Mathematics

http://www.aimspress.com/journal/Math

AIMS Mathematics, 6(11): 11733–11748.
DOI: 10.3934/math.2021682
Received: 15 April 2021
Accepted: 05 August 2021
Published: 12 August 2021

Research article

Exact divisibility by powers of the integers in the Lucas sequences of the first and second kinds

Kritkhajohn Onphaeng and Prapanpong Pongsriiam*

Department of Mathematics, Faculty of Science, Silpakorn University, Nakhon Pathom, 73000, Thailand

* **Correspondence:** Email: prapanpong@gmail.com, pongsriiam_p@silpakorn.edu.

Abstract: Lucas sequences of the first and second kinds are, respectively, the integer sequences $(U_n)_{n\geq 0}$ and $(V_n)_{n\geq 0}$ depending on parameters $a, b \in \mathbb{Z}$ and defined by the recurrence relations $U_0 = 0$, $U_1 = 1$, and $U_n = aU_{n-1} + bU_{n-2}$ for $n \geq 2$, $V_0 = 2$, $V_1 = a$, and $V_n = aV_{n-1} + bV_{n-2}$ for $n \geq 2$. In this article, we obtain exact divisibility results concerning U_n^k and V_n^k for all positive integers n and k. This and our previous article extend many results in the literature and complete a long investigation on this problem from 1970 to 2021.

Keywords: Lucas sequence; Lucas number; Fibonacci number; exact divisibility; p-adic valuation
Mathematics Subject Classification: 11B39, 11B37, 11A05

1. Introduction

Throughout this article, let a and b be relatively prime integers and let $(U_n)_{n\geq 0}$ and $(V_n)_{n\geq 0}$ be the Lucas sequences of the first and second kinds which are defined by the recurrence relations

$$U_0 = 0,\ U_1 = 1,\ U_n = aU_{n-1} + bU_{n-2} \text{ for } n \geq 2,$$

$$V_0 = 2,\ V_1 = a, \text{ and } V_n = aV_{n-1} + bV_{n-2} \text{ for } n \geq 2.$$

To avoid triviality, we also assume that $b \neq 0$ and α/β is not a root of unity where α and β are the roots of the characteristic polynomial $x^2 - ax - b$. In particular, this implies that $\alpha \neq \beta$, $\alpha \neq -\beta$, the discriminant $D = a^2 + 4b \neq 0$, $U_n \neq 0$, and $V_n \neq 0$ for all $n \geq 1$. If $a = b = 1$, then $(U_n)_{n\geq 0}$ reduces to the sequence of Fibonacci numbers F_n; if $a = 6$ and $b = -1$, then $(U_n)_{n\geq 0}$ becomes the sequence of balancing numbers; if $a = 2$ and $b = 1$, then $(U_n)_{n\geq 0}$ is the sequence of Pell numbers; and many other famous integer sequences are just special cases of the Lucas sequences of the first and second kinds.

The divisibility by powers of the Fibonacci numbers has attracted some attentions because it is used in Matijasevich's solution to Hilbert's 10th problem [5–7]. More precisely, Matijasevich show that

$$F_n^2 \mid F_{nm} \quad \text{if and only if} \quad F_n \mid m. \tag{1.1}$$

From that point, Hoggatt and Bicknell-Johnson [4], Benjamin and Rouse [1], Seibert and Trojovský [19], Pongsriiam [15], Onphaeng and Pongsriiam [9, 10], Panraksa and Tangboonduangjit [11], and Patra, Panda, and Khemaratchatakumthorn [12] have made some contributions on the extensions of (1.1). For more details about the timeline and the development of this problem, we refer the reader to the introduction of our previous article [8]. In fact, the most general results in this direction has recently been given by us [8] as follows.

Theorem 1. [8, Theorem 10] *Let $k, m, n \in \mathbb{N}$, $a, b \in \mathbb{Z}$, $(a, b) = 1$, $n \geq 2$, and $U_n^k \parallel m$. Then*

(i) *if a is odd and b is even, then $U_n^{k+1} \parallel U_{nm}$;*
(ii) *if a is even and b is odd, then $U_n^{k+1} \parallel U_{nm}$;*
(iii) *if a and b are odd and $n \not\equiv 3 \pmod 6$, then $U_n^{k+1} \parallel U_{nm}$;*
(iv) *if a and b are odd, $n \equiv 3 \pmod 6$, and $\frac{U_n^{k+1}}{2} \nmid m$, then $U_n^{k+1} \parallel U_{nm}$;*
(v) *if a and b are odd, $n \equiv 3 \pmod 6$, $\frac{U_n^{k+1}}{2} \mid m$, and $2 \parallel a^2 + 3b$, then $U_n^{k+1} \parallel U_{nm}$;*
(vi) *if a and b are odd, $n \equiv 3 \pmod 6$, $\frac{U_n^{k+1}}{2} \mid m$, and $4 \mid a^2 + 3b$, then $U_n^{k+t+1} \parallel U_{nm}$, where*

$$t = \min(\{v_2(U_6) - 2\} \cup \{y_p - k \mid p \text{ is an odd prime factor of } U_n\}) \text{ and}$$
$$y_p = \left\lfloor \frac{v_p(m)}{v_p(U_n)} \right\rfloor \text{ for each odd prime } p \text{ dividing } U_n.$$

Theorem 2. [8, Theorem 12] *Let $k, m, n \in \mathbb{N}$, $a, b \in \mathbb{Z}$, $(a, b) = 1$, $n \geq 2$, and $U_n^{k+1} \parallel U_{nm}$. Then*

(i) *if a is odd and b is even, then $U_n^k \parallel m$;*
(ii) *if a is even and b is odd, then $U_n^k \parallel m$;*
(iii) *if a and b are odd and $n \not\equiv 3 \pmod 6$, then $U_n^k \parallel m$;*
(iv) *if a and b are odd, $n \equiv 3 \pmod 6$, and $2 \parallel a^2 + 3b$, then $U_n^k \parallel m$;*
(v) *if a and b are odd, $n \equiv 3 \pmod 6$, $4 \mid a^2 + 3b$, and $v_2(m) \geq k$, then $U_n^k \parallel m$;*
(vi) *if a and b are odd, $n \equiv 3 \pmod 6$, $4 \mid a^2 + 3b$, and $v_2(m) < k$, then*

$$m \text{ is even}, \ v_2(m) \geq k + 1 - v_2(a^2 + 3b), \text{ and } U_n^{v_2(m)} \parallel m.$$

For other related and recent results on Fibonacci, Lucas, balancing, and Lucas-balancing numbers, see for example in [3, 13, 14, 16, 17, 20] and references there in.

In this article, we extend Theorems 1 and 2 to the case of V_n and the mix of U_n and V_n. For example, we obtain in Theorem 18 that if a and m are even, b is odd, and $V_n^{k+1} \parallel U_{nm}$, then $2 \mid n$ implies $V_n^{\min(k, v_2(m))} \parallel m$; while $2 \nmid n$ implies $V_n^k \mid m$ and the exponent k can be replaced by $k + 1$ if and only if $\frac{V_n^{k+2}}{2} \mid U_{nm}$.

2. Preliminaries and lemmas

In this section, we recall some definition and well known results, and give some useful lemmas for the reader's convenience. The order (or the rank) of appearance of $n \in \mathbb{N}$ in the Lucas sequence

$(U_n)_{n\geq 0}$ is defined as the smallest positive integer m such that $n \mid U_m$ and is denoted by $\tau(n)$. The exact divisibility $m^k \parallel n$ means that $m^k \mid n$ and $m^{k+1} \nmid n$. The letter p is always a prime. For $n \in \mathbb{N}$, the p-adic valuation of n, denoted by $v_p(n)$ is the power of p in the prime factorization of n. We sometimes write the expression such as $a \mid b \mid c = d$ to mean that $a \mid b$, $b \mid c$, and $c = d$. For each $x \in \mathbb{R}$, we write $\lfloor x \rfloor$ to denote the largest integer less than or equal to x. So $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$. We let $D = a^2 + 4b$ be the discriminant and let α and β be the roots of the characteristic polynomial $x^2 - ax - b$. Then it is well known that if $D \neq 0$, then the Binet formula

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \text{ and } V_n = \alpha^n + \beta^n \text{ holds for all } n \geq 0.$$

Next, we recall Sanna's result [18] on the p-adic valuation of the Lucas sequence of the first kind.

Lemma 3. [18, Theorem 1.5] *Let p be a prime number such that $p \nmid b$. Then, for each positive integer n,*

$$v_p(U_n) = \begin{cases} v_p(n) + v_p(U_p) - 1 & \text{if } p \mid D \text{ and } p \mid n, \\ 0 & \text{if } p \mid D \text{ and } p \nmid n, \\ v_p(n) + v_p(U_{p\tau(p)}) - 1 & \text{if } p \nmid D,\ \tau(p) \mid n, \text{ and } p \mid n, \\ v_p(U_{\tau(p)}) & \text{if } p \nmid D,\ \tau(p) \mid n, \text{ and } p \nmid n, \\ 0 & \text{if } p \nmid D \text{ and } \tau(p) \nmid n. \end{cases}$$

In particular, if p is an odd prime such that $p \nmid b$, then, for each positive integer n,

$$v_p(U_n) = \begin{cases} v_p(n) + v_p(U_p) - 1 & \text{if } p \mid D \text{ and } p \mid n, \\ 0 & \text{if } p \mid D \text{ and } p \nmid n, \\ v_p(n) + v_p(U_{\tau(p)}) & \text{if } p \nmid D \text{ and } \tau(p) \mid n, \\ 0 & \text{if } p \nmid D \text{ and } \tau(p) \nmid n. \end{cases}$$

From Lemma 3, and the fact that $V_n = U_{2n}/U_n$, we easily obtain the following result.

Lemma 4. *If p is an odd prime and $p \nmid b$. Then, for each positive integer n,*

$$v_p(V_n) = \begin{cases} v_p(n) + v_p(U_{\tau(p)}) & \text{if } p \nmid D,\ \tau(p) \nmid n \text{ and } \tau(p) \mid 2n, \\ 0 & \text{otherwise}. \end{cases}$$

Proof. This follows from the application of Lemma 3, a straightforward calculation, and the fact that $v_p(V_n) = v_p\left(\frac{U_{2n}}{U_n}\right) = v_p(U_{2n}) - v_p(U_n)$. □

Next, we give some old and new lemmas that are needed in the proof of main theorems.

Lemma 5. *Let $n \geq 1$ and $(a, b) = 1$. If $p \mid U_n$ or $p \mid V_n$, then $p \nmid b$. Consequently, $(U_n, b) = (V_n, b) = 1$ for all $n \geq 1$.*

Proof. The case for U_n is already given in [8, Lemma 7]. So suppose by way of contradiction that $p \mid V_n$ and $p \mid b$. Since $V_n = aV_{n-1} + bV_{n-2}$ and $(a, b) = 1$, we obtain $p \mid V_{n-1}$. Repeating this argument, we see that $p \mid V_m$ for $1 \leq m \leq n$. In particular, $p \mid V_1 = a$ contradicting $(a, b) = 1$. So if $p \mid V_n$, then $p \nmid b$, and the proof is complete. □

Lemma 6. [8, Lemma 8] *Let a and b be odd,* $(a, b) = 1$*, and* $v_2(U_6) \geq v_2(U_3) + 2$*. Then* $v_2(U_3) = 1$.

For convenience, we also calculate the 2-adic valuation of U_n and V_n as follows.

Lemma 7. *Assume that a is odd, b is even, and* $n \geq 1$*. Then* $v_2(U_n) = v_2(V_n) = 0$.

Proof. Since $U_1 = 1$ and $U_2 = a$ are odd, and $U_r = aU_{r-1} + bU_{r-2} \equiv U_{r-1} \pmod 2$ for $r \geq 3$, it follows by induction that U_n is odd. Since $V_n = \frac{U_{2n}}{U_n}$, V_n is also odd. This proves this lemma. □

Lemma 8. *Assume that a is even, b is odd, and* $n \geq 1$*. Then*

$$v_2(U_n) = \begin{cases} v_2(n) + v_2(a) - 1 & \text{if } 2 \mid n, \\ 0 & \text{if } 2 \nmid n, \end{cases}$$

$$v_2(V_n) = \begin{cases} 1 & \text{if } 2 \mid n, \\ v_2(a) & \text{if } 2 \nmid n, \end{cases}$$

Proof. Since $2 \mid D$, we obtain by Lemma 3 that for each $n \in \mathbb{N}$, $v_2(U_n) = v_2(n) + v_2(U_2) - 1$ if $2 \mid n$ and $v_2(U_n) = 0$ if $2 \nmid n$. Since $U_2 = a$, the formula for $v_2(U_n)$ is verified. Then $v_2(V_n)$ can be obtained from a straightforward calculation and the fact that $V_n = \frac{U_{2n}}{U_n}$. This completes the proof. □

Lemma 9. *Assume that a and b are odd, and* $n \geq 1$*. Then*

$$v_2(U_n) = \begin{cases} v_2(n) + v_2(U_6) - 1 & \text{if } n \equiv 0 \pmod 6, \\ v_2(U_3) & \text{if } n \equiv 3 \pmod 6, \\ 0 & \text{if } n \not\equiv 0 \pmod 3, \end{cases}$$

$$v_2(V_n) = \begin{cases} 1 & \text{if } n \equiv 0 \pmod 6, \\ v_2(U_6) - v_2(U_3) & \text{if } n \equiv 3 \pmod 6, \\ 0 & \text{if } n \not\equiv 0 \pmod 3, \end{cases}$$

Proof. Since U_1 and U_2 are odd, and $U_3 = a^2 + b$ is even, we have $\tau(2) = 3$. In addition, $2 \nmid D$. Furthermore, $3 \mid n$ and $2 \mid n$ if and only if $n \equiv 0 \pmod 6$; $3 \mid n$ and $2 \nmid n$ if and only if $n \equiv 3 \pmod 6$. Then applying Lemma 3 and the fact that $V_n = \frac{U_{2n}}{U_n}$, we obtain the desired result. □

3. Main results

We begin with the simplest theorem of this paper.

Theorem 10. *Assume that* $k, m, n \in \mathbb{N}$*,* $a, b \in \mathbb{Z}$*,* $(a, b) = 1$*, and m is odd. Then*

(i) *if* $V_n^k \mid m$*, then* $V_n^{k+1} \mid V_{nm}$*;*
(ii) *if* $V_n^k \parallel m$*, then* $V_n^{k+1} \parallel V_{nm}$*;*
(iii) *if* $V_n^k \mid V_{nm}$*, then* $V_n^{k-1} \mid m$*;*
(iv) *if* $V_n^k \parallel V_{nm}$*, then* $V_n^{k-1} \parallel m$.

Proof. We use Lemma 5 without reference. For (i), assume that $V_n^k \mid m$. Since m is odd, V_n is also odd, and so $v_2(V_n^{k+1}) = 0$. If $p > 2$ and $p \mid V_n$, then $p \nmid b$ and we obtain by Lemma 4 that

$$\begin{aligned} v_p(V_{nm}) &= v_p(mn) + v_p(U_{\tau(p)}) \\ &= v_p(m) + v_p(n) + v_p(U_{\tau(p)}) \\ &\geq v_p(V_n^k) + v_p(V_n) = v_p(V_n^{k+1}). \end{aligned}$$

Therefore $v_p(V_{nm}) \geq v_p(V_n^{k+1})$ for all primes p dividing V_n. This implies $V_n^{k+1} \mid V_{nm}$.

For (ii), assume that $V_n^k \parallel m$. By (i), it is enough to show that $V_n^{k+2} \nmid V_{nm}$. Since $V_n^{k+1} \nmid m$, there exists a prime p dividing V_n such that $v_p(V_n^{k+1}) > v_p(m)$. Here we remark that the letter p in the proof of (i) and in the proof of (ii) may be different or may be the same. We believe that there is no ambiguity since (i) is already done. Now since $V_n^k \mid m$ and m is odd, V_n is also odd, and so $v_2(V_n^{k+1}) = v_2(m) = 0$. Therefore p is odd. By Lemma 4, we obtain

$$\begin{aligned} v_p(V_{nm}) = v_p(nm) + v_p(U_{\tau(p)}) &= v_p(m) + v_p(n) + v_p(U_{\tau(p)}) \\ &= v_p(m) + v_p(V_n) < v_p(V_n^{k+1}) + v_p(V_n) = v_p(V_n^{k+2}). \end{aligned}$$

This shows that $V_n^{k+2} \nmid V_{nm}$, as required.

For (iii), assume that $V_n^k \mid V_{nm}$. We show that $v_p(V_n^{k-1}) \leq v_p(m)$ for all primes p dividing V_n. If p is odd and $p \mid V_n$, then we apply Lemma 4 to obtain that

$$\begin{aligned} v_p(V_n) + v_p(V_n^{k-1}) = v_p(V_n^k) \leq v_p(V_{nm}) &= v_p(nm) + v_p(U_{\tau(p)}) \\ &= v_p(m) + v_p(n) + v_p(U_{\tau(p)}) \\ &= v_p(m) + v_p(V_n), \end{aligned}$$

and so $v_p(V_n^{k-1}) \leq v_p(m)$. It remains to show that $v_2(V_n^{k-1}) \leq v_2(m)$. If a is odd and b is even, then it follows from Lemma 7 that $v_2(V_n^{k-1}) = 0 \leq v_2(m)$. Recall that $(a, b) = 1$, so a and b cannot be both even. So we have the following two remaining cases: (a is even and b is odd) or (a and b are odd).

Case 1 a is even and b is odd. We will show that k must be 1, and so $v_2(V_n^{k-1}) = 0 \leq v_2(m)$. If $2 \mid n$, then we apply Lemma 8 and the assumption that $V_n^k \mid V_{nm}$ to obtain

$$1 \leq k = v_2(V_n^k) \leq v_2(V_{nm}) = 1.$$

Similarly, if $2 \nmid n$, then $2 \nmid nm$ and we can use Lemma 8 again to obtain

$$kv_2(a) = v_2(V_n^k) \leq v_2(V_{nm}) = v_2(a).$$

In any case, $k = 1$, as asserted.

Case 2 a and b are odd. We use Lemma 9 in this case. If $n \not\equiv 0 \pmod 3$, then $v_2(V_n^{k-1}) = 0 \leq v_2(m)$. If $n \equiv 0 \pmod 6$, then $nm \equiv 0 \pmod 6$, and so $k = v_2(V_n^k) \leq v_2(V_{nm}) = 1$; thus $v_2(V_n^{k-1}) = 0 \leq v_2(m)$. We now suppose $n \equiv 3 \pmod 6$. Since m is odd, $nm \equiv 3 \pmod 6$. Therefore

$$k(v_2(U_6) - v_2(U_3)) = v_2(V_n^k) \leq v_2(V_{nm}) = v_2(U_6) - v_2(U_3).$$

So $k = 1$ and thus $v_2(V_n^{k-1}) = 0 \leq v_2(m)$. Hence $v_p(V_n^{k-1}) \leq v_p(m)$ for all primes p dividing V_n, as desired. This proves (iii).

For (iv), assume that $V_n^k \parallel V_{nm}$. By (iii), we have $V_n^{k-1} \mid m$. If $V_n^k \mid m$, then we obtain by (i) that $V_n^{k+1} \mid V_{nm}$ which contradicts $V_n^k \parallel V_{nm}$. Therefore $V_n^{k-1} \parallel m$. This completes the proof. □

Remark 11. Let $k, m, n \in \mathbb{N}$, $a, b \in \mathbb{Z}$, $(a, b) = 1$, and m is even. Let p be an odd prime dividing V_n. By Lemma 4, we have $p \nmid D$, $\tau(p) \nmid n$ and $\tau(p) \mid 2n$. Since m is even and $\tau(p) \mid 2n$, we obtain $\tau(p) \mid mn$. By Lemma 4, we have $p \nmid V_{nm}$, and so $V_n \nmid V_{nm}$. This shows that m in Theorem 10 cannot be even unless $V_n = 2^r$ for some $r \in \mathbb{N}$.

Remark 12. The argument in Remark 11 works provided that there exists an odd prime p dividing V_n. The case $V_n = 2^k$ for some $k \in \mathbb{N} \cup \{0\}$ may occur but it is very rare. For example, when $a = b = 1$, we know from the result of Bugeaud, Mignotte, and Siksek [2] that V_n is 1 or is a power of 2 if and only if $n = 0, 1, 3$. Therefore we do not consider this rare case in our theorems.

Lemma 13. *Let $k, m, n \in \mathbb{N}$, $a, b \in \mathbb{Z}$, and $(a, b) = 1$. Suppose m is odd and there exists an odd prime p dividing V_n. Then $v_p(U_{nm}) = 0$ and $V_n \nmid U_{nm}$.*

Proof. By Lemma 4, we have $p \nmid D$, $\tau(p) \nmid n$ and $\tau(p) \mid 2n$. Therefore $\tau(p)$ is even and $v_2(\tau(p)) = v_2(n) + 1$. So $\tau(p) \nmid nm$. By Lemma 3, $v_p(U_{nm}) = 0$. Therefore $V_n \nmid U_{nm}$. □

Lemma 14. *Let $k, m, n \in \mathbb{N}$, $a, b \in \mathbb{Z}$, and $(a, b) = 1$. Suppose there exists an odd prime $p \mid U_n$. Then $v_p(V_{nm}) = 0$ and $U_n \nmid V_{nm}$.*

Proof. By Lemma 3, we have (i) $v_p(U_n) = v_p(n) + v_p(U_p) - 1$ if $p \mid D$ and $p \mid n$, and (ii) $v_p(U_n) = v_p(n) + v_p(U_{\tau(p)})$ if $p \nmid D$ and $\tau(p) \mid n$. For (i), we have $v_p(U_n) > 0$ and $p \mid D$, and therefore $v_p(V_{nm}) = 0$ and $U_n \nmid V_{nm}$. For (ii), we have $\tau(p) \mid nm$ and so $v_p(V_{nm}) = 0$ and $U_n \nmid V_{nm}$. □

Remark 15. By Lemma 13 and a reason similar to that in Remark 12, we do not consider the case where m is odd in Theorems 16 to 20. In addition, by Lemma 14, we do not study the divisibility relation such as $U_n^k \mid V_{nm}$.

We now have the exact divisibility results for U_n and V_n separately. In the next theorem, we consider them together. In other words, we investigate the relations of the type $V_n^c \mid m$ implies $V_n^d \mid U_{nm}$; and $V_n^c \parallel U_{nm}$ implies $V_n^d \parallel m$. We divide the results into 5 theorems according to the parities of a and b. From this point on, we apply Lemma 5 without reference.

Theorem 16. *Suppose that $k, m, n \in \mathbb{N}$, $a, b \in \mathbb{Z}$, $(a, b) = 1$, a is odd, b is even, and m is even. Then*

(i) *if $V_n^k \mid m$, then $V_n^{k+1} \mid U_{nm}$;*
(ii) *if $V_n^k \parallel m$, then $V_n^{k+1} \parallel U_{nm}$;*
(iii) *if $V_n^{k+1} \mid U_{nm}$, then $V_n^k \mid m$;*
(iv) *if $V_n^{k+1} \parallel U_{nm}$, then $V_n^k \parallel m$.*

Proof. For (i), assume that $V_n^k \mid m$. We show that $v_p(V_n^{k+1}) \leq v_p(U_{nm})$ for all primes p dividing V_n. By Lemma 7, we have $v_2(V_n) = 0$. So let p be an odd prime dividing V_n. By Lemma 4, $p \nmid D$, $\tau(p) \nmid n$, and $\tau(p) \mid 2n$. Then $\tau(p) \mid nm$. By Lemmas 3 and 4, we obtain

$$v_p(U_{nm}) = v_p(nm) + v_p(U_{\tau(p)}) = v_p(m) + v_p(n) + v_p(U_{\tau(p)}) \geq v_p(V_n^k) + v_p(n) + v_p(U_{\tau(p)})$$
$$= v_p(V_n^k) + v_p(V_n) = v_p(V_n^{k+1}), \text{ as required.}$$

For (ii), assume that $V_n^k \parallel m$. By (i), it is enough to show that $V_n^{k+2} \nmid U_{nm}$. Since $V_n^{k+1} \nmid m$, there exists a prime p such that $v_p(V_n^{k+1}) > v_p(m)$. By Lemma 7, $v_2(V_n^{k+1}) = 0$, and so $p \neq 2$. Since $p \mid V_n$, we know that $p \nmid D$ and $\tau(p) \mid nm$. Therefore we obtain by Lemmas 3 and 4 that

$$v_p(U_{nm}) = v_p(nm) + v_p(U_{\tau(p)}) = v_p(m) + v_p(n) + v_p(U_{\tau(p)}) = v_p(m) + v_p(V_n)$$

$$< v_p(V_n^{k+1}) + v_p(V_n) = v_p(V_n^{k+2}), \text{ as desired.}$$

For (iii), assume that $V_n^{k+1} \mid U_{nm}$. By Lemma 7, $v_2(m) \geq 0 = v_2(V_n^k)$. If p is odd and $p \mid V_n$, then we apply Lemmas 3 and 4 again to obtain

$$\begin{aligned} v_p(V_n) + v_p(V_n^k) = v_p(V_n^{k+1}) \leq v_p(U_{nm}) &= v_p(nm) + v_p(U_{\tau(p)}) \\ &= v_p(m) + v_p(n) + v_p(U_{\tau(p)}) \\ &= v_p(m) + v_p(V_n). \end{aligned}$$

This shows that $v_p(V_n^k) \leq v_p(m)$ for every prime p dividing V_n. So $V_n^k \mid m$.

For (iv), suppose $V_n^{k+1} \parallel U_{nm}$. By (iii), it is enough to show that $V_n^{k+1} \nmid m$. If $V_n^{k+1} \mid m$, we apply (i) to obtain $V_n^{k+2} \mid U_{nm}$ contradicting $V_n^{k+1} \parallel U_{nm}$. Therefore the proof is complete. □

Theorem 17. *Assume that $k, m, n \in \mathbb{N}$, $a, b \in \mathbb{Z}$, $(a, b) = 1$, a is even, b is odd and m is even. Let*

$$t = \min(\{v_2(n) + v_2(a) - 2\} \cup \{y_p - k \mid p \text{ is an odd prime factor of } V_n\}) \text{ and}$$
$$y_p = \left\lfloor \frac{v_p(m)}{v_p(V_n)} \right\rfloor \text{ for each odd prime } p \text{ dividing } V_n.$$

Then

(i) *if $V_n^k \mid m$ and $2 \mid n$, then $V_n^{k+1} \mid U_{nm}$;*
if $V_n^k \mid m$ and $2 \nmid n$, then $\frac{V_n^{k+1}}{2} \mid U_{nm}$;
if $V_n^k \mid m$, $2 \nmid n$, and $v_2(m) \geq v_2(V_n^k) + 1$, then $V_n^{k+1} \mid U_{nm}$;
if $V_n^k \mid m$, $2 \mid n$, and $\frac{V_n^{k+1}}{2} \mid m$, then $t \geq 0$, $v_2(m) \geq k$, and $V_n^{k+t+1} \mid U_{nm}$;

(ii) *if $V_n^k \parallel m$, $2 \mid n$ and $\frac{V_n^{k+1}}{2} \nmid m$, then $V_n^{k+1} \parallel U_{nm}$;*

(iii) *if $V_n^k \parallel m$, $2 \mid n$ and $\frac{V_n^{k+1}}{2} \mid m$, then $V_n^{k+t+1} \parallel U_{nm}$;*

(iv) *if $V_n^k \parallel m$, $2 \nmid n$ and $v_2(m) = v_2(V_n^k)$, then $V_n^k \parallel U_{nm}$;*

(v) *if $V_n^k \parallel m$, $2 \nmid n$ and $v_2(m) \geq v_2(V_n^k) + 1$, then $V_n^{k+1} \parallel U_{nm}$.*

Proof. For (i), assume that $V_n^k \mid m$. If p is an odd prime and $p \mid V_n$, then $p \nmid D$, $\tau(p) \mid nm$, and we can apply Lemmas 3 and 4, to obtain

$$\begin{aligned} v_p(U_{nm}) &= v_p(nm) + v_p(U_{\tau(p)}) \\ &= v_p(m) + v_p(n) + v_p(U_{\tau(p)}) \\ &\geq v_p(V_n^k) + v_p(V_n) = v_p(V^{k+1}). \end{aligned}$$

From this point on, we sometimes use Lemmas 3 and 4 without reference. Next, we consider $v_2(V_n^{k+1})$ and $v_2(U_{nm})$. If $2 \mid n$, then we apply Lemma 8 to obtain

$$\begin{aligned} v_2(U_{nm}) = v_2(nm) + v_2(a) - 1 &= v_2(m) + v_2(n) + v_2(a) - 1 \\ &\geq v_2(V_n^k) + v_2(n) + v_2(a) - 1 \\ &\geq v_2(V_n^k) + 1 = v_2(V_n^k) + v_2(V_n) = v_2(V_n^{k+1}). \end{aligned}$$

This implies the first part of (i). Since m is even, $2 \mid nm$. So if $2 \nmid n$, then we can still apply Lemma 8 to obtain

$$\begin{aligned} v_2(U_{nm}) &= v_2(nm) + v_2(a) - 1 \\ &= v_2(m) + v_2(a) - 1 \\ &\geq v_2(V_n^k) + v_2(a) - 1 = v_2(V_n^k) + v_2(V_n) - 1 = v_2\left(\frac{V_n^{k+1}}{2}\right). \end{aligned} \tag{3.1}$$

This implies the second part of (i). For the third part of (i), we assume that $2 \nmid n$ and $v_2(m) \geq v_2(V_n^k) + 1$, and then we repeat the argument used in the second part to obtain

$$v_2(U_{nm}) = v_2(m) + v_2(a) - 1 \geq v_2(V_n^k) + v_2(a) = v_2(V_n^{k+1}).$$

Therefore $v_p(U_{nm}) \geq v_p(V_n^{k+1})$ for all primes p, which implies the desired result. Next, we prove the last part of (i). Assume that $V_n^k \mid m$, $2 \mid n$, and $\frac{V_n^{k+1}}{2} \mid m$. Since a and n are even, $v_2(n) + v_2(a) - 2 \geq 0$. In addition, $v_p(m) \geq v_p(V_n^k) = kv_p(V_n)$, and so $y_p \geq k$. Therefore $t \geq 0$ and $t + 1 \leq v_2(n) + v_2(a) - 1$. By Lemma 8, we have $v_p(V_n) = 1$, and therefore $v_p(m) \geq k$ and

$$v_2(U_{nm}) = v_2(nm) + v_2(a) - 1 = v_2(m) + v_2(n) + v_2(a) - 1 \geq k + t + 1 = v_2(V_n^{k+t+1}).$$

If p is an odd prime and $p \mid V_n$, then

$$\begin{aligned} v_p(U_{nm}) &= v_p(m) + v_p(n) + v_p(U_{\tau(p)}) = v_p(m) + v_p(V_n) \geq y_p v_p(V_n) + v_p(V_n) \\ &= (y_p + 1)v_p(V_n) \geq (k + t + 1)v_p(V_n) = v_p(V_n^{k+t+1}). \end{aligned}$$

Hence $v_p(U_{nm}) \geq v_p(V_n^{k+t+1})$ for all primes p dividing V_n. Thus $V_n^{k+t+1} \mid U_{nm}$, as desired.

Next, we prove (ii). Assume that $V_n^k \parallel m$, $2 \mid n$ and $\frac{V_n^{k+1}}{2} \nmid m$. By (i), it is enough to show that $V_n^{k+2} \nmid U_{nm}$. By Lemma 8, we know that $v_2(V_n) = 1$. Then $v_2(m) \geq v_2(V_n^k) = v_2\left(\frac{V_n^{k+1}}{2}\right)$. Since $\frac{V_n^{k+1}}{2} \nmid m$, there exists an odd prime p dividing V_n such that $v_p(V_n^{k+1}) > v_p(m)$. Then $p \nmid D$, $\tau(p) \mid nm$, and

$$\begin{aligned} v_p(V_n^{k+2}) = v_p(V_n^{k+1}) + v_p(V_n) &> v_p(m) + v_p(V_n) \\ &= v_p(m) + v_p(n) + v_p(U_{\tau(p)}) \\ &= v_p(U_{nm}). \end{aligned}$$

This implies $V_n^{k+2} \nmid U_{nm}$.

For (iii), assume that $V_n^k \parallel m$, $2 \mid n$, and $\frac{V_n^{k+1}}{2} \mid m$. By (i), we obtain $t \geq 0$, $v_2(m) \geq k$, and $V_n^{k+t+1} \mid U_{nm}$. So it remains to show that $V_n^{k+t+2} \nmid U_{nm}$. We first observe that since $\frac{V_n^{k+1}}{2} \mid m$, we obtain $v_p(V_n^{k+1}) \leq v_p(m)$ for every odd prime p. If $v_2(m) \geq k + 1$, then $v_2(m) \geq v_2(V_n^{k+1})$ which implies $V_n^{k+1} \mid m$ contradicting the assumption $V_n^k \parallel m$. Therefore $v_2(m) = k$. Next, we show that $V_n^{k+t+2} \nmid U_{nm}$. If $t = y_p - k$ for some odd prime p dividing V_n, then we apply Lemmas 3 and 4 to obtain

$$\begin{aligned} v_p(U_{nm}) &= v_p(nm) + v_p(U_{\tau(p)}) \\ &= v_p(m) + v_p(V_n) = \left(\frac{v_p(m)}{v_p(V_n)} + 1\right) v_p(V_n) \end{aligned}$$

$$< (y_p + 2)v_p(V_n) = (k + t + 2)v_p(V_n) = v_p(V_n^{k+t+2}),$$

and so $V_n^{k+t+2} \nmid U_{nm}$. If $t = v_2(n) + v_2(a) - 2$, then we obtain by Lemma 8 that

$$v_2(U_{nm}) = v_2(nm) + v_2(a) - 1 = v_2(m) + v_2(n) + v_2(a) - 1 = k + t + 1 < v_2(V_n^{k+t+2}),$$

and so $V_n^{k+t+2} \nmid U_{nm}$. This proves (iii).

Next, we prove (iv). Assume that $V_n^k \parallel m$, $2 \nmid n$ and $v_2(m) = v_2(V_n^k)$. By (i), we have $\frac{V_n^{k+1}}{2} \mid U_{nm}$. To show that $V_n^k \mid U_{nm}$, it suffices to prove that $v_2(V_n^k) \leq v_2(U_{nm})$. Recall from (3.1) in the proof of the second part of (i) that

$$v_2(U_{nm}) = v_2(m) + v_2(a) - 1 = v_2(V_n^k) + v_2(a) - 1 \geq v_2(V_n^k),$$

and

$$v_2(U_{nm}) = v_2(m) + v_2(a) - 1 = v_2(V_n^k) + v_2(V_n) - 1 < v_2(V_n^{k+1}).$$

So $V_n^k \mid U_{nm}$ and $V_n^{k+1} \nmid U_{nm}$. Thus $V_n^k \parallel U_{nm}$.

For (v), assume that $V_n^k \parallel m$, $2 \nmid n$, and $v_2(m) \geq v_2(V_n^k) + 1$. By (i), it suffices to show that $V_n^{k+2} \nmid U_{nm}$. Since $V_n^{k+1} \nmid m$, there exists a prime p dividing V_n such that $v_p(V_n^{k+1}) > v_p(m)$. If $p = 2$, then we obtain by Lemma 8 that

$$v_2(U_{nm}) = v_2(m) + v_2(a) - 1 < v_2(V_n^{k+1}) + v_2(V_n) - 1 < v_2(V_n^{k+2}),$$

and so $V_n^{k+2} \nmid U_{nm}$. If $p > 2$, then we obtain

$$v_p(U_{nm}) = v_p(nm) + v_p(U_{\tau(p)}) = v_p(m) + v_p(V_n) < v_p(V_n^{k+1}) + v_p(V_n) = v_p(V_n^{k+2}),$$

which implies $V_n^{k+2} \nmid U_{nm}$. This completes the proof. □

From this point on, we apply Lemmas 3, 4, 5, and 8 without reference.

Theorem 18. *Suppose that $k, m, n \in \mathbb{N}$, $a, b \in \mathbb{Z}$, $(a, b) = 1$, a is even, b is odd, and m is even. Then*

(i) *for all odd primes p, if $v_p(V_n^{k+1}) \leq v_p(U_{nm})$, then $v_p(V_n^k) \leq v_p(m)$;*
(ii) *if $V_n^{k+1} \mid U_{nm}$ and $2 \mid n$, then $V_n^{\min(k, v_2(m))} \mid m$;*
if $V_n^{k+1} \parallel U_{nm}$ and $2 \mid n$, then $V_n^{\min(k, v_2(m))} \parallel m$;
(iii) *if $V_n^{k+1} \mid U_{nm}$ and $2 \nmid n$, then $V_n^k \mid m$;*
(iv) *if $V_n^{k+1} \parallel U_{nm}$, $2 \nmid n$ and $\frac{V_n^{k+2}}{2} \nmid U_{nm}$, then $V_n^k \parallel m$;*
(v) *if $V_n^{k+1} \parallel U_{nm}$, $2 \nmid n$, and $\frac{V_n^{k+2}}{2} \mid U_{nm}$, then $V_n^{k+1} \parallel m$.*

Proof. For (i), assume that p is an odd prime and $v_p(V_n^{k+1}) \leq v_p(U_{nm})$. If $p \mid V_n$, then

$$\begin{aligned} v_p(V_n) + v_p(V_n^k) = v_p(V_n^{k+1}) \leq v_p(U_{nm}) &= v_p(nm) + v_p(U_{\tau(p)}) \\ &= v_p(m) + v_p(n) + v_p(U_{\tau(p)}) \\ &= v_p(m) + v_p(V_n), \end{aligned}$$

which implies (i). By (i), we only need to consider the 2-adic valuation in the proofs of (ii), (iii), (iv), and (v).

For (ii), assume that $V_n^{k+1} \mid U_{nm}$ and $2 \mid n$. For convenience, let $c = \min(k, v_2(m))$. If $v_2(m) \geq k$, then $v_2(V_n^k) = k \leq v_2(m)$, and so $V_n^k \mid m$. If $v_2(m) < k$, then $v_2(V_n^{v_2(m)}) = v_2(m)$ and $v_p(V_n^{v_2(m)}) \leq v_p(V_n^k) \leq v_p(m)$ for all odd primes p, and therefore $V_n^{v_2(m)} \mid m$. In any case, we obtain $V_n^c \mid m$. This proves the first part of (ii). Suppose further that $V_n^{k+1} \parallel U_{nm}$ but $V_n^{c+1} \mid m$. Then

$$v_2(m) \geq v_2(V_n^{c+1}) = \min(k, v_2(m)) + 1,$$

which implies $c = k$. Then $V_n^{k+1} = V_n^{c+1} \mid m$. By (i) of Theorem 17, we obtain $V_n^{k+2} \mid U_{nm}$ contradicting $V_n^{k+1} \parallel U_{nm}$. This completes the proof of (ii).

For (iii), assume that $V_n^{k+1} \mid U_{nm}$ and $2 \nmid n$. Then

$$v_2(a) + v_2(V_n^k) = v_2(V_n^{k+1}) \leq v_2(U_{nm}) = v_2(nm) + v_2(a) - 1 = v_2(m) + v_2(a) - 1.$$

Therefore $v_2(V_n^k) < v_2(m)$, and so $V_n^k \mid m$.

For (iv), assume that $V_n^{k+1} \parallel U_{nm}$, $2 \nmid n$, and $\frac{V_n^{k+2}}{2} \nmid U_{nm}$. By (iii), $V_n^k \mid m$. If $V_n^{k+1} \mid m$, then we obtain from (i) of Theorem 17 that $\frac{V_n^{k+2}}{2} \mid U_{nm}$, a contradiction. So $V_n^k \parallel m$.

For (v), assume that $V_n^{k+1} \parallel U_{nm}$, $2 \nmid n$, and $\frac{V_n^{k+2}}{2} \mid U_{nm}$. Then

$$v_2(V_n^{k+1}) + v_2(a) - 1 = v_2(V_n^{k+2}) - 1 \leq v_2(U_{nm}) = v_2(nm) + v_2(a) - 1 = v_2(m) + v_2(a) - 1,$$

and so $v_2(V_n^{k+1}) \leq v_2(m)$. Therefore $V_n^{k+1} \mid m$. If $V_n^{k+2} \mid m$, we obtain from (i) of Theorem 17 that $\frac{V_n^{k+3}}{2} \mid U_{nm}$, which implies $V_n^{k+2} \mid U_{nm}$ contradicting $V_n^{k+1} \parallel U_{nm}$. Therefore $V_n^{k+1} \parallel m$ and the proof is complete. □

Theorem 19. *Suppose that $k, m, n \in \mathbb{N}$, $a, b \in \mathbb{Z}$, $(a, b) = 1$, a and b are odd, and m is even. Let $c = v_2(U_6) - 1$,*

$$\begin{aligned} t &= \min(\{v_2(n) + c - 1\} \cup \{y_p - k \mid \text{ } p \text{ is an odd prime factor of } V_n\}), \\ s &= \min(\{c - 1\} \cup \{y_p - k \mid p \text{ is an odd prime factor of } V_n\}), \text{ and} \\ y_p &= \left\lfloor \frac{v_p(m)}{v_p(V_n)} \right\rfloor \text{ for each odd prime } p \text{ dividing } V_n. \end{aligned}$$

Then

(i) *if $V_n^k \mid m$, then $V_n^{k+1} \mid U_{nm}$;*
(ii) *if $V_n^k \parallel m$ and $n \not\equiv 0 \pmod 3$, then $V_n^{k+1} \parallel U_{nm}$;*
(iii) *if $V_n^k \parallel m$, $n \equiv 0 \pmod 6$ and $\frac{V_n^{k+1}}{2} \nmid m$, then $V_n^{k+1} \parallel U_{nm}$;*
(iv) *if $V_n^k \mid m$, $n \equiv 0 \pmod 6$, and $\frac{V_n^{k+1}}{2} \mid m$, then $t \geq 0$ and $V_n^{k+t+1} \mid U_{nm}$;*
if $V_n^k \parallel m, n \equiv 0 \pmod 6$ and $\frac{V_n^{k+1}}{2} \mid m$, then $V_n^{k+t+1} \parallel U_{nm}$;
(v) *if $V_n^k \parallel m$, $n \equiv 3 \pmod 6$, $2 \parallel a^2 + 3b$ and $\frac{V_n^{k+1}}{2} \nmid m$, then $V_n^{k+1} \parallel U_{nm}$;*
(vi) *if $V_n^k \mid m$, $n \equiv 3 \pmod 6$, $2 \parallel a^2 + 3b$, and $\frac{V_n^{k+1}}{2} \mid m$, then $s \geq 0$ and $V_n^{k+s+1} \mid U_{nm}$;*
if $V_n^k \parallel m$, $n \equiv 3 \pmod 6$, $2 \parallel a^2 + 3b$ and $\frac{V_n^{k+1}}{2} \mid m$, then $V_n^{k+s+1} \parallel U_{nm}$;
(vii) *if $V_n^k \parallel m$, $n \equiv 3 \pmod 6$, $4 \mid a^2 + 3b$ and $\frac{V_n^{k+1}}{2^c} \nmid m$, then $V_n^{k+1} \parallel U_{nm}$;*

(viii) *if* $V_n^k \mid m$, $n \equiv 3 \pmod 6$, $4 \mid a^2 + 3b$ *and* $\frac{V_n^{k+1}}{2^c} \mid m$, *then* $V_n^{k+2} \mid 2^c U_{nm}$;
if $V_n^k \parallel m$, $n \equiv 3 \pmod 6$, $4 \mid a^2 + 3b$ *and* $\frac{V_n^{k+1}}{2^c} \mid m$, *then* $V_n^{k+2} \parallel 2^c U_{nm}$.

Proof. As usual, to prove that $V_n^d \mid U_{nm}$, we show that $v_p(V_n^d) \le v_p(U_{nm})$ for all primes p dividing V_n. Similarly, if we would like to prove that $V_n^d \nmid U_{nm}$, then we show that $v_p(V_n^d) > v_p(U_{nm})$ for some prime p. If p is odd, then we apply Lemmas 3 and 4; if $p = 2$, then we use Lemma 9; and we will do this without further reference. For (i), assume that $V_n^k \mid m$. If p is odd and $p \mid V_n$, then

$$v_p(U_{nm}) = v_p(nm) + v_p(U_{\tau(p)}) = v_p(m) + v_p(n) + v_p(U_{\tau(p)}) \ge v_p(V_n^k) + v_p(V_n) = v_p(V^{k+1}).$$

So it remains to show that $v_2(U_{nm}) \ge v_2(V_n^{k+1})$. If $n \not\equiv 0 \pmod 3$, then $v_2(V_n^{k+1}) = 0 \le v_2(U_{nm})$. So suppose that $n \equiv 0 \pmod 3$. Then $nm \equiv 0 \pmod 6$ and so

$$v_2(U_{nm}) = v_2(nm) + v_2(U_6) - 1 \ge v_2(V_n^k) + v_2(n) + v_2(U_6) - 1. \tag{3.2}$$

Since $U_3 = a^2 + b$ is even and $U_6 = a(a^2 + 3b)U_3$, we know that $v_2(U_3) \ge 1$ and $v_2(U_6) \ge 1$. So if $n \equiv 0 \pmod 6$, then $v_2(n) \ge 1$ and (3.2) implies that

$$v_2(U_{nm}) \ge v_2(V_n^k) + v_2(U_6) \ge v_2(V_n^k) + v_2(V_n) = v_2(V_n^{k+1}).$$

If $n \equiv 3 \pmod 6$, then (3.2) implies

$$v_2(U_{nm}) \ge v_2(V_n^k) + v_2(U_6) - 1 \ge v_2(V_n^k) + v_2(U_6) - v_2(U_3) = v_2(V_n^{k+1}).$$

In any case, $v_2(U_{nm}) \ge v_2(V_n^{k+1})$. This proves (i).

For (ii), assume that $V_n^k \parallel m$ and $n \not\equiv 0 \pmod 3$. By (i), it is enough to show that $V_n^{k+2} \nmid U_{nm}$. Since $V_n^{k+1} \nmid m$, there exists a prime p dividing V_n such that $v_p(V_n^{k+1}) > v_p(m)$. Since $v_2(V_n^{k+1}) = 0$, we see that $p \neq 2$. Then

$$v_p(U_{nm}) = v_p(nm) + v_p(U_{\tau(p)}) = v_p(m) + v_p(n) + v_p(U_{\tau(p)}) < v_p(V_n^{k+1}) + v_p(V_n) = v_p(V_n^{k+2}), \text{ as desired.}$$

For (iii), assume that $V_n^k \parallel m$, $n \equiv 0 \pmod 6$, and $\frac{V_n^{k+1}}{2} \nmid m$. By (i), it is enough to show that $V_n^{k+2} \nmid U_{nm}$. Since $\frac{V_n^{k+1}}{2} \nmid m$ and $v_2(\frac{V_n^{k+1}}{2}) = v_2(V_n^k) \le v_2(m)$, we see that there exists an odd prime p dividing V_n such that $v_p(V_n^{k+1}) > v_p(m)$. Then

$$v_p(U_{nm}) = v_p(nm) + v_p(U_{\tau(p)}) = v_p(m) + v_p(V_n) < v_p(V_n^{k+1}) + v_p(V_n) = v_p(V_n^{k+2}).$$

Therefore $V_n^{k+2} \nmid U_{nm}$, as required.

For (iv), we first assume that $V_n^k \mid m$, $n \equiv 0 \pmod 6$, and $\frac{V_n^{k+1}}{2} \mid m$. Since $v_2(n) \ge 1$ and $v_2(U_6) \ge v_2(U_3) \ge 1$, it is not difficult to see that $t \ge 0$. If p is an odd prime dividing V_n, then

$$\begin{aligned} v_p(U_{nm}) &= v_p(nm) + v_p(U_{\tau(p)}) = v_p(m) + v_p(V_n) \\ &\ge y_p v_p(V_n) + v_p(V_n) = (y_p + 1)v_p(V_n) \\ &\ge (k + t + 1)v_p(V_n) = v_p(V_n^{k+t+1}). \end{aligned}$$

In addition,

$$v_2(U_{nm}) = v_2(nm) + v_2(U_6) - 1 = v_2(m) + v_2(n) + v_2(U_6) - 1$$

$$\geq v_2(V_n^k) + t + 1 = k + t + 1 = v_2(V_n^{k+t+1}).$$

Therefore $V_n^{k+t+1} \mid U_{nm}$. This proves the first part of (iv). Next, assume further that $V_n^k \parallel m$. It is enough to show that $V_n^{k+t+2} \nmid U_{nm}$. Recall that $y_p = \left\lfloor \frac{v_p(m)}{v_p(V_n)} \right\rfloor$, so $v_p(m) < (y_p+1)v_p(V_n)$. So if $t = y_p - k$ for some odd prime p dividing V_n, then

$$v_p(U_{nm}) = v_p(nm) + v_p(U_{\tau(p)}) = v_p(m) + v_p(V_n) < (y_p+2)v_p(V_n) = (k+t+2)v_p(V_n) = v_p(V_n^{k+t+2}),$$

which implies $V_n^{k+t+2} \nmid U_{nm}$. So suppose $t = v_2(n) + v_2(U_6) - 2$. Since $\frac{V_n^{k+1}}{2} \mid m$, we see that $v_p(m) \geq v_p(V_n^{k+1})$ for all odd primes p. If $v_2(m) \geq k+1$, then $v_2(m) \geq v_2(V_n^{k+1})$,which implies $V_n^{k+1} \mid m$ contradicting the assumption $V_n^k \parallel m$. Therefore $v_2(m) \leq k$. Then

$$v_2(U_{nm}) = v_2(nm) + v_2(U_6) - 1 = v_2(m) + v_2(n) + v_2(U_6) - 1 \leq k + t + 1 < v_2(V_n^{k+t+2}).$$

Therefore, $V_n^{k+t+2} \nmid U_{nm}$ as required.

For (v), assume that $V_n^k \parallel m$, $n \equiv 3 \pmod 6$, $2 \parallel a^2 + 3b$, and $\frac{V_n^{k+1}}{2} \nmid m$. By (i), it suffies to show that $V_n^{k+2} \nmid U_{nm}$. Since $U_6 = a(a^2+3b)U_3$ and $2 \parallel a^2+3b$, we obtain $v_2(V_n) = v_2(U_6) - v_2(U_3) = 1$. Since $\frac{V_n^{k+1}}{2} \nmid m$ and $v_2\left(\frac{V_n^{k+1}}{2}\right) = v_2(V_n^k) \leq v_2(m)$, there exists an odd prime p dividing V_n such that $v_p(V_n^{k+1}) > v_p(m)$. Therefore

$$v_p(U_{nm}) = v_p(nm) + v_p(U_{\tau(p)}) = v_p(m) + v_p(V_n) < v_p(V_n^{k+1}) + v_p(V_n) = v_p(V_n^{k+2}), \text{ as desired.}$$

For (vi), assume that $V_n^k \mid m$, $n \equiv 3 \pmod 6$, $2 \parallel a^2+3b$, and $\frac{V_n^{k+1}}{2} \mid m$. Since a^2+3b and U_3 are even, and $U_6 = a(a^2+3b)U_3$, we have $v_2(U_6) - 2 \geq 0$. Since $V_n^k \mid m$, we have $y_p \geq k$ for all odd primes p dividing V_n. Therefore $s \geq 0$. By the same argument as in the proof of (v), we obtain $v_2(V_n) = 1$. In addition, $v_2(m) \geq v_2(V_n^k) = k$ and $v_p(V_n^{k+1}) = v_p(\frac{V_n^{k+1}}{2}) \leq v_p(m)$ for every odd prime p. If $V_n^k \parallel m$ and $v_2(m) \geq k+1 = v_2(V_n^{k+1})$, then $V_n^{k+1} \mid m$ which is a contradiction. Therefore,

$$\text{if } V_n^k \parallel m, \text{ then } v_2(m) = k. \tag{3.3}$$

We will apply (3.3) later. For now, we only need to apply $v_2(m) \geq k$. We obtain

$$v_2(U_{nm}) = v_2(nm) + v_2(U_6) - 1 = v_2(m) + v_2(U_6) - 1 \geq k + v_2(U_6) - 1 \geq k + s + 1 = v_2(V_n^{k+s+1}).$$

If $p > 2$ and $p \mid V_n$, then

$$v_p(U_{nm}) = v_p(nm) + v_p(U_{\tau(p)}) = v_p(m) + v_p(V_n) \geq (y_p+1)v_p(V_n) \geq (k+s+1)v_p(V_n) = v_p(V_n^{k+s+1}).$$

This implies $V_n^{k+s+1} \mid U_{nm}$. Next, assume further that $V_n^k \parallel m$. It remains to show that $V_n^{k+s+2} \nmid U_{nm}$. By the definition of y_p, we know that $(y_p+1)v_p(V_n) > v_p(m)$. So if $s = y_p - k$ for some odd prime p dividing V_n, then

$$v_p(U_{nm}) = v_p(nm) + v_p(U_{\tau(p)}) = v_p(m) + v_p(V_n) < (y_p+2)v_p(V_n) = (k+s+2)v_p(V_n) = v_p(V_n^{k+s+2}),$$

which implies $V_n^{k+s+2} \nmid U_{nm}$. By (3.3), we know that $v_2(m) = k$. So if $s = v_2(U_6) - 2$, then

$$v_2(U_{nm}) = v_2(nm) + v_2(U_6) - 1 = v_2(m) + v_2(U_6) - 1 = k + s + 1 < v_2(V_n^{k+s+2}).$$

So in any case, $V_n^{k+s+2} \nmid U_{nm}$, as required.

For (vii), we let $c = v_2(U_6) - 1$ and assume that $V_n^k \parallel m$, $n \equiv 3 \pmod 6$, $4 \mid a^2 + 3b$, and $\frac{V_n^{k+1}}{2^c} \nmid m$. By (i), it is enough to show that $V_n^{k+2} \nmid U_{nm}$. Since $4 \mid a^2 + 3b$ and $U_6 = a(a^2 + 3b)U_3$, we have $v_2(U_6) \geq v_2(U_3) + 2$. By Lemma 6, we obtain $v_2(U_3) = 1$, and so $v_2(V_n) = v_2(U_6) - v_2(U_3) = v_2(U_6) - 1 = c$. Since $\frac{V_n^{k+1}}{2^c} \nmid m$ and

$$v_2\left(\frac{V_n^{k+1}}{2^c}\right) = (k+1)v_2(V_n) - v_2(V_n) = v_2(V_n^k) \leq v_2(m),$$

there exists an odd prime p dividing V_n such that $v_p(V_n^{k+1}) > v_p(m)$. Then

$$v_p(U_{nm}) = v_p(nm) + v_p(U_{\tau(p)}) = v_p(m) + v_p(V_n) < v_p(V_n^{k+1}) + v_p(V_n) = V_p(V_n^{k+2}).$$

Therefore $V_n^{k+2} \nmid U_{nm}$.

For (viii), assume that $V_n^k \mid m$, $n \equiv 3 \pmod 6$, $4 \mid a^2 + 3b$, and $\frac{V_n^{k+1}}{2^c} \mid m$. Then for each odd prime p dividing V_n, we have

$$v_p(V_n^{k+1}) = v_p\left(\frac{V_n^{k+1}}{2^c}\right) \leq v_p(m). \tag{3.4}$$

Since $4 \mid a^2+3b$ and $U_6 = a(a^2+3b)U_3$, we obtain $v_2(U_6) \geq v_2(U_3)+2$. By the same argument as in the proof of (vii), we obtain $v_2(V_n) = v_2(U_6) - 1 = c$. Since $V_n^k \mid m$, we see that $v_2(m) \geq v_2(V_n^k) = kv_2(V_n)$. If $V_n^k \parallel m$ and $v_2(m) \geq (k+1)v_2(V_n)$, then $v_p(m) \geq v_p(V_n^{k+1})$ for all primes p, and so $V_n^{k+1} \mid m$, a contradiction. Therefore

$$v_2(m) \geq kv_2(V_n), \tag{3.5}$$

and

$$\text{if } V_n^k \parallel m, \text{ then } kv_2(V_n) \leq v_2(m) < (k+1)v_2(V_n). \tag{3.6}$$

We will apply (3.6) later. For now (3.5) is good enough. We obtain

$$\begin{aligned} v_2(2^c U_{nm}) &= v_2(U_6) - 1 + v_2(U_{nm}) = v_2(U_6) - 1 + v_2(nm) + v_2(U_6) - 1 \\ &= 2(v_2(U_6) - 1) + v_2(m) \\ &\geq 2(v_2(U_6) - 1) + kv_2(V_n) \\ &= 2(v_2(U_6) - 1) + k(v_2(U_6) - 1) \\ &= (k+2)(v_2(U_6) - 1) = v_2(V_n^{k+2}). \end{aligned}$$

If $p > 2$ and $p \mid V_n$, then

$$v_p(2^c U_{nm}) = v_p(U_{nm}) = v_p(nm) + v_p(U_{\tau(p)}) = v_p(m) + v_p(V_n) \geq v_p(V_n^{k+1}) + v_p(V_n) = v_p(V_n^{k+2}),$$

where the last inequality is obtained from (3.4). This implies that $V_n^{k+2} \mid 2^c U_{nm}$. So the first part of (viii) is proved. Next, assume further that $V_n^k \parallel m$. To prove the second part, it now suffices to show that $V_n^{k+3} \nmid 2^c U_{nm}$. We have

$$v_2(2^c U_{nm}) = v_2(U_6) - 1 + v_2(U_{nm})$$

$$
\begin{aligned}
&= \nu_2(U_6) - 1 + \nu_2(nm) + \nu_2(U_6) - 1 \\
&= 2(\nu_2(U_6) - 1) + \nu_2(m) \\
&< 2(\nu_2(U_6) - 1) + (k+1)(\nu_2(U_6) - 1) \\
&= (k+3)(\nu_2(U_6) - 1) = \nu_2(V_n^{k+3}),
\end{aligned}
$$

where the inequality is obtained form (3.6) and the fact that $\nu_2(V_n) = \nu_2(U_6) - 1$. This completes the proof. □

Theorem 20. *Suppose that $k, m, n \in \mathbb{N}$, $a, b \in \mathbb{Z}$, $(a, b) = 1$, a and b are odd and m is even. Then*

(i) *for every odd prime p dividing V_n, if $\nu_p(V_n^{k+1}) \le \nu_p(U_{nm})$, then $\nu_p(V_n^k) \le \nu_p(m)$;*
(ii) *if $V_n^{k+1} \mid U_{nm}$ and $n \not\equiv 0 \pmod 3$, then $V_n^k \mid m$;*
if $V_n^{k+1} \parallel U_{nm}$ and $n \not\equiv 0 \pmod 3$, then $V_n^k \parallel m$;
(iii) *if $V_n^{k+1} \mid U_{nm}$, $n \equiv 0 \pmod 6$, and $\nu_2(m) \ge k$, then $V_n^k \mid m$;*
if $V_n^{k+1} \parallel U_{nm}$, $n \equiv 0 \pmod 6$, and $\nu_2(m) \ge k$, then $V_n^k \parallel m$;
if $V_n^{k+1} \mid U_{nm}$, $n \equiv 0 \pmod 6$, and $\nu_2(m) < k$, then $V_n^{\nu_2(m)} \parallel m$;
(iv) *if $V_n^{k+1} \mid U_{nm}$, $n \equiv 3 \pmod 6$, $2 \parallel a^2 + 3b$, and $\nu_2(m) \ge k$, then $V_n^k \mid m$;*
if $V_n^{k+1} \parallel U_{nm}$, $n \equiv 3 \pmod 6$, $2 \parallel a^2 + 3b$, and $\nu_2(m) \ge k$, then $V_n^k \parallel m$;
if $V_n^{k+1} \mid U_{nm}$, $n \equiv 3 \pmod 6$, $2 \parallel a^2 + 3b$, and $\nu_2(m) < k$, then $V_2^{\nu_2(m)} \parallel m$;
(v) *if $V_n^{k+1} \mid U_{nm}$, $n \equiv 3 \pmod 6$, and $4 \mid a^2 + 3b$, then $V_n^k \mid m$;*
if $V_n^{k+1} \parallel U_{nm}$, $n \equiv 3 \pmod 6$, and $4 \mid a^2 + 3b$, then $V_n^k \parallel m$.

Proof. We apply Lemmas 3, 4, and 9 throughout the proof without reference. For (i), assume that p is an odd prime dividing V_n and $\nu_p(V_n^{k+1}) \le \nu_p(U_{nm})$. Then

$$
\nu_p(V_n) + \nu_p(V_n^k) = \nu_p(V_n^{k+1}) \le \nu_p(U_{nm}) \le \nu_p(nm) + \nu_p(U_{\tau(p)}) = \nu_p(m) + \nu_p(V_n),
$$

which implies (i). Therefore we only need to consider the 2-adic valuation in the proof of (ii) to (v).

For (ii), assume that $V_n^{k+1} \mid U_{nm}$ and $n \not\equiv 0 \pmod 3$. Since $\nu_2(V_n^k) = 0 \le \nu_2(m)$, we obtain by (i) that $V_n^k \mid m$. Suppose futher that $V_n^{k+1} \parallel U_{nm}$. If $V_n^{k+1} \mid m$, then (i) of Theorem 19 implies $V_n^{k+2} \mid U_{nm}$, which contradicts $V_n^{k+1} \parallel U_{nm}$, and so $V_n^k \parallel m$.

For (iii), assume that $V_n^{k+1} \mid U_{nm}$ and $n \equiv 0 \pmod 6$.

Case 1 $\nu_2(m) \ge k$. Then $\nu_2(V_n^k) = k \le \nu_2(m)$. So we obtain by (i) that $V_n^k \mid m$. If $V_n^{k+1} \parallel U_{nm}$, then we obtain by (i) of Theorem 19 that $V_n^{k+1} \nmid m$, and so $V_n^k \parallel m$. This proves (iii) in the case $\nu_2(m) \ge k$.

Case 2 $\nu_2(m) < k$. For convenience, let $d = \nu_2(m)$. Since $\nu_2(V_n^d) = d = \nu_2(m)$ and $\nu_p(V_n^d) \le \nu_p(V_n^k) \le \nu_p(m)$ for every odd prime p dividing V_n, we obtain $V_n^d \mid m$. If $V_n^{d+1} \mid m$, then $d+1 = \nu_2(V_n^{d+1}) \le \nu_2(m) = d$, a contradiction. So $V_n^d \parallel m$.

For (iv), assume that $V_n^{k+1} \mid U_{nm}$, $n \equiv 3 \pmod 6$, and $2 \parallel a^2 + 3b$. Since $U_6 = a(a^2 + 3b)U_3$ and $2 \parallel a^2 + 3b$, we obtain $\nu_2(V_n) = \nu_2(U_6) - \nu_2(U_3) = 1$.

Case 1 $\nu_2(m) \ge k$. Then $\nu_2(V_n^k) = k \le \nu_2(m)$, and so we obtain by (i) that $V_n^k \mid m$. If $V_n^{k+1} \parallel U_{nm}$, then we obtain by (i) of Theorem 19 that $V_n^k \parallel m$. This proves (iv) in the case $\nu_2(m) \ge k$.

Case 2 $\nu_2(m) < k$. For convenience, let $d = \nu_2(m)$. Then $\nu_2(V_n^d) = d = \nu_2(m)$ and $\nu_p(V_n^d) \le \nu_p(V_n^k) \le \nu_p(m)$. Therefore $V_n^d \mid m$. If $V_n^{d+1} \mid m$, then $d + 1 = \nu_2(V_n^{d+1}) \le \nu_2(m) = d$, a contradiction. Therefore $V_n^d \parallel m$.

For (v), assume that $V_n^{k+1} \mid U_{nm}$, $n \equiv 3 \pmod 6$, and $4 \mid a^2 + 3b$. Since $U_6 = a(a^2 + 3b)U_3$ and $4 \mid a^2 + 3b$, we obtain $v_2(U_6) \geq v_2(U_3) + 2$. By Lemma 6, we have $v_2(U_3) = 1$. Then $v_2(V_n) = v_2(U_6) - v_2(U_3) = v_2(U_6) - 1$ and

$$v_2(V_n^k) + v_2(V_n) = v_2(V_n^{k+1}) \leq v_2(U_{nm}) = v_2(nm) + v_2(U_6) - 1 = v_2(m) + v_2(V_n).$$

So $v_2(V_n^k) \leq v_2(m)$. By (i), we obtain $V_n^k \mid m$. If $V_n^{k+1} \parallel U_{nm}$, then we obtain by (i) of Theorem 19 that $V_n^{k+1} \nmid m$, and so $V_n^k \parallel m$. This completes the proof. □

4. Conclusions

We obtain exact divisibility theorems for the Lucas sequences of the first and second kinds, which complete a long investigation on this problem from 1970 to 2021.

Acknowledgments

We are grateful to both referees for their kind words and suggestions which improve the quality of this paper. Kritkhajohn Onphaeng receives a scholarship from Development and Promotion for Science and Technology Talents Project (DPST). Prapanpong Pongsriiam's research project is funded jointly by Faculty of Science Silpakorn University and the National Research Council of Thailand (NRCT), Grant Number NRCT5-RSA63021-02.

Conflict of interest

The authors declare that there is no conflict of interests regarding the publication of this article.

References

1. A. Benjamin, J. Rouse, *When does F_m^L divide F_n? A combinatorial solution*, Proceedings of the Eleventh International Conference on Fibonacci Numbers and Their Applications, **194**, Congressus Numerantium, 2009, 53–58.
2. Y. Bugeaud, M. Mignotte, S. Siksek, Classical and modular approaches to exponential Diophantine equations I. Fibonacci and Lucas perfect powers, *Ann. Math.*, **163** (2006), 969–1018.
3. P. Cubre, J. Rouse, Divisibility properties of the Fibonacci entry point, *Proc. Amer. Math. Soc.*, **142** (2014), 3771–3785.
4. V. E. Hoggatt Jr., M. Bicknell-Johnson, Divisibility by Fibonacci and Lucas squares, *Fibonacci Quart.*, **15** (1977), 3–8.
5. Y. Matijasevich, Enumerable Sets are Diophantine, *Proc. Academy Sci. USSR*, **11** (1970), 354–358.
6. Y. Matijasevich, My collaboration with Julia Robison, *Math. Intell.*, **14** (1992), 38–45.
7. Y. Matijasevich, *Hilbert's Tenth Problem*, MIT Press, 1996.
8. K. Onphaeng, P. Pongsriiam, Exact divisibility by powers of the integers in the Lucas sequence of the first kind, *AIMS Math.*, **5** (2020), 6739–6748.

9. K. Onphaeng, P. Pongsriiam, Subsequences and divisibility by powers of the Fibonacci numbers, *Fibonacci Quart.*, **52** (2014), 163–171.
10. K. Onphaeng, P. Pongsriiam, The converse of exact divisibility by powers of the Fibonacci and Lucas numbers, *Fibonacci Quart.*, **56** (2018), 296–302.
11. C. Panraksa, A. Tangboonduangjit, p-adic valuation of Lucas iteration sequences, *Fibonacci Quart.*, **56** (2018), 348–353.
12. A. Patra, G. K. Panda, T. Khemaratchatakumthorn, Exact divisibility by powers of the balancing and Lucas-balancing numbers, *Fibonacci Quart.*, **59** (2021), 57–64.
13. P. Phunphayap, P. Pongsriiam, Explicit formulas for the p-adic valuations of Fibonomial coefficients, *J. Integer Seq.*, **21** (2018), Article 18.3.1.
14. P. Phunphayap, P. Pongsriiam, Explicit formulas for the p-adic valuations of Fibonomial coefficients II, *AIMS Math.*, **5** (2020), 5685–5699.
15. P. Pongsriiam, Exact divisibility by powers of the Fibonacci and Lucas numbers, *J. Integer Seq.*, **17** (2014), Article 14.11.2.
16. P. Pongsriiam, *Fibonacci and Lucas numbers associated with Brocard-Ramanujan equation*, *Commun. Korean Math. Soc.*, **32** (2017), 511–522.
17. M. K. Sahukar, G. K. Panda, Diophantine equations with balancing-like sequences associated to Brocard-Ramanujan-type problem, *Glas Mat.*, **54** (2019), 255–270.
18. C. Sanna, The p-adic valuation of Lucas sequences, *Fibonacci Quart.*, **54** (2016), 118–124.
19. J. Seibert, P. Trojovský, On divisibility of a relation of the Fibonacci numbers, *Int. J. Pure Appl. Math.*, **46** (2008), 443–448.
20. C. L. Stewart, On divisors of Lucas and Lehmer numbers, *Acta Math.*, **211** (2013), 291–314.

AIMS Press