p-ADIC VALUATION OF LUCAS ITERATION SEQUENCES

CHATCHAWAN PANRAKSA AND ARAM TANGBOONDUANGJIT

Abstract. This work generalizes results on exact divisibility of powers of the Fibonacci number F_n^k into another Fibonacci number $G_k(n)$ defined iteratively by $G_1(n) = F_n$ and $G_k(n) = F_{nG_{k-1}(n)}$ for $k \geq 2$. In particular, we prove analogous results on nondegenerate Lucas sequences by providing explicit formulas for p-adic valuation of iterative terms in these sequences. The proof makes use of recent results by Sanna regarding the p-adic valuation of Lucas sequences.

1. Introduction

Let P and Q be fixed relatively prime integers. The Lucas sequence, denoted $U_n(P,Q)$, is defined by $U_0(P,Q) = 0$, $U_1(P,Q) = 1$, and

$$U_n(P,Q) = P \cdot U_{n-1}(P,Q) - Q \cdot U_{n-2}(P,Q) \quad \text{for } n \geq 2.$$

For example, the Fibonacci numbers F_n and the Mersenne numbers $2^n - 1$ correspond to $U_n(1,-1)$ and $U_n(3,2)$, respectively. We associate the characteristic polynomial $x^2 - Px + Q$ with the sequence $U_n(P,Q)$. Let $D = P^2 - 4Q$ be the discriminant of this polynomial. If $D \neq 0$, then the characteristic polynomial $x^2 - Px + Q$ has two distinct zeros α and β and $U_n(P,Q)$ can be expressed explicitly as

$$U_n(P,Q) = \frac{\alpha^n - \beta^n}{\alpha - \beta} = \frac{\alpha^n - \beta^n}{\sqrt{D}}.$$

If not stated otherwise, the sequence U_n in this work is referred to as $U_n(P,Q)$ for some fixed relatively prime integers P and Q and assumed to be nondegenerate, that is, $Q \neq 0$ and the ratio of the two roots of the characteristic polynomial $x^2 - Px + Q$ is not a root of unity. Consequently, the two roots of such characteristic polynomial are distinct and the discriminant $D = P^2 - 4Q \neq 0$. Let $n \geq 0$. Define the Lucas iteration sequence $G_k(n)$ by $G_1(n) = U_n$ and $G_k(n) = U_{nG_{k-1}(n)}$ for $k \geq 2$. For example, the first three terms of the sequence $G_k(n)$ are

$$G_1(n) = U_n, \quad G_2(n) = U_{nU_n}, \quad \text{and} \quad G_3(n) = U_{nU_{nU_n}}.$$

The sequence $G_k(n)$ corresponding to the Fibonacci sequence $U_n(1,-1)$ was studied by Tangboonduangjit and Wiboonton [5] where they proved that F_n^k divides $G_k(n)$. A year later, Panraksa, Tangboonduangjit, and Wiboonton [2] proved that the divisibility is exact for $n > 3$ and gave explicit formulas for the quotient $G_k(n)/F_n^k$ modulo F_n for the cases $k = 2$ and $k = 3$. Another year later, however, Onphaeng and Pongsriiam [1] generalized the sequence $G_k(n)$ and were able to give explicit formulas for the quotient $G_k(n)/F_n^k$ modulo F_n for all $k \geq 2$. For each prime number p, we recall that the p-adic valuation $\nu_p(m)$ of non-zero integer m is defined to be the exponent of p in the prime factorization of m, whereas $\nu_p(0)$ is defined to be infinity. In this paper, we generalize some results in [2] to the Lucas sequence $U_n(P,Q)$. In particular, we give explicit formulas for p-adic valuation of the sequence $G_k(n)$. The main result is presented in section 3.

2. Preliminary

Sanna [4] gives a complete account of the p-adic valuation of nondegenerate Lucas sequences. The results needed in this work are stated as Theorem 1.5 and Corollary 1.6 in [4]. We recall them here as a single theorem. If p is prime such that $p \nmid Q$, then the rank of apparition of p in the sequence U_n, denoted $\tau(p)$, is defined to be the least positive integer such that $p \mid U_{\tau(p)}$. These basic facts about $\tau(p)$ are well-known: $\tau(p)$ exists for each p, and $p \mid U_n$ if and only if $\tau(p) \mid n$.

Theorem 2.1. *Let p be prime such that $p \nmid Q$. Then, for each positive integer n,*

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

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

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

The following theorem by Riasat [3] generalizes "lifting the exponent" lemma to the ring of algebraic integers.

Theorem 2.2. *Let K be an algebraic number field and $\mathcal{O}_K$ its ring of integers. Let $\alpha, \beta \in \mathcal{O}_K$ such that the ideals (α) and (β) are relatively prime to (p) for some prime p. Define the sequence a_n by*

$$a_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}.$$

If a_n is an integer for all $n \geq 0$, then, for all $k \geq 0$ and $n \geq 0$,

$$\nu_p(a_{kp^n}) = n + \nu_p(a_k).$$

The following lemma is inspired by the above theorem.

Lemma 2.3. *Let $n, k \geq 1$ and p a prime factor of U_k such that $p \nmid Q$. Then,*

(1) *if (i) p is odd, or (ii) $p = 2$ and k is even, or (iii) $p = 2$ and n is odd, we have*

$$\nu_p(U_{kn}) = \nu_p(n) + \nu_p(U_k);$$

(2) *if k and D are odd and n is even, we have*

$$\nu_2(U_{kn}) = \nu_2(n) + \nu_2(U_k) + \Big(\nu_2(U_{2\tau(2)}) - \nu_2(U_{\tau(2)}) - 1\Big) \geq \nu_2(n) + \nu_2(U_k).$$

Proof. We distinguish two main cases.

Case 1. $p \mid D$. This implies $p \mid k$ (and therefore $p \mid kn$), since otherwise we have, by the second case of Theorem 2.1, $\nu_p(U_k) = 0$, which contradicts the assumption that p is a prime factor of U_k. Consequently, the first case of Theorem 2.1 yields

$$\nu_p(U_{kn}) = \nu_p(kn) + \nu_p(U_p) - 1 = \nu_p(n) + \big(\nu_p(k) + \nu_p(U_p) - 1\big).$$

According to Theorem 2.1, the value of $\nu_p(U_k)$ is $\nu_p(k) + \nu_p(U_p) - 1$ or 0; however, since, by assumption, $\nu_p(U_k) > 0$, it could not be the latter. Thus,

$$\nu_p(U_{kn}) = \nu_p(n) + \nu_p(U_k).$$

Case 2. $p \nmid D$. Since $p \mid U_k$, it follows that $\tau(p) \mid k$ (and therefore $\tau(p) \mid kn$). We consider two sub-cases.

Case 2.1. $p \mid k$. Then $p \mid kn$, so that by the third case of Theorem 2.1, we have

$$\nu_p(U_{kn}) = \nu_p(kn) + \nu_p(U_{p\tau(p)}) - 1 = \nu_p(n) + \Big(\nu_p(k) + \nu_p(U_{p\tau(p)}) - 1\Big) = \nu_p(n) + \nu_p(U_k).$$

Case 2.2. $p \nmid k$. We consider two sub-cases.

Case 2.2.1. p is odd. Then by the third case of Theorem 2.1 for the case when p is an odd prime, we have

$$\nu_p(U_{kn}) = \nu_p(kn) + \nu_p(U_{\tau(p)}) = \nu_p(n) + \Big(\nu_p(k) + \nu_p(U_{\tau(p)})\Big) = \nu_p(n) + \nu_p(U_k).$$

Case 2.2.2. $p = 2$. We consider two sub-cases.

Case 2.2.2.1. n is even. This implies $p \mid kn$. Then by the third case of Theorem 2.1, we have

$$\begin{aligned}\nu_p(U_{kn}) &= \nu_p(kn) + \nu_p(U_{p\tau(p)}) - 1 = \nu_p(n) + \nu_p(k) + \nu_p(U_{p\tau(p)}) - 1\\ &= \nu_p(n) + \nu_p(U_{\tau(p)}) + \Big(\nu_p(U_{p\tau(p)}) - \nu_p(U_{\tau(p)}) - 1\Big).\end{aligned}$$

Since $p \nmid k$, the fourth case of Theorem 2.1 yields,

$$\nu_p(U_k) = \nu_p(k) + \nu_p(U_{\tau(p)}) = 0 + \nu_p(U_{\tau(p)}) = \nu_p(U_{\tau(p)}).$$

Thus, $\nu_p(U_{kn}) = \nu_p(n) + \nu_p(U_k) + \Big(\nu_p(U_{p\tau(p)}) - \nu_p(U_{\tau(p)}) - 1\Big) \geq \nu_p(n) + \nu_p(U_k)$, where the last inequality follows from Lemma 3.2 in [4].

Case 2.2.2.2. n is odd. Then $p \nmid kn$, and so, by the fourth case of Theorem 2.1, we have

$$\nu_p(U_{kn}) = \nu_p(U_\tau(p)) = \nu_p(U_k) = 0 + \nu_p(U_k) = \nu_p(n) + \nu_p(U_k).$$

□

3. The Main Theorem

Theorem 3.1. *Let $n \geq 1$ and p a prime factor of U_n. Then, for $k \geq 1$,*

(1) *if (i) p is odd, or (ii) $p = 2$ and $2 \mid D$, or (iii) $p = 2$ and $\nu_2(U_n) \geq 2$, we have*

$$\nu_p(G_k(n)) = k \cdot \nu_p(U_n);$$

(2) *if $2 \nmid D$ and $\nu_2(U_n) = 1$, we have*

$$\nu_2(G_k(n)) = (\gamma - 1)k + 2 - \gamma,$$

where $\gamma = \nu_2(U_{2\tau(2)}) = \nu_2(U_6)$.

Proof. Let $n \geq 1$ be given and let p be a prime factor of U_n. We first prove assertion (1) with assumption (i). Suppose that p is odd. For $n = 1$, the formula holds trivially, since $G_k(1) = 1 = U_1$ for all k. Let $n > 1$ and suppose that $\nu_p(U_n) = s$. We want to show that $\nu_p(G_k(n)) = s \cdot k$. We prove this by induction on k. For $k = 1$, we have $\nu_p(G_1(n)) = \nu_p(U_n) = s = s \cdot 1$. Hence, the formula holds for $k = 1$. Assume the formula holds for some $k \geq 1$, which is $\nu_p(G_k(n)) = s \cdot k$. We want to show that $\nu_p(G_{k+1}(n)) = s(k+1)$. By the definition and Lemma 2.3(1), we have

$$\nu_p(G_{k+1}(n)) = \nu_p(U_{nG_k(n)}) = \nu_p(U_n) + \nu_p(G_k(n)) = s + sk = s(k+1).$$

This proves assertion (1) with assumption (i). Now we prove assertion (1) with assumption (ii). Assume that $p = 2$ and $2 \mid D$. Then P is even and Q is odd, since $\gcd(P, Q) = 1$. Together with the assumption that $\nu_2(U_n) > 0$, Theorem 2.1 implies $2 \mid n$, that is n is even and $\nu_2(U_n) = \nu_2(n) + \nu_2(U_2) - 1$. By induction (similar to the proof of assertion (1) with assumption (i) above), we have $\nu_2(G_k(n)) = k\nu_2(U_n)$. Theorem 2.1 allows us to express $\nu_2(G_k(n))$ in simpler terms as follows.

$$\nu_2(G_k(n)) = k\nu_2(U_n) = k(\nu_2(n) + \nu_2(U_2) - 1).$$

To prove assertion (1) with assumption (iii), we assume that $p = 2$ and $\nu_2(U_n) \geq 2$. If $2 \mid D$, then it is proved in the previous case. So we may assume that $2 \nmid D$. Then from $D = P^2 - 4Q$, we have P is odd. Assume that Q is even. From the recurrence $U_n = PU_{n-1} - QU_{n-2}$, since P is odd and $U_1 = 1$, it follows by induction that U_n is odd for all $n \geq 1$. This contradicts the assumption that $\nu_2(U_n) \geq 2$. Hence, Q is odd.

If n is even, then Lemma 2.3(1) implies that

$$\nu_2(G_{k+1}(n)) = \nu_2(U_{nG_k(n)}) = \nu_2(G_k(n)) + \nu_2(U_n).$$

Then again by induction, we have $\nu_2(G_k(n)) = k\nu_2(U_n)$.

If n is odd, then since $U_3 = PU_2 - QU_1 = P^2 - Q$, and P and Q are odd, it follows that U_3 is even. Since $U_1 = 1$ and $U_2 = P$ are not divisible by 2, but U_3 is, we have $\tau(2) = 3$, so that $2\tau(2) = 6$. By direct computation from the recurrence of U_n, we find that

$$U_3 = P^2 - 3Q \quad \text{and} \quad U_6 = P^5 - 4P^3Q + 3PQ^2 = P(P^2 - 3Q)(P^2 - Q).$$

Since $2 \nmid n$ and $\nu_2(U_n) \neq 0$ by assumption, it follows by the fourth case of Theorem 2.1 that $\nu_2(U_n) = \nu_2(U_{\tau(2)}) = \nu_2(U_3)$ and therefore, $2^\ell \mid\mid U_3$ for some $\ell \geq 2$. Consequently, $2 \mid\mid P^2 - 3Q$, since $P^2 - 3Q = (P^2 - Q) - 2Q$ and $2 \mid\mid 2Q$. Thus, $\nu_2(U_{2\tau(2)}) = \nu_2(U_{\tau(2)}) + 1$. By Lemma 2.3(2), we have

$$\begin{aligned}\nu_2(G_{k+1}(n)) = \nu_2(U_{nG_k(n)}) &= \nu_2(G_k(n)) + \nu_2(U_n) + \nu_2(U_{2\tau(2)}) - \nu_2(U_{\tau(2)}) - 1\\ &= \nu_2(G_k(n)) + \nu_2(U_n) + 0 = \nu_2(G_k(n)) + \nu_2(U_n).\end{aligned}$$

Then by induction as before, $\nu_2(G_k(n)) = k\nu_2(U_n)$.

We make the following observation before proving assertion (2). If $2 \nmid D$ and $\nu_2(U_n) = 1$, then n is odd. Assume otherwise; then since $D = P^2 - 4Q$, it follows that $2 \nmid P$ and by Lemma 3.2 in [4] that $\nu_2(U_{2\tau(2)}) \geq \nu_2(U_{\tau(2)}) + 1$. Now since $2 \mid n$, the third case of Theorem 2.1 applies and gives

$$1 = \nu_2(U_n) = \nu_2(n) + \nu_2(U_{2\tau(2)}) - 1 \geq 1 + \Big(\nu_2(U_{\tau(2)}) + 1\Big) - 1 = \nu_2(U_{\tau(2)}) + 1 \geq 2,$$

which is a contradiction.

Now we proceed to prove assertion (2). Assume that $2 \nmid D$ and $\nu_2(U_n) = 1$. By the observation above, we have n is odd. We prove the formula by induction on k. For $k = 1$, we have $\nu_2(G_1(n)) = \nu_2(U_n) = 1 = (\gamma - 1) \cdot 1 + 2 - \gamma$. Assuming that the formula holds for some positive integer k, we want to show that it holds for $k + 1$. We have

$$\begin{aligned}\nu_2(G_{k+1}(n)) = \nu_2(U_{nG_k(n)}) &= \nu_2(nG_k(n)) + \nu_2(U_{2\tau(2)}) - 1 = \nu_2(n) + \nu_2(G_k(n)) + \gamma - 1\\ &= 0 + ((\gamma - 1)k + 2 - \gamma) + \gamma - 1 = (\gamma - 1)k + 1 = (\gamma - 1)(k + 1) + 2 - \gamma,\end{aligned}$$

where the second equality follows from the third case of Theorem 2.1. This establishes the inductive step. Hence, the formula holds for all positive integers k. □

Corollary 3.2. *Let $n \geq 1$ and p a prime factor of U_n. If $2 \nmid D$ and $\nu_2(U_n) = 1$, then, for $k \geq 1$, we have $\nu_2(G_k(n)) \geq 2k - 1$.*

Proof. We will prove that $\gamma = \nu_2(U_6) \geq 3$. Then, Theorem 3.1(2) implies that

$$\nu_2(G_k(n)) = (\gamma - 1)k + 2 - \gamma = \gamma(k-1) + 2 - k \geq 3(k-1) + 2 - k = 2k - 1.$$

By direct computation from the recurrence of Lucas sequence, we find

$$U_6 = P^5 - 4P^3Q + 3PQ^2 = P(P^2 - 3Q)(P^2 - Q).$$

It will be shown in the proof of Theorem 3.1 that P and Q are odd. Consequently, the factors $P^2 - 3Q$ and $P^2 - Q$ of U_6 are even and therefore, $\nu_2(U_6) \geq 2$. However, considering in modulo 4, we find that $4 \mid P^2 - 3Q$ or $4 \mid P^2 - Q$. Hence, $8 \mid U_6$ or $\nu_2(U_6) \geq 3$, as desired. □

We make a remark here that the value of $\gamma = \nu_2(U_6) \geq 3$ can be any integer. We demonstrate this by proving that for each $\ell \geq 3$, there exists a Lucas sequence U_n such that $\nu_2(U_6) = \ell$. Indeed, letting $\ell \geq 3$, we consider the Lucas sequence $U_n(P,Q)$ with $P = 1$ and $Q = 1 - 2^{\ell-1}$. We find that

$$U_6 = P(P^2 - 3Q)(P^2 - Q) = (1 - 3(1 - 2^{\ell-1}))(1 - (1 - 2^{\ell-1})) = 2^{\ell}(3 \cdot 2^{\ell-2} - 1).$$

Since $3 \cdot 2^{\ell-2} - 1$ is odd for $\ell \geq 3$, it follows that $\nu_2(U_6) = \ell$. The following corollary of exact divisibility is stated as Theorem 3.3 in [2]. We present an alternative proof based on the main result of this work.

Corollary 3.3. *Let F_n be the Fibonacci sequence. Then, for all $k \geq 1$,*

1. *$F_n^k \mid\mid G_k(n)$ for all $n > 3$;*
2. *$F_3^{2k-1} \mid\mid G_k(3)$.*

Proof. For the Fibonacci sequence $F_n = U_n(1,-1)$, we have $P = 1 = -Q$ so that $D = P^2 - 4Q = 5$. We note first that F_n divides $G_k(n)$ for all $n, k \geq 1$. The statement is obviously true for $k = 1$. For $k > 1$, using F_n is a divisibility sequence, we have $F_n \mid F_{nG_{k-1}(n)}$ or $F_n \mid G_k(n)$. To prove (1), we let $n > 3$. It suffices to show that F_n has a prime factor p such that $\nu_p(G_k(n)) = k \cdot \nu_p(F_n)$. If F_n has an odd prime factor, then we let p be that prime factor, and the hypothesis of Theorem 3.1(1) part (i) is satisfied. If F_n has no odd prime factor, then we let $p = 2$. Since $F_3 = 2$ and the Fibonacci sequence F_n is strictly increasing for $n \geq 3$, it follows that $\nu_2(F_n) \geq 2$. Hence, the hypothesis of Theorem 3.1(1) part (iii) is satisfied. In all cases, we conclude that there is a prime factor p of F_n such that $\nu_p(G_k(n)) = k \cdot \nu_p(F_n)$, as we wanted to show. To prove (2), we consider that for $n = 3$, the number $\gamma = \nu_2(F_6) = \nu_2(8) = 3$. Since $2 \nmid D$ and $\nu_2(F_3) = \nu_2(2) = 1$, Theorem 3.1(2) implies that $\nu_2(G_k(3)) = (3-1)k + 2 - 3 = 2k - 1$. Thus, $F_3^{2k-1} \mid\mid G_k(3)$. □

Acknowledgements

We thank the referee for a careful reading of the manuscript and for many suggestions, which improved the structure and presentation of the paper. The second author is supported by the MUIC Seed Grant Research Fund.

References

[1] K. Onphaeng and P. Pongsriiam, *Subsequences and divisibility by powers of the Fibonacci numbers*, The Fibonacci Quarterly, **52.2** (2014), 163–171.

[2] C. Panraksa, A. Tangboonduangjit, and K. Wiboonton, *Exact divisibility properties of some subsequences of Fibonacci numbers*, The Fibonacci Quarterly, **51.4** (2013), 307–318.

[3] Samin Riasat's Blog (2013), A generalisation of 'lifting the exponent', `https://sriasat.wordpress.com/2013/08/26/a-generalisation-of-lifting-the-exponent/`.

[4] C. Sanna, *The p-adic valuation of Lucas sequences*, The Fibonacci Quarterly, **54.2** (2016), 118–124.

[5] A. Tangboonduangjit and K. Wiboonton, *Divisibility properties of some subsequences of Fibonacci numbers*, East-West J. Math., Special Volume, (2012), 331–336.

MSC2010: 11B39, 33C05

Mahidol University International College, Salaya, Nakhonpathom, Thailand
E-mail address: `chatchawan.pan@mahidol.edu`

Mahidol University International College, Salaya, Nakhonpathom, Thailand
E-mail address: `aram.tan@mahidol.edu`