Journal of Integer Sequences, Vol. 25 (2022),
Article 22.8.1

On the p-adic Valuations of Sums of Powers of Integers

Gombodorj Bayarmagnai and Sainjargal Delger
Department of Mathematics
National University of Mongolia
Baga Toirog
Ulaanbaatar 14200
Mongolia
bayarmagnai@num.edu.mn
sdelger96@gmail.com

Abstract

In this paper we obtain a simple formula for the number of matching p-ary digits of certain terms of Lucas sequences for any odd prime p. Using this formula, we present a simple sufficient condition for the sequence $(v_p(a_1^n + a_2^n + \cdots + a_k^n))_{n\geq 0}$ to be unbounded, where $a_1, a_2, \ldots, a_k$ $(k \geq 2)$ are given integers and v_p is the p-adic valuation.

1 Introduction

The p-adic valuations of integer sequences have been objects of interest because of their surprising properties such as k-regularity (Allouche et al. [1], Bell [2], and Murru et al. [6]) and exponent lifting (Birkhoff et al. [3] and Sanna [9]). In the paper we focus on the p-adic valuations of sequences given by sums of powers of integers and differences of terms of Lucas sequences.

Given an integer $k \geq 2$ and integers $a_1, a_2, \ldots, a_k$ satisfying $|a_i| \geq 2$ for each $1 \leq i \leq k$, let $(s_n)_{n\geq 1}$ be the sequence defined by

$$s_n = a_1^n + a_2^n + \cdots + a_k^n$$

for each $n \geq 1$. For $k = 2$, the sequence of the p-adic valuations $(v_p(s_n))_{n\geq 1}$ is well known (Birkhoff et al. [3]) and in particular, the sequence is unbounded if p divides a term of $(s_n)_{n\geq 1}$, where p is an odd prime and v_p is the p-adic valuation. But it is not true in general. The first purpose of this paper is to present a sufficient condition for the unboundedness of the sequence $(v_p(s_n))_{n\geq 1}$, especially for the case $k \geq 3$.

Now, we formulate our main result:

Theorem 1. *Let p be an odd prime dividing s_ℓ for some index ℓ such that $\ell < p$. If*

$$\sum_{(a_i,p)=1} q(a_i)a_i^\ell \not\equiv 0 \pmod p \tag{1}$$

then $(v_p(s_n))_{n\geq 1}$ is unbounded, where $q(a) = \frac{a^{p-1}-1}{p}$ is the Fermat quotient of p with base a.

Our next purpose is to study the rate of growth in the number of matching p-ary digits of certain terms of Lucas sequences. This will be useful in the proof Theorem 1. More precisely, throughout the paper, a Lucas sequence $(U_n)_{n\geq 0}$ is a sequence given by $U_0 = 0$, $U_1 = 1$, and

$$U_n = aU_{n-1} - bU_{n-2},\ n = 2, 3, \ldots,$$

where a, b are relatively prime integers. We require that $(U_n)_{n\geq 0}$ is nondegenerate, that is, $b \neq 0$ and the ratio α/β of the two roots α, β of the characteristic polynomial $x^2 - ax + b$ is not a root of unity. It is well known that the Lucas quotient U_τ/p is an integer for any prime p not dividing $2b$ (Ribenboim [8]), where $(\frac{\cdot}{p})$ is the Legendre symbol and $\tau = p - (\frac{a^2-4b}{p})$. Then our next result is the following.

Theorem 2. *Let $(U_n)_{n\geq 0}$ be a Lucas sequence, and let D denote the discriminant of its characteristic polynomial. For a prime p not dividing $2b$ we have*

$$v_p(U_{\tau p^\ell} - pU_{\tau p^{\ell-1}}) = \begin{cases} 2\ell + \delta + \sigma + v_p(\tau), & \text{if } b^2 \neq 1; \\ 3\ell + 3\sigma + v_p(D/3) + 1, & \text{if } b^2 = 1, \end{cases}$$

for $\ell > \delta$, where δ and σ are the p-adic valuations of $b^{p-1} - 1$ and U_τ/p, respectively.

The theorem is analogous to the results of Lengyel [4, 5] for the sequences of Motzkin numbers, central binomial coefficients and Catalan numbers. Note that $\sigma = 0$ if p is a Lucas non-Wieferich prime. Assuming the ABC conjecture, Ribenboim [7] showed that there are infinitely many Lucas non-Wieferich primes.

2 The number of matching digits

In this section we prove Theorem 2. Before that we need some preliminary results stating properties of the subsequence $(U_{\tau p^\ell})_{\ell\geq 0}$. Finally, we see that the sequence defined by the last nonzero digits of $U_{\tau p^\ell}$ in base p is constant. This property is key in the proof of Theorem 1.

Lemma 3. *If p is a prime not dividing $2b$ and n is a positive integer divisible by τ then*

$$v_p(U_{np^{\ell+1}}) = v_p(U_{np^\ell}) + 1$$

for each positive integer ℓ.

Proof. Let $\rho_U(p)$ be the rank of appearance of p in the sequence $(U_n)_{n\geq 0}$. It is known that $p \mid U_n$ if and only if $\rho_U(p) \mid n$ (see for example, [8, (3.3), p. 12]). Thus τ is divisible by $\rho_U(p)$ and hence the formula follows from [9, Corollary 1.6]. □

We read the p-ary digits of $U_{\tau p^\ell}$ from left to right and consider the number of matching p-ary digits of $U_{\tau p^\ell}$ and $pU_{\tau p^{\ell-1}}$, i.e., $v_p(U_{\tau p^\ell} - pU_{\tau p^{\ell-1}})$. All the first $\ell + v_p(U_\tau)$ digits of the two numbers are zero by Lemma 3, and moreover, the number of matching digits is determined by the p-adic valuation of the difference $u_\ell - u_{\ell-1}$, where u_ℓ is the p-free part of the term $U_{\tau p^\ell}$, i.e.,

$$u_\ell = p^{-v_p(U_{\tau p^\ell})} U_{\tau p^\ell}.$$

Lemma 4. *For each odd $k \geq 1$ we have*

$$U_{k\tau p^\ell}/U_{\tau p^\ell} = D \sum_{i=1}^{(k-1)/2} b^{(\frac{k-1}{2}-i)\tau p^\ell} U_{i\tau p^\ell}^2 + kb^{\frac{k-1}{2}\tau p^\ell}.$$

Proof. It is well-known that for all integers $n \geq 0$, it holds $U_n = (\alpha^n - \beta^n)/(\alpha - \beta)$. Hence we have $U_{k\tau p^\ell}/U_{\tau p^\ell} = \sum_{i=0}^{k-1} \alpha^{i\tau p^\ell} \beta^{(k-1-i)\tau p^\ell}$ for any integer $k \geq 1$. For odd k the latter equals

$$\sum_{i=1}^{(k-1)/2} b^{(\frac{k-1}{2}-i)\tau p^\ell} \left(\alpha^{i\tau p^\ell} - \beta^{i\tau p^\ell}\right)^2 + kb^{\frac{k-1}{2}\tau p^\ell},$$

since $b = \alpha\beta$. Thus the lemma follows from this identity and $D = (\alpha - \beta)^2$. □

Lemma 5. *For each positive integer ℓ there exists an integer t_ℓ such that*

$$\frac{u_{\ell+1}}{u_\ell} = DU_{\tau p^\ell}^2 \left(pt_\ell + \frac{p^2-1}{24} b^{\frac{p-3}{2}\tau p^\ell}\right) + b^{\frac{p-1}{2}\tau p^\ell}.$$

Proof. For any positive integer ℓ, by Lemma 4, we have

$$\frac{u_{\ell+1}}{u_\ell} = \frac{DU_{\tau p^\ell}^2}{p} \left(\sum_{k=1}^{(p-1)/2} b^{(\frac{p-1}{2}-k)\tau p^\ell} (U_{k\tau p^\ell}/U_{\tau p^\ell})^2 \right) + b^{\frac{p-1}{2}\tau p^\ell}.$$

We claim that $(U_{k\tau p^\ell}/U_{\tau p^\ell})^2 \equiv k^2 b^{(k-1)\tau p^\ell} \pmod{p^{2(\ell+\sigma+1)}}$ for each $1 \leq k \leq (p-1)/2$. The claim follows easily from Lemma 4 if k is odd. For even k we have the identity

$$(U_{k\tau p^\ell}/U_{k\tau p^\ell/2})^2 = DU_{k\tau p^\ell/2}^2 + 4b^{k\tau p^\ell/2},$$

which, by induction on k, yields the claim. Thus we can conclude from the claim that

$$\sum_{k=1}^{(p-1)/2} b^{(\frac{p-1}{2}-k)\tau p^\ell}(U_{k\tau p^\ell}/U_{\tau p^\ell})^2 \equiv \frac{p^3-p}{24} b^{\frac{p-3}{2}\tau p^\ell} \pmod{p^{2(\ell+\sigma+1)}},$$

completing the proof. □

We are now ready to prove Theorem 2.

Proof of Theorem 2. **The case $b^2 = 1$:** We claim that $b^{\frac{p-1}{2}\tau} = 1$. If p is not a divisor of D then it is clear since τ is even. Suppose p is a divisor of D. Then $\tau = p$ which is odd. If $b = -1$ then $D = a^2 + 4$ and hence $p \equiv 1 \pmod 4$, implying the claim.

From Lemma 5 and the claim we obtain

$$\frac{u_{\ell+1} - u_\ell}{u_\ell^3} = Dp^{2(\ell+\sigma+1)}\left(pt_\ell + \frac{p^2-1}{24} b^{\frac{p-3}{2}\tau p^\ell}\right)$$

for some integer t_ℓ. Therefore

$$v_p(u_{\ell+1} - u_\ell) = 2(\ell+\sigma+1) + v_p(D/3) \tag{2}$$

for each positive integer ℓ.

The case $b^2 \neq 1$: We claim that b^τ is a square residue modulo p. If p is not a divisor of D then the claim is clear since τ is even. Suppose p is a divisor of D. Then $\tau = p$ and hence we have

$$b \equiv \frac{\left(\alpha^{(\tau+1)/2} + \beta^{(\tau+1)/2}\right)^2}{\left(\alpha^{(\tau-1)/2} + \beta^{(\tau-1)/2}\right)^2} \pmod p,$$

since U_τ is divisible by p. Moreover, the right hand side is equal to $(U_{\tau+1}U_{\frac{\tau-1}{2}}(U_{\tau-1}U_{\frac{\tau+1}{2}})^{-1})^2$, showing the claim.

By applying Lemma 3 and Lemma 4 we obtain

$$v_p(u_{\ell+1} - u_\ell) = v_p(b^{\frac{p-1}{2}\tau p^\ell} - 1)$$

if $\ell > \delta$. Since $v_p(b^{\frac{p-1}{2}\tau} - 1) \neq 0$ by the above claim, we have $v_p(u_{\ell+1} - u_\ell) = v_p(\tau) + \delta + \ell$ when $\ell > \delta$, completing the proof of Theorem 2. □

Example 6. The Fibonacci sequence $(F_n)_{n\geq 0}$ is a Lucas sequence with characteristic polynomial $x^2 - x - 1$. Since $\tau = p \pm 1$ if $p^2 \equiv \pm 1 \pmod 5$ and $\tau = p$ if $p = 5$, we have

$$v_p(f_{\ell+1} - f_\ell) = \begin{cases} 2\ell + 1, & \text{if } p = 3; \\ 2\ell + 3, & \text{if } p = 5; \\ 2\ell + 2v_p(F_\tau), & \text{if } p \geq 7. \end{cases}$$

Here f_ℓ denotes the p-free part of the τp^ℓ-th Fibonacci number.

Let $\hat{u}_\ell$ denote the last nonzero digit of $U_{\tau p^\ell}$ in base p. Theorem 2 implies that the sequence $(\hat{u}_\ell)_{\ell\geq 0}$ is eventually constant since $\hat{u}_\ell \equiv u_\ell \pmod p$ for each positive integer ℓ.

Lemma 7. *The sequence $(\hat{u}_\ell)_{\ell\geq 0}$ is constant.*

Proof. For our purpose it suffices to show that $v_p(u_{\ell+1} - u_\ell) \geq 1$ for any integer $\ell \geq 0$. If $b^2 = 1$ then this follows from (1). In the proof of Theorem 2, we have seen that $v_p(b^{\frac{p-1}{2}\tau} - 1) = \delta + v_p(\tau) \geq 1$ if $b^2 \neq 1$. Thus, by Lemma 3 and Lemma 5, we obtain

$$v_p(u_{\ell+1} - u_\ell) \geq \min(v_p(DU^2_{\tau p^\ell}/3), v_p(b^{\frac{p-1}{2}\tau p^\ell} - 1)) \geq \min(\sigma + 1, \delta + v_p(\tau)),$$

completing the proof. $\square$

3 On sums of powers of integers

We begin this section with a key lemma which is a version of the lifting the exponent (LTE) lemma and then use it to prove Theorem 1.

Let $a_1, a_2, \ldots, a_k$ be integers satisfying $|a_i| \geq 2$ and $p \nmid a_i$ for $1 \leq i \leq k$. For each index i define a sequence $q_n^{(i)}$ by the difference $q_n^{(i)} = a_i^n - 1$ for any integer $n \geq 0$. Then the sequence of the quotients $\left(q_n^{(i)}/q_1^{(i)}\right)_{n\geq 0}$ is a Lucas sequence with characteristic polynomial $x^2 - (a_i + 1)x + a_i$.

Lemma 8. *Let p be an odd prime. If there exist integers $c_1, c_2, \ldots, c_k$ and $\ell \geq 0$ such that*

$$c_1 q^{(1)}_{(p-1)p^\ell} + c_2 q^{(2)}_{(p-1)p^\ell} + \cdots + c_k q^{(k)}_{(p-1)p^\ell} \equiv 0 \pmod{p^{\ell+\chi+1}} \tag{3}$$

then (3) holds for all $\ell \geq 0$, where χ is the minimum among all $v_p(q^{(i)}_{p-1})$.

Proof. Denote by χ_i $(1 \leq i \leq k)$ the exponent $v_p(q^{(i)}_{p-1})$ which is clearly not zero. For the sequence $\left(q_n^{(i)}/q_1^{(i)}\right)_{n\geq 0}$, we have $\tau_i = p$ if $p \mid a_i - 1$ and $\tau_i = p - 1$ otherwise.

If $\tau_i = p - 1$ then apply Lemma 7 to the sequence $\left(q_n^{(i)}/q_1^{(i)}\right)_{n\geq 0}$. Then we obtain

$$(q^{(i)}_{(p-1)p^n}/q^{(i)}_1)/p^{\chi_i+n-v_p(q^{(i)}_1)} \equiv (q^{(i)}_{p-1}/q^{(i)}_1)/p^{\chi_i-v_p(q^{(i)}_1)} \pmod p$$

for any integer $n \geq 0$. This yields that $q^{(i)}_{(p-1)p^n}/p^{\chi_i+n} \equiv q^{(i)}_{(p-1)p^\ell}/p^{\chi_i+\ell} \pmod p$ for any $n \geq 0$.

If $\tau_i = p$ then $v_p(q^{(i)}_{(p-1)\tau_i}) = 1 + \chi_i$. By applying Lemma 7 to the Lucas sequence $(q^{(i)}_{(p-1)n}/q^{(i)}_{p-1})_{n\geq 0}$ we similarly obtain

$$q^{(i)}_{(p-1)p^n}/p^{\chi_i+n} \equiv q^{(i)}_{(p-1)p^\ell}/p^{\chi_i+\ell} \pmod p$$

for any integer $n \geq 0$, since $q^{(i)}_{(p-1)p}/p^{\chi_i+1} \equiv q^{(i)}_{p-1}/p^{\chi_i} \pmod p$. Consequently we have

$$q^{(i)}_{(p-1)p^n}/p^{\chi+n} \equiv q^{(i)}_{(p-1)p^\ell}/p^{\chi+\ell} \pmod p$$

for each index i. Substituting these congruences into

$$c_1 q^{(1)}_{(p-1)p^\ell}/p^{\chi+\ell} + \cdots + c_k q^{(k)}_{(p-1)p^\ell}/p^{\chi+\ell} \equiv 0 \pmod p,$$

which is equivalent to (3), we complete the proof of the lemma. □

Remark 9. Let p be an odd prime. For fixed integers a, b satisfying $p \nmid ab$ and $p \mid a-b$, the classical LTE lemma states that $v_p(a^n - b^n) = v_p(n) + v_p(a-b)$. Hence, for each index i, we have $v_p(q^{(i)}_{(p-1)p^\ell}) = \ell + \chi_i$. Thus Lemma 8 does not follow from the LTE lemma since $q^{(i)}_{(p-1)p^\ell}/p^{\ell+\chi} \not\equiv 0 \pmod p$ for some index i.

We are now ready to present a proof of Theorem 1.

Proof of Theorem 1. For each a_i which is prime to p we set $c_i = a_i^\ell$ and define a sequence $(q^{(i)}_n)_{n\geq 1}$ by $q^{(i)}_n = a_i^n - 1$ for each integer $n \geq 1$. Then the assumption is clearly equivalent to the condition that

$$\sum_{(a_i,p)=1} c_i q^{(i)}_{p-1}/p \not\equiv 0 \pmod p. \tag{4}$$

Under this condition we show the existence of an unbounded subsequence of $(v_p(s_n))_{n\geq 1}$ by induction. We claim that there is an integer $N \geq 1$ such that

$$v_p(s_N) > m \text{ and } N \equiv \ell \pmod{p-1}$$

for a fixed integer $m \geq 0$. Firstly, if $m = 0$ then we choose $N = \ell$ which is the base case of our induction. Assume the claim holds for an integer N such that $m = v_p(s_N) > 0$. We now show that there is an integer n such that $v_p(s_n) > m$ and $n \equiv \ell \pmod{p-1}$. For this purpose we consider the set S defined by

$$S = \{s_{n_t} \mid n_t = N + \varphi(p^m)t,\ t = 1, 2, \ldots, p\},$$

where φ denotes the Euler's totient function. It follows from Euler's theorem and the induction hypothesis that $v_p(s_{n_t}) \geq m$ for each t. Suppose each element of S is not divisible by p^{m+1}. Then, by Pigeonhole principle, there are two different elements s_{n_j} and $s_{n_{j+t}}$ of S $(t \neq 0)$ which are congruent modulo p^{m+1}. Hence we obtain

$$\sum_{(a_i,p)=1} c_i q^{(i)}_{t\varphi(p^m)}/p^m \equiv 0 \pmod p$$

since $N \equiv \ell \pmod{p-1}$ and j, t are non-zero integers. Clearly, we have

$$q^{(i)}_{\varphi(p^m)t}/p^m \equiv t q^{(i)}_{\varphi(p^m)}/p^m \pmod{p}$$

for each index i. Therefore, using these congruences, it follows from Lemma 2 that

$$\sum_{(a_i,p)=1} c_i q^{(i)}_{\varphi(p)}/p \equiv 0 \pmod{p},$$

contradicting (4). Thus S contains an element s_{n_t} satisfying $v_p(s_{n_t}) \geq m+1$. Clearly, $n_t \equiv \ell \pmod{p-1}$ by the induction hypothesis. This completes the induction step. $\square$

Remark 10. Theorem 1 provides a sufficient but not necessary condition: consider the sequence $(s_n)_{n\geq 1}$ given by $s_n = 1 + 2^n + 3^n$ for all $n \geq 0$. Set $p = 7$. Then

$$s_4 \equiv 2^4(2^{p-1}-1)/p + 3^4(3^{p-1}-1)/p \equiv 0 \pmod{p},$$

but the subsequence $(v_p(s_{4p^n}))_{n\geq 1}$ is unbounded since $v_p(s_{4p^n}) = n + 2$ for each $n \geq 0$.

Corollary 11. *Let p be a prime divisor of the sequence $(s_n)_{n\geq 1}$. Assume that $a_1, a_2, \ldots, a_k$ and k are not divisibly by p and $v_p(s_\ell) = 1$ for each s_ℓ such that $1 \leq \ell < p$ and $p \mid s_\ell$. Then the sequence $(v_p(s_n))_{n\geq 1}$ is bounded by 1 if and only if (1) does not hold.*

Proof. If $(v_p(s_n))_{n\geq 1}$ is bounded then Theorem 1 implies that (1) does not hold.

Suppose (1) does not hold. For any integers $n, j \geq 1$ we have

$$s_{n+\varphi(p)j} = \sum a_i^n (pq(a_i) + 1)^j$$

and hence

$$s_{n+\varphi(p)j} \equiv s_n \pmod{p^2} \iff \sum_{i=1}^{k} a_i^n q(a_i) \equiv 0 \pmod{p}. \tag{5}$$

If $v_p(s_n) \neq 0$ then $v_p(s_\ell) \neq 0$, where ℓ is an integer satisfying $n = \ell + \varphi(p)j$ with $0 < \ell < \varphi(p)$. Therefore (5) implies that $v_p(s_n) = 1$ and thus the sequence $(v_p(s_n))_{n\geq 1}$ is bounded by 1. $\square$

Example 12. Let $a_1 = 6$, $a_2 = 13$, $a_3 = 97$ and $p = 19$. Clearly, if $\ell < p$ and $p \mid s_\ell$ then $\ell = 2$. Moreover, $v_p(s_2) = 1$ and the sum

$$a_1^2(a_1^{p-1}-1)/p + a_2^2(a_2^{p-1}-1)/p + a_3^2(a_3^{p-1}-1)/p$$

is divisible by p. Thus, by Corollary 11, each term of the sequence $(s_n)_{n\geq 1}$ is not divisible by p^2.

4 Acknowledgment

The authors would like to thank the referee for carefully reading the paper. The research has received funding from the National University of Mongolia under grant agreement P2020-3943.

References

[1] J.-P. Allouche and J. Shallit, The ring of k-regular sequences, *Theoret. Comput. Sci.* **98** (1992), 163–197.

[2] J. P. Bell, p-adic valuations and k-regular sequences, *Discrete Math.* **307** (2007), 3070–3075.

[3] G. D. Birkhoff and H. S. Vandiver, On the integral divisors of $a^n - b^n$, *Ann. of Math.* **5** (1904), 173–180.

[4] T. Lengyel, Exact p-adic orders for differences of Motzkin numbers, *Int. J. Number Theory* **10** (2014), 653–667.

[5] T. Lengyel, On divisibility properties of some differences of the central binomial coefficients and catalan numbers, *Integers* **13** (2013), A10.

[6] N. Murru and C. Sanna, On the k-regularity of the k-adic valuation of Lucas sequences, *J. Théor. Nombres Bordeaux* **30** (2018), 227–237.

[7] P. Ribenboim, On square factors of terms of binary recurring sequences and the *ABC* conjecture, *Publ. Math. Debrecen* **59** (2001), 459–469.

[8] P. Ribenboim, *My Numbers, My Friends*, Springer-Verlag, 2002.

[9] C. Sanna, The p-adic valuation of Lucas sequences, *Fibonacci Quart.* **54** (2016), 118–124.

2010 *Mathematics Subject Classification*: Primary 11B39; Secondary 11B50.

Keywords: sums of powers of integers, p-adic valuation, Lucas sequence.

Received July 11 2022; revised versions received August 5 2022; August 31 2022; September 13 2022. Published in *Journal of Integer Sequences*, October 7 2022.
