i) We get $V_{n+22} \equiv -V_n \pmod{A_{11}} \equiv -V_n \pmod{34761632124320657}$. We see that 34761632124320657 = 17·2113·967724510017. So $V_{n+22} \equiv -V_n$ (mod 2113). The sequence V_n (mod 2113) has period 44. We have $n \not\equiv 9$, 17, 25, 29 (mod 44). Also $V_{n+22} \equiv -V_n \pmod{967724510017}$. The sequence V_n (mod 967724510017) has period 44. We get $n \not\equiv 13$, 37, 41 (mod 44).

(j) We have $V_{n+44} \equiv -V_n \pmod{A_{22}} \equiv -V_n \pmod{74915060494433}$. We see that 74915060494433 = 577·129835460129. Therefore $V_{n+44} \equiv -V_n$ (mod 129835460129). The sequence V_n (mod 129835460129) has period 88. When $n \equiv 5, 49 \pmod{88}$, we have respectively

$$29V_n^2 - 196 \equiv 51293333469, 51271172096 \pmod{129835460129}.$$

Therefore $29V_n^2 - 196$ cannot be a square. This implies that $n \not\equiv 5, 49$ (mod 88). Similarly, we see that $n \not\equiv 21, 33 \pmod{88}$.

(k) We obtain $V_{n+88} \equiv -V_n \pmod{A_{44}} \equiv -V_n \pmod{2331170689}$. The sequence V_n (mod 2331170689) has a period of 176. We check that $n \not\equiv 65 \pmod{176}$.

Steps (d), (i), (j) and (k) leave only the possibility $n \equiv 1 \pmod{44}$. Consequently a solution requires $n \equiv 1 \pmod 4$, $n \equiv 1 \pmod 3$, $n \equiv 1 \pmod 5$, $n \equiv 1 \pmod 7$ and $n \equiv 1 \pmod{11}$. By the Chinese remainder theorem, then, $n \equiv 1 \pmod{2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11}$.

Now we establish that the relation $Z^2 = 29V_n^2 - 196$ is impossible for such values of n. For this purpose, we need two functions, which we now describe.

6.1. *The functions $a(t)$ and $b(t)$.* Throughout this subsection we keep the notation of page 259 for the solutions of the Pell equation $A^2 - DB^2 = 1$: the fundamental solution is written $a + b\sqrt{D}$ and its n-th power is $A_n + B_n\sqrt{D}$. We further consider the equation $U^2 - DV^2 = N$, singling out a class of solutions $U_n + V_n\sqrt{D} = (u + v\sqrt{D})(a + b\sqrt{D})^n$.

Definition [Mohanty and Ramasamy 1985, p. 205]. For t a natural number, define

$$\boldsymbol{a}(t) = A_{2^{t-1}} \quad \text{and} \quad \boldsymbol{b}(t) = B_{2^{t-1}}. \tag{26}$$

These functions will be used in defining a generalized characteristic number of our system of simultaneous Pell's equations. We follow [Ramasamy 2006, pp. 714–715]. We have the equalities

$$\boldsymbol{a}(t+1) = 2(\boldsymbol{a}(t))^2 - 1, \tag{27}$$

$$\boldsymbol{b}(t+1) = 2\boldsymbol{a}(t)\boldsymbol{b}(t). \tag{28}$$

Next, we have the recursion relations

$$A_n = 2aA_{n-1} - A_{n-2} \quad (n \geq 2), \tag{29}$$

$$B_n = 2aB_{n-1} - B_{n-2} \quad (n \geq 2), \tag{30}$$

which are particular cases of (15) and (16). Repeated application of these relations shows that A_n can be expressed as a polynomial in a, while B_n can be expressed as a polynomial in a and b:

$$A_n = \alpha_{n,n}a^n - \alpha_{n,n-2}a^{n-2} + \alpha_{n,n-4}a^{n-4} - \cdots, \tag{31}$$

$$B_n = \beta_{n,n}a^{n-1}b - \beta_{n,n-2}a^{n-3}b + \beta_{n,n-4}a^{n-5}b - \cdots. \tag{32}$$

Now we state a key result with reference to a system of two simultaneous Pell's equations

$$U^2 - DV^2 = N, \quad Z^2 - gV^2 = h, \tag{33}$$

where g and h are integers.

Definition and Lemma [Ramasamy 2006, Theorem 13]. *Fix odd primes $p_1 = p$, $p_2, \ldots, p_s$, not necessarily distinct. Let $P = p_1p_2\cdots p_s$. Take $\tau \geq 1$. Set either*

(i) $m = 2^\tau \cdot p$ *and* $n = i + p \cdot 2^t(2\mu+1)$, $t \geq 1$, *or*

(ii) $m = 2^\tau \cdot P$ *and* $n = i + P \cdot 2^t(2\mu+1)$, $t \geq 1$,

where i is a fixed residue (*mod m*) *and μ is a nonnegative integer. In Case* (ii), *let $F_1, F_2, \ldots$ be the polynomials contributed by the distinct primes among $p_1, p_2, \ldots, p_s$ and let $G_1, G_2, \ldots$ be the irreducible polynomials arising due to their various products, so that $F_1, F_2, \ldots$ and $G_1, G_2, \ldots$ are factors of the polynomial*

$$\beta_{P,P}D^{(P-1)/2}(\boldsymbol{b}(t+1))^{P-1} + \beta_{P,P-2}D^{(P-3)/2}(\boldsymbol{b}(t+1))^{P-3} + \cdots + \beta_{P,1}.$$

(*A prime p_i contributes a polynomial of degree $p_i - 1$. The product of two distinct primes p_i, p_j yields a factor of degree $(p_i-1)(p_j-1)$, and so on.*) *Let*

$$\phi := gU_i^2 - Dh \tag{34}$$

be the ***characteristic number*** *of the system* (33) (*for the given residue i*).

Then, for each $t \geq 1$, if at least one of the Jacobi symbols

$$\left(\frac{\phi}{(\boldsymbol{a}(t))^2 + D(\boldsymbol{b}(t))^2}\right) \quad \textit{and} \quad \left(\frac{\phi}{\beta_{p,p} D^{(p-1)/2}(\boldsymbol{b}(t+1))^{p-1} + \cdots + \beta_{p,1}}\right)$$

equals -1 in Case (i), *and if at least one of*

$$\left(\frac{\phi}{(\boldsymbol{a}(t))^2 + D(\boldsymbol{b}(t))^2}\right), \quad \left(\frac{\phi}{F_1}\right), \quad \left(\frac{\phi}{F_2}\right), \quad \ldots, \quad \left(\frac{\phi}{G_1}\right), \quad \left(\frac{\phi}{G_2}\right), \quad \ldots$$

equals -1 in Case (ii), *the system has no solution with $V = V_n$ for $n \equiv i \pmod m$, except possibly $V = V_i$.*

6.2. *Application of the characteristic number.* The modulus in the present case consists of four distinct odd primes: 3, 5, 7 and 11. The characteristic number $gU_i^2 - Dh$ of the system (4), (5) for $i = 1$ is 52277; see (34). The sequence $\boldsymbol{a}(t)$ (mod 52277) is periodic with period 265 and $\boldsymbol{b}(t)$ (mod 52277) is periodic with period 530. Thus when we deal with the characteristic number of the system, we encounter computational complexities posed by the large periods of the two sequences. To overcome this difficulty, instead of working with the characteristic number directly, we consider the prime factors of the characteristic number, which are 61 and 857. The sequences $\boldsymbol{a}(t)$ (mod 61) and $\boldsymbol{b}(t)$ (mod 61) are periodic with period 5 — see Table 1 — whereas $\boldsymbol{a}(t)$ (mod 857) is periodic with period 53 and $\boldsymbol{b}(t)$ (mod 857) is periodic with period 106; moreover,

$$\boldsymbol{b}(t + 53) \equiv -\boldsymbol{b}(t) \pmod{857}. \tag{35}$$

Thus Table 2 lists only the values of $\boldsymbol{a}$ and $\boldsymbol{b}$ (mod 857) with argument up to 52. For residue calculations with respect to the factors 61 and 857, we require the values of $\boldsymbol{a}(t+1)$ and powers of $D(\boldsymbol{b}(t+1))^2$ modulo 61 and 857.

We take $P = 3 \cdot 5 \cdot 7 \cdot 11$ and $m = 2^\tau \cdot P$ with $\tau \geq 1$. In the notation of Case (ii) of the Definition and Lemma, we have

$$Z^2 \equiv 1185 \pmod{\boldsymbol{a}(t+1) \cdot F_1 \cdots F_4 \cdot G_1 \cdots G_{11}} \tag{36}$$

where the polynomials $F_1, \ldots, G_{11}$ are illustrated in Table 3.

$t-1$	$\boldsymbol{a}(t)$	$\boldsymbol{b}(t)$
0	17	4
1	28	14
2	42	52
3	50	37
4	58	40

Table 1. Values of $\boldsymbol{a}(t)$ and $\boldsymbol{b}(t)$ (mod 61).

$t-1$	$\boldsymbol{a}(t)$	$\boldsymbol{b}(t)$	$t-1$	$\boldsymbol{a}(t)$	$\boldsymbol{b}(t)$	$t-1$	$\boldsymbol{a}(t)$	$\boldsymbol{b}(t)$	$t-1$	$\boldsymbol{a}(t)$	$\boldsymbol{b}(t)$	$t-1$	$\boldsymbol{a}(t)$	$\boldsymbol{b}(t)$
0	**17**	4	11	**652**	391	22	**563**	369	33	454	825	44	72	611
1	577	136	12	**63**	806	23	**614**	706	34	**14**	82	45	83	570
2	825	113	13	**224**	430	24	688	541	35	**391**	582	46	**65**	350
3	**333**	481	14	82	672	25	559	540	36	**669**	57	47	736	79
4	**671**	685	15	**592**	512	26	208	392	37	413	850	48	**143**	593
5	**631**	566	16	**758**	309	27	827	242	38	51	217	49	**618**	769
6	168	411	17	747	522	28	85	49	39	**59**	709	50	**260**	71
7	**742**	119	18	**203**	855	29	737	617	40	**105**	533	51	650	69
8	**739**	54	19	**145**	45	30	518	181	41	**624**	520	52	**854**	572
9	**423**	111	20	**56**	195	31	**165**	690	42	**595**	211			
10	488	493	21	**272**	415	32	**458**	595	43	167	846			

Table 2. Values of $\boldsymbol{a}(t)$ and $\boldsymbol{b}(t)$ (mod 857). For the boldface, see Note on p. 266.

$$
\begin{aligned}
F_1 &= 4\bar{\boldsymbol{b}}^2+1\\
F_2 &= 16\bar{\boldsymbol{b}}^4+12\bar{\boldsymbol{b}}^2+1\\
F_3 &= 64\bar{\boldsymbol{b}}^6+80\bar{\boldsymbol{b}}^4+24\bar{\boldsymbol{b}}^2+1\\
F_4 &= 1024\bar{\boldsymbol{b}}^{10}+2304\bar{\boldsymbol{b}}^8+1792\bar{\boldsymbol{b}}^6+560\bar{\boldsymbol{b}}^4+60\bar{\boldsymbol{b}}^2+1\\
G_1 &= 256\bar{\boldsymbol{b}}^8+576\bar{\boldsymbol{b}}^6+416\bar{\boldsymbol{b}}^4+96\bar{\boldsymbol{b}}^2+1\\
G_2 &= 4096\bar{\boldsymbol{b}}^{12}+13312\bar{\boldsymbol{b}}^{10}+16384\bar{\boldsymbol{b}}^8+9344\bar{\boldsymbol{b}}^6+2368\bar{\boldsymbol{b}}^4+192\bar{\boldsymbol{b}}^2+1\\
G_3 &= 1048576\bar{\boldsymbol{b}}^{20}+5505024\bar{\boldsymbol{b}}^{18}+12320768\bar{\boldsymbol{b}}^{16}+15302656\bar{\boldsymbol{b}}^{14}+11493376\bar{\boldsymbol{b}}^{12}\\
&\quad+5326848\bar{\boldsymbol{b}}^{10}+1487104\bar{\boldsymbol{b}}^8+232256\bar{\boldsymbol{b}}^6+17440\bar{\boldsymbol{b}}^4+480\bar{\boldsymbol{b}}^2+1\\
G_4 &= 16777216\bar{\boldsymbol{b}}^{24}+104857600\bar{\boldsymbol{b}}^{22}+287309824\bar{\boldsymbol{b}}^{20}+453246976\bar{\boldsymbol{b}}^{18}+454557696\bar{\boldsymbol{b}}^{16}\\
&\quad+301907968\bar{\boldsymbol{b}}^{14}+134123520\bar{\boldsymbol{b}}^{12}+39298048\bar{\boldsymbol{b}}^{10}+7287808\bar{\boldsymbol{b}}^8+785792\bar{\boldsymbol{b}}^6\\
&\quad+40896\bar{\boldsymbol{b}}^4+576\bar{\boldsymbol{b}}^2+1
\end{aligned}
$$

Table 3. Expressions for some of the polynomials in (36). We use the shorthand $\bar{\boldsymbol{b}} = \sqrt{D}\,\boldsymbol{b}(t+1)$. The polynomials $G_5, \ldots, G_{11}$ have degrees 40, 60, 48, 80, 120, 240, 480, respectively.

We still have to determine an appropriate value of t. For the application of the quadratic reciprocity law, we require the values of the polynomials modulo 4. By induction, we obtain the following results for the present problem:

$$\boldsymbol{a}(t+1) \equiv 1 \pmod 4 \quad \text{for all } t \geq 1, \tag{37}$$

$$\boldsymbol{b}(t+1) \equiv 0 \pmod 4 \quad \text{for all } t \geq 1. \tag{38}$$

We see that, for all $t \geq 1$ and i = 1, 2, 3, 4,

$$F_i, G_i \equiv 1 \pmod 4. \tag{39}$$

Considering the values of F_i and G_i modulo 857, it follows from relation (35) that F_i at $t+53$ is the same as at t, and G_i at $t+53$ is the same as at t, for all positive integers t.

6.3. ***Computations involved in the proof of the Theorem.*** With the background just provided, we are now in a position to employ the characteristic number of the present system consisting of (4) and (5). For the remaining part of our work, stagewise computation becomes necessary. The details of calculations in 9 stages required for our problem are presented in the sequel.

The characteristic number of the generalized version discussed in Section 6.1 offers several polynomials for consideration to solve a given problem, as seen from (36). First, we employ the factor $(\boldsymbol{a}(t))^2 + D(\boldsymbol{b}(t))^2$ provided by the Definition and Lemma to rule out as many possible values of t as we can.

1. *Working with* $\boldsymbol{a}(t+1)$. We consider the Jacobi symbol

$$\left(\frac{52277}{\boldsymbol{a}(t+1)}\right).$$

Using the quadratic reciprocity law and the relation (37), we evaluate this to

$$\left(\frac{61}{\boldsymbol{a}(t+1)}\right)\cdot\left(\frac{857}{\boldsymbol{a}(t+1)}\right) = \left(\frac{\boldsymbol{a}(t+1)}{61}\right)\cdot\left(\frac{\boldsymbol{a}(t+1)}{857}\right).$$

From Table 1, when $t \equiv 2, 4 \pmod 5$, we have $\boldsymbol{a}(t+1) \equiv 42, 58 \pmod{61}$, respectively; these are quadratic residues of 61. When $t \equiv 0, 1, 3 \pmod 5$, we have, respectively, $\boldsymbol{a}(t+1) \equiv 17, 28, 50 \pmod{61}$; all are quadratic nonresidues of 61.

Note. We have indicated with an asterisk in Table 2 the values of $\boldsymbol{a}(t)$ that are quadratic nonresidues of 857.

Using the fact that the product of a quadratic residue of 52277 and a nonresidue of 52277 is a nonresidue, we determine the values of t for which $\boldsymbol{a}(t+1)$ is a quadratic nonresidue of 52277. They are 1, 4, 6, 7, 9, 10, 12, 19, 22, 25, 26, 28, 30, 32, 33, 34, 38, 39, 42, 43, 45, 49, 51, 52, 55, 57, 62, 63, 64, 69, 70, 72, 74, 78, 80, 81, 83, 84, 86, 87, 89, 90, 91, 92, 94, 96, 98, 99, 100, 102, 108, 109, 114, 116, 117, 119, 120, 122, 123, 124, 127, 129, 130, 131, 133, 135, 136, 137, 142, 143, 147, 150, 151, 152, 153, 154, 159, 160, 161, 162, 164, 165, 167, 172, 173, 174, 176, 177, 179, 182, 183, 185, 186, 188, 194, 196, 199, 203, 206, 207, 209, 210, 212, 213, 217, 218, 219, 224, 226, 227, 232, 234, 236, 238, 240, 241, 244, 245, 247, 250, 252, 254, 255, 256, 262, 263, 264 (mod 265). It follows that the relation $Z^2 = 29V_n^2 - 196$ is impossible for these values of t. Therefore these values of t have to be excluded. In the sequel we consider the remaining values of t (mod 265).

t	F_1	F_2	F_3	t	F_1	F_2	F_3	t	F_1	F_2	F_3	t	F_1	F_2	F_3	t	F_1	F_2	F_3
0	**296**	**497**	**766**	11	**125**	323	**294**	22	370	149	61	33	**27**	755	**545**	44	**165**	822	**24**
1	**792**	**731**	416	12	**447**	**574**	**462**	23	518	**600**	648	34	**781**	**557**	**294**	45	**129**	**486**	**490**
2	**665**	**677**	292	13	**163**	164	166	24	**260**	**156**	177	35	480	**346**	**545**	46	**614**	529	775
3	484	778	623	14	**326**	**333**	**583**	25	**415**	**382**	**809**	36	825	**134**	**163**	47	**285**	94	32
4	404	**789**	**337**	15	658	836	72	26	796	**231**	**770**	37	101	**17**	776	48	378	142	**306**
5	335	292	79	16	**636**	**627**	**258**	27	169	**448**	575	38	117	**93**	573	49	519	**781**	240
6	**626**	**852**	**524**	17	**405**	**742**	**40**	28	616	**420**	**567**	39	209	**182**	**303**	50	**442**	**409**	775
7	**620**	**226**	35	18	289	680	658	29	**178**	**152**	**463**	40	390	800	**462**	51	**850**	41	**618**
8	**845**	**131**	**285**	19	111	433	393	30	329	587	**556**	41	**332**	2	334	52	33	264	373
9	**118**	329	468	20	**543**	**583**	**376**	31	58	**850**	386	42	**333**	668	816				
10	446	**537**	**490**	21	**268**	103	15	32	50	**835**	542	43	**143**	23	598				

Table 4. Values of F_1, F_2 and F_3 (mod 857) as functions of t (mod 53). Quadratic nonresidues of 857 are in bold.

2. *Working with* F_1. Now we consider

$$\left(\frac{52277}{F_1}\right) = \left(\frac{61}{F_1}\right) \cdot \left(\frac{857}{F_1}\right) = \left(\frac{F_1}{61}\right) \cdot \left(\frac{F_1}{857}\right),$$

in view of (39). When $t \equiv 1 \pmod 5$, we have $F_1 \equiv 22 \pmod{61}$ which is a quadratic residue of 61. When $t \equiv 0, 2, 3, 4 \pmod 5$, we have $F_1 \equiv 55, 38, 54, 33 \pmod{61}$; all are quadratic nonresidues of 61. As for the modulus 857, Table 4 shows the values of F_1, with the quadratic nonresidues in bold.

Consequently, we see that the relation $Z^2 = 29V_n^2 - 196$ is not true when $t \equiv 3$, 5, 11, 15, 16, 18, 21, 23, 27, 35, 37, 40, 41, 46, 48, 58, 61, 66, 68, 75, 79, 85, 88, 93, 105, 106, 110, 125, 126, 128, 132, 134, 138, 144, 145, 155, 156, 158, 163, 166, 169, 171, 178, 187, 189, 190, 195, 197, 198, 201, 208, 215, 221, 222, 226, 230, 235, 239, 242, 243, 246, 248, 249, 260 (mod 265).

3. *Working with* F_2. Next we have

$$\left(\frac{52277}{F_2}\right) = \left(\frac{61}{F_2}\right) \cdot \left(\frac{857}{F_2}\right) = \left(\frac{F_2}{61}\right) \cdot \left(\frac{F_2}{857}\right).$$

When $t \equiv 3 \pmod{61}$, we have $F_2 \equiv 41 \pmod{61}$, which is a quadratic residue of 61. When $t \equiv 0, 1, 2, 4 \pmod 5$, we have, respectively, $F_2 \equiv 29, 17, 17, 23 \pmod{61}$, all of which are quadratic nonresidues of 61. Further, Table 4 shows the values of F_2 modulo 857, with the quadratic nonresidues in bold.

Consequently, we see that the relation $Z^2 = 29V_n^2 - 196$ does not hold when $t \equiv 8$, 44, 47, 53, 56, 71, 73, 95, 97, 101, 103, 104, 111, 113, 115, 118, 121, 139, 146, 149, 157, 170, 180, 181, 192, 193, 200, 202, 205, 211, 225, 228, 231, 259 (mod 265).

4. *Working with F_3.* Next we have

$$\left(\frac{52277}{F_3}\right) = \left(\frac{61}{F_3}\right) \cdot \left(\frac{857}{F_3}\right) = \left(\frac{F_3}{61}\right) \cdot \left(\frac{F_3}{857}\right).$$

When $t \equiv 1, 2, 3 \pmod 5$, we have respectively $F_3 \equiv 3, 15, 5 \pmod{61}$, all of which are quadratic residues of 61. When $t \equiv 0, 4 \pmod 5$, we have respectively $F_3 \equiv 44, 17 \pmod{61}$ both of which are quadratic nonresidues of 61. Further, Table 4 shows the values of F_3 modulo 857, with the quadratic nonresidues in bold.

As a result, the relation $Z^2 = 29V_n^2 - 196$ does not hold when $t \equiv$ 17, 24, 36, 50, 54, 60, 67, 82, 112, 141, 214, 216, 223, 237, 251, 257 (mod 265).

5. *Working with F_4.* Next we have

$$\left(\frac{52277}{F_4}\right) = \left(\frac{61}{F_4}\right) \cdot \left(\frac{857}{F_4}\right) = \left(\frac{F_4}{61}\right) \cdot \left(\frac{F_4}{857}\right).$$

When $t \equiv 0, 1, 4 \pmod 5$, we have respectively $F_4 \equiv 42, 34, 4 \pmod{61}$, all of which are quadratic residues of 61. When $t \equiv 2, 3 \pmod 5$, we have respectively $F_4 \equiv 55, 55 \pmod{61}$. It is checked that 55 is a quadratic nonresidue of 61. The relevant values modulo 857 are as follows (bold indicates quadratic nonresidues):

t (mod 53)	2	9	13	14	42	16	23	32
F_4 (mod 857)	407	827	762	**792**	619	**415**	**437**	**557**

Consequently, the relation $Z^2 = 29V_n^2 - 196$ does not hold when $t \equiv$ 2, 13, 14, 76, 148, 168, 175, 191 (mod 265).

6. *Working with G_1.* Next we have

$$\left(\frac{52277}{G_1}\right) = \left(\frac{61}{G_1}\right) \cdot \left(\frac{857}{G_1}\right) = \left(\frac{G_1}{61}\right) \cdot \left(\frac{G_1}{857}\right),$$

because of (39). When $t \equiv 3 \pmod 5$, we have $G_1 \equiv 46 \pmod{61}$, which is a quadratic residue of 61. When $t \equiv 0, 1, 2, 4 \pmod 5$, we have respectively $G_1 \equiv 55, 51, 26, 28 \pmod{61}$, all of which are quadratic nonresidues of 61. The relevant values modulo 857 are as follows (again, bold indicates quadratic nonresidues):

t (mod 53)	0	6	12	17	20	21	46
G_1 (mod 857)	774	737	57	487	785	**367**	**210**

As a result, it is seen that the relation $Z^2 = 29V_n^2 - 196$ does not hold when $t \equiv 0, 20, 59, 65, 229, 233, 258 \pmod{265}$.

7. *Working with G_2.* Next we have

$$\left(\frac{52277}{G_2}\right)=\left(\frac{61}{G_2}\right)\cdot\left(\frac{857}{G_2}\right)=\left(\frac{G_2}{61}\right)\cdot\left(\frac{G_2}{857}\right).$$

When $t\equiv 1,2,4 \pmod 5$, we have respectively $G_2\equiv 60,34,49 \pmod{61}$, all of which are quadratic residues of 61. When $t\equiv 0,3 \pmod 5$, we have respectively $G_2\equiv 23,6 \pmod{61}$ both of which are quadratic nonresidues of 61.

When $t\equiv 8,34,41 \pmod{53}$, we have respectively $G_2\equiv 72,177,439 \pmod{857}$, all of which are quadratic residues of 857. When $t\equiv 25,29,31,45 \pmod{53}$, we have respectively $G_2\equiv 840,718,507,781 \pmod{857}$, all of which are quadratic nonresidues of 857. As a consequence, the relation $Z^2=29V_n^2-196$ does not hold when $t\equiv 29,31,140,184,204,220,253 \pmod{265}$.

8. *Working with G_3.* Next we have

$$\left(\frac{52277}{G_3}\right)=\left(\frac{61}{G_3}\right)\cdot\left(\frac{857}{G_3}\right)=\left(\frac{G_3}{61}\right)\cdot\left(\frac{G_3}{857}\right).$$

When $t\equiv 4 \pmod 5$, we have $G_3\equiv 34 \pmod{61}$, which is a quadratic residue of 61. When $t\equiv 0,1,2,3 \pmod 5$, we have respectively $G_3\equiv 59,2,50,21 \pmod{61}$, all of which are quadratic nonresidues of 61. When $t\equiv 49 \pmod{53}$, we have $G_3\equiv 453 \pmod{857}$ which is a quadratic residue of 857. Hence the relation $Z^2=29V_n^2-196$ does not hold when $t\equiv 261 \pmod{265}$.

9. *Working with G_4.* Next we have

$$\left(\frac{52277}{G_4}\right)=\left(\frac{61}{G_4}\right)\cdot\left(\frac{857}{G_4}\right)=\left(\frac{G_4}{61}\right)\cdot\left(\frac{G_4}{857}\right).$$

When $t\equiv 0,2 \pmod 5$, we have respectively $G_4\equiv 14,16 \pmod{61}$, both of which are quadratic residues of 61. Modulo 61, G_4 attains the same value of 31 at $t\equiv 1 \pmod 5$ and $3 \pmod 5$. When $t\equiv 4 \pmod 5$, we have $G_4\equiv 38 \pmod{61}$. It is seen that 31 and 38 are quadratic nonresidues of 61. When $t\equiv 1,24 \pmod{53}$, we have, respectively, $G_4\equiv 612,851 \pmod{857}$ both of which are quadratic nonresidues of 857. Therefore it is seen that the relation $Z^2=29V_n^2-196$ does not hold when $t\equiv 77,107 \pmod{265}$.

Conclusion of the argument for solutions of the form (24)**.** As mentioned, the characteristic number (in the generalized version given in [Ramasamy 2006] and explained earlier in this section) places several polynomials at our disposal for solving the problem. Each polynomial can potentially exclude several values of t. Once all values of t are excluded, we need not examine the remaining polynomials. In the present case we used the polynomials $\boldsymbol{a}(t+1)$, F_1 through F_4 and G_1 through G_4 appearing in (36), and we exhausted, in the 9 steps above, all possible values of

t; that is, we showed that the relation $Z^2 = 29V_n^2 - 196$ does not hold for any value of t (mod 265). Thus we need not consider the values attained by the polynomials G_5 through G_{11} modulo 52277. This exemplifies the usefulness of the generalized characteristic number.

The conclusion is that the system of Pell's equations $U^2 - 18V^2 = -119$, $Z^2 - 29V^2 = -196$ has no solution V_n of the form (24) except possibly for $n = 1$. When $n = 1$ we obtain a common solution with $U = \pm 41$, $V = \pm 10$ and $Z = \pm 52$.

7. Solutions of the form (25)

We finally turn to the possible solutions of the form (25):

$$\begin{aligned} U_0 &= -41, \quad U_1 = 23, \quad U_{n+2} = 34U_{n+1} - U_n, \\ V_0 &= 10, \quad V_1 = 6, \quad V_{n+2} = 34V_{n+1} - V_n. \end{aligned}$$

A case-by-case calculation as in the previous section shows that the possibilities are $n \equiv 0 \pmod 4$, $n \equiv 0 \pmod 3$, $n \equiv 0 \pmod 5$, $n \equiv 0 \pmod 7$ and $n \equiv 0$ (mod 11). We establish that the relation $Z^2 = 29V_n^2 - 196$ is impossible in these cases as before. The characteristic number $gU_i^2 - Dh$ of the system (4) and (5) for $i = 0$ is again 52277. Since this is the same as for the previous case, the results for the solutions in Section 6 are applicable here also.

We have now taken care of all four cases (22)–(25). Putting together the conclusions of the last four sections, we see that the proof of the Theorem is complete.

Acknowledgement

The authors are thankful to the referee for suggestions towards the improvement of the paper.

References

[Baker and Davenport 1969] A. Baker and H. Davenport, "The equations $3x^2 - 2 = y^2$ and $8x^2 - 7 = z^2$", *Quart. J. Math.* **20**:1 (1969), 129–137. MR 40 #1333 Zbl 0177.06802

[Dujella 1995] A. Dujella, "Diophantine quadruples for squares of Fibonacci and Lucas numbers", *Portugal. Math.* **52**:3 (1995), 305–318. MR 97f:11015 Zbl 0844.11015

[Dujella 1999] A. Dujella, "A proof of the Hoggatt–Bergum conjecture", *Proc. Amer. Math. Soc.* **127**:7 (1999), 1999–2005. MR 99j:11015 Zbl 0937.11011

[Hoggatt and Bergum 1977] V. E. Hoggatt, Jr. and G. E. Bergum, "A problem of Fermat and the Fibonacci sequence", *Fibonacci Quart.* **15**:4 (1977), 323–330. MR 56 #15547 Zbl 0383.10007

[Kangasabapathy and Ponnudurai 1975] P. Kangasabapathy and T. Ponnudurai, "The simultaneous Diophantine equations $y^2 - 3x^2 = -2$ and $z^2 - 8x^2 = -7$", *Quart. J. Math.* **26**:1 (1975), 275–278. MR 52 #8027 Zbl 0309.10008

[Mohanty and Ramasamy 1985] S. P. Mohanty and A. M. S. Ramasamy, "The characteristic number of two simultaneous Pell's equations and its application", *Simon Stevin* **59**:2 (1985), 203–214. MR 87c:11023 Zbl 0575.10010

[Nagell 1951] T. Nagell, *Introduction to number theory*, Wiley, New York, 1951. MR 13,207b Zbl 0042.26702

[Ramasamy 2006] A. M. S. Ramasamy, "Generalized version of the characteristic number of two simultaneous Pell's equations", *Rocky Mountain J. Math.* **36**:2 (2006), 699–720. MR 2007b:11036 Zbl 1140.11017

[Ramasamy 2007] A. M. S. Ramasamy, "Sets, sequences and polynomials linked with a question of Diophantus", *Bull. Kerala Math. Assoc.* **4**:1 (2007), 109–125. MR 2008g:11046

[Tzanakis 1993] N. Tzanakis, "Explicit solution of a class of quartic Thue equations", *Acta Arith.* **64**:3 (1993), 271–283. MR 94e:11022 Zbl 0774.11014

[Tzanakis 2002] N. Tzanakis, "Effective solution of two simultaneous Pell equations by the elliptic logarithm method", *Acta Arith.* **103**:2 (2002), 119–135. MR 2003b:11022 Zbl 1003.11064

Received: 2010-10-30 Revised: 2011-10-06 Accepted: 2011-12-18

ramasamy.mat@pondiuni.edu.in *Department of Mathematics, Pondicherry University, R.V.Nagar, Kalapet, Pondicherry 605014, India*
www.pondiuni.edu.in

dsaraswathynathan@gmail.com *Department of Mathematics, Pondicherry University, R.V.Nagar, Kalapet, Pondicherry 605014, India*

involve

msp.org/involve

See inside back cover or msp.org/involve for submission instructions. The subscription price for 2012 is US $105/year for the electronic version, and $145/year (+$35, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues from the last three years and changes of subscribers address should be sent to MSP.

Involve (ISSN 1944-4184 electronic, 1944-4176 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840, is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

Involve peer review and production are managed by EditFLOW® from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

involve

2012 vol. 5 no. 3

1944-4176(2012)5:3;1-A