THE p-ADIC VALUATION OF LUCAS SEQUENCES

CARLO SANNA

Abstract. Let $(u_n)_{n\geq 0}$ be a nondegenerate Lucas sequence with characteristic polynomial $X^2 - aX - b$, for some relatively prime integers a and b. For each prime number p and each positive integer n, we give simple formulas for the p-adic valuation $\nu_p(u_n)$, in terms of $\nu_p(n)$ and the rank of apparition of p in $(u_n)_{n\geq 0}$. This generalizes a previous result of Lengyel on the p-adic valuation of Fibonacci numbers, and also the folkloristic "lifting-the-exponent lemma".

1. Introduction

Fix two relatively prime integers a and b and let $(u_n)_{n\geq 0}$ be the Lucas sequence with characteristic polynomial $f(X) = X^2 - aX - b$, i.e., $(u_n)_{n\geq 0}$ is the integral sequence satisfying $u_0 = 0$, $u_1 = 1$, and $u_n = au_{n-1} + bu_{n-2}$, for all integers $n \geq 2$. The purpose of this paper is to give simple formulas for the p-adic valuation $\nu_p(u_n)$, for all prime numbers p and all positive integers n. To this end, we will see that there is no loss of generality in assuming that the Lucas sequence $(u_n)_{n\geq 0}$ is nondegenerate, i.e., $b \neq 0$ and the ratio α/β of the two roots $\alpha, \beta \in \mathbb{C}$ of $f(X)$ is not a root of unity. In particular, this implies that α and β are distinct and hence the discriminant Δ of $f(X)$ is nonzero.

The p-adic valuation of some special Lucas sequences has been studied before by many authors. Lengyel [3] considered the sequence of Fibonacci numbers $(F_n)_{n\geq 0}$ and proved the following theorem.

Theorem 1.1. *For each positive integer n and each prime number $p \neq 2, 5$, we have*

$$\nu_2(F_n) = \begin{cases} 0 & \text{if } n \equiv 1, 2 \mod 3, \\ 1 & \text{if } n \equiv 3 \mod 6, \\ 3 & \text{if } n \equiv 6 \mod 12, \\ \nu_2(n) + 2 & \text{if } n \equiv 0 \mod 12; \end{cases}$$

$$\nu_5(F_n) = \nu_5(n);$$

$$\nu_p(F_n) = \begin{cases} \nu_p(n) + \nu_p(F_{\ell(p)}) & \text{if } n \equiv 0 \bmod \ell(p), \\ 0 & \text{if } n \not\equiv 0 \bmod \ell(p); \end{cases}$$

where $\ell(p)$ is the least positive integer such that $p \mid F_{\ell(p)}$.

Furthermore, the following lemma, often used in olympic problem solving contests [2], belongs to the folklore and is typically attributed to Lucas [4] and Carmichael [1].

Lemma 1.2 (Lifting-the-exponent lemma)**.** *For all odd prime numbers p, all integers c and d such that $p \nmid cd$ and $p \mid c - d$, and every positive integer n, we have*

$$\nu_p(c^n - d^n) = \nu_p(n) + \nu_p(c - d).$$

It is well-known that for all nonnegative integers n, it holds

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}. \tag{1.1}$$

Hence, an immediate consequence of Lemma 1.2 is the following corollary.

Corollary 1.3. *If α and β are integers and p is an odd prime number such that $p \nmid b$ and $p \mid \Delta$, then $\nu_p(u_n) = \nu_p(n)$ for each positive integer n.*

Ward [6] studied the p-adic valuation of second order linear recurrences over the field of p-adic numbers $\mathbb{Q}_p$. However, his results applied to Lucas sequences are not as much effective as Theorem 1.1 or Corollary 1.3. Precisely, in the simplest case he obtained the following theorem.

Theorem 1.4. *For each prime p such that $p \nmid ab\Delta$, we have*

$$\nu_p(u_n) = \begin{cases} \nu_p(\xi_p + n/\tau(p)) + \nu_p(u_{\tau(p)}) & \text{if } n \equiv 0 \bmod \tau(p) \\ 0 & \text{if } n \not\equiv 0 \bmod \tau(p); \end{cases}$$

where $\tau(p)$ is the least positive integer such that $p \mid u_{\tau(p)}$, and ξ_p is given by the p-adic logarithm of $(\alpha\beta^{-1})^{\tau(p)} - 1$, with α and β being considered as elements of the quadratic extension $\mathbb{Q}_p\big(\sqrt{\Delta}\big)$.

Our main result is the following theorem, which provides formulas for $\nu_p(u_n)$ close in the spirit to Theorem 1.1.

Theorem 1.5. *If p is a prime number such that $p \nmid b$, then*

$$\nu_p(u_n) = \begin{cases} \nu_p(n) + \nu_p(u_p) - 1 & \text{if } p \mid \Delta,\ p \mid n, \\ 0 & \text{if } p \mid \Delta,\ p \nmid n, \\ \nu_p(n) + \nu_p(u_{p\tau(p)}) - 1 & \text{if } p \nmid \Delta,\ \tau(p) \mid n,\ p \mid n, \\ \nu_p(u_{\tau(p)}) & \text{if } p \nmid \Delta,\ \tau(p) \mid n,\ p \nmid n, \\ 0 & \text{if } p \nmid \Delta,\ \tau(p) \nmid n, \end{cases}$$

for each positive integer n.

Note that considering only prime numbers p which do not divide b is not a loss of generality. In fact, it is well-known that if $p \mid b$ then $p \nmid u_n$ for each positive integer n. The statement of Theorem 1.5 is quite complicated, but in the cases $p \geq 3$ and $p \geq 5$ we show that it can be simplified.

Corollary 1.6. *If $p \geq 3$ is a prime number such that $p \nmid b$, then*

$$\nu_p(u_n) = \begin{cases} \nu_p(n) + \nu_p(u_p) - 1 & \text{if } p \mid \Delta,\ p \mid n, \\ 0 & \text{if } p \mid \Delta,\ p \nmid n, \\ \nu_p(n) + \nu_p(u_{\tau(p)}) & \text{if } p \nmid \Delta,\ \tau(p) \mid n, \\ 0 & \text{if } p \nmid \Delta,\ \tau(p) \nmid n, \end{cases}$$

for each positive integer n.

Corollary 1.7. *If $p \geq 5$ is a prime number such that $p \nmid b$, then*

$$\nu_p(u_n) = \begin{cases} \nu_p(n) & \text{if } p \mid \Delta, \\ \nu_p(n) + \nu_p(u_{\tau(p)}) & \text{if } p \nmid \Delta,\ \tau(p) \mid n, \\ 0 & \text{if } p \nmid \Delta,\ \tau(p) \nmid n, \end{cases}$$

for each positive integer n.

With a little computation, it follows quite easily that Theorem 1.5, Corollary 1.6, and Corollary 1.7 are indeed generalizations of Theorem 1.1 and Corollary 1.3.

It is worth mentioning that some results of a paper by Young [7, Corollary 1 and Proposition 2] can be used to prove Theorem 1.5. However, we think that our proof has the peculiarity to use much more elementary tools (integer congruences) than those of Young's proofs (p-adic analysis in the ring of integers of a quadratic extension of $\mathbb{Q}_p$), so it might be interesting per se.

2. Preliminaries on Lucas Sequences

In this section we collect some basic facts about Lucas sequences. First of all, we have to justify our claim that in order to study $\nu_p(u_n)$ there is no loss of generality in assuming that $(u_n)_{n\geq 0}$ is nondegenerate. If $(u_n)_{n\geq 0}$ is a degenerate Lucas sequence, then it is known [5, pp. 5–6] that $(a,b) \in \{(\pm 2,-1),(\pm 1,-1),(0,\pm 1),(\pm 1,0)\}$ and in each of such cases $(u_n)_{n\geq 0}$ is either definitely periodic with values in $\{0,-1,+1\}$, or equal to $(n)_{n\geq 0}$, or equal to $((-1)^{n-1}n)_{n\geq 0}$, so in conclusion the study of $\nu_p(u_n)$ is trivial.

We recall that the *companion sequence* of $(u_n)_{n\geq 0}$ is the sequence of integers $(v_n)_{n\geq 0}$ defined by $v_0 = 1$, $v_1 = a$, and $v_n = av_{n-1} + bv_{n-2}$ for all integers $n \geq 2$. Moreover, it holds $v_n = \alpha^n + \beta^n$, for all nonnegative integers n. Note that, assuming $(u_n)_{n\geq 0}$ nondegenerate, we have $u_n \neq 0$ and $v_n \neq 0$, for all positive integers n. In particular, $\nu_p(u_n)$ is always finite.

The next lemma summarizes some basic divisibility properties of $(u_n)_{n\geq 0}$ and $(v_n)_{n\geq 0}$.

Lemma 2.1. *Let p be a prime number.*

(i) If $p \mid b$, then $p \nmid u_n$ and $p \nmid v_n$, for each positive integer n.
(ii) $u_p \equiv \left(\frac{\Delta}{p}\right) \bmod p$, where $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol.
(iii) If $p \nmid b$, then it is well-defined $\tau(p) := \min\{k \geq 1 : p \mid u_k\}$, which is called the rank of apparition of p in $(u_n)_{n\geq 0}$.
(iv) If $p \nmid b$, then for each positive integer n it holds $p \mid u_n$ if and only if $\tau(p) \mid n$.
(v) If $p \nmid b$, then $\tau(p) = p$ if and only if $p \mid \tau(p)$ if and only if $p \mid \Delta$.

Now we state a well-known formula relating u_n to binomial coefficients.

Lemma 2.2. *For each positive integer n,*

$$2^{n-1}u_n = \sum_{k=0}^{\lfloor (n-1)/2 \rfloor} \binom{n}{2k+1} a^{n-(2k+1)}\Delta^k.$$

Proof. The claim follows easily from (1.1), the binomial theorem, and the fact that we can take $\alpha = (a+\sqrt{\Delta})/2$ and $\beta = (a-\sqrt{\Delta})/2$. □

We conclude this section with a kind of "multiplication formula", which will be fundamental in our next arguments.

Lemma 2.3. *For all positive integers k and n, we have $u_{kn} = \widetilde{u}_k u_n$, where $(\widetilde{u}_m)_{m\geq 0}$ is the Lucas sequence with characteristic polynomial $\widetilde{f}(X) = X^2 - v_n X + (-b)^n$. Moreover, $\gcd(v_n,(-b)^n) = 1$, $(\widetilde{u}_m)_{m\geq 0}$ is nondegenerate, and the discriminant of $\widetilde{f}$ is $\widetilde{\Delta} = u_n^2\Delta$.*

Proof. We have $v_n = \alpha^n + \beta^n$ and $(-b)^n = (\alpha\beta)^n = \alpha^n\beta^n$. Therefore, $\widetilde{\alpha} := \alpha^n$ and $\widetilde{\beta} := \beta^n$ are the two roots of $\widetilde{f}$, so that $(\widetilde{u}_m)_{m\geq 0}$ is nondegenerate and

$$\widetilde{\Delta} = \left(\widetilde{\alpha} - \widetilde{\beta}\right)^2 = \left(\frac{\alpha^n - \beta^n}{\alpha - \beta} \cdot (\alpha - \beta)\right)^2 = u_n^2\Delta.$$

In particular $\widetilde{\Delta} \neq 0$, so that

$$u_{kn} = \frac{\alpha^{kn} - \beta^{kn}}{\alpha - \beta} = \frac{\widetilde{\alpha}^k - \widetilde{\beta}^k}{\widetilde{\alpha} - \widetilde{\beta}} \cdot \frac{\alpha^n - \beta^n}{\alpha - \beta} = \widetilde{u}_k u_n.$$

Finally, $\gcd(v_n, (-b)^n) = 1$, in the light of Lemma 2.1(i). □

3. Preliminaries for the Proof of Theorem 1.5

In this section, we derive some basic properties of the p-adic valuation of $(u_n)_{n\geq 0}$, that will be used later to prove Theorem 1.5.

Lemma 3.1. *If $p \geq 5$ is a prime number such that $p \nmid b$ and $p \mid \Delta$, then $\nu_p(u_p) = 1$.*

Proof. From Lemma 2.2 it follows that

$$\begin{aligned} 2^{p-1} u_p &\equiv \sum_{k=0}^{\lfloor (p-1)/2 \rfloor} \binom{p}{2k+1} a^{p-(2k+1)} \Delta^k \qquad (3.1) \\ &\equiv p a^{p-1} + \binom{p}{3} a^{p-3} \Delta + \cdots \equiv p a^{p-1} \pmod{p^2}, \end{aligned}$$

since $p \mid \Delta$ and $p \geq 5$ yields $p \mid \binom{p}{3}$. Moreover, having assumed that $p \nmid b$ and $p \geq 5$, we get from $p \mid \Delta = a^2 + 4b$ that $p \nmid a$, which, together with (3.1), implies $\nu_p(u_p) = \nu_p(2^{p-1} u_p) = 1$. □

Lemma 3.2. *If p is a prime number such that $p \nmid b$, then*

$$\nu_p(u_{p\tau(p)}) \geq \nu_p(u_{\tau(p)}) + 1, \qquad (3.2)$$

with equality if either $p \geq 5$, or $p = 3$ and $3 \nmid \Delta$.

Proof. From Lemma 2.3 we know that $u_{p\tau(p)} = \widetilde{u}_p u_{\tau(p)}$, where $(\tilde{u}_n)_{n\geq 0}$ is the Lucas sequence with characteristic polynomial $\tilde{f}(X) = X^2 - v_{\tau(p)} X + (-b)^{\tau(p)}$. Hence,

$$\nu_p(u_{p\tau(p)}) = \nu_p(u_{\tau(p)}) + \nu_p(\widetilde{u}_p).$$

Clearly $p \mid u_{\tau(p)}$, so a fortiori $p \mid \widetilde{\Delta} = u_{\tau(p)}^2 \Delta$, where $\tilde{\Delta}$ is the discriminant of $\tilde{f}(X)$. From Lemma 2.1(ii) we obtain that $p \mid \widetilde{u}_p$, and hence (3.2) holds.

As for the rest, we get from Lemma 3.1 that if $p \geq 5$ then $\nu_p(\widetilde{u}_p) = 1$ and thus in (3.2) we have equality. So suppose from now on that $p \geq 3$ and $3 \nmid \Delta$. We have, $\widetilde{u}_p = \widetilde{u}_3 = v_{\tau(3)}^2 - (-b)^{\tau(3)}$. On the one hand, if $3 \mid a$, then $\tau(3) = 2$, hence,

$$\widetilde{u}_3 = (a^2 + 2b)^2 - b^2 = (a^2 + b)(a^2 + 3b),$$

and $\nu_3(\widetilde{u}_3) = 1$, since $3 \nmid a^2 + b$ and $3 \,||\, a^2 + 3b$. On the other hand, if $3 \nmid a$, then

$$b \equiv 4b \not\equiv -a^2 \equiv -1 \pmod{3},$$

hence $b \equiv 1 \pmod{3}$, and $\tau(3) = 4$. Thus,

$$\widetilde{u}_3 = (a^4 + 4a^2 b + 2b^2)^2 - b^4 = (a^2 + b)(a^2 + 3b)(a^4 + 4a^2 b + b^2),$$

and again $\nu_3(\widetilde{u}_3) = 1$, since $3 \nmid (a^2 + b)(a^2 + 3b)$ and

$$3 \,||\, a^4 + 4a^2 b + b^2 = (a^2 + 2b)^2 - 3b^2.$$

Putting it all together, the proof is thus complete. □

We conclude this section with an easy lemma regarding the p-adic valuation of general linearly recurring sequences of integers.

Lemma 3.3. *Let $(r_n)_{n\geq 0}$ be a linearly recurring sequence of order $k \geq 2$ given by*

$$r_n = a_1 r_{n-1} + \cdots + a_k r_{n-k}, \tag{3.3}$$

for each integer $n \geq k$, where $r_0, \ldots, r_{k-1}$ and $a_1, \ldots, a_k$ are all integers. Suppose that there exists a prime number p such that $p \nmid a_k$ and

$$\min\{\nu_p(a_j) : 1 \leq j < k\} > \max\{\nu_p(r_m) - \nu_p(r_n) : 0 \leq m, n < k\}. \tag{3.4}$$

Then $\nu_p(r_n) = \nu_p(r_{(n \bmod k)})$, for each nonnegative integer n.

Proof. We proceed by induction on n. For $n = 0, \ldots, k-1$ the claim is obvious. Thus assume $n \geq k$ and that the claim holds for all the nonnegative integers less than n. By (3.4) and by induction hypothesis, for each $j = 1, \ldots, k-1$ we have

$$\begin{aligned}
\nu_p(a_j r_{n-j}) &= \nu_p(a_j) + \nu_p(r_{n-j}) \\
&= \nu_p(a_j) + \nu_p(r_{(n-j \bmod k)}) \\
&\quad > \nu_p(r_{(n-k \bmod k)}) - \nu_p(r_{(n-j \bmod k)}) + \nu_p(r_{(n-j \bmod k)}) \\
&= \nu_p(r_{(n-k \bmod k)}) \\
&= \nu_p(r_{n-k}) = \nu_p(a_k r_{n-k}).
\end{aligned}$$

Therefore, from (3.3) and from induction hypothesis, it follows that

$$\nu_p(r_n) = \nu_p(a_k r_{n-k}) = \nu_p(a_k r_{(n-k \bmod k)}) = \nu_p(r_{(n \bmod k)}),$$

which is our claim. □

4. Proof of Theorem 1.5 and Corollaries 1.6, 1.7

We are now ready to prove Theorem 1.5. The proof is substantially split in four lemmas.

Lemma 4.1. *If p is a prime number such that $p \nmid b$ and $p \mid \Delta$, then*

$$\nu_p(u_{pn}) = \nu_p(u_n) + \begin{cases} 1 & \text{if } p \mid n, \\ \nu_p(u_p) & \text{if } p \nmid n, \end{cases}$$

for each positive integer n.

Proof. From Lemma 2.3, we know that $u_{pn} = \widetilde{u}_p u_n$, where $(\widetilde{u}_m)_{m\geq 0}$ is the Lucas sequence with characteristic polynomial $X^2 - v_n X + (-b)^n$. Hence, $\nu_p(u_{pn}) = \nu_p(u_n) + \nu_p(\widetilde{u}_p)$, and we need to compute $\nu_p(\widetilde{u}_p)$. Note that $\widetilde{u}_p = \widetilde{u}_p(n)$ depends on n. If $p \geq 5$, since $p \mid \Delta$ and consequently $p \mid \widetilde{\Delta} = u_n^2 \Delta$, we get from Lemma 3.1 that $\nu_p(\widetilde{u}_p) = \nu_p(u_p) = 1$, thus the claim follows. Therefore, assume $p = 2$ or $p = 3$, and define $r_0 := p$ and $r_n := \widetilde{u}_p(n)$, for each positive integer n. Suppose first that $p = 2$. Hence, $r_n = \widetilde{u}_2 = v_n$, for each integer $n \geq 0$, so that

$$r_n = a r_{n-1} + b r_{n-2},$$

for all the integers $n \geq 2$. Furthermore, $2 \mid a$, since $2 \mid \Delta = a^2 + 4b$, and $2 \nmid b$, by hypothesis. Therefore, one can easily check that $(r_n)_{n\geq 0}$ satisfies the hypotheses of Lemma 3.3, and so

$$\nu_2(r_n) = \nu_2(r_{n \bmod 2}) = \begin{cases} \nu_2(r_0) & \text{if } 2 \mid n, \\ \nu_2(r_1) & \text{if } 2 \nmid n. \end{cases} = \begin{cases} 1 & \text{if } 2 \mid n, \\ \nu_2(u_2) & \text{if } 2 \nmid n. \end{cases}$$

Suppose now that $p = 3$. Then from (1.1) we obtain

$$r_n = \frac{u_{3n}}{u_n} = \frac{\alpha^{3n} - \beta^{3n}}{\alpha^n - \beta^n} = \alpha^{2n} + \beta^{2n} + (\alpha\beta)^n, \tag{4.1}$$

for all positive integers n. In fact, since $r_0 = 3$, it turns out that (4.1) holds also for $n = 0$. Hence, from (4.1) it follows that $(r_n)_{n\geq 0}$ is a third order linearly recurrent sequence with characteristic polynomial

$$(X - \alpha^2)(X - \beta^2)(X - \alpha\beta) = X^3 - u_3X^2 - bu_3X + b^3,$$

so that $r_n = u_3r_{n-1} + bu_3r_{n-2} - b^3r_{n-3}$, for each integer $n \geq 3$. Moreover, $r_0 = 3$, $r_1 = u_3$, and $r_2 = (a^2 + 3b)u_3$. Note that $3 \nmid a$, since $3 \mid \Delta = a^2 + 4b$ and $3 \nmid b$. Thus,

$$\nu_3(r_1) = \nu_3(r_2) = \nu_3(u_3).$$

Now $(r_n)_{n\geq 0}$ satisfies the hypotheses of Lemma 3.3, hence,

$$\begin{aligned}\nu_3(r_n) = \nu_3(r_{n \bmod 3}) &= \begin{cases}\nu_2(r_0) & \text{if } n \equiv 0 \pmod 3,\\ \nu_2(r_1) & \text{if } n \equiv 1 \pmod 3,\\ \nu_2(r_2) & \text{if } n \equiv 2 \pmod 3.\end{cases}\\ &= \begin{cases}1 & \text{if } 3 \mid n,\\ \nu_3(u_3) & \text{if } 3 \nmid n.\end{cases}\end{aligned}$$

This completes the proof. □

Lemma 4.2. *If p is a prime number such that $p \nmid b$ and $p \mid \Delta$, then*

$$\nu_p(u_{p^v}) = \begin{cases}0 & \text{if } v = 0,\\ v + \nu_p(u_p) - 1 & \text{if } v > 0,\end{cases}$$

for each nonnegative integer v.

Proof. We proceed by induction on v. For $v = 0$ and $v = 1$, the claim is trivial. Suppose $v \geq 2$ and that the claim is true for $v - 1$. Since $p \mid p^{v-1}$, by Lemma 4.1 we get

$$\nu_p(u_{p^v}) = \nu_p(u_{p\cdot p^{v-1}}) = \nu_p(u_{p^{v-1}}) + 1 = (v - 1) + \nu_p(u_p) - 1 + 1 = v + \nu_p(u_p) - 1,$$

which is our claim. □

Lemma 4.3. *If p is a prime number such that $p \nmid b$ and $p \mid \Delta$, then*

$$\nu_p(u_n) = \begin{cases}\nu_p(n) + \nu_p(u_p) - 1 & \text{if } p \mid n,\\ 0 & \text{if } p \nmid n,\end{cases}$$

for each positive integer n.

Proof. Write $n = mp^v$, where $v \geq 0$ is an integer and m is a positive integer such that $p \nmid m$. Let $(\widetilde{u}_\ell)_{\ell\geq 0}$ be the Lucas sequence with characteristic polynomial $X^2 - v_mX + (-b)^m$. From Lemma 2.3, we know that $u_n = \widetilde{u}_{p^v}u_m$, $u_{pm} = \widetilde{u}_p u_m$, and $p \mid \widetilde{\Delta} = u_m^2\Delta$. Moreover, since $p \mid \Delta$, we obtain from Lemma 2.1(v) that $\tau(p) = p \nmid m$. From Lemma 2.1(iv) it follows that $p \nmid u_m$, hence, $\nu_p(u_n) = \nu_p(\widetilde{u}_{p^v})$. If $v = 0$ then, obviously, $\nu_p(u_n) = \nu_p(\widetilde{u}_1) = \nu_p(1) = 0$. If $v \geq 1$ then we obtain from Lemmas 4.2 and 4.1 that

$$\begin{aligned}\nu_p(u_n) = \nu_p(\widetilde{u}_{p^v}) &= v + \nu_p(\widetilde{u}_p) - 1 = v + \nu_p(u_{pm}) - \nu_p(u_m) - 1\\ &= v + \nu_p(u_p) - 1 = \nu_p(n) + \nu_p(u_p) - 1,\end{aligned}$$

which is our claim. □

Lemma 4.4. *If p is a prime number such that $p \nmid b$, $p \nmid \Delta$, and $\tau(p) \mid n$, then*

$$\nu_p(n) = \begin{cases} \nu_p(n) + \nu_p(u_{p\tau(p)}) - 1 & \text{if } p \mid n, \\ \nu_p(u_{\tau(p)}) & \text{if } p \nmid n, \end{cases}$$

for each positive integer n.

Proof. Write $n = m\tau(p)$, where m is a positive integer. Let $(\widetilde{u}_\ell)_{\ell \geq 0}$ be the Lucas sequence with characteristic polynomial $X^2 - v_{\tau(p)}X + (-b)^{\tau(p)}$. From Lemma 2.3, we know that $u_n = \widetilde{u}_m u_{\tau(p)}$, $u_{p\tau(p)} = \widetilde{u}_p u_{\tau(p)}$, and $p \mid \widetilde{\Delta} = u_{\tau(p)}^2 \Delta$. Since $p \nmid \Delta$, it follows from Lemma 2.1(v) that $p \nmid \tau(p)$ and $\nu_p(m) = \nu_p(n)$. On the one hand, if $p \mid n$ then $p \mid m$ and by Lemma 4.3 we get

$$\begin{aligned} \nu_p(u_n) &= \nu_p(\widetilde{u}_m) + \nu_p(u_{\tau(p)}) \\ &= \nu_p(m) + \nu_p(\widetilde{u}_p) - 1 + \nu_p(u_{\tau(p)}) \\ &= \nu_p(m) + \nu_p(u_{p\tau(p)}) - \nu_p(u_{\tau(p)}) - 1 + \nu_p(u_{\tau(p)}) \\ &= \nu_p(n) + \nu_p(u_{p\tau(p)}) - 1. \end{aligned}$$

On the other hand, if $p \nmid n$ then $p \nmid m$, and again by Lemma 4.3 we get

$$\nu_p(u_n) = \nu_p(\widetilde{u}_m) + \nu_p(u_{\tau(p)}) = \nu_p(u_{\tau(p)}),$$

as claimed. □

At this point, Theorem 1.5 follows immediately from Lemmas 4.3, 4.4, and 2.1(iv). Moreover, Corollaries 1.6 and 1.7 are direct consequences of Theorem 1.5 and Lemmas 3.1 and 3.2.

Acknowledgements

The author is grateful to Salvatore Tringali (Texas A&M University of Qatar) for many useful comments. The author also thanks the anonymous referee for pointing out the existence of Young's paper.

References

[1] R. D. Carmichael, *On the numerical factors of certain arithmetic forms*, Amer. Math. Monthly, **16.10** (1909), 153–159.
[2] S. Cuellar and J. A. Samper, *A nice and tricky lemma (lifting the exponent)*, Mathematical Reflection, **3** (2007).
[3] T. Lengyel, *The order of the Fibonacci and Lucas numbers*, The Fibonacci Quarterly, **33.3** (1995), 234–239.
[4] É. Lucas, *Théorie des fonctions numériques simplement periodiques*, Amer. J. Math., **1** (1878), 184–196, 197–240, 289–321.
[5] P. Ribenboim, *My Numbers, My Friends: Popular Lectures on Number Theory*, Universitext – Springer-Verlag, Springer, 2000.
[6] M. Ward, *The linear p-adic recurrence of order two*, Illinois J. Math., **6** (1962), 40–52.
[7] P. T. Young, *p-adic congruences for generalized Fibonacci sequences*, The Fibonacci Quarterly, **32.1** (1994), 2–10.

MSC2010: 11A99, 11B39, 11B37

Department of Mathematics, Università degli Studi di Torino, Via Carlo Alberto 10, 10123 Torino, Italy
E-mail address: carlo.sanna.dev@gmail.com