ARAB JOURNAL OF
MATHEMATICAL SCIENCES

Arab J Math Sci 23 (2017) 148–156

On the equation $V_n = wx^2 \mp 1$

ÜMMÜGÜLSÜM ÖĞÜT, REFİK KESKİN*
Sakarya University, Mathematics Department, Sakarya, Turkey

Received 25 February 2016; accepted 11 June 2016
Available online 30 June 2016

Abstract. Let $P \geq 3$ be an integer and (V_n) denote Lucas sequence of the second kind defined by $V_0 = 2, V_1 = P$, and $V_{n+1} = PV_n - V_{n-1}$ for $n \geq 1$. In this study, when P is odd and $w \in \{10, 14, 15, 21, 30, 35, 42, 70, 210\}$, we solved the equation $V_n = wx^2 \mp 1$. We showed that only V_1 can be of the form $wx^2 + 1$ and only V_1 or V_2 can be of the form $wx^2 - 1$.

2010 Mathematics Subject Classification: 11B37; 11B39; 11B50; 11B99; 11D41

Keywords: Lucas sequence of the second kind; Congruences; Diophantine equations

1. INTRODUCTION

Let $P \geq 3$ be an integer and (V_n) denote Lucas sequence of the second kind defined by $V_0 = 2, V_1 = P$, and $V_{n+1} = PV_n - V_{n-1}$ for $n \geq 1$.

In [1], the authors showed that when $a \neq 0$ and $b \neq \pm 2$, the equation $V_n = ax^2 + b$ has only a finite number of solutions n. In [5], Keskin solved the equations $V_n = wx^2 + 1$ and $V_n = wx^2 - 1$ for $w = 1, 2, 3, 6$ when P is odd. In [4], when P is odd, Karaatlı and Keskin solved the equations $V_n = 5x^2 \pm 1$ and $V_n = 7x^2 \pm 1$. In the present paper, when P is odd, we solve the equations $V_n = wx^2 \pm 1$ for $w = 10, 14, 15, 21, 35, 42, 70, 210$. We show that only V_1 can be of the form $wx^2 + 1$ and only V_1 or V_2 can be of the form $wx^2 - 1$.

We will use the Jacobi symbol throughout this study. Our method of proof is similar to that used by Cohn, Ribenboim and McDaniel in [3] and [6,7], respectively.

* Corresponding author.
E-mail addresses: uogut@sakarya.edu.tr (Ü. Öğüt), rkeskin@sakarya.edu.tr (R. Keskin).

Peer review under responsibility of King Saud University.

ELSEVIER Production and hosting by Elsevier

http://dx.doi.org/10.1016/j.ajmsc.2016.06.004

2. Preliminaries

The following theorem is given in [8].

Theorem 2.1. *Let $n \in \mathbb{N} \cup \{0\}$ and $m, r \in \mathbb{Z}$. Then*

$$V_{2mn+r} \equiv (-1)^n V_r \pmod{V_m}. \tag{2.1}$$

If $n = 2 \cdot 2^k a + r$ with a odd, then we get

$$V_n = V_{2 \cdot 2^k a + r} \equiv -V_r \pmod{V_{2^k}} \tag{2.2}$$

by (2.1).

When P is odd, an induction method shows that

$$V_{2^k} \equiv 7 \pmod 8$$

and thus

$$\left(\frac{2}{V_{2^k}}\right) = 1 \tag{2.3}$$

and

$$\left(\frac{-1}{V_{2^k}}\right) = -1 \tag{2.4}$$

for all $k \geq 1$.

Moreover, if P is odd and $3 \nmid P$, then $V_{2^k} \equiv -1 \pmod 3$ and therefore

$$\left(\frac{3}{V_{2^k}}\right) = 1 \tag{2.5}$$

for all $k \geq 1$.

If P is odd and $3|P$, then $V_{2^k} \equiv -1 \pmod 3$ and therefore

$$\left(\frac{3}{V_{2^k}}\right) = 1 \tag{2.6}$$

for all $k \geq 2$.

Thus (2.5) and (2.6) shows that

$$\left(\frac{3}{V_{2^k}}\right) = 1 \tag{2.7}$$

for all $k \geq 2$.

When P is odd, we have

$$\left(\frac{P-1}{V_{2^k}}\right) = \left(\frac{P+1}{V_{2^k}}\right) = 1 \tag{2.8}$$

for $k \geq 1$.

If P is odd, then $V_{2^k} \equiv -1 (\bmod P^2 - 3)$ and therefore

$$\left(\frac{P^2-3}{V_{2^k}}\right) = 1 \tag{2.9}$$

for all $k \geq 2$.

When P is odd, we have

$$\left(\frac{5}{V_{2^k}}\right) = \begin{cases} -1, & \text{if } 5|P \\ 1, & \text{if } P^2 \equiv 1 (\bmod 5) \\ -1, & \text{if } P^2 \equiv -1 (\bmod 5), \end{cases} \tag{2.10}$$

and

$$\left(\frac{7}{V_{2^k}}\right) = \begin{cases} -1, & \text{if } P^2 \equiv 4 (\bmod 7) \\ 1, & \text{if } P^2 \equiv 1 (\bmod 7) \end{cases} \tag{2.11}$$

for all $k \geq 1$.

Now we give some identities concerning the terms of the Lucas sequence:

$$V_{-n} = V_n,$$
$$V_{2n} = V_n^2 - 2. \tag{2.12}$$

When $P^2 \equiv -1 (\bmod 5)$, we have

$$V_n \equiv \begin{cases} 2 (\bmod 5), & \text{if } n \text{ is even,} \\ P (\bmod 5), & \text{if } n \text{ is odd.} \end{cases} \tag{2.13}$$

When $P^2 \equiv 4 (\bmod 7)$, by using induction, it can be seen that

$$V_n \equiv \begin{cases} 2 (\bmod 7), & \text{if } n \text{ is even,} \\ P (\bmod 7), & \text{if } n \text{ is odd.} \end{cases} \tag{2.14}$$

If $P^2 \equiv 2 (\bmod 7)$, then we have $7|V_2$ and $V_{8q+r} \equiv V_r \ (\bmod V_2)$ by (2.1). Therefore we get,

$$V_n \equiv \begin{cases} 0, \pm 2 (\bmod 7), & \text{if } n \text{ is even,} \\ \pm P (\bmod 7), & \text{if } n \text{ is odd.} \end{cases} \tag{2.15}$$

The following lemma can be given from Theorem 2.1.

Lemma 1. *If n is a positive integer, then $V_{2n} \equiv \pm 2 (\bmod P)$ and $P|V_n$ if n is odd.*

3. Main theorems

From now on, we will assume that n is a positive integer and P is an odd positive integer.

Theorem 3.1. *Let $w \in S = \{2^{a_1}3^{a_2}5^{a_3}7^{a_4} : a_i \in \{0, 1\}$ and $a_3 \neq 0$ or $a_4 \neq 0\}$. If $V_n = wx^2 + 1$ for some positive integer x, then $n = 1$.*

Proof. Assume that n is even. Then $V_n = V_{2m} = V_m^2 - 2$ by (2.12) and thus $V_m^2 - 2 = wx^2 + 1$. Therefore $V_m^2 = 3 \ (\bmod w)$. If $a_3 \neq 0$ or $a_4 \neq 0$, then $V_m^2 = 3 \ (\bmod 5)$ or $V_m^2 = 3 \ (\bmod 7)$, respectively. These are impossible. And so n is odd and therefore $P|V_n$

by Lemma 1. Thus it can be seen that $(w, P) = 1$. Let $3|w$. Then $3 \nmid P$ since $(w, P) = 1$. Therefore $\left(\frac{3}{V_{2^k}}\right) = 1$ by (2.5). If $3 \nmid w$, then $a_2 = 0$ and we conclude that

$$\left(\frac{3^{a_2}}{V_{2^k}}\right) = 1. \tag{3.1}$$

Now we divide the proof into three cases.

Case 1: Assume that $a_3 \neq 0$ and $a_4 = 0$. Then $5|w$ and thus $5 \nmid P$ since $(w, P) = 1$. Moreover we have $V_n \equiv 1(\bmod 5)$ in this case. If $P^2 \equiv -1(\bmod 5)$, then $V_n \equiv P \equiv \pm 2(\bmod 5)$ by (2.13), which is impossible since $V_n \equiv 1(\bmod 5)$. Assume that $P^2 \equiv 1(\bmod 5)$ and $n > 1$. Then $n = 4q \pm 1$ for some positive integer $q > 0$. Thus $n = 2 \cdot 2^k a \pm 1$ with a odd and $k \geq 1$. Therefore,

$$wx^2 = -1 + V_n \equiv -1 - V_{\pm 1}(\bmod V_{2^k})$$

by (2.2). This shows that

$$wx^2 \equiv -(P+1)(\bmod V_{2^k}),$$

which implies that

$$\left(\frac{w}{V_{2^k}}\right) = \left(\frac{-1}{V_{2^k}}\right)\left(\frac{P+1}{V_{2^k}}\right),$$

i.e.

$$\left(\frac{w}{V_{2^k}}\right) = -1$$

by (2.4) and (2.8). But $\left(\frac{w}{V_{2^k}}\right) = 1$ since $\left(\frac{2^{a_1}}{V_{2^k}}\right) = 1$, $\left(\frac{5}{V_{2^k}}\right) = 1$ and $\left(\frac{3^{a_2}}{V_{2^k}}\right) = 1$ by (2.3), (2.10), and (3.1), respectively. This contradicts the fact that $\left(\frac{w}{V_{2^k}}\right) = -1$.

Case 2: Assume that $a_3 = 0$ and $a_4 \neq 0$. Then $7|w$ and so $V_n \equiv 1(\bmod 7)$. Moreover, $7 \nmid P$ since $(w, P) = 1$. If $P^2 \equiv 2, 4(\bmod 7)$ then $V_n \equiv \pm P \equiv \pm 2, \pm 3(\bmod 7)$ by (2.14) and (2.15), which is impossible since $V_n \equiv 1(\bmod 7)$. Now assume that $P^2 \equiv 1(\bmod 7)$ and $n > 1$. Then $n = 4q \pm 1$ for some $q > 0$. Thus $n = 2 \cdot 2^k a \pm 1$ with a odd and $k \geq 1$. Therefore,

$$wx^2 = -1 + V_n \equiv -1 - V_{\pm 1}(\bmod V_{2^k})$$

by (2.2). This shows that

$$wx^2 \equiv -(P+1)(\bmod V_{2^k}),$$

which implies that

$$\left(\frac{w}{V_{2^k}}\right) = \left(\frac{-1}{V_{2^k}}\right)\left(\frac{P+1}{V_{2^k}}\right).$$

Therefore,

$$\left(\frac{w}{V_{2^k}}\right) = -1$$

by (2.4) and (2.8). But $\left(\frac{w}{V_{2^k}}\right) = 1$ since $\left(\frac{2^{a_1}}{V_{2^k}}\right) = 1$, $\left(\frac{7}{V_{2^k}}\right) = 1$, and $\left(\frac{3^{a_2}}{V_{2^k}}\right) = 1$ by (2.3), (2.11), and (3.1), respectively. This contradicts the fact that $\left(\frac{w}{V_{2^k}}\right) = -1$.

Case 3: Assume that $a_3 \neq 0$ and $a_4 \neq 0$. Then $5|w$ and $7|w$ and so $V_n \equiv 1(\operatorname{mod} 35)$. Moreover, $5 \nmid P$ and $7 \nmid P$ since $(w, P) = 1$. If $P^2 \equiv 2, 4(\operatorname{mod} 7)$, then $V_n \equiv \pm P \equiv \pm 2, \pm 3(\operatorname{mod} 7)$ by (2.14) and (2.15), respectively. This is impossible since $V_n \equiv 1(\operatorname{mod} 7)$. If $P^2 \equiv -1(\operatorname{mod} 5)$, then $V_n \equiv P \equiv \pm 2(\operatorname{mod} 5)$ by (2.13), which is impossible since $V_n \equiv 1(\operatorname{mod} 5)$. Therefore $P^2 \equiv 1(\operatorname{mod} 5)$ and $P^2 \equiv 1(\operatorname{mod} 7)$. Let $n > 1$. Then $n = 4q \pm 1$ for some positive integer $q > 0$. Thus $n = 2 \cdot 2^k a \pm 1$ with a odd and $k \geq 1$. Therefore,

$$wx^2 = -1 + V_n \equiv -1 - V_{\pm 1}(\operatorname{mod} V_{2^k})$$

by (2.2). This shows that

$$wx^2 \equiv -(P+1)(\operatorname{mod} V_{2^k}),$$

which implies

$$\left(\frac{w}{V_{2^k}}\right) = \left(\frac{-1}{V_{2^k}}\right)\left(\frac{P+1}{V_{2^k}}\right).$$

Then it follows that

$$\left(\frac{w}{V_{2^k}}\right) = -1$$

by (2.4) and (2.8). But this is impossible since $\left(\frac{2^{a_1}}{V_{2^k}}\right) = 1$, $\left(\frac{5}{V_{2^k}}\right)$, $\left(\frac{7}{V_{2^k}}\right) = 1$, and $\left(\frac{3^{a_2}}{V_{2^k}}\right) = 1$ by (2.3), (2.10), (2.11), and (3.1), respectively. Therefore $n = 1$. ■

Theorem 3.2. *Let $w \in S = \{2^{a_1}3^{a_2}5^{a_3}7^{a_4} : a_i \in \{0,1\}$ and $a_3 \neq 0$ or $a_4 \neq 0\}$. If $V_n = wx^2 - 1$ for some positive integer x, then $n = 1$ or $n = 2$.*

Proof. If $n = 4q$ for some $q > 0$. Then we get

$$wx^2 - 1 = V_{4t} = V_{2t}^2 - 2 = \left(V_t^2 - 2\right)^2 - 2 = V_t^4 - 4V_t^2 + 2,$$

and then $wx^2 = V_t^4 - 4V_t^2 + 3$. But the integer points on $wX^2 = Y^4 - 4Y^2 + 3$ are easily determined by using MAGMA [2] to be $(X, Y) = (0, \pm 1)$. This implies that $V_t = 1$, which is impossible. Thus $n \neq 4q$. Let n be odd and $3|w$. Then $3 \nmid P$ since $P|V_n$ when n is odd by Lemma 1. Therefore $\left(\frac{3}{V_{2^k}}\right) = 1$ by (2.5). If $3 \nmid w$, then $a_2 = 0$ and we conclude that

$$\left(\frac{3^{a_2}}{V_{2^k}}\right) = 1. \tag{3.2}$$

Now we divide the proof into three cases.

Case 1: Assume that $a_3 \neq 0$ and $a_4 = 0$. Then $5|w$ and so $V_n \equiv -1(\bmod 5)$. If $5|P$, then $V_n \equiv 0, \pm 2(\bmod 5)$ by Lemma 1, which is impossible since $V_n \equiv -1(\bmod 5)$. If $P^2 \equiv -1(\bmod 5)$, then $V_n \equiv 2, P \equiv \pm 2(\bmod 5)$ by (2.13), which is impossible since $V_n \equiv -1(\bmod 5)$. Assume that $P^2 \equiv 1(\bmod 5)$. Let $n > 1$ be odd. Then $P|V_n$ by Lemma 1. Thus it can be seen that $(w, P) = 1$. Since n is odd, $n = 4q \pm 1$ for some positive integer q. Thus $n = 2 \cdot 2^k a \pm 1$ with a odd and $k \geq 1$. Therefore,

$$wx^2 = 1 + V_n \equiv 1 - V_{\pm 1}(\bmod V_{2^k})$$

by (2.2). This shows that

$$wx^2 \equiv -(P-1)(\bmod V_{2^k}),$$

which implies

$$\left(\frac{w}{V_{2^k}}\right) = \left(\frac{-1}{V_{2^k}}\right)\left(\frac{P-1}{V_{2^k}}\right),$$

i.e.

$$\left(\frac{w}{V_{2^k}}\right) = -1$$

by (2.4) and (2.8). This is impossible since $\left(\frac{2^{a_1}}{V_{2^k}}\right) = 1$, $\left(\frac{3^{a_2}}{V_{2^k}}\right) = 1$, and $\left(\frac{5}{V_{2^k}}\right) = 1$ by (2.3), (3.2), and (2.10), respectively. Now, let $n > 2$ be even. Then $n = 4q$ or $n = 8q \pm 2$ for some $q > 0$. But $n \neq 4q$, which was shown at the beginning of the proof. Then $n = 8q \pm 2$. And so $n = 2 \cdot 2^k a \pm 2$ with a odd and $k \geq 2$. Then,

$$wx^2 = 1 + V_n \equiv 1 - V_{\pm 2}(\bmod V_{2^k})$$

by (2.2). This shows that

$$wx^2 \equiv -(P^2 - 3)(\bmod V_{2^k}),$$

which implies

$$\left(\frac{w}{V_{2^k}}\right) = \left(\frac{-1}{V_{2^k}}\right)\left(\frac{P^2-3}{V_{2^k}}\right),$$

i.e.,

$$\left(\frac{w}{V_{2^k}}\right) = -1$$

by (2.4) and (2.9). This is impossible since $\left(\frac{2^{a_1}}{V_{2^k}}\right) = 1$, $\left(\frac{5}{V_{2^k}}\right) = 1$, and $\left(\frac{3^{a_2}}{V_{2^k}}\right) = 1$ by (2.3), (2.10), and (2.7), respectively.

Case 2: Assume that $a_3 = 0$ and $a_4 \neq 0$. Then $7|w$ and so $V_n \equiv -1(\bmod 7)$. If $7|P$, then $V_n \equiv 0, \pm 2(\bmod P)$, i.e., $V_n \equiv 0, \pm 2(\bmod 7)$ by Lemma 1, which is impossible since $V_n \equiv -1(\bmod 7)$. Therefore $7 \nmid P$. If $P^2 \equiv 2, 4(\bmod 7)$, then $V_n \equiv 0, \pm P, \pm 2$

$\equiv 0, \pm 2, \pm 3 \pmod 7$ by (2.14) and (2.15), which is impossible since $V_n \equiv -1 \pmod 7$. Now assume that $P^2 \equiv 1 \pmod 7$. Let $n > 1$ be odd. Then $n = 4q \pm 1$ for some $q > 0$. Thus $n = 2 \cdot 2^k a \pm 1$ with a odd and $k \geq 1$. Therefore,

$$wx^2 = 1 + V_n \equiv 1 - V_{\pm 1} \pmod{V_{2^k}}$$

by (2.2). This shows that

$$wx^2 \equiv -(P-1) \pmod{V_{2^k}},$$

which implies

$$\left(\frac{w}{V_{2^k}}\right) = \left(\frac{-1}{V_{2^k}}\right)\left(\frac{P-1}{V_{2^k}}\right),$$

i.e.,

$$\left(\frac{w}{V_{2^k}}\right) = -1,$$

by (2.4) and (2.8). This is impossible since $\left(\frac{2^{a_1}}{V_{2^k}}\right) = 1$, $\left(\frac{3^{a_2}}{V_{2^k}}\right) = 1$, and $\left(\frac{7}{V_{2^k}}\right) = 1$ by (2.3), (3.2), and (2.11), respectively. Now let $n > 2$ be even. Then $n = 8q \pm 2$ for some $q > 0$ since $n \neq 4q$. Thus $n = 2 \cdot 2^k a \pm 2$ with a odd and $k \geq 2$. Then,

$$wx^2 = 1 + V_n \equiv 1 - V_{\pm 2} \pmod{V_{2^k}}$$

by (2.2). This shows that

$$wx^2 \equiv -(P^2-3) \pmod{V_{2^k}},$$

which implies that

$$\left(\frac{w}{V_{2^k}}\right) = \left(\frac{-1}{V_{2^k}}\right)\left(\frac{P^2-3}{V_{2^k}}\right),$$

i.e.,

$$\left(\frac{w}{V_{2^k}}\right) = -1$$

by (2.9) and (2.4). This is impossible since $\left(\frac{2^{a_1}}{V_{2^k}}\right) = 1$, $\left(\frac{7}{V_{2^k}}\right) = 1$, and $\left(\frac{3^{a_2}}{V_{2^k}}\right) = 1$ by (2.3), (2.11), and (2.7), respectively.

Case 3: Assume that $a_3 \neq 0$ and $a_4 \neq 0$. Then $5|w$ and $7|w$ and so $V_n \equiv -1 \pmod{35}$. Since $V_n \equiv 0, \pm 2 \pmod P$ by Lemma 1, it follows that $5 \nmid P$ and $7 \nmid P$. If $P^2 \equiv 2, 4 \pmod 7$, then $V_n \equiv 0, \pm P, \pm 2 \equiv 0, \pm 2, \pm 3 \pmod 7$ by (2.14) and (2.15), which is impossible since $V_n \equiv -1 \pmod 7$. If $P^2 \equiv -1 \pmod 5$, then $V_n \equiv 2, P \equiv \pm 2 \pmod 5$ by (2.13), which is impossible since $V_n \equiv -1 \pmod 5$. Therefore $P^2 \equiv 1 \pmod 5$ and $P^2 \equiv 1 \pmod 7$. Let n be odd and $n > 1$. Then $n = 4q \pm 1$ for some $q > 0$. Thus $n = 2 \cdot 2^k a \pm 1$ with a odd and $k \geq 1$. Therefore,

$$wx^2 = 1 + V_n \equiv 1 - V_{\pm 1} \pmod{V_{2^k}}$$

by (2.2). This shows that

$$wx^2 \equiv -(P-1)(\text{mod}\, V_{2^k}),$$

which implies

$$\left(\frac{w}{V_{2^k}}\right) = \left(\frac{-1}{V_{2^k}}\right)\left(\frac{P-1}{V_{2^k}}\right).$$

Then we get

$$\left(\frac{w}{V_{2^k}}\right) = -1$$

by (2.4) and (2.8), which is impossible since $\left(\frac{2^{a_1}}{V_{2^k}}\right) = 1$, $\left(\frac{3^{a_2}}{V_{2^k}}\right) = 1$, $\left(\frac{5}{V_{2^k}}\right) = 1$ and $\left(\frac{7}{V_{2^k}}\right) = 1$ by (2.3), (3.2), (2.10), and (2.11), respectively. Now let $n > 2$ be even. Thus $n = 8q \pm 2$ for some $q > 0$. And so $n = 2 \cdot 2^k a \pm 2$ with a odd and $k \geq 2$. Therefore,

$$wx^2 = 1 + V_n \equiv 1 - V_{\pm 2}(\text{mod}\, V_{2^k})$$

by (2.2). This shows that

$$wx^2 \equiv -(P^2-3)(\text{mod}\, V_{2^k}),$$

which implies that

$$\left(\frac{w}{V_{2^k}}\right) = \left(\frac{-1}{V_{2^k}}\right)\left(\frac{P^2-3}{V_{2^k}}\right),$$

i.e.,

$$\left(\frac{w}{V_{2^k}}\right) = -1,$$

by (2.4) and (2.9). This is impossible since $\left(\frac{2^{a_1}}{V_{2^k}}\right) = 1$, $\left(\frac{7}{V_{2^k}}\right) = 1$, $\left(\frac{5}{V_{2^k}}\right) = 1$ and $\left(\frac{3^{a_2}}{V_{2^k}}\right) = 1$ by (2.3), (2.11), (2.10), and (2.7), respectively. Consequently, we have $n = 1$ or $n = 2$. ■

References

[1] M.A. Alekseyev, S. Tengely, On integral points on biquadratic curves and near-multiples of squares in Lucas sequences, J. Integer Seq. 17 (6) (2014) Article 14.6.6.

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

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

[4] O. Karaatlı, R. Keskin, Generalized Lucas numbers of the form $5kx^2$ and $7kx^2$, Bull. Korean Math. Soc. 52 (5) (2015) 1467–1480.

[5] R. Keskin, Generalized Fibonacci and Lucas numbers of the form wx^2 and $wx^2 \pm 1$, Bulletin of the Korean Mathematical Society 51 (2014) 1041–1054.

[6] P. Ribenboim, W.L. McDaniel, The square terms in Lucas sequences, Journal of Number Theory 58 (1996) 104–123.
[7] P. Ribenboim, W.L. McDaniel, On Lucas sequence terms of the form kx^2, in: Number Theory: Proceedings of the Turku Symposium on Number Theory in Memory of Kustaa Inkeri (Turku, 1999), de Gruyter, Berlin, 2001, pp. 293–303.
[8] Z. Şiar, R. Keskin, Some new identities concerning generalized Fibonacci and Lucas numbers, Hacet. J. Math. Stat. 42 (3) (2013) 211–222.