GENERALIZED FIBONACCI NUMBERS AND SOME DIOPHANTINE EQUATIONS

JANNIS A. ANTONIADIS
University of Thessaloniki, Greece

(Submitted May 1983)

1. INTRODUCTION

The object of this paper is to generalize the results of Finkelstein [3], [4], and Robbins [8] about the Fibonacci and Lucas numbers of the form $z^2 \pm 1$, by using the method of Cohn [2]. Some results which contain the Fibonacci and Lucas numbers of the form $2z^2 \pm 1$ as special cases are also given.

In all cases we obtain information about the solution of an infinite class of biquadratic diophantine equations, with the exception of Theorems 8 and 10, where it is not known if the class considered is finite or infinite [5].

The following notation will be used:

- F_m, L_m for the (usual) Fibonacci, Lucas numbers.
- $a \equiv b \pmod{c}$ or $a \equiv b(c)$ for congruences.
- (a/b) for the Jacobi quadratic symbol.
- The solutions $(\pm x, \pm y)$ of a diophantine equation are counted *once* if x and y possess only even exponents.

2. PRELIMINARIES

Definition 1: Let $d \in \mathbb{N}$, $d \neq 0$, and d not be a square.

(i) d will be called of the *first kind* if the Pellian equation $x^2 - dy^2 = -4$ has a solution with both x and y odd integers.

(ii) d will be called of the *second kind* if d is not of the first kind and the Pellian equation $x^2 - dy^2 = 4$ has a solution with both x and y odd integers.

Remark: A necessary but not sufficient condition for d to be of the first or second kind is $d \equiv 5(8)$. A counterexample is $d = 37$.

Definition 2: Let $d \in \mathbb{N}$ be of the first or the second kind with $d = 5 + 8\nu$. Let $\alpha = \frac{1}{2}(a + b\sqrt{d})$ be the fundamental solution (see [7]) of $x^2 - dy^2 = -4$ or $x^2 - dy^2 = 4$ and $\beta = \frac{1}{2}(a - b\sqrt{d})$. We define, for all integers n,

$$\begin{cases} U_n = d^{-1/2}(\alpha^n - \beta^n) \\ V_n = \alpha^n + \beta^n. \end{cases}$$

It is easy to see that $U_0 = 0$, $U_1 = b$, $V_0 = 2$, $V_1 = a$, and U_n, V_n are integers for each $n \in \mathbb{Z}$.

Supported by the Deutsche Forschungsgemeinschaft.

The terms of the sequence $\{U_n\}$, $n \in \mathbf{N}$ ($\{V_n\}$, $n \in \mathbf{N}$) will be called *generalized Fibonacci (Lucas)* numbers.

Remarks: (i) From Definitions 1 and 2, it follows that both a and b must be odd.

(ii) If $b = 1$, then our definition of generalized Fibonacci numbers agrees with the Fibonacci polynomials $U_n = F_n(a)$, a odd, but in general, b can be different from one as for example in the case $d = 61$, $a = 39$, $b = 5$.

From now on, d will always be of the first kind with the fundamental solution $\frac{1}{2}(a + b\sqrt{d})$ of the corresponding Pellian equation $x^2 - dy^2 = -4$. According to [2], the following identities hold:

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

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

$$U_{-n} = (-1)^{n-1}U_n, \tag{3}$$

$$V_{-n} = (-1)^n V_n, \tag{4}$$

$$2U_{m+n} = U_m V_n + U_n V_m, \tag{5}$$

$$2V_{m+n} = dU_m U_n + V_m V_n, \tag{6}$$

$$(-1)^n 4 = V_n^2 - dU_n^2, \tag{7}$$

$$V_n^2 = V_{2n} + (-1)^n \cdot 2, \tag{8}$$

$$2 \mid U_n \text{ iff } 2 \mid V_n \text{ iff } 3 \mid n, \tag{9}$$

$$(U_n, V_n) = \begin{cases} 1 & \text{if } 3 \nmid n \\ 2 & \text{if } 3 \mid n, \end{cases} \tag{10}$$

$$V_{n+12} \equiv V_n \pmod 8, \tag{11}$$

$$2U_{m+2N} \equiv (-1)^{N-1} 2U_m \pmod{V_N}, \tag{12}$$

$$2V_{m+2N} \equiv (-1)^{N-1} 2V_m \pmod{V_N}, \tag{13}$$

$$2U_{m+2N} \equiv (-1)^N 2U_m \pmod{U_N}, \tag{14}$$

$$2V_{m+2N} \equiv (-1)^N 2V_m \pmod{U_N}, \tag{15}$$

$$V_n \equiv 2 \pmod a \text{ if } 2 \mid n, \tag{16}$$

$$V_n \equiv (-1)^{n/2} \cdot 2 \pmod b \text{ if } 2 \mid n, \tag{17}$$

$$b \equiv 1(4), \tag{18}$$

and, furthermore, for $k \in \mathbf{Z}$, with $2 \mid k$, $3 \nmid k$,

$$V_k > 0 \text{ and } V_k \equiv \begin{cases} 3(8) & \text{if } k \equiv 2(4) \\ 7(8) & \text{if } 4 \mid k, \end{cases} \tag{19}$$

$$\left(\frac{2}{V_k}\right) = (-1)^{k/2}, \tag{20}$$

$$U_{m+2k} \equiv -U_m \pmod{V_k}, \tag{21}$$

$$V_{m+2k} \equiv -V_m \pmod{V_k}, \tag{22}$$

$$\left(\frac{a}{V_k}\right) = \left(\frac{-2}{a}\right), \tag{23}$$

$$\left(\frac{V_3}{V_k}\right) = \left(\frac{-2}{a}\right), \tag{24}$$

$$\left(\frac{V_k}{U_5}\right) = -\left(\frac{2}{b}\right) \text{ provided that } 5 \nmid k, \tag{25}$$

the general solution of $x^2 - dy^2 = -4$ is $x = V_{2n+1}$, $y = U_{2n+1}$, (26)

the general solution of $x^2 - dy^2 = 4$ is $x = V_{2n}$, $y = U_{2n}$, (27)

$$\text{if } V_n = x^2, \text{ then } \begin{cases} n = 1 & \text{if } a = t^2 \text{ and } d \neq 5 \\ n = 1, 3 & \text{if } d = 5 \\ n = 3 & \text{if } d = 13, \end{cases} \tag{28}$$

$$\text{if } V_n = 2x^2, \text{ then } \begin{cases} n = 0 \\ \text{ and} \\ n = \pm 6 & \text{if } d = 5, 29, \end{cases} \tag{29}$$

$$\text{if } U_n = x^2, \text{ then } \begin{cases} n = 0 \\ n = 12 & \text{if } d = 5 \\ n = 2 & \text{if } a = t^2 \text{ and } b = r^2 \\ n = \pm 1 & \text{if } b = r^2, \end{cases} \tag{30}$$

$$\text{if } U_n = 2x^2, \text{ then } \begin{cases} n = 0 \\ n = 6 \quad \text{if } d = 5 \\ \text{and possibly the solutions } n = \pm 3. \end{cases} \tag{31}$$

We also need some values for U_n and V_n:

n	U_n	V_n
0	0	2
1	b	a
2	ab	$a^2 + 2$
3	$(a^2 + 1)b$	$a^3 + 3a$
4	$(a^3 + 2a)b$	$a^4 + 4a^2 + 2$
5	$(a^4 + 3a^2 + 1)b$	$a^5 + 5a^3 + 5a$
6	$(a^5 + 4a^3 + 3a)b$	$a^6 + 6a^4 + 9a^2 + 2$

3. GENERALIZED FIBONACCI NUMBERS OF THE FORM $\mu z^2 + \nu$

Theorem 1: Let $a \equiv 1, 3(8)$ and $b \equiv 1(8)$. Then the equation

$U_m = az^2 + b$, $m \equiv 1(2)$,

has

(a) the solutions $m = \pm 1$, ± 3, and ± 5 if $d = 5$,

(b) the solutions $m = \pm 1$, ± 5 if $d = 13$,

(c) the solutions $m = \pm 1$, ± 3 if a and b are both perfect squares, $d \neq 5$,

(d) only the solutions $m = \pm 1$ in all other cases.

Proof: It is sufficient by (3) to consider only the cases $m \equiv 1(8)$, $3(16)$, and $5(16)$.

Case 1. Let $m \equiv 1(8)$. For $m = 1$, $z = 0$ is a solution. If $m \neq 1$, then we write $m = 1 + 2 \cdot 3^s \cdot n$, where $4|n$, $3 \nmid n$, and $az^2 + b = U_m \equiv -U_1 \pmod{V_n}$ by (21). Thus $(az)^2 \equiv -2ab \pmod{V_n}$. But

$$\left(\frac{-2ab}{V_n}\right) = -1$$

by (19), (20), (16), (17), and the assumption. Hence, $U_m \neq az^2 + b$.

Case 2. Let $m \equiv 3(16)$. If $m = 3$, then $az^2 + b = (a^2 + 1)b$ iff $z^2 = ab$ iff a and b are both perfect squares, since $(a, b) = 1$.

If $m \neq 3$, then we write $m = 3 + 2 \cdot 3^s \cdot n$, where $8|n$, $3 \nmid n$, and $az^2 + b = U_m \equiv -U_3 \pmod{V_n} \equiv -(a^2 + 1)b \pmod{V_n}$, by (21). Thus $(az)^2 \equiv -abV_2 \pmod{V_n}$.

By applying (13) repeatedly, we obtain

$$2V_n \equiv -2V_{n-4} \equiv 2V_{n-8} \equiv \cdots \equiv 2V_0 \equiv 4 \pmod{V_2}, \tag{32}$$

which by (19) implies $V_n \equiv 2 \pmod{V_2}$. Thus $(V_n, V_2) = (2, V_2) = 1$ and

$$\left(\frac{V_2}{V_n}\right) = -\left(\frac{V_n}{V_2}\right) = -\left(\frac{2}{V_2}\right) = \pm 1.$$

Now $(-abV_2/V_n)$ can be calculated to be -1 by using (19), (16), (17), (33), and the assumption. Hence, $U_m \neq az^2 + b$.

Case 3. Let $m \equiv 5(16)$. If $m = 5$, then there exists a solution iff $az^2 + b = (a^4 + 3a^2 + 1)b$ iff $z^2 = a(a^2 + 3)b$. Since b is odd and $b|U_3$,

$$(b, V_3)/(U_3, V_3) = 2,$$

which implies $(b, V_3) = 1$. Hence,

$$z^2 = a(a^2 + 3)b = V_3 b \text{ iff } b = r^2 \text{ and } a(a^2 + 3) = z_1^2.$$

By [1], the last equation has only the solutions $(z_1, a) = (0, 0), (\pm 2, 1), (\pm 6, 3), (\pm 42, 12)$. Since we have $a \equiv 1(2)$, the only possible solutions are $(z_1, a) = (\pm 2, 1), (\pm 6, 3)$. For $a = 1$, we have $b = 1 = r^2$ and $d = 5$. For $a = 3$, we have $b = 1 = r^2$ and $d = 13$.

If $m \neq 5$, then $m = 5 + 2 \cdot 3^s \cdot n$ with $8|n$, $3 \nmid n$, and thus

$$U_m \equiv -U_5 \pmod{V_n} \equiv -(a^4 + 3a^2 + 1)b \pmod{V_n} \text{ by (21).}$$

Applying (15) repeatedly and using (4), we have

$$2V_n \equiv -2V_{n-6} \equiv 2V_{n-12} \equiv \cdots \equiv \pm 2V_2 \pmod{U_3}. \tag{34}$$

Since $(V_n, V_2) = 1$ implies $(2V_n, U_3) = 2$, we see that

$$\left(\frac{U_3/2}{V_n}\right) = \left(\frac{(a^2 + 1)/2}{V_n}\right)\left(\frac{b}{V_n}\right) = \left(\frac{V_n}{(a^2 + 1)/2}\right)\left(\frac{b}{V_n}\right)$$
$$= \left(\frac{\pm V_2}{(a^2 + 1)/2}\right)\left(\frac{b}{V_n}\right) = \left(\frac{b}{V_n}\right). \tag{35}$$

Now, if $az^2 + b = U_m$, we have

$$(ax)^2 \equiv -a(a^4 + 3a^2 + 2)b \equiv -abV_2U_3 \pmod{V_n},$$

which is impossible because $(-abV_2U_3/V_n) = -1$ by (19), (16), (17), (33), (35), and the assumption. Hence, $U_m \neq az^2 + b$.

Corollary 1: The diophantine equation $x^2 = a^2dz^4 + 2abdz^2 + a^2$ with $a \equiv 1, 3(8)$ and $b \equiv 1(8)$, has

(a) three solutions $(x, y) = (\pm 1, 0), (\pm 4, \pm 1), (\pm 11, \pm 2)$ if $d = 5$,

(b) two solutions $(x, z) = (\pm 3, 0), (\pm 393, 16)$ if $d = 13$,

(c) two solutions $(x, z) = (\pm a, 0), (\pm a(a^2 + 3), \pm tr)$, where $a = t^2$ and $b = r^2$ are both perfect squares, $d \neq 5$,

(d) only one solution $(x, z) = (\pm a, 0)$ in all other cases.

Proof: This follows directly from (26), Theorem 1, and Definition 2.

Following the arguments of Theorem 1 and Corollary 1, we have

Theorem 2: Let $b \equiv 1(8)$. Then the equation $U_m = z^2 + b$, $m \equiv 1(2)$, has

(a) the solutions $m = \pm 1, \pm 3, \pm 5$, if $d = 5$,

(b) the solutions $m = \pm 1, \pm 3$, if $b = r^2$, $d \neq 5$,

(c) only the solutions $m = \pm 1$ in all other cases,

and

Corollary 2: The diophantine equation $x^2 = dz^4 + 2dbz^2 + a^2$ with $b \equiv 1(8)$ has

(a) three solutions $(x, z) = (\pm 1, 0), (\pm 4, \pm 1), (\pm 11, \pm 2)$, if $d = 5$,

(b) two solutions $(x, z) = (\pm a, 0), (\pm a(a^2 + 3), \pm ar)$ if $b = r^2$, $d \neq 5$,

(c) only one solution $(x, z) = (\pm a, 0)$ in all other cases.

We now show the following results, which are similar to the above but with m even.

Theorem 3: Let $a \equiv 1, 3(8)$ and $b \equiv 1(8)$ or $a \equiv 5, 7(8)$ and $b \equiv 5(8)$. Then the equation $U_m = z^2 + ab$, $m \equiv 0(2)$, has only the solution $m = 2$.

Proof:

Case 1. Let $m \equiv 0(4)$. No solution exists for $m = 0$; but if $m \neq 0$, then we write $m = 2 \cdot 3^s \cdot n$ with $2|n$, $3\nmid n$, and thus $U_m \equiv 0 \pmod{V_n}$ by (21). If $U_m = z^2 + ab$ for some m, then we have $z^2 \equiv -ab \pmod{V_n}$, which is impossible, since $(-ab/V_n) = -1$ by (19), (16), (17), and the assumption.

Case 2: Let $m \equiv 2(8)$. For $m = 2$, we have the solution $z = 0$. If $m \neq 2$, then we write $m = 2 + 2 \cdot 3^s \cdot n$ with $4|n$, $3\nmid n$, and thus

$$U_m \equiv -U_2 \pmod{V_n} \equiv -ab \pmod{V_n} \text{ by (21),}$$

Thus, if $U_m = z^2 + ab$, we should have $z^2 \equiv -2ab \pmod{V_n}$, which is impossible, since $(-2ab/V_n) = -1$ by (19), (20), (16), (17), and the assumption.

Case 3: Let $m = 6(8)$. If $m = 6$, we have a solution iff

$$z^2 + ab = (a^5 + 4a^3 + 3a)b \text{ iff } z^2 = a(a^4 + 4a^2 + 2)b = aV_4b.$$

But $b|U_4$; hence,

$$(b, V_4)/(U_4, V_4) = 1 \text{ by (10).}$$

Therefore, it follows that $b = t^2$, $a = r^2$, and $a^4 + 4a^2 + 2 = V_4 = s^2$, which is impossible mod 4.

If $m \neq 6$, then we write $m = 6 + 2 \cdot 3^s \cdot n$ with $4 | n$, $3 \nmid n$, and thus

$U_m \equiv -U_6 \pmod{V_n} \equiv -(a^5 + 4a^3 + 3a)b \pmod{V_n}$ by (21).

Hence, if $U_m = z^2 + ab$, we have $z^2 \equiv -ab(a^4 + 4a^2 + 4) \equiv -ab(a^2 + 2)^2 \pmod{V_n}$, which is impossible since

$$\left(\frac{-ab(a^2 + 2)^2}{V_n}\right) = \left(\frac{-ab}{V_n}\right) = -1 \text{ by (19), (16), (17), and the assumption.}$$

Applying Theorem 1(a) and Theorem 3, we now have

Corollary 3: (Theorem of Finkelstein [3], [9], [1])

$F_m = z^2 + 1$ iff $m = \pm 1, 2, \pm 3, \pm 5$.

Using an argument similar to that of Theorem 3, we have Theorem 4 and two immediate corollaries.

Theorem 4: Let $b \equiv 1(8)$. Then, the equation $U_m = az^2 + ab$, $m \equiv 0(2)$, has only the solution $m = 2$.

Corollary 4: Let $d = a^2 + 4$, $2 \nmid a$. Then, the equation $U_m = az^2 + a$ has only the solution $m = 2$.

Corollary 5: The diophantine equation $x^2 = a^2dz^4 + 2a^2dbz^2 + (a^2 + 2)^2$ with $b \equiv 1(8)$ has only the solution $(x, y) = (\pm(a^2 + 2), 0)$.

An argument similar to Theorem 3 will also give us the following extended result of Theorem 1.

Theorem 5: Let $a \equiv 1, 3(8)$ and $b \equiv 1(8)$. Then, each of the equations

$U_m = 2az^2 + b$, $U_m = 2z^2 + b$, $m \equiv 1(2)$,

has only the solutions $m = \pm 1$.

Corollary 6: Let $a \equiv 1, 3(8)$ and $b \equiv 1(8)$. Then, the equations

$x^2 = 4a^2dz^4 + 4abdz^2 + a^2$ and $x^2 = 4dz^4 + 4dbz^2 + a^2$

have only the solution $(x, z) = (\pm a, 0)$.

The following is an extended result of Theorem 3 and is similar to Theorem 5 but with m even.

Theorem 6: Let $a \equiv 1, 3(8)$ and $b \equiv 1(8)$, or $a \equiv 5, 7(8)$ and $b \equiv 5(8)$. Then, the equation $U_m = 2z^2 + ab$, $m \equiv 0(2)$ has

(a) the solutions $m = 2, 4$ if $d = 5$,

(b) only the solution $m = 2$ in all other cases.

Proof:

Case 1. Let $m \equiv 0(8)$. If $m = 0$, $2z^2 + ab = 0$ is impossible. If $m \neq 0$, we write $m = 2 \cdot 3^s \cdot n$ with $4|n$, $3\nmid n$, and therefore $U_m \equiv 0 \pmod{V_n}$ by (21). Thus, if $2z^2 + ab = U_m$, we have $(2z)^2 \equiv -2ab \pmod{V_n}$, which is impossible, since

$\left(\frac{-2ab}{V_n}\right) = -1$ by (19), (20), (16), (17), and the assumption.

Case 2. Let $m \equiv 4(8)$. If $m = 4$, then there exists a solution iff $2z^2 = ab(a^2 + 1)$. Since $a^2 - db^2 = -4$, we have $(b, a^2 + 1) = 1$ or 3. But $a^2 + 1 \not\equiv 0(3)$; therefore, $(b, a^2 + 1) = 1$. It is obvious that $(a, b) = (a, a + 1) = 1$. So we must have $a = t^2$, $b = r^2$, and $a^2 + 1 = 2\lambda^2$, so that $t^4 + 1 = 2\lambda^2$. In [6] W. Ljunggren proved that the diophantine equation $Ax^2 - By^4 = 1$ has at most one solution in positive numbers x and y. In our case, this is $(t, \lambda) = (\pm 1, \pm 1)$, which corresponds to $a = 1$, so $b = 1 = r^2$ and $d = 5$.

If $m \neq 4$, then we write $m = 4 + 2 \cdot 3^s \cdot n$ with $4|n$, $3\nmid n$, and therefore,

$U_m \equiv -(a^3b + 2ab) \pmod{V_n}$ by (21).

Hence, if $2z^2 + ab = U_m$, we have $2z^2 \equiv -ab(a^2 + 3) \equiv -2bV_3 \pmod{V_n}$, which is impossible, since

$\left(\frac{-2bV_3}{V_n}\right) = -1$ by (19), (20), (16), (17), (24), and the assumption.

Case 3. Let $m \equiv 2(4)$. If $m = 2$, then $z = 0$ is a solution. If $m \neq 2$, then we write $m = 2 + 2 \cdot 3^s \cdot n$, with $2|n$, $3\nmid n$, and thus,

$U_m \equiv -ab \pmod{V_n}$ by (21).

Hence, if $2z^2 + ab = U_m$, we have $(2z)^2 \equiv -4ab \pmod{V_n}$, which is impossible, since

$\left(\frac{-4ab}{V_n}\right) = -1$ by (19), (16), (17), and the assumption.

The following corollaries are direct results of the previous theorems. Hence, the proofs are omitted.

Corollary 7: Let $a \equiv 1, 3(8)$ and $b \equiv 1(8)$, or $a \equiv 5, 7(8)$ and $b \equiv 7(8)$. Then, the equation $x^2 = 4dz^4 + 4abdz^2 + (a^2 + 2)^2$ has

(a) two solutions $(x, z) = (\pm 3, 0), (\pm 7, \pm 1)$ if $d = 5$,

(b) only the one solution $(x, z) = (\pm(a^2 + 2), 0)$ in all other cases.

Corollary 8: $F_m = 2z^2 + 1$ iff $m = \pm 1, 2, 4$.

4. GENERALIZED FIBONACCI NUMBERS OF THE FORM $\mu z^2 - \nu$

Lemma 1: The generalized Fibonacci numbers U_m have the form

$U_{2n+1} = b(f_{2n+1}(a^2) + 1), \quad U_{2m} = abf_{2n}(a^2)$

and the generalized Lucas numbers V_m have the form

$V_{2n+1} = ag_{2n+1}(a^2), \quad V_{2n} = g_{2n}(a^2) + 2,$

where f_m, $g_m \in \mathbf{Z}[a^2]$ for each $m \in \mathbf{Z}$ and f_{2n+1}, g_{2n} have no constant term.

Proof: $U_{2n+1} = b(f_{2n+1}(a^2) + 1)$. The proof is by induction on n. If $n = 0$, we have $U_1 = b$, and the relation is true for $f_1(a^2) \equiv 0$. Let us now assume the proposition is true for all values less than or equal to n. Then we have

$$\begin{aligned} U_{2n+3} &= aU_{2n+2} + U_{2n+1} && \text{by (1)} \\ &= a(aU_{2n+1} + U_{2n}) + U_{2n+1} \\ &= (a^2 + 1)b(f_{2n+1}(a^2) + 1) + aU_{2n} && \text{by assumption} \\ &= (a^2 + 1)b(f_{2n+1}(a^2) + 1) + a(aU_{2n-1} + U_{2n-2}) \\ &= (a^2 + 1)b(f_{2n+1}(a^2) + 1) + a^2b(f_{2n-1}(a^2) + 1) + aU_{2n-2} && \text{by assumption} \\ &= \cdots = b(f_{2n+3}(a^2) + 1) + aU_0 = b(f_{2n+3}(a^2) + 1), \end{aligned}$$

with $f_{2n+3}(a^2)$ having no constant term.

In the same way, we can prove the other cases.

Lemma 2: The following identities hold:

$$U_{4n\pm1} = U_{2n\pm1}V_{2n} - b \tag{36}$$
$$U_{4n} = U_{2n-1}V_{2n+1} - ab \tag{37}$$
$$U_{4n} = U_{2n+1}V_{2n-1} + ab \tag{38}$$
$$U_{4n-2} = U_{2n}V_{2n-2} - ab \tag{39}$$
$$U_{4n-2} = U_{2n-2}V_{2n} + ab \tag{40}$$
$$bV_{m+n} = U_{m-1}V_n + U_mV_{n+1} \tag{41}$$
$$V_{2n+1} = V_nV_{n+1} - (-1)^n a \tag{42}$$

Proof of (36): We have $2U_{4n\pm1} = U_{2n\pm1}V_{2n} + U_{2n}V_{2n\pm1}$ by (5); thus,

$$U_{4n\pm1} + b = \frac{U_{2n\pm1}V_{2n} + U_{2n}V_{2n\pm1} + 2b}{2}.$$

It is therefore sufficient to show that

$$U_{2n}V_{2n+1} + 2b = U_{2n+1}V_{2n} \tag{43}$$

and

$$U_{2n}V_{2n-1} + 2b = U_{2n-1}V_{2n}. \tag{44}$$

We will prove (43) by induction on n. For $n = 0$, (43) is true, because $U_0V_{\pm1} + 2b = U_{\pm1}V_0$. Under the assumption that (43) is true for n, it is enough to show that $U_{2n+2}V_{2n+3} + 2b = U_{2n+3}V_{2n}$. By using (1) and (2), we find that it is equivalent to $U_{2n}V_{2n+1} + 2b = U_{2n+1}V_{2n}$, which holds by assumption. In the same way, (44) can be proved.

Proof of (37): By using (5), it is enough to show that

$$U_{2n}V_{2n} = U_{2n-1}V_{2n+1} - ab, \tag{45}$$

which can be proved by induction on n with the aid of (1) and (2). Similarly, (38), (39), and (40) can be proved.

Proof of (41): We again use induction on n. For $n = 0$, it must first be proved that $bV_m = U_{m-1}V_0 + U_mV_1 = 2U_{m-1} + aU_m$. This can be proved by induction on m. The remainder of the proof is straightforward.

Proof of (42): This follows by induction on n using (8) and (2).

Lemma 3: If $b = 1$, then $(U_m, V_{m\pm n})|V_n$.

Proof: By (4), it suffices to show that $g|V_n$, where $g = (U_m, V_{m+n})$. By (41), $g|U_{m-1}V_n$. If $g_1 = (g, U_{m-1})$, then $g_1|U_m$ and $g_1|U_{m-1}$, so that $g_1|U_{m-2}$. Hence, $g_1|b$. But $b = 1$. Therefore, $g_1 = 1$ and $g|V_n$.

Corollary 9: If $b = 1$, then $(U_{2n\pm 1}, V_{2n}) = 1$.

Proof: Let g be as in Lemma 3, with $m = 2n \pm 1$ and $n = \mp 1$, then $g|V_{\pm 1}$ or $g|a$. Since $g|U_{2n\pm 1}$ and $g|a$, Lemma 1 implies $g|b$. However, $(a, b) = 1$. Hence, $g = 1$.

Theorem 7: Let $b = 1$. Then, the equation $U_m = z^2 - b$, $m \equiv 1(2)$, has no solution.

Proof: By (36), we have $U_{2n\pm 1}V_{2n} = z^2$. Hence, Corollary 9 implies that $U_{2n\pm 1} = z_1^2$ and $V_{2n} = z_2^2$, which is impossible by (28).

Theorem 8: Let $b = 1$ and $a^2 + 2 = p$, p a prime. Then, the equation

$$U_m = z^2 - a,\ m \equiv 0(2),$$

has

(a) the solutions $m = -2, 0, 4, 6$, if $d = 5$,

(b) the solutions $m = -2, 4$, if $d = 13$,

(c) the solutions $m = -2, 0, 6$, if a is a perfect square, $d \neq 5$,

(d) only the solution $m = -2$ in all other cases.

Proof:

Case 1. Let $m = 4n - 2$. By (39), $U_{2n}V_{2n-2} = z^2$. Lemma 3 implies that

$$(U_{2n}, V_{2n-2})|p.$$

Hence, we have two possibilities:

(a) $U_{2n} = W_1^2$ and $V_{2n-2} = W_2^2$ or (b) $U_{2n} = pW_1^2$ and $V_{2n-2} = pW_2^2$.

The first is impossible by (28). The second can be written by (5) as

$$U_nV_n = pW_1^2,\ V_{2n-2} = pW_2^2.$$

Let $n \not\equiv 0(3)$. Then equation (10) implies that $(U_n, V_n) = 1$, and so

$$U_n = pt^2,\ V_n = r^2,\ V_{2n-2} = pW_2^2 \tag{46}$$

$$U_n = t^2,\ V_n = pr^2,\ V_{2n-2} = pW_2^2. \tag{47}$$

Equation (46) does not possess any solution, since the possible values of n, by (28), in order for V_n to be a perfect square, do not yield a solution of $U_n = pt^2$.

By using (30) and direct computation, we find that (47) has only one solution, which is $n = 2$ or $m = 6$ provided a is a perfect square.

Let $n \equiv 0(3)$. Equation (10) implies that $(U_n, V_n) = 2$, and so we have to check the following subcases:

$$U_{3\lambda} = 2pt^2,\ V_{3\lambda} = 2r^2,\ V_{2n-2} = pW_2^2, \tag{48}$$

or

$$U_{3\lambda} = 2t^2,\ V_{3\lambda} = 2pr^2,\ V_{2n-2} = pW_2^2,\ (n = 3\lambda). \tag{49}$$

By (29) and the assumption, $V_{3\lambda} = 2r^2$ is possible only for $\lambda = 0$ or $\lambda = \pm 2$ in the case $d = 5$. The value $\lambda = 0$ implies $n = 0$ or $m = -2$, which gives a solution to (48). The values $\lambda = \pm 2$, $d = 5$, do not give a solution, since $F_{\pm 6} = \pm 8 \neq 2pt^2$.

According to (31), the only values of λ for which a solution of (49) may exist are $\lambda = 2$ if $d = 5$, or $\lambda = 0$ and $\lambda = \pm 1$. Now, $\lambda = 0$ does not give any solution, because we would have $pr^2 = 1$. Similarly, $\lambda = \pm 1$ does not give any solution, since we would have $V_{\pm 3} = \pm a(a^2 + 3) = 2pt^2$, which is impossible because $p \nmid a$ and $p \nmid (a^2 + 3)$ when $a^2 + 3 = p + 1$. Finally, $\lambda = 2$, $d = 5$, does not give any solution, since $L_6 = 18 \neq 2 \cdot 3r^2$.

Case 2. Let $m = 4n$. By (37), $U_{2n-1}V_{2n+1} = z^2$. Now Lemma 3 implies that $(U_{2n-1}, V_{2n+1}) | p$, so we have two possibilities, which are

$$U_{2n-1} = W_1^2,\ V_{2n+1} = W_2^2 \tag{50}$$

or

$$U_{2n-1} = pt^2 = V_2t^2,\ V_{2n+1} = V_2r^2. \tag{51}$$

By using (28) and (30), we find that (50) has only the solutions:

(a) $m = 0, 4$, if $d = 5$,

(b) $m = 4$, if $d = 13$,

(c) $m = 0$, if a is a perfect square, $d \neq 5$.

Using (13) for $2n + 1 = 4\lambda \pm 1$, we have

$$2V_{2n\pm 1} \equiv -2V_{4\lambda - 4 \pm 1} \equiv \cdots \equiv \pm 2V_{\pm 1} \pmod{V_2}.$$

Therefore, since $V_{2n+1} = pr^2 = V_2r^2$, we have $(a^2 + 2) | V_{\pm 1}$ or $p | a$, which is impossible. Thus, (51) has no solution.

Corollary 10: For each $d = a^2 + 4$, $a \equiv 1(2)$, the diophantine equation

$$x^2 = dz^4 - 2dz^2 + a^2$$

has no solution.

Corollary 11: Let $d = a^2 + 4$ and $a^2 + 2 = p$, where p is a prime. Then, the diophantine equation $x^2 = dz^4 - 2adz^2 + (a^2 + 2)^2$ has:

(a) Four solutions, $(x, z) = (\pm 3, 0), (\pm 2, \pm 1), (\pm 7, \pm 2), (\pm 18, \pm 3)$, if $d = 5$.

(b) Two solutions, $(x, z) = (\pm 11, 0), (\pm 119, \pm 6)$, if $d = 13$.

(c) Three solutions, $(x, z) = (\pm(a^2 + 2), 0), (\pm 2, \pm t), (\pm(a^6 + 6a^4 + 9a^2 + 2), \pm t(a^2 + 2))$, if $a = t^2$ is a perfect square.

(d) Only the solution $(x, z) = (\pm(a^2 + 2), 0)$ in all other cases.

When $a = 1$ in Theorem 8, we have the following result, found in [8].

Corollary 12: $F_m = z^2 - 1$ iff $m = -2, 0, 4, 6$.

The next result is an extension of Theorem 7.

Theorem 9: Let $b = 1$. Then, the equation $U_m = 2z^2 - b$, $m \equiv 1(2)$, has only the solutions $m = \pm 1$.

Proof: Equation (36) implies that $U_{2n\pm1}V_{2n} - b = 2z^2 - b$, for $m = 4n \pm 1$. Hence, $U_{2m\pm1}V_{2n} = 2z^2$. By Corollary 9,

$$U_{2n\pm1} = 2t^2,\ V_{2n} = r^2 \quad \text{or} \quad U_{2n\pm1} = t^2,\ V_{2n} = 2r^2.$$

Now $V_{2n} = r^2$ is impossible by (28) and the second case implies, using (30) and (29), that $n = 0$ or $m = \pm 1$.

The following result is an extended parallel of Theorem 8.

Theorem 10: Let $b = 1$ and $a^2 + 2 = p$, where p is a prime. Then, the equation $U_m = 2z^2 - a$, $m \equiv 0(2)$ has

(a) the solutions $m = -2, 2$ if a is a perfect square,

(b) only the solution $m = -2$ in all other cases.

Proof:

Case 1. Let $m = 4n - 2$. Equation (39) implies that $U_{2n}V_{2n-2} = 2z^2$. But, by Lemma 3, $(U_{2n}, V_{2n-2})|V_2$, where $V_2 = p$, so that $(U_{2n}, V_{2n-2}) = 1$ or p. If $(U_{2n}, V_{2n-2}) = 1$, then we must have

$$U_{2n} = 2t^2,\ V_{2n-2} = r^2 \quad \text{or} \quad U_{2n} = t^2,\ V_{2n-2} = 2r^2.$$

The first case is impossible by (28). The second case has, by (30) and (29), only the solution $n = 1$ or $m = 2$ if a is a perfect square.

Now, let $(U_{2n}, V_{2n-2}) = p$. We then have to check two possibilities:

$$U_{2n} = pt^2,\ V_{2n-2} = 2pr^2 \quad \text{or} \quad U_{2n} = 2pt^2,\ V_{2n-2} = pr^2.$$

In the first case we must have, by (9), $n \equiv 1(3)$, say $n = 3\lambda + 1$. By (5), we also have $U_nV_n = pt^2$. But $(U_n, V_n) = 1$; therefore, we have

$$U_n = pW_1^2,\ V_n = W_2^2,\ V_{2n-2} = 2pr^2, \tag{52}$$

or

$$U_n = W_1^2,\ V_n = pW_2^2,\ V_{2n-2} = 2pr^2. \tag{53}$$

Equation (52) has no solution since, by (28), the only solution of $V_n = W_2^2$ is $n = 1$, for which $U_n = pW_1^2$ is impossible. Equation (53) has no solution either since, by (30), the only possible value for n of $U = W_1^2$ is $n = 1$, but then $V_1 = a = pW_2^2$, which is impossible.

For the second case we must have, by (9), $3|n$, say $n = 3\lambda$. By (5), we have $U_{3\lambda}V_{3\lambda} = 2pt^2$. Since, by (10), $(U_{3\lambda}, V_{3\lambda}) = 2$, we must check the following subcases:

$$U_{3\lambda} = 4pr_1^2,\ V_{3\lambda} = 2r_2^2,\ V_{2n-2} = pr^2; \tag{54}$$

$$U_{3\lambda} = (2r_1)^2,\ V_{3\lambda} = 2pr_2^2,\ V_{2n-2} = pr^2; \tag{55}$$

$$U_{3\lambda} = 2pr_1^2,\ V_{3\lambda} = (2r_2)^2,\ V_{2n-2} = pr^2; \tag{56}$$

$$U_{3\lambda} = 2r_1^2,\ V_{3\lambda} = 4pr_2^2,\ V_{2n-2} = pr^2. \tag{57}$$

By (29), the only possible solutions of (54) are $\lambda = 0$ for each d, and $\lambda = \pm 2$ if $d = 5$. We know $\lambda = 0$ is a solution, since $U_0 = 0 = 4pr_1^2$ with $r_1 = 0$ and $V_{-2} = pr^2 = V_2 r^2$ with $r = \pm 1$.

Since $F_{\pm 6} = \pm 8 \neq 4 \cdot 3 \cdot r_1^2$, $\lambda = \pm 2$ is not a solution of (54). By (30), the only possible solutions of (55) are $\lambda = 0$, and $\lambda = 4$ if $d = 5$. It is obvious that $\lambda = 0$ is not a solution, since $V_0 = 2 \neq 2 \cdot V_2^2$. Neither is $\lambda = 4$ a solution, since $L_{12} = 322 \neq 2 \cdot 3 \cdot r_2^2$. In the same way, we can prove that (56) and (57) have no solutions. The possible values $\lambda = \pm 1$ in (57) do not yield a solution, since $p = a^2 + 2 \nmid a(a^2 + 3) = V_{\pm 3}$.

Case 2. Let $m = 4n$. By (37), $U_{2n-1}V_{2n+1} = 2z^2$. Using Lemma 3 and the assumption, $(U_{2n-1}, V_{2n+1}) = 1$ or p.

If $(U_{2n-1}, V_{2n+1}) = 1$, we have

$$U_{2n-1} = 2t^2, \; V_{2n+1} = r^2 \tag{58}$$

or

$$U_{2n-1} = t^2, \; V_{2n+1} = 2r^2. \tag{59}$$

By (31) and (28), (58) has no solution. By (29), (59) has no solution.

If $(U_{2n-1}, V_{2n+1}) = p$, we have

$$U_{2n-1} = 2pz_1^2, \; V_{2n+1} = pz_2^2 \tag{60}$$

or

$$U_{2n-1} = pz_1^2, \; V_{2n+1} = 2pz_2^2. \tag{61}$$

Neither (60) nor (61) has a solution by using a proof similar to that given at the end of Theorem 8.

The following are immediate consequences of the preceding theorems.

Corollary 13: If $d = a^2 + 4$, $a \equiv 1(2)$, then the equation $x^2 = 4dz^4 - 4dz^2 + a^2$ has only the solution $(x, z) = (\pm a, 0)$.

Corollary 14: Let $d = a^2 + 4$ and $a^2 + 2 = p$, where p is a prime. Then, the equation $x^2 = 4dz^4 - 4adz^2 + (a^2 + 2)^2$ has

(a) two solutions, $(x, z) = (\pm(a^2 + 2), 0)$, $(\pm(a^2 + 2), \pm r)$ if a is a perfect square, $a = r^2$,

(b) only the one solution $(x, z) = (\pm(a^2 + 2), 0)$ in all other cases.

Corollary 15: $F_m = 2z^2 - 1$ iff $m = \pm 1, \pm 2$.

5. GENERALIZED LUCAS NUMBERS OF THE FORM $\mu z^2 \pm \nu$

Theorem 11: The equation $V_m = z^2 + a$, $m \equiv 1(2)$, has only the solution $m = 1$.

Proof:

Case 1. Let $m = 4n - 1$. By (42), $V_{2n-1}V_{2n} = z^2$. Since $(V_{2n-1}, V_{2n}) = 1$, we have $V_{2n-1} = t^2$, $V_{2n} = r^2$, which is impossible by (28).

Case 2. Let $m = 4n + 1$. By (42), $V_{2n}V_{2n+1} - 2a = z^2$. Hence, using (8) and (42), we have

$$\{V_n^2 - 2(-1)^n\}\{V_n V_{n+1} - (-1)^n a\} - 2a = z^2,$$

which implies that $V_nM_n = z^2$ with $M_n = V_n^2V_{n+1} - (-1)^n aV_n - 2(-1)^n V_{n+1}$. Let p be an odd prime and let $p^e \| V_n$. Since $(V_{n+1}, V_n) = \cdots = (V_1, V_0) = (a, 2) = 1$, it follows that $p \nmid M_n$. This implies $e \equiv 0(2)$ and therefore $V_n = t^2$ or $V_n = 2t^2$. Using (28) and (29), we find that the possible solutions are $m = 1, 5, 13, 25, -23$ if $d = 5$, $m = 1, 13$ if $d = 13$, $m = 1, 5, 25, -23$ if $d = 29$, $m = 1, 5$ if $a = t^2$ and $d \neq 5$, $m = 1$ otherwise. Obviously, $m = 1$ is a solution. For $m = 5$ and $a = t^2$, we have $(a^2 + 2)^2 + a^2 = r^2$, which is impossible because both a and $a^2 + 2$ are odd. By a direct computation of each corresponding V_m in all other cases, we see that no other solutions exist. Note that for $d = 29$,

$$V_{25} = 766628450142675125.$$

Following an argument similar to Theorem 11, we can prove Theorem 12.

Theorem 12: The equation $V_m = z^2 - a$, $m \equiv 1(2)$ has only the solution $m = -1$.

Corollary 16: If $b = 1$, then the diophantine equations

$$dy^2 = z^4 + 2az^2 + a^2 + 4 \quad \text{and} \quad dy^2 = z^4 - 2az^2 + a^2 + 4$$

have only the solution $(y, z) = (\pm 1, 0)$.

The next two theorems are similar to the last two, but m is even.

Theorem 13: Let p be an odd prime. Then, the equation $V_m = z^2 + (p - 2)$, $m \equiv 0(2)$ has

(a) the solution $m = 0$ if $p = 3$,

(b) the solutions $m = \pm 2, \pm 4$ if $d = 5$ and $p = 5$,

(c) at most $\prod_{i=1}^{r} (s_i + 1) + 1$ solutions if

$$p - 4 = q_1^{s_1} \cdot q_2^{s_2} \cdot \cdots \cdot q_r^{s_r}$$

as its unique factorization.

Proof:

Case 1. Let $m = 4n$. By (8), $V_{2n}^2 - z^2 = p$, which implies that

$$V_{2n} = \pm\frac{p+1}{2} \quad \text{or} \quad V_{2n} = \frac{p+1}{2} \text{ by (19).}$$

If $p = 3$, then $V_{2n} = 2$, which implies that $n = 0$ or $m = 0$ is a solution with $z = 0$. If $p = 5$, then $V_{2n} = 3$, which can only be true if $n = \pm 1$ and $d = 5$ or $m = \pm 4$ and $d = 5$. If $p > 5$, there exists at most one solution.

Case 2. Let $m = 4n + 2$. By (8), $V_{2n+1}^2 - z^2 = p - 4$. If $p = 3$, then $V_{2n+1} = 0$, which is impossible. If $p = 5$, then $V_{2n+1} = \pm 1$ and the only possibilities for solutions are $n = 0$ or -1 and $d = 5$ or $m = \pm 2$ and $d = 5$. If $p > 5$, then

$$V_{2n+1} = \pm\frac{d_1 + d_2}{2}, \; d_1 > 0, \; d_2 > 0,$$

where (d_1, d_2) runs over all the divisors of $p - 4$ with $d_1 d_2 = p - 4$. Since the number of divisors of $p - 4$ is $\prod_{i=1}^{r}(s_i + 1)$, the theorem is proved.

In the same way, we can prove

Theorem 14: Let p be an odd prime. Then, the equation $V_m = z^2 - (p - 2)$, $m \equiv 0(2)$, has

(a) the solutions $m = \pm 2$, $d = 5$, if $p = 3$,

(b) no solution if $p = 5$,

(c) at most
$$\begin{cases} \frac{1}{2}\left[\prod_{i=1}^{r}(s_i + 1) - 1\right] + 2 \text{ solutions if } p - 4 \text{ is a perfect square} \\ \frac{1}{2}\prod_{i=1}^{r}(s_i + 1) + 2 \text{ solutions if } p - 4 \text{ is not a perfect square,} \end{cases}$$

where $p - 4 = q_1^{s_1}q_2^{s_2} \ldots q_r^{s_r}$ as its unique factorization.

Corollary 17:

(i) The diophantine equation $z^4 + 2(p - 2)z^2 + p(p - 4) = dy^2$ has

(a) one solution for each d if $p = 3$,

(b) four solutions for $d = 5$ if $p = 5$,

(c) at most $\prod_{i=1}^{r}(s_i + 1) + 1$ solutions if $p > 5$ and $p - 4 = q_1^{s_1} \ldots q_r^{s_r}$ as its unique factorization.

(ii) The diophantine equation $z^4 - 2(p - 2)z^2 + p(p - 4) = dy^2$ has

(a) one solution for each d is $p = 3$,

(b) no solution for each d if $p = 5$,

(c) at most
$$\begin{cases} \frac{1}{2}\left[\prod_{i=1}^{r}(s_i + 1) - 1\right] + 2 \text{ solutions if } p - 4 \text{ is a perfect square} \\ \frac{1}{2}\prod_{i=1}^{r}(s_i + 1) + 2 \text{ solutions if } p - 4 \text{ is not a perfect square,} \end{cases}$$

where $p > 5$ and $p - 4 = q_1^{s_1} \ldots q_r^{s_r}$ as its unique factorization.

Corollary 18: The following can be found in [4] and [8]:

$L_m = z^2 + 1$ iff $m = 0, 1$,

$L_m = z^2 - 1$ iff $m = -1, \pm 2$.

By an argument similar to Theorems 11 and 12, we can prove

Theorem 15:

(i) The equation $V_m = 2z^2 + a$, $m \equiv 1(2)$, has only the solution $m = 1$.

(ii) The equation $V_m = 2z^2 - a$, $m \equiv 1(2)$, has

(a) the solutions $m = \pm 1$ is a is a perfect square,

(b) only the solution $m = -1$ in all other cases.

By using the method of Cohn, as before, we can also prove

Theorem 16: $L_m = 2z^2 + 1$, $m \equiv 0(2)$, iff $m = \pm 2$,
$L_m = 2z^2 - 1$, $m \equiv 0(2)$, iff $m = \pm 4$.

Corollary 19: $L_m = 2z^2 + 1$ iff $m = \pm 2, 1$,
$L_m = 2z^2 - 1$ iff $m = \pm 1, \pm 4$.

REFERENCES

1. J. A. Antoniadis. "Über die Kennzeichnung zweiklassiger imaginär-quadratischer Zahlkörper durch Lösungen Diophantischer Gleichungen." *Journal für die reine und angewandte Math. 339* (1983):27-81.
2. J. H. E. Cohn. "Eight Diophantine Equations." *Proc. of the L.M.S.* (3) *16* (1966):155-166, *Addendum* (3) *17* (1967):381.
3. R. Finkelstein. "On Fibonacci Numbers Which Are One More Than a Square." *Journal für die reine und angewandte Math. 262-63* (1973):171-178.
4. R. Finkelstein. "On Lucas Numbers Which Are More Than a Square." *The Fibonacci Quarterly 13*, no. 4 (1975):340-342.
5. R. K. Guy. *Unsolved Problems in Number Theory.* New York: Springer-Verlag, 1981.
6. W. Ljunggren. "Über die unbestimmte Gleichung $Ax^2 - By^4 = C$." *Archic for Math. og Naturvidenskab 41*, no. 10 (1938), 38 pp.
7. T. Nagell. *Introduction to Number Theory.* New York: Wiley, 1951.
8. N. Robbins. "Fibonacci and Lucas Numbers of the Forms $w^2 - 1$, $w^3 \pm 1$." *The Fibonacci Quarterly 19*, no. 5 (1981):369-373.
9. H. C. Williams. "On Fibonacci Numbers of the Form $k^2 + 1$." *The Fibonacci Quarterly 13*, no. 3 (1975):213-214.

◆◇◆◇◆