THE p-ADIC VALUATION OF LUCAS SEQUENCES WHEN p IS A SPECIAL PRIME

CHRISTIAN BALLOT

ABSTRACT. The behavior of the p-adic valuation of the terms of Lucas sequences has basically been known since the seminal work of Lucas in 1878, although it has been revisited many times with partial or complete results. However, the assumption always seems to be that the parameters P and Q of the recursion are coprime, i.e., that the sequence is regular. We complete the picture by evaluating the valuation of Lucas sequences with respect to a special prime, i.e., one dividing P and Q.

1. INTRODUCTION

Given two integers P and Q, $Q \neq 0$, one defines a pair of Lucas sequences $\{U, V\}$. Both U and V satisfy the second-order linear recursion

$$X_{n+2} = PX_{n+1} - QX_n, \tag{1}$$

for all $n \geq 0$, $X = U$ or V. The *fundamental* sequence U has initial values $U_0 = 0$ and $U_1 = 1$, whereas the *companion*, or *associate* sequence V satisfies $V_0 = 2$ and $V_1 = P$. Therefore, both U and V have integral terms. Lucas studied many properties of these two sequences in his seminal memoir [6]. Even today, they continue to be an object of study and curiosity for many amateurs and researchers and have found numerous applications. We refer the reader to the book [9] and, for their arithmetic properties, to the fourth chapter of that book.

The *rank of appearance* of a prime p is the smallest index $n > 0$, if it exists, such that $p \mid U_n$. A *regular* prime p is one that does not divide $\gcd(P, Q)$. All primes $p \nmid Q$ admit a rank of appearance denoted by $\rho = \rho(p)$. The *rank exponent* ν of p is the full exponent of p that divides U_ρ, i.e., the p-adic valuation of U_ρ, $\nu_p(U_\rho)$, which we also write as $p^\nu \,||\, U_\rho$. Note that if $U_\rho = 0$, then $\nu = +\infty$. A regular prime that divides Q does not have a rank.

If $p \nmid Q$, then the p-adic valuation of all U and V terms is well-known (see e.g., [2, 1, 4, 5, 6, 8, 9]). For instance, if $p \geq 3$, then for all $n \geq 1$

$$\nu_p(U_n) = \begin{cases} 0, & \text{if } \rho \nmid n; \\ (\nu - 1) + \nu_p(n), & \text{if } \rho \mid n. \end{cases} \tag{2}$$

With a few caveats, the same phenomenon occurs for the prime $p = 2$. The valuation is positive if and only if $\rho \mid n$, and, with a starting value of ν for the valuation of U_ρ, higher valuations appear exactly as they enter n in $U_{\rho n}$, a phenomenon known as the *lifting-of-the-exponent*.

It is worth stressing that the hypothesis that U be regular, i.e., that $\gcd(P, Q) = 1$, is not necessary and that the p-adic valuation of U and V, $p \nmid Q$, obeys the same rules regardless of the value of $\gcd(P, Q)$.

In this note, we address the problem of determining the p-adic valuation of the terms of Lucas sequences when p is a *special* prime, that is, one that divides $\gcd(P, Q)$. The exponents of p in P and Q are denoted by a and b throughout. Thus, we have $p^a \,||\, P$ and $p^b \,||\, Q$, where a and b are positive integers, unless $P = 0$ in which case $a = +\infty$. It is clear from (1) that

these p-adic valuations will accrue as n gets larger. Whatever the positive values of a and b, there is an obvious lower bound for $\nu_p(U_n)$ given in the next theorem.

Theorem 1.1. *Suppose p is a special prime, i.e., p divides* $\gcd(P,Q)$. *Then,*

$$\nu_p(U_n) \geq \left\lfloor \frac{n}{2} \right\rfloor$$

for all $n \geq 1$.

Proof. We proceed by induction on n after noting that as $U_1 = 1$ and $U_2 = P$, we clearly have $\nu_p(U_1) = 0 \geq \lfloor \frac{1}{2} \rfloor$ and $\nu_p(U_2) \geq 1 = \lfloor \frac{2}{2} \rfloor$. Suppose $n \geq 3$ and $\nu_p(U_k) \geq \lfloor \frac{k}{2} \rfloor$ for $k = n-2$ and $n-1$. Then,

$$\begin{aligned} \nu_p(U_n) &\geq \min\{\nu_p(PU_{n-1}), \nu_p(QU_{n-2})\} \\ &\geq 1 + \min\{\nu_p(U_{n-1}), \nu_p(U_{n-2})\} \\ &= 1 + \left\lfloor \frac{n-2}{2} \right\rfloor = \left\lfloor \frac{n}{2} \right\rfloor. \end{aligned}$$

□

Theorem 1.1 marks a clear difference with regular primes as the limit of $\nu_p(U_n)$ tends to infinity as $n \to \infty$. The real question is whether, as for regular primes, a complete simple description of these valuations can be achieved. Lurking behind the steady growth, is there also a full regularity and an occasional presence of the lifting of the exponent? We were not sure. Some numerical experiments such as the following were definitely helpful.

I. $(P,Q) = (6,3),\ p = 3,\ a = b = 1$

n	2	3	4	5	6	7	8	9	10	11	12	13
$\nu_3(U_n)$	1	1	2	2	5	3	4	4	5	5	8	6

n	14	15	16	17	18	19	20	21	22	23	24
$\nu_3(U_n)$	7	7	8	8	12	9	10	10	11	11	14

– TABLE 1 –

Table 1 seems to suggest the conjecture

$$\nu_3(U_n) = \left\lfloor \frac{n}{2} \right\rfloor + \big(1 + \nu_3(n)\big) \cdot [6 \mid n],$$

where we used the Iverson symbol '$[-]$' defined in (3).

II. $(P,Q) = (5,10),\ p = 5,\ a = b = 1$

n	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
$\nu_5(U_n)$	2	2	3	3	4	4	6	5	6	6	7	7	8	8	9	9	11	10

n	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37
$\nu_5(U_n)$	11	11	12	12	13	13	14	14	16	15	16	16	17	17	18	18

n	38	39	40	41	42	43	44	45	46	47	48	49	50	51
$\nu_5(U_n)$	19	19	21	20	21	21	22	22	23	23	24	24	27	25

– TABLE 2 –

Table 2 suggests the conjecture

$$\nu_5(U_n) = \left\lfloor \frac{n}{2} \right\rfloor + \nu_5(n) \cdot [10 \mid n].$$

Although we give the complete and compact result we sought within this introduction, we retained the sinuous order in which we addressed the problem in Section 2, where proofs are given. Instead of only adopting, as usual, the somewhat dull theorem-followed-by-proof presentation, we left much of the research scaffolding in place, increasing the length of the note — proofs can be shortened, some omitted — and on occasions making our foolishness conspicuous, but hopefully making for a more pleasant read.

Here is our main theorem, a summary of the various partial theorems of Section 2.

Theorem 1.2. *Suppose $U(P,Q)$ is a fundamental Lucas sequence, where $P = p^a P'$, $Q = p^b Q'$, $p \nmid P'Q'$ for some prime p and positive a and b with possibly $a = +\infty$. Then for all $n \geq 1$,*

$$\nu_p(U_n) = \begin{cases} (n-1)a, & \textbf{\textit{if}}\ b > 2a; \\ (n-1)a + \nu_p(U'_n), & \textbf{\textit{if}}\ b = 2a, \end{cases}$$

*where $U' = U(P',Q')$, whereas, **for** $b < 2a$, we find that*

$$\begin{aligned} \nu_p(U_{2n+1}) &= bn,\ (n \geq 0),\ \textit{and} \\ \nu_p(U_{2n}) &= bn + (a-b) + \nu_p(n) + \lambda_n, \end{aligned}$$

where

$$\lambda_n = \begin{cases} \nu_p(P'^2 - Q'), & \textit{if } 2 \leq p \leq 3,\ 2a = b+1,\ \textit{and } p \mid n; \\ 0, & \textit{otherwise.} \end{cases}$$

Surprisingly, perhaps, at first sight, the prime 2 and the prime 3 show idiosyncracies not shared by other primes. The prime 3, as a regular prime, does not stand out, only the prime 2 does. But, this is not entirely true. The rank exponent of a regular prime $p \geq 5$ that divides $P^2 - 4Q$ is always 1. Only the primes 2 and 3 do not necessarily follow this rule. Note that special primes divide $P^2 - 4Q$. We point out that our results include the case of *degenerate* Lucas sequences, i.e., sequences for which there exists an $n > 0$ with $U_n = 0$. For instance, if $\lambda_n = +\infty$, then $U_{2n} = 0$, a degenerate case the theorem allows.

Because $U_{2n} = U_n V_n$, we see that $\nu_p(V_n) = \nu_p(U_{2n}) - \nu_p(U_n)$. Hence, we obtain the immediate corollary.

Corollary 1.3. *With the same notation and hypotheses as in Theorem 1.2, for all $n \geq 1$ we have*

$$\nu_p(V_n) = \begin{cases} na, & \textbf{\textit{if}}\ b > 2a; \\ na + \nu_p(V'_n), & \textbf{\textit{if}}\ b = 2a, \end{cases}$$

*where $V' = V(P',Q')$, whereas, **for** $b < 2a$, we obtain*

$$\begin{aligned} \nu_p(V_{2n+1}) &= bn + a + \nu_p(2n+1) + \mu_n,\ (n \geq 0),\ \textit{and} \\ \nu_p(V_{2n}) &= \begin{cases} bn, & \textit{if } p \geq 3; \\ bn+1, & \textit{if } p = 2 \textit{ and, if } 2a > b+1 \textit{ or } 2 \mid n; \\ bn + 1 + \nu_2(P'^2 - Q'), & \textit{if } p = 2,\ 2a = b+1 \textit{ and } 2 \nmid n, \end{cases} \end{aligned}$$

where

$$\mu_n = \begin{cases} \nu_p(P'^2 - Q'), & \textit{if } p = 3,\ 2a = b+1,\ \textit{and } n \equiv 1 \pmod 3; \\ 0, & \textit{otherwise.} \end{cases}$$

We use the Iverson symbol $[-]$, a boolean function that may only take two values 1 or 0. If $\mathcal{P}$ is a statement, then

$$[\mathcal{P}] = \begin{cases} 1, & \text{if } \mathcal{P} \text{ is true;} \\ 0, & \text{otherwise.} \end{cases} \tag{3}$$

There are two formulas of Lucas that we use in Section 2. Lucas [7, p. 312] observes that each U_n, $n \geq 1$ is a polynomial in P and Q, which is homogeneous in P and $\sqrt{Q}$ of degree $n-1$. We give these polynomials for $1 \leq n \leq 5$ below.

n	1	2	3	4	5
U_n	1	P	P^2-Q	P^3-2PQ	$P^4-3P^2Q+Q^2$

Lucas [6, p. 207] derives a formula for these polynomials, namely for all $n \geq 1$.

$$U_n = \Phi(n) = \sum_{k=0}^{\lfloor (n-1)/2 \rfloor} (-1)^k \binom{n-k-1}{k} P^{n-1-2k} Q^k. \tag{4}$$

(One may check that $(\Phi(n))$ satisfies recursion (1) and that $\Phi(1) = 1 = U_1$ and $\Phi(2) = P = U_2$.)

Secondly, we recall that if $P^2 - 4Q \neq 0$, then

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad \text{and} \quad V_n = \alpha^n + \beta^n,$$

where α and β are the zeros of $x^2 - Px + Q$. Thus, we see that

$$U_{kn}(P,Q) = \frac{\alpha^{kn} - \beta^{kn}}{\alpha - \beta} = \frac{\alpha^k - \beta^k}{\alpha - \beta} \cdot \frac{\alpha^{kn} - \beta^{kn}}{\alpha^k - \beta^k} = U_k(P,Q) \cdot U_n(V_k, Q^k). \tag{5}$$

Note that the identity $U_{kn}(P,Q) = U_k(P,Q) \cdot U_n(V_k, Q^k)$ remains valid if $P^2 - 4Q = 0$, when $U_n(P,Q) = n\alpha^{n-1}$.

2. The Proofs

There are two cases, namely $b > 2a$ and $b = 2a$, where describing the valuations of all U_n is a simple task.

The case $b > 2a$.

Theorem 2.1. *Suppose p divides P and Q with $p^a \,||\, P$ and $p^b \,||\, Q$ where $b > 2a$. Then,*

$$\nu_p(U_n) = (n-1)a$$

for all $n \geq 1$.

Proof. We proceed by induction on n. Clearly, $\nu_p(U_1) = 0 = (1-1)a$ and $\nu_p(U_2) = \nu_p(P) = a = (2-1)a$.

Assuming $n \geq 3$ and $\nu_p(U_k) = (k-1)a$ for $k = n-1$ and $n-2$, we obtain

$$\begin{aligned} \nu_p(PU_{n-1}) &= a + (n-2)a = (n-1)a, \\ \nu_p(QU_{n-2}) &= b + (n-3)a > 2a + (n-3)a = (n-1)a. \end{aligned}$$

Thus, $\nu_p(PU_{n-1}) < \nu_p(QU_{n-2})$. Hence,

$$\nu_p(U_n) = \nu_p(PU_{n-1} - QU_{n-2}) = \nu_p(PU_{n-1}) = (n-1)a,$$

finishing the proof. □

For **the case** $b = 2a$, the p-adic valuation of U_n is expressed in terms of the p-adic valuation of another Lucas sequence $U' = U(P', Q')$ with respect to which p is regular.

Theorem 2.2. *Suppose p is a special prime with $p^a \,||\, P$ and $p^b \,||\, Q$ and $b = 2a$. Then for all $n \geq 1$,*

$$\nu_p(U_n) = (n-1)a + \nu_p(U'_n),$$

where $U' = U(P', Q')$, $P = p^a P'$, and $Q = p^b Q'$.

Proof. By (4), for all $n \geq 1$, we find that

$$\begin{aligned} U_n &= \sum_{k\geq 0} (-1)^k \binom{n-k-1}{k} p^{(n-1-2k)a} (P')^{n-1-2k} \cdot p^{2ka} (Q')^k \\ &= p^{(n-1)a} \sum_{k\geq 0} (-1)^k \binom{n-1-k}{k} (P')^{n-1-2k} (Q')^k = p^{(n-1)a} \Phi_n(P', Q') = p^{(n-1)a} U'_n, \end{aligned}$$

which proves the claim. □

Finally, we tackle **the case** $b < 2a$.

Theorem 2.3. *Suppose p is a special prime, $P = p^a P'$, $Q = p^b Q'$ with $b < 2a$ and $p \nmid P'Q'$. Then, for all $n \geq 0$,*

$$\nu_p(U_{2n+1}) = bn. \tag{6}$$

If $p \geq 5$, then we find that

$$\nu_p(U_{2n}) = bn + (a-b) + \nu_p(n) \tag{7}$$

for all $n \geq 1$. Moreover, whether $p \geq 5$, or $p = 2$ or 3,

$$\nu_p(U_{2n}) = bn + (a-b) \tag{8}$$

for all $n \geq 1$ prime to p. For $p = 3$, equation (7), i.e.,

$$\nu_3(U_{2n}) = bn + (a-b) + \nu_3(n) \tag{9}$$

also holds for all $n \geq 1$, if $2a > b+1$ or if $Q' \equiv 2 \pmod 3$. But if $2a = b+1$, $Q' \equiv 1 \pmod 3$, and $3 \mid n$, then

$$\nu_3(U_{2n}) > bn + (a-b) + \nu_3(n). \tag{10}$$

Proof. By (4), we obtain

$$U_{2n+1} = \sum_{k=0}^{n} (-1)^k \binom{2n-k}{k} P^{2n-2k} Q^k.$$

The p-adic valuation of $P^{2n-2k}Q^k$ is $2na - (2a-b)k$, a strictly decreasing function of k. Hence, it reaches a minimum only at $k = n$. As $\binom{2n-n}{n} = 1$, $\nu_p(U_{2n+1})$ is the value of $2na - (2a-b)k$ at $k = n$, i.e., bn. This proves (6).

Again using (4), we find that

$$U_{2n} = \sum_{k=0}^{n-1} (-1)^k \binom{2n-1-k}{k} P^{2n-1-2k} Q^k.$$

Putting $\ell = n - k$, we get

$$\begin{aligned} U_{2n} &= \sum_{\ell=1}^{n} (-1)^{n-\ell} \binom{n+\ell-1}{n-\ell} P^{2\ell-1} Q^{n-\ell} \\ &= \sum_{\ell=1}^{n} (-1)^{n-\ell} a_\ell P^{2\ell-1} Q^{n-\ell}, \end{aligned}$$

where

$$a_\ell = \binom{n+\ell-1}{2\ell-1}. \tag{11}$$

Now, the p-adic valuation of $P^{2\ell-1}Q^{n-\ell}$ is $(2a-b)\ell + nb - a$, a strictly increasing function of ℓ. Thus, it is minimal for $\ell = 1$ and equal to

$$nb + (a-b).$$

Clearly, if we find out that

$$\nu_p(a_1 PQ^{n-1}) < \nu_p(a_\ell P^{2\ell-1} Q^{n-\ell}) \text{ for all } 2 \le \ell \le n, \tag{12}$$

then

$$\nu_p(U_{2n}) = \nu_p(a_1 PQ^{n-1}) = \nu_p(a_1) + nb + (a-b).$$

Since $a_1 = n$, condition (12) certainly holds if $p \nmid n$. In particular, (8) holds.

Thus, from now on we assume $p \mid n$. A necessary condition for (12) to fail is the existence of some ℓ, $2 \le \ell \le n$, for which

$$\nu_p(a_\ell) + (2a-b)\ell + nb - a \le \nu_p(a_1) + (2a-b) + nb - a,$$

i.e., an ℓ such that

$$\nu_p\left(\frac{a_1}{a_\ell}\right) \ge (2a-b)(\ell-1). \tag{13}$$

Observing that for all $\ell \ge 2$

$$\begin{aligned} a_\ell &= \frac{(n+\ell-1)\dots(n-\ell+1)}{(2\ell-1)!} \\ &= \frac{(n+\ell-1)(n-\ell+1)}{(2\ell-2)(2\ell-1)} a_{\ell-1} \\ &= \frac{n^2-(\ell-1)^2}{2(\ell-1)(2\ell-1)} a_{\ell-1}, \end{aligned}$$

we obtain that

$$\frac{a_1}{a_\ell} = \frac{2^{\ell-1}(\ell-1)! \prod_{k=1}^{\ell-1}(2k+1)}{\prod_{k=1}^{\ell-1}(n^2-k^2)}. \tag{14}$$

Since $(\ell-1)!$ divides any product of $\ell-1$ consecutive integers, it divides $\prod_{k=1}^{\ell-1}(n^2-k^2)$. Therefore, for p odd,

$$\nu_p\big(\frac{a_1}{a_\ell}\big) \le \nu_p\big(\prod_{k=1}^{\ell-1}(2k+1)\big) = \nu_p\big((2\ell-1)!\big) - \nu_p\big((\ell-1)!\big).$$

Combining the above inequality with (13), we see that we must have

$$\ell - 1 \le (2a-b)(\ell-1) \le \nu_p\big((2\ell-1)!\big) - \nu_p\big((\ell-1)!\big). \tag{15}$$

However, using the (near-obvious) formula of Legendre for the p-adic valuation of factorials, namely

$$\nu_p(n!) = \sum_{k\geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor,$$

we see that

$$\nu_p((2\ell-1)!) < \sum_{k\geq 1} \frac{2\ell-1}{p^k} = \frac{2\ell-1}{p-1} \leq \begin{cases} \frac{2\ell}{4} \leq \ell-1, & \text{if } p \geq 5; \\ \frac{2\ell-1}{2} < \ell, & \text{if } p = 3 \end{cases} \tag{16}$$

for all $2 \leq \ell \leq n$. If $p \geq 5$, then, by (15) and (16), we must have

$$\ell - 1 \leq \nu_p\big((2\ell-1)!\big) < \ell - 1,$$

a contradiction. Therefore, (7) holds. If $p = 3$ and (12) fails, then by (15) and (16), we see that

$$\ell - 1 \leq (2a-b)(\ell-1) \leq \nu_3\big((2\ell-1)!\big) - \nu_3\big((\ell-1)!\big) \leq \ell - 1 - \nu_3\big((\ell-1)!\big)$$

for some $2 \leq \ell \leq n$. This forces $2a - b = 1$ and $\nu_3\big((\ell-1)!\big) = 0$. Thus, $2 \leq \ell \leq 3$. But, by (11), $a_3 = \binom{n+2}{5}$ and $3 \mid n$ implies that $\nu_3(a_1/a_3) = 1$. So for $\ell = 3$, (13) is not satisfied because $(2a-b)(\ell-1) = 2$. For $\ell = 2$, $a_2 = \binom{n+1}{3}$, and $\nu_3(a_2) = \nu_3(a_1) - 1$. Thus, (13) is satisfied. The 3-adic valuation of U_{2n} is then often decided by

$$nPQ^{n-1} - a_2P^3Q^{n-2},$$

i.e., if $\nu_3(nPQ^{n-1} - a_2P^3Q^{n-2}) = \nu_3(nPQ^{n-1})$, then (9) holds, whereas if $\nu_3(nPQ^{n-1} - a_2P^3Q^{n-2}) > \nu_3(nPQ^{n-1})$, then (10) is true. It remains to find explicit conditions under which the former case holds. Now, as $2a = b + 1$,

$$\begin{aligned} nPQ^{n-1} - a_2P^3Q^{n-2} &= nPQ^{n-2}\left(Q - \frac{n^2-1}{6}P^2\right) \\ &= nPQ^{n-2}\left(3^bQ' - \frac{n^2-1}{2}3^{2a-1}P'^2\right) \\ &= \frac{n}{2}3^{nb+a-b}P'Q'^{n-2}\big(2Q' - (n^2-1)P'^2\big), \end{aligned}$$

implying that

$$\nu_3(nPQ^{n-1} - a_2P^3Q^{n-2}) = \nu_3(n) + nb + (a-b) + \nu_3(2Q' + P'^2 - n^2P'^2).$$

As 3^2 divides $n^2P'^2$, we see our two final claims, (9) and (10), hold. □

Numerical experiments seem to suggest that simple regularity also rules the 3-adic valuation of the terms U_{2n} when $3 \mid n$, $2a = b + 1$, and $Q' \equiv 1 \pmod 3$. Hence, we hope to improve on inequality (10). Besides Table 1, we give numerical tables for a couple of additional cases.

III. $(P, Q) = (3, 12),\ a = b = 1,\ Q' = 4 \equiv 1 \pmod 3$

n	3	6	9	12	15	18	21	24	27
$\nu_3(U_{2n})$	5	8	12	14	17	21	23	26	31

– TABLE 3 –

IV. $(P,Q) = (36,27),\ a = 2;\ b = 3,\ Q' = 1$

n	3	6	9	12	15	18	21	24	27
$\nu_3(U_{2n})$	10	19	29	37	46	56	64	73	84

– TABLE 4 –

Table 3 suggests we conjecture for $U(3,12)$,

$$\nu_3(U_{2n}) = n + \big(1 + \nu_3(n)\big) \cdot [3 \mid n],$$

whereas Table 4 suggests for $U(36,27)$ the conjecture

$$\nu_3(U_{2n}) = 3n - 1 + \big(1 + \nu_3(n)\big) \cdot [3 \mid n].$$

So the question arises as to whether one may replace (10) with

$$\nu_3(U_{2n}) = bn + (a-b) + (c + \nu_3(n)) \cdot [3 \mid n],$$

for some $c \geq 1$?

Thus, we suppose that $2a = b+1$, $Q' \equiv 1 \pmod 3$, and $3 \mid n$. Putting $n = 3k$, we recall that, by (5),

$$U_{2n} = U_{6k} = U_6(P,Q) \cdot U_k(V_6, Q^6). \tag{17}$$

However, the Lucas sequence $U' = U(V_6, Q^6)$ is such that $a' = \nu_3(V_6) = 3b$ and $b' = \nu_3(Q^6) = 6b$. That is, we are in the case $b' = 2a'$. Indeed, let us check that $\nu_3(V_6) = 3b$. We have $V_6 = V_3^2 - 2Q^3$ and $V_3 = P(P^2 - 3Q)$. Since $\nu_3(V_3) = a + 2a + \nu'$, where $\nu' = \nu_3(P'^2 - Q')$,

$$\nu_3(V_3^2) = 6a + 2\nu' \geq 3b + 3 + 2 = 3b + 5, \tag{18}$$

whereas $\nu_3(2Q^3) = 3b$. Thus, using Theorem 2.2, we find that

$$\nu_3(U'_k) = (k-1)a' + \nu_3\big(U_k(V_6/3^{3b}, Q^6/3^{6b})\big).$$

We claim the rank of 3 in $U(V_6/3^{3b}, Q^6/3^{6b})$ is 3 and its rank exponent is 1. Indeed, $Q^6/3^{6b} = Q'^6$ and $U_3(V_6/3^{3b}, Q'^6) = (V_6/3^{3b})^2 - Q'^6$. A simple calculation gives

$$\left(\frac{V_6}{3^{3b}}\right)^2 - Q'^6 = \frac{P^4(P^2-3Q)^2}{3^{6b}} - 4Q'^3\frac{P^2(P^2-3Q)^2}{3^{3b}} + 3Q'^6. \tag{19}$$

By (18), the 3-adic valuation of the first two terms on the right side of (19) is at least 5, but the term $3Q'^6$ has 3-adic valuation 1, proving our claims. We go back to evaluating $\nu_3(U_{2n})$ using (17). Therefore, again as $b' = 2a'$, we deduce from Theorem 2.2 and from (2) that

$$\nu_3(U'_k) = (k-1)a' + (1-1) + \nu_3(k).$$

Since $U_6 = U_3V_3 = (P^2 - Q)V_3$, $\nu_3(U_6) = b + (3a + \nu')$. Hence,

$$\begin{aligned} \nu_3(U_{2n}) &= \nu_3(U_6) + \nu_3(U'_k) = (3a + b + \nu') + ((k-1)3b + \nu_3(k)) \\ &= 3a - 2b + nb + \nu' + \nu_3(k) = bn + (a-b) + 1 + \nu' + (\nu_3(n) - 1) \\ &= bn + (a-b) + \nu_3(n) + \nu'. \end{aligned}$$

Combining this result with (9) we have the special theorem.

Theorem 2.4. *Suppose 3 is a special prime, $P = 3^aP'$, $Q = 3^bQ'$ with $b < 2a$ and $3 \nmid P'Q'$. Then for all $n \geq 1$, we find that*

$$\nu_3(U_{2n}) = bn + (a-b) + \nu_3(n) + \nu_3(P'^2 - Q') \cdot [2a = b+1] \cdot [3 \mid n],$$

with the use of the Iverson symbol.

In the course of proving Theorem 2.3, we omitted to treat the 2-adic valuation of terms U_{2n} when $2 \mid n$. Indeed, there seemed to be a bifurcation in evaluating $\nu_p(a_1/a_\ell)$ from its expression in (14), depending on whether p were odd or even. This is not as true as it may seem. Indeed, we recall that

$$U_{2n} = \sum_{\ell=1}^{n} (-1)^{n-\ell} a_\ell P^{2\ell-1} Q^{n-\ell},$$

with $a_\ell = \binom{n+\ell-1}{2\ell-1}$. We usually expect the 2-adic valuation of U_{2n} to be given by the first term $a_1 PQ^{n-1}$. For this to fail, we saw that condition (13) had to hold for some $2 \le \ell \le n$. However, from (14), we obtain

$$\begin{aligned} \nu_2(a_1/a_\ell) &= \ell - 1 + \nu_2\big((\ell-1)!\big) - \nu_2\Big(\prod_{k=1}^{\ell-1}(n^2-k^2)\Big) \\ &\le \ell - 1 + \nu_2\big((\ell-1)!\big) - 2\nu_2\big((\ell-1)!\big) \\ &= \ell - 1 - \nu_2\big((\ell-1)!\big), \end{aligned}$$

because the product $\prod_{k=1}^{\ell-1}(n^2-k^2)$ contains two factors, each a product of $\ell-1$ consecutive integers. That is, each such factor is a multiple of $(\ell-1)!$. Using (13), we must have the double inequality

$$\ell - 1 \le (2a-b)(\ell-1) \le \ell - 1 - \nu_2\big((\ell-1)!\big),$$

which may only hold if $2a-b=1$ and $\nu_2\big((\ell-1)!\big) = 0$, i.e., if $2a-b=1$ and $\ell = 2$. Therefore, if $2a \ge b+2$, then

$$\nu_2(U_{2n}) = \nu_2(a_1 PQ^{n-1}) = \nu_2(n) + a + (n-1)b = nb + (a-b) + \nu_2(n). \tag{20}$$

Thus, if $2a = b+1$, then $\nu_2(U_{2n})$ is often determined by the 2-adic valuation of $nPQ^{n-1} - \frac{(n^2-1)n}{6} P^3 Q^{n-2}$. Instead, we turn to the method used for $p=3$ in (17). Thus, we write, with $n = 2k$,

$$U_{2n} = U_{4k} = U_4 \cdot U_k(V_4, Q^4).$$

As $U_4 = P(P^2-2Q)$ and $2a = b+1$, we see that $\nu_2(U_4) = a + 2a + \nu_2(P'^2 - Q')$, where P' and Q' are defined as in Theorems 2.2 or 2.3. Noting that $\nu_2(P^4) = 2b+2$, $\nu_2(4P^2Q) = 2b+3$, and $\nu_2(2Q^2) = 2b+1$, we see that $a' := \nu_2(V_4) = 2b+1$, since $V_4 = P^4 - 4P^2Q + 2Q^2$. Now $b' := \nu_2(Q^4) = 4b$. Hence, the prime 2 is special in $U(V_4, Q^4)$ with $2a' = 4b+2 \ge b'+2$. Therefore, using (6) and (20) and writing $\nu' = \nu_2(P'^2 - Q')$, we obtain

$$\begin{aligned} \nu_2(U_{2n}) &= \nu_2(U_4) + \nu_2\big(U_k(V_4, Q^4)\big) \\ &= (3a+\nu') + \begin{cases} b'(k-1)/2, & \text{if } 2 \nmid k; \\ b'k/2 + (a'-b') + \nu_2(k/2), & \text{if } 2 \mid k; \end{cases} \\ &= a+b+1+\nu' + \begin{cases} bn - 2b, & \text{if } 2 \nmid k; \\ bn + (1-2b) + (\nu_2(n) - 2), & \text{if } 2 \mid k; \end{cases} \\ &= bn + (a-b) + \nu_2(n) + \nu'. \end{aligned}$$

With the next theorem, we complete the description of the p-adic valuation of terms of a Lucas sequence U in all cases. The next theorem combines (8) and the information we just gathered for n even.

Theorem 2.5. *Suppose 2 is special, $P = 2^a P'$, $Q = 2^b Q'$ with $b < 2a$ and $2 \nmid P'Q'$. Then for all positive n, we find that*

$$\nu_2(U_{2n}) = bn + (a-b) + \nu_2(n) + \nu_2(P'^2 - Q') \cdot [2a = b+1] \cdot [2 \mid n],$$

with the use of the Iverson symbol.

(Note that $\nu_2(U_{2n})$ may be $+\infty$ if $U_2 = P = 0$ and $n \geq 1$, or if $2a = b+1$, $U_4 = P(P^2 - 2Q) = 0$, and $2 \mid n$.)

3. Epilogue

As mentioned in the introduction, we can prove those results, using the same elementary tools, in a much more effective and concise way [3]. This can be achieved by using the technique of Theorem 2.2 even in the more difficult case $2a > b$.

The lower bound obtained in Theorem 1.1 can be improved if we know the values of a and b. Indeed, since each U_n is a polynomial in P and Q, homogeneous of degree $n-1$ in P, and $\sqrt{Q}$, each term of that polynomial is of the form

$$P^\lambda (\sqrt{Q}\,)^{2\mu} = P^\lambda Q^\mu,$$

with $\lambda + 2\mu = n - 1$. Thus,

$$\begin{aligned} \nu_p(P^\lambda Q^\mu) &= \lambda a + \mu b = \lambda a + 2\mu \frac{b}{2} \\ &\geq (\lambda + 2\mu) \cdot \min\left\{a, \frac{b}{2}\right\} \\ &= (n-1) \cdot \min\left\{a, \frac{b}{2}\right\}. \end{aligned}$$

The same inductive proof of Theorem 1.1 may also be used. Since each V_n is a polynomial in P and Q, homogeneous of degree n in P and $\sqrt{Q}$, we obtain the following theorem, also valid, of course, if p is regular.

Theorem 3.1. *If p is a prime and $p^a \,||\, P$, $p^b \,||\, Q$, then for all $n \geq 1$,*

$$\begin{aligned} \nu_p(U_n) &\geq \left\lceil (n-1) \cdot \min\left\{a, \frac{b}{2}\right\} \right\rceil; \\ \nu_p(V_n) &\geq \left\lceil n \cdot \min\left\{a, \frac{b}{2}\right\} \right\rceil. \end{aligned}$$

To bring up another insight, the referee made the following comment. By extending the p-adic valuation to the quadratic field $\mathbb{Q}(\alpha)$, there are two cases to consider. When $b > 2a$, the roots α and β have distinct valuations, say $\nu_p(\alpha) = a$ for the dominant root and $\nu_p(\beta) = b - a$ for the root of larger valuation; however when $b \leq 2a$ the two roots have the same valuation $b/2$. This gives an idea as to why the cases $b > 2a$ and $b = 2a$ are the simplest cases. From the Binet formula

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} = \frac{\alpha^n}{\alpha - \beta}\left(1 - \left(\frac{\beta}{\alpha}\right)^n\right),$$

one can read directly, say, the result of Theorem 2.1. Also, the lower bound obtained in Theorem 3.1 is easily seen by observing that

$$\min\{\nu_p(\alpha), \nu_p(\beta)\} = \min\left\{a, \frac{b}{2}\right\}.$$

4. Acknowledgments.

We thank the anonymous referee for his appreciation and his valuable comments.

References

[1] C. Ballot, *Divisibility of Fibonomials and Lucasnomials via a general Kummer rule*, The Fibonacci Quarterly, **53.3** (2015), 194–205.
[2] C. Ballot, *Lucas sequences with cyclotomic root field*, Dissertationes Math., **490** (2013), 92 pp.
[3] C. Ballot and H. C. Williams, *The Lucas Sequences: Theory and Applications*, work in progress.
[4] R. D. Carmichael, *On the numerical factors of the arithmetic forms* $\alpha^n \pm \beta^n$, Ann. of Math., (2) **15**, (1913–14), no. 1–4, 30–48, 49–70.
[5] T. Lengyel, *The order of the Fibonacci and Lucas numbers*, The Fibonacci Quarterly, **33.3** (1995), 234–239.
[6] É. Lucas, *Théorie des fonctions simplement périodiques*, Amer. J. Math., **1** (1878), 184–240, 289–321.
[7] É. Lucas, *Théorie des Nombres*, Éditions Jacques Gabay, 1991. (Authorized re-edition of the original 1891 Gauthier-Villars edition.)
[8] C. Sanna, *The p-adic valuation of Lucas sequences*, The Fibonacci Quarterly, **54.2** (2016), 118–124.
[9] H. C. Williams, *Édouard Lucas and primality testing*, Wiley, Canadian Math. Soc. Series of Monographs and Advanced Texts, 1998.

2010 MSC: 11A99, 11B39

Université de Caen, Département de Mathématiques et Informatique, 14032 Caen, France
Email address: christian.ballot@unicaen.fr