

Divisibility and Modular Periodicity of a Prime-Discriminant Lucas Sequence Modulo Prime Powers

Kaan Buyukhatipoglu¹, Dervis Hopikoglu²

^{1,2}Students, Eyuboglu High School, Istanbul, Turkiye

Abstract

This study examines the divisibility and modular periodicity of a restricted Lucas sequence whose discriminant is a prime congruent to one modulo four. A congruence relation is derived modulo the associated prime and used to prove that the prime divides a sequence term if and only if it divides the corresponding index. This establishes the rank of apparition, and the period modulo the prime is also derived. The investigation then tests an extension of the period formula to higher prime powers using Python. All 80 eligible primes below 1000 were examined for exponents one through four, giving 320 different cases. Candidate periods were checked using modular matrix exponentiation, and their minimality was tested by examining divisors obtained from their prime factors. In every tested scenario, the period followed a pattern determined by the prime power and the multiplicative order of four modulo the prime. These computations support the proposed extension over the specified range, without representing a general proof for higher prime powers.

Keywords: Lucas Sequences, Prime Powers, Modular Periodicity, Divisibility, Rank of Apparition, p-Adic Valuation

1. Introduction

Integer sequences defined by linear recurrence relations form an important part of number theory. Among these, Lucas sequences provide a broad framework for studying recurrence relations, divisibility, prime factors, and modular arithmetic. A Lucas sequence of the first kind, in general, is determined by two integer parameters P and Q , and many classical integer sequences can be interpreted within this framework. Modern treatments of Lucas sequences examine their characteristic equations, closed forms and divisibility properties [1].

Pell equations form another classical topic in number theory and are closely related to second-order recurrence sequences. The standard Pell equation

$$x^2 - Dy^2 = 1,$$

where D is a positive nonsquare integer, can be studied using continued fractions, quadratic irrationalities, and recurrence relations [2]. These connections make Pell-related recurrence sequences particularly suitable for investigations involving divisibility and modular behavior.

The sequence examined in this study is based on primes of the form

$$p \equiv 1 \pmod{4}.$$

For such a prime, let

$$p = 4k + 1.$$

The parameters

$$P = 2k + 1$$

and

$$Q = k^2$$

then satisfy

$$P^2 - 4Q = (2k + 1)^2 - 4k^2 = 4k + 1 = p$$

Using these parameters, the sequence is defined by [3]

$$U_{k,0} = 0, \quad U_{k,1} = 1$$

and, for $n \geq 2$,

$$U_{k,n} = (2k + 1)U_{k,n-1} - k^2U_{k,n-2} \quad (1)$$

The corresponding characteristic equation is

$$x^2 - (2k + 1)x + k^2 = 0 \quad (2)$$

whose discriminant is exactly

$$\Delta = 4k + 1 = p$$

Thus, the prime p is directly incorporated into the algebraic structure of the recurrence. Since the discriminant of the recurrence is equal to the prime p , we refer to this sequence as a prime-discriminant Lucas sequence in this study.

Modular arithmetic provides a useful framework for analysing recurrence sequences because reducing sequence terms modulo an integer can reveal patterns of divisibility, repetition, and congruence. Classical Fibonacci and Lucas sequences exhibit structured behavior when considered modulo primes [4]. More generally, modular periods and related divisibility properties create an important part of the arithmetic theory of recurrence sequences.

The analysis becomes particularly interesting when the modulus is extended from a prime p to its powers p^r , $r \geq 1$.

Concepts such as the rank of apparition, modular period, and p -adic valuation provide mathematical tools for describing when primes divide terms of a recurrence sequence and how this behavior develops for higher prime powers [5, 6]. These concepts are well established in the general theory of Lucas sequences and form the theoretical basis for this study.

The purpose of this study is to investigate the divisibility and modular periodicity of the sequence $U_{k,n}$ under the restriction

$$p = 4k + 1$$

where p is prime. In particular, the study examines the behavior of

$$U_{k,n} \pmod{p^r}$$

The investigation focuses on congruence relations, divisibility by powers of the associated prime, and modular periods. Mathematical derivations are combined with systematic computational experiments in order to compare theoretical properties with observed behavior for different primes satisfying

$$p \equiv 1 \pmod{4}.$$

The distinction between proof and computation is central to the scope of this paper: the prime-level divisibility and period results are established algebraically, whereas the proposed extension to higher prime powers is tested over the finite range described in Section 5.

2. Related Research Work

Lucas sequences have been studied within number theory, particularly in relation to divisibility, prime factors, and modular arithmetic. The general theory of Lucas sequences provides results concerning their characteristic equations, recurrence structures, and divisibility properties, allowing many classical recurrence sequences to be examined within a common framework [1]. Modular investigations of Fibonacci and Lucas sequences have also established structured congruence properties modulo primes. Hence, these findings demonstrate the relevance of modular arithmetic to the study of second-order recurrence sequences [4]. An important part of this theory involves identifying the indices at which primes and their powers divide sequence terms. The rank of apparition provides a way of describing the first occurrence of such divisibility, while the p -adic valuation determines the highest power of a prime dividing a given term. Previous results have connected these concepts to divisibility and periodicity in nondegenerate Lucas sequences [5, 7]. These results provide an established theoretical basis for examining the behavior of recurrence sequences modulo powers of a prime.

Previous studies have extended the study of modular periods, entry points, and orders from classical Fibonacci and Lucas sequences to the general Lucas sequences

$$U_n(P, Q)$$

and

$$V_n(P, Q)$$

Such results provide a useful framework for analysing periodic behavior modulo an integer m [6]. The present study considers the restricted parameter family

$$P = 2k + 1, \quad Q = k^2,$$

for which

$$P^2 - 4Q = 4k + 1 = p$$

is prime. The objective is to examine how the established theory of divisibility and modular periodicity applies to this prime-discriminant family, with particular emphasis on its behavior modulo

$$p^r.$$

Theoretical derivations are combined with computational verification to determine the patterns that occur from this special parameter structure.

Earlier studies of Lucas sequences provide a broad framework for studying divisibility and ranks of apparition [5, 7]. In this paper, the prime-level divisibility relation is derived explicitly for the selected parameter family. Then, the investigation examines the modular periods of this family through computational verification over a specified range of prime powers.

3. Mathematical Background and Definitions

This section introduces the mathematical definitions and related concepts needed to interpret the theoretical and computational results.

3.1. Lucas Sequence and the Prime-Discriminant Family

A Lucas sequence of the first kind is defined by two integer parameters P and Q as [1]

$$\begin{aligned} U_0 &= 0, & U_1 &= 1, \\ U_n &= PU_{n-1} - QU_{n-2}, n \geq 2. \end{aligned} \quad (3)$$

The associated characteristic equation is

$$x^2 - Px + Q = 0,$$

with discriminant

$$\Delta = P^2 - 4Q \quad (4)$$

If α and β are the two distinct roots of the equation, then the sequence can be expressed using the Binet-type formula

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad (5)$$

For the sequence considered in this study,

$$p = 4k + 1$$

is prime, and

$$P = 2k + 1, \quad Q = k^2$$

Therefore,

$$\Delta = (2k + 1)^2 - 4k^2 = p$$

$$\alpha = \frac{2k+1+\sqrt{p}}{2}, \quad \beta = \frac{2k+1-\sqrt{p}}{2},$$

Moreover,

$$\alpha - \beta = \sqrt{p},$$

Hence,

$$U_{k,n} = \frac{\alpha^n - \beta^n}{\sqrt{p}} \quad (6)$$

Equation (6) provides an algebraic representation of the sequence, while the congruence relations in Section 4 are derived directly from its recurrence relation.

3.2. Modular Divisibility and Periodicity

For a prime p and a nonzero integer N , the p -adic valuation $v_p(N)$ is the largest nonnegative integer s such that

$$p^s \mid N.$$

Equivalently,

$$v_p(N) = s$$

when

$$p^s \mid N$$

but

$$p^{s+1} \nmid N.$$

The p -adic valuation is particularly useful for studying divisibility of Lucas sequence terms by successive powers of a prime. General formulas relating p -adic valuations of Lucas sequence terms to their indices and ranks of apparition are known [7].

The rank of apparition of a positive integer m , denoted here by $\rho(m)$, is the smallest positive integer n for which

$$m \mid U_n,$$

provided that such an index exists. In particular,

$$\rho(p) = \min\{n \geq 1 : p \mid U_n\}. \quad (7)$$

The behavior of ranks of apparition for Lucas sequences and their powers has been studied in connection with periodicity and p -adic order [5].

For a positive integer modulus m , the modular period $\pi(m)$ is the smallest positive integer T such that

$$U_{n+T} \equiv U_n \pmod{m} \quad (8)$$

for every $n \geq 0$.

Period, entry point, and related modular statistics have been developed for general Lucas sequences $U_n(P, Q)$ [6].

For the moduli considered in this study, $Q = k^2$ and $\gcd(k, p) = 1$, since $p = 4k + 1$. The transition matrix therefore has determinant Q and is invertible modulo p^r . Consequently, the recurrence is periodic from its initial state.

A final quantity required later is the multiplicative order of an integer a modulo a prime p . If $p \nmid a$, then

$$\text{ord}_p(a)$$

is the smallest positive integer d satisfying

$$a^d \equiv 1 \pmod{p}. \quad (9)$$

In this study, the quantity

$$\text{ord}_p(4)$$

will be particularly relevant when the modular period of $U_{k,n}$ is investigated.

4. Theoretical Results

This section investigates the arithmetic properties of the prime-discriminant Lucas sequence introduced in (1). The analysis begins with the reduction of the recurrence modulo its associated prime $p = 4k + 1$. The resulting congruence will later provide the basis for studying divisibility and modular periodicity modulo higher powers of p .

4.1. Congruence Modulo p

Recall that

$$p = 4k + 1$$

is prime. Therefore,

$$4k \equiv -1 \pmod{p}.$$

From this relation,

$$2(2k + 1) = 4k + 2 \equiv 1 \pmod{p},$$

so,

$$2k + 1 \equiv 2^{-1} \pmod{p}.$$

Similarly,

$$16k^2 = (4k)^2 \equiv 1 \pmod{p},$$

and hence

$$k^2 \equiv 16^{-1} \pmod{p}$$

Substituting these congruences into the recurrence relation in (1) gives

$$U_{k,n} \equiv 2^{-1}U_{k,n-1} - 16^{-1}U_{k,n-2} \pmod{p}. \quad (10)$$

Since $p \equiv 1 \pmod{4}$, the prime p is odd and therefore 2, 4, and 16 all have multiplicative inverses modulo p .

Proposition 1

For every integer $n \geq 1$,

$$U_{k,n} \equiv n4^{1-n} \pmod{p} \quad (11)$$

where negative powers of 4 denote powers of the multiplicative inverse of 4 modulo p .

Proof

The result is proved by induction.

For $n = 1$,

$$U_{k,1} = 1,$$

while

$$1 \cdot 4^0 = 1.$$

Therefore, (11) holds for $n = 1$.

For $n = 2$,

$$U_{k,2} = 2k + 1.$$

Since

$$2k + 1 \equiv 2^{-1} \pmod{p},$$

we obtain

$$U_{k,2} \equiv \frac{1}{2} \pmod{p}.$$

On the other hand,

$$2 \cdot 4^{-1} = \frac{1}{2},$$

so (11) also holds for $n = 2$.

Assume now that the result is true for $n - 1$ and $n - 2$.

Thus,

$$U_{k,n-1} \equiv (n - 1)4^{2-n} \pmod{p}$$

and

$$U_{k,n-2} \equiv (n - 2)4^{3-n} \pmod{p}$$

Using (10),

$$U_{k,n} \equiv 2^{-1}(n - 1)4^{2-n} - 16^{-1}(n - 2)4^{3-n} \pmod{p}.$$

The first term simplifies to

$$2(n - 1)4^{1-n},$$

while the second term becomes

$$(n - 2)4^{1-n}.$$

Therefore,

$$U_{k,n} \equiv [2(n - 1) - (n - 2)]4^{1-n} \pmod{p}$$

Since

$$2(n - 1) - (n - 2) = n,$$

it follows that

$$U_{k,n} \equiv n4^{1-n} \pmod{p}$$

Hence, the result holds for every $n \geq 1$.

Corollary 1

For every $n \geq 1$,

$$p \mid U_{k,n} \Leftrightarrow p \mid n. \quad (12)$$

Proof

From Proposition 1,

$$U_{k,n} \equiv n4^{1-n} \pmod{p}.$$

Because $p \neq 2$, the factor

$$4^{1-n}$$

is invertible modulo p . Consequently,

$$U_{k,n} \equiv 0 \pmod{p}$$

if and only if

$$n \equiv 0 \pmod{p}$$

Therefore,

$$p \mid U_{k,n} \Leftrightarrow p \mid n.$$

An immediate consequence of Corollary 1 is that the first positive index for which p divides a term of the sequence is $n = p$. Therefore, using the definition of rank of apparition given in (7),

$$\rho(p) = p. \quad (13)$$

This establishes a direct relationship between the discriminant prime p and the index structure of the sequence. It also provides the starting point for investigating divisibility by higher powers p^r .

Proposition 2 (Period Modulo p)

For each prime $p = 4k + 1$ in the specified family, the modular period of the sequence modulo p is

$$\pi(p) = \text{ord}_p(4).$$

Proof

A positive integer T is a period if and only if $U_{k,T} \equiv 0 \pmod{p}$ and $U_{k,T+1} \equiv 1 \pmod{p}$. By Proposition 1, the first condition is equivalent to $p \mid T$. Under this condition, the second becomes $4^{-T} \equiv 1 \pmod{p}$, which holds exactly when $\text{ord}_p(4) \mid T$.

Since $\text{ord}_p(4)$ divides $p - 1$, it is coprime to p . The smallest positive T satisfying both divisibility conditions is therefore $\text{ord}_p(4)$, proving the stated period formula.

5. Computational Verification and Results

To support the theoretical analysis, computational experiments were performed for primes satisfying

$$p \equiv 1 \pmod{4}$$

For each prime p , the parameter

$$k = \frac{p-1}{4}$$

was calculated, and the recurrence

$$U_{k,0} = 0, \quad U_{k,1} = 1$$

$$U_{k,n} = (2k+1)U_{k,n-1} - k^2U_{k,n-2}$$

was evaluated using modular arithmetic. The computations were carried out for prime-power moduli

$$p, p^2, p^3, p^4.$$

The calculations were performed in Python using exact integer modular arithmetic. For each prime-power modulus, the recurrence was represented by a two-by-two transition matrix whose first row contains the recurrence coefficients P and negative Q and whose second row is $(1, 0)$. Matrix powers were calculated by repeated squaring, reducing each entry modulo the chosen prime power after every multiplication.

Starting from the initial state $(U_1, U_0) = (1, 0)$, this method determines the recurrence state at a candidate index without constructing every preceding term. No floating-point approximations were required.

To check the modular period, the ordered pair of consecutive sequence terms was treated as the recurrence state. Since the next state is uniquely determined by the current pair, the sequence returns to its initial state when the following two congruences hold:

$$U_{k,T} \equiv 0 \pmod{p^r}$$

and

$$U_{k,T+1} \equiv 1 \pmod{p^r}.$$

The smallest positive integer T satisfying these two conditions was taken as the period $\pi(p^r)$.

The prime-modulus period established in Section 4 motivated the following candidate for higher prime powers, which was tested separately for each selected modulus:

$$T = p^r \text{ord}_p(4).$$

After verifying that the sequence returned to its initial state at T , the prime divisors of T were examined to determine whether any proper divisor of T also produced the initial state. This ensured that the calculated value was the smallest period rather than merely a multiple of the period.

The computation was performed for all primes

$$p < 1000$$

satisfying

$$p \equiv 1 \pmod{4}$$

There are 80 such primes. For each of these primes, the cases

$$r = 1, 2, 3, 4$$

were examined. No exception was observed to the relation

$$\pi(p^r) = p^r \text{ord}_p(4).$$

Representative computational results are shown below.

Table 1: Representative Computational Results

p	k	ord_p(4)	π(p)	π(p²)
5	1	2	10	50
13	3	6	78	1014
17	4	4	68	1156
29	7	14	406	11774
37	9	18	666	24642
41	10	10	410	16810
53	13	26	1378	73034

For example, when

$$p = 13,$$

we have

$$k = 3$$

and

$$\text{ord}_{13}(4) = 6.$$

The observed periods are therefore

$$\pi(13) = 13(6) = 78, \pi(13^2) = 13^2(6) = 1014,$$

and

$$\pi(13^3) = 13^3(6) = 13182.$$

The same relationship was observed throughout the computational range.

The computational results therefore agree with the theoretical pattern developed in Section 4. In particular, increasing the modulus from p^r to p^{r+1} multiplies the observed period by p :

$$\pi(p^{r+1}) = p \pi(p^r).$$

The investigations provide systematic computational evidence across a collection of primes and prime-power moduli. Although these results do not establish a general mathematical proof, the consistency between the theoretical analysis and computational evidence supports the identified modular period pattern of the prime-discriminant sequence.

6. Discussion

The theoretical and computational results reveal a regular modular structure for the prime-discriminant Lucas sequence examined in this study. The congruence obtained modulo p establishes a direct relationship between the index n and the divisibility of $U_{k,n}$ by the related discriminant prime. In particular, the result

$$p \mid U_{k,n} \Leftrightarrow p \mid n$$

implies that the rank of apparition of p is p . This behavior follows naturally from the special parameter choice

$$P = 2k + 1$$

and

$$Q = k^2,$$

for which the discriminant of the recurrence is itself the prime

$$p = 4k + 1.$$

The prime-level divisibility and period formulas are proved for every prime in the defined family. The proposed extension to higher prime powers was checked for 80 primes below 1000 and for exponents two through four, corresponding to 240 cases. Including the 80 prime-modulus cases (exponent one), the computational analysis covered 320 cases in total. General studies of Lucas-sequence valuations and periods [6, 7] give context for these questions, but the extension to arbitrary higher prime powers has not been proved here. The computations support the relation

$$\pi(p^r) = p^r \text{ord}_p(4)$$

in all 320 tested cases. Checking the recurrence state at the candidate return time established that it was a period in each case, while testing the candidate divided by each distinct prime factor excluded a shorter period.

The main limitation of the computational analysis is that verification over a finite set of primes and exponents cannot by itself establish a result for all p and r . Consequently, computational agreement should

be interpreted as supporting evidence rather than as a substitute for a general proof. A potential extension of this work would be to obtain a complete theoretical characterization of the period modulo

$$p^r$$

and to investigate whether similar behavior occurs for other restricted Lucas families whose discriminants satisfy comparable arithmetic conditions.

7. Conclusion

This study investigated the divisibility and modular periodicity of a restricted Lucas sequence defined by

$$U_{k,0} = 0, \quad U_{k,1} = 1,$$

and

$$U_{k,n} = (2k + 1)U_{k,n-1} - k^2U_{k,n-2},$$

where

$$p = 4k + 1$$

is prime. The parameter choice gives the recurrence the discriminant

$$P^2 - 4Q = p,$$

allowing the associated prime to play a direct role in the arithmetic structure of the sequence.

The theoretical analysis established the congruence

$$U_{k,n} \equiv n4^{1-n} \pmod{p}$$

From this relation, it follows that

$$p \mid U_{k,n} \Leftrightarrow p \mid n,$$

and therefore the rank of apparition of p is

$$\rho(p) = p.$$

The first positive index at which the associated prime divides a sequence term is therefore identified by an algebraic argument.

The modular period modulo the associated prime is also established theoretically as $\pi(p) = \text{ord}_p(4)$.

The computational investigation extended the analysis to moduli of the form

$$p^r.$$

Across the selected range, the modular periods were consistent with the pattern

$$\pi(p^r) = p^r \text{ord}_p(4).$$

These calculations support the proposed extension of the prime-modulus period formula to higher prime powers. Since this extension has not been proved for arbitrary exponents, it should be interpreted as a computationally supported pattern.

Overall, the study illustrates that combining the general theory of Lucas sequences with a restricted prime-discriminant parameterization leads to a clear and structured modular behavior. Additional research could focus on proving the observed period formula for arbitrary r and investigating whether comparable results apply to other parameterized Lucas sequences.

References

1. Christian J.-C. Ballot, Hugh C. Williams, The Lucas Sequences: Theory and Applications, Springer, 2023. <https://doi.org/10.1007/978-3-031-37238-4>
2. Edward J. Barbeau, Pell's Equation, Springer, 2003. <https://doi.org/10.1007/b97610>

3. Arzu Özkoç, Bazı Tamsayı Dizileri ve Pell Denklemleri, PhD Thesis, Uludağ Üniversitesi, Fen Bilimleri Enstitüsü, Matematik Anabilim Dalı, 2013. <https://acikerisim.uludag.edu.tr/bitstream/11452/6129/1/341918.pdf>
4. Dorin Andrica, Vlad Crişan, Fawzi Al-Thukair, “On Fibonacci and Lucas Sequences Modulo a Prime and Primality Testing”, Arab Journal of Mathematical Sciences, 2018, 24 (1), 9–15. <https://doi.org/10.1016/j.ajmsc.2017.06.002>
5. Prasanta Kumar Ray, Nurettin Irmak, Bijan Kumar Patel, “The Rank of Apparition of Powers of Lucas Sequence”, Turkish Journal of Mathematics, 2018, 42 (4), 1566–1570. <https://doi.org/10.3906/mat-1705-116>
6. Morgan Fiebig, aBa Mbirika, Jürgen Spilker, “Period Patterns, Entry Points, and Orders in the Lucas Sequences: Theory and Applications”, The Fibonacci Quarterly, 2025, 63 (2), 345–376. <https://doi.org/10.1080/00150517.2024.2442591>
7. Carlo Sanna, “The p-Adic Valuation of Lucas Sequences”, The Fibonacci Quarterly, 2016, 54 (2), 118–124. <https://doi.org/10.1080/00150517.2016.12427821>