PRIMITIVE DIVISORS OF LUCAS SEQUENCES IN POLYNOMIAL RINGS

JOAQUIM CERA DA CONCEIÇÃO

Abstract. It is known that all terms U_n of a classical regular Lucas sequence have a primitive prime divisor if $n > 30$ [2]. In addition, a complete description of all regular Lucas sequences and their terms U_n, $2 \leq n \leq 30$, which do not have a primitive divisor is also known. Here, we prove comparable results for Lucas sequences in polynomial rings, correcting some previous theorem on the same subject. The first part of our paper develops some elements of Lucas theory in several abstract settings before proving our main theorem in polynomial rings.

Contents

1. Introduction

Let a and b be non-zero integers such that $a \neq \pm b$. In 1892, Zsimondy [6] proved that for all $n \geq 1$ but a few exceptions, there exists a prime number that divides $a^n - b^n$ but not any $a^k - b^k$, for $1 \leq k < n$. Such a prime is called a primitive divisor of $a^n - b^n$. In particular, there always exists a primitive prime divisor for $n \geq 7$. Knowing that $a - b$ divides $a^n - b^n$ for all $n \geq 1$, numbers of the form

$$\frac{a^n - b^n}{a - b}, \tag{1}$$

also have a primitive divisor for $n \geq 7$. Moreover, such a formula defines a second order linear recurrence known as a Lucas sequence. Indeed, a Lucas sequence $U = (U_n)_{n \geq 0}$ with parameters $P, Q \in \mathbb{Z}$ is a sequence with initial terms $U_0 = 0$ and $U_1 = 1$ satisfying

$$U_{n+2} = PU_{n+1} - QU_n,$$

2020 *Mathematics Subject Classification.* 11B39, 11C08, 13A05.

Key words and phrases. Polynomial ring, Lucas sequence, primitive divisor, Zsigmondy's theorem, Carmichael's theorem.

for all $n \geq 0$. The polynomial $f(X) = X^2 - PX + Q$ is the characteristic polynomial of U. We denote its discriminant $P^2 - 4Q$ by Δ. If a and b are the roots of f in $\mathbb{Q}(\sqrt{\Delta})$, then either

$$U_n = na^{n-1} \quad \text{or} \quad U_n = \frac{a^n - b^n}{a - b},$$

for all $n \geq 0$, depending on whether $a = b$ or $a \neq b$ respectively. Therefore, (1) leads to another generalization of Zsimondy's theorem with a and b not only integers, but also quadratic conjugates: is there an $n_0 \geq 1$ such that U_n has a primitive prime divisor $p \nmid \Delta = (a-b)^2$ for all $n \geq n_0$? If n_0 exists, can we classify all sequences U and integers $1 \leq n \leq n_0$ for which U_n fails to have a primitive divisor?

A partial answer was given by Carmichael [3] in the case $\gcd(P, Q) = 1$ and $\Delta > 0$, where $n_0 = 13$. For instance, let $P = 1$ and $Q = -1$. Then U is the Fibonacci sequence F which has the form

$$F_n = \frac{\phi^n - \bar{\phi}^n}{\sqrt{5}},$$

for all $n \geq 0$, where ϕ is the golden ratio and $\bar{\phi}$ its quadratic conjugate. Carmichael showed that F has a primitive prime divisor that does not divide Δ for all $n \notin \{1, 2, 5, 6, 12\}$. A full answer was given by Bilu, Hanrot, and Voutier [2] when P and Q are relatively prime. Their theorem states that U has a primitive prime divisor $p \nmid \Delta$ for all $n \geq 31$. Moreover, they give a full description of the sequences U and indices $1 \leq n \leq 30$ for which the theorem fails. Note that all such sequences, except for one, satisfy Carmichael's bound $n_0 = 13$. Indeed, the only exception is the Lucas sequence with parameters $P = 1$ and $Q = 2$ for which U_{30} does not have a primitive divisor.

Further generalizations may be considered. Here, we are concerned with polynomial rings $R[T]$ with R a field or a unique factorization domain. In both cases, $R[T]$ is a unique factorization domain in which the irreducible elements are irreducible polynomials. In this setting, we call a *primitive prime divisor* of U_n an irreducible polynomial that divides U_n, but no U_k for all $1 \leq k \leq n$, for U a Lucas sequence. Recently, Sha [4] investigated the case of rings A of multivariate polynomials over an arbitrary field K. In particular, Sha studied the case of Lucas sequences $L = (L_n)_{n \geq 1}$ with coprime parameters $P, Q \in A$ and proved the following theorem which we state as Sha did:

Theorem 1. *Suppose the characteristic $p > 0$ and let L' be the sequence obtained from $(L_n)_{n \geq 1}$ by deleting the terms L_n with $p \mid n$, then each term of L' beyond the second has a primitive prime divisor. If $p = 0$, then each term of $(L_n)_{n \geq 1}$ beyond the second has a primitive prime divisor.*

However, there seems to be a small mistake towards the end of Sha's proof, invalidating his result. Let us give a few counter examples to Theorem 1. Let A be any multivariate polynomial ring over a field K with characteristic $p \neq 3$, $P \in A$ be non-zero and $\lambda \in K^\times$. Let U be the Lucas sequence with characteristic polynomial

$$f(X) = X^2 - PX + (P^2 - \lambda).$$

Then, the first terms of U are $U_0 = 0, U_1 = 1, U_2 = P$ and $U_3 = \lambda$. Since λ is a non-zero constant, we see that U_3 does not have a primitive prime divisor. For a more specific example, we let $A = \mathbb{F}_q[T]$, where $\mathbb{F}_q$ is the finite field with $q = 7^s$

elements, $s \geq 1$. Define U with characteristic polynomial

$$f(X) = X^2 - 4TX + (3T^2 - 1).$$

We find that $U_6 = 2U_2U_3$. Thus, U_6 has no primitive prime divisor. The object of this paper is to obtain a corrected version of Sha's theorem for $R[T]$, where R is a field or a unique factorization domain. We use the same approach as Yabuta [5], who gave a simplified proof of Carmichael's result.

Section 2 is split in two parts. We first define and prove various divisibility properties of Lucas sequences in integral domains and fields. The proofs given are similar, if not the same, as the ones given for the usual Lucas sequences in $\mathbb{Z}$. See [1, Theorems 38 and 2, Lemma 2, Theorem 3, Lemmas 8 and 7, and Theorem 8] for the $\mathbb{Z}$-analogues of Lemmas 1, 2, and 4, Proposition 2, Lemmas 5 and 6, and Proposition 3 respectively. Then, we study prime ideals that divide terms of a Lucas sequence in a unique factorization domain.

We prove our main theorem in Section 3. For a Lucas sequence U and an integer $n \geq 1$, we show that if $p \nmid n$ then U_n has a primitive prime divisor except for $n = 1$ and possibly at most one value in $\{2, 3, 4, 6\}$. For each n in $\{2, 3, 4, 6\}$, we give a condition on P and Q for U_n to not have a primitive prime divisor.

Throughout this paper, the letter R denotes an integral domain with identity element 1. We use the letter p for the characteristic of R, where p stands for zero or a prime number. For $x \in R$, we use the notation (x) for the principal ideal in R generated by x. We let K be the field of fractions of R and $\bar{K}$ denote an algebraic closure of K. We let n denote a positive integer and ζ_n a primitive root of unity in $\bar{K}$. The notation (m, n) is used to denote the greatest common divisor of integers m and n.

2. Basic properties of general Lucas sequences

Let $P, Q \in R$ be non-zero. We consider $f(X) = X^2 - PX + Q \in R[X]$ with roots $a, b \in \bar{K}$. If $p \neq 2$, then using the discriminant method, we have $\Delta = P^2 - 4Q$ and

$$a = \frac{P + \sqrt{\Delta}}{2} \quad \text{and} \quad b = \frac{P - \sqrt{\Delta}}{2}.$$

This method does not work in characteristic 2. However, if a is a root of f then $b = a + P$ is the other root of f. Putting $\Delta = P^2 - 4Q = P^2$ in this case, we see that $a - b = \sqrt{\Delta}$ for all values of p. Let $U = U(P, Q)$ be the sequence defined by $U_0 = 0$, $U_1 = 1$ and $U_{n+2} = PU_{n+1} - QU_n$ for all integers $n \geq 0$. We see that U has characteristic polynomial f and, with a and b the roots of f, we find the explicit classic formula for U_n to be

$$U_n = \frac{a^n - b^n}{a - b},$$

or $U_n = na^{n-1}$ for all $n \geq 0$, depending on whether $a \neq b$ or $a = b$ respectively. We call U the *Lucas sequence* with parameters $P, Q \in R$.

We split this section into two subsections. We first give properties related to Lucas sequences in R a field or an integral domain. Next, we assume that R is a unique factorization domain and we study the behavior of prime ideals in a Lucas sequence.

2.1. **Fields and integral domains.** We consider two types of Lucas sequences: the degenerate and non-degenerate Lucas sequences. A sequence U such that $U_n = 0$ for some positive n is said to be degenerate. Therefore, a Lucas sequence which is not zero for all $n \geq 1$ is called non-degenerate. The following result shows that degeneracy can be expressed as a relation between the roots of the characteristic polynomial:

Lemma 1. *A Lucas sequence U is degenerate if and only if $a = \zeta b$ for some root of unity $\zeta \in K(\sqrt{\Delta})$, where $\zeta \neq 1$ if $p = 0$.*

Proof. If $a = b$, then $U_n = na^{n-1} = 0$ if and only if $p \mid n$ because $Q \neq 0$. If $a \neq b$, then $U_n = 0$ for some $n \geq 1$ if and only if

$$\frac{a^n - b^n}{a - b} = 0 \iff \left(\frac{a}{b}\right)^n = 1 \iff a = \zeta_n b,$$

where ζ_n is an n-th root of unity in $K(\sqrt{\Delta})$. □

Clearly, if U is zero for some $n \geq 1$, it follows that U cannot have primitive divisors past that term. Therefore, we assume throughout this paper that U is non-degenerate.

Proposition 1. *For all $m > n \geq 0$, we have $U_m = U_{n+1}U_{m-n} - QU_nU_{m-n-1}$.*

Proof. Induction on $m \geq n + 1$ for a fixed $n \geq 0$. □

Note that this proposition is valid for Lucas sequences in any commutative ring and is widely used throughout this section. Another important tool is the next lemma, which states that U is a divisibility sequence:

Lemma 2 (Divisibility sequence)**.** *For all $m, n \geq 0$, we have $(U_{mn}) \subset (U_n)$.*

Proof. By induction on $m \geq 0$, and using Proposition 1. □

We recall that two ideals I and J in R are said to be coprime if $I + J$ is equal to the whole ring R. For $R = \mathbb{Z}$ it is known that if P and Q are coprime, U satisfies interesting and strong properties. We now study the properties a general Lucas sequence may satisfy with the assumption $(P) + (Q) = R$.

Lemma 3. *Let $x, y, z \in R$. If $(y) + (z) = R$, then $(xy) + (z) = (x) + (z)$.*

Proof. One inclusion is trivial. Let $\alpha \in (x) + (z)$. Then, $\alpha = ax + bz$ for some $a, b \in R$. But $R = (y) + (z)$, so $a = uy + vz$ for some $u, v \in R$. Hence $\alpha = uxy + (b + xv)z \in (xy) + (z)$. □

Lemma 4. *If $(P) + (Q) = R$, then $(Q) + (U_n) = R$ for all $n \geq 1$.*

Proof. We proceed by induction on $n \geq 1$. If $n = 1$, then $(Q) + (1) = R$. Assume that the result is true for some $n \geq 1$. We have

$$\begin{aligned}(Q) + (U_{n+1}) &= (Q) + (PU_n - QU_{n-1}) \\ &= (Q) + (PU_n) \\ &= (Q) + (P) \\ &= R\end{aligned}$$

where we used Lemma 3 with $x = P$, $y = U_n$ and $z = Q$ in the last step and the assumption $(P) + (Q) = R$. The result follows by induction. □

Proposition 2. *We have $(P)+(Q)=R$ if and only if $(U_m)+(U_n)=(U_{(m,n)})$ for all $m,n\geq 0$.*

Proof. For the "if" part, $R=(U_2)+(U_3)=(P)+(P^2-Q)=(P)+(Q)$. For the converse, we start by showing the result holds for $m=n+1$ by induction on $n\geq 0$. The case $n=0$ is trivial, thus assume the result is valid for some integer $n\geq 0$. We have

$$(U_{n+2})+(U_{n+1})=(PU_{n+1}-QU_n)+(U_{n+1})=(QU_n)+(U_{n+1}).$$

By Lemma 4, we have $R=(Q)+(U_{n+1})$. Thus, by Lemma 3 with $x=U_n$, we obtain

$$(U_{n+2})+(U_{n+1})=(U_n)+(U_{n+1}),$$

and we conclude by the induction hypothesis. Next, let $m\geq 0$ be an integer. Since $(m,n)=(n,m)$, we may assume without loss of generality that $m\geq n$ and write $m=qn+r$, where $q\geq 0$ and $0\leq r<n$. By Proposition 1, we have

$$(U_m)=(U_{r+1}U_{nq}-QU_rU_{nq-1})\subset(U_{nq})+(QU_rU_{nq-1}).$$

We already know that $(U_{nq})+(U_{nq-1})=R$, so that

$$(U_{nq})+(QU_rU_{nq-1})=(U_{nq})+(QU_r)$$

by Lemma 3. Moreover, since $(U_{nq})+(Q)=R$, we obtain

$$(U_{nq})+(QU_rU_{nq-1})=(U_{nq})+(U_r),$$

by Lemmas 3 and 4. By Lemma 2, we have $(U_{nq})\subset(U_n)$ and thus

$$(U_m)+(U_n)\subset(U_{nq})+(U_r)+(U_n)=(U_n)+(U_r).$$

We obtain $(U_m)+(U_n)\subset(U_{(m,n)})$ by applying the Euclidean algorithm to this method. The other inclusion follows trivially from Lemma 2. □

A non-degenerate Lucas sequence $U=U(P,Q)$ with $(P)+(Q)=R$ is called a *regular* Lucas sequence. In addition, if $\Delta\neq 0$, then U is called a Δ-*regular* Lucas sequence.

From now on, we assume that R is an integral domain that is not a field. Let $\mathfrak{a}\subset R$ be an ideal. We define the rank of $\mathfrak{a}$ in U, denoted by $\rho_U(\mathfrak{a})$ or ρ, to be the least integer $n\geq 1$ such that $(U_n)\subset\mathfrak{a}$. If the rank does not exist, we write $\rho_U(\mathfrak{a})=+\infty$. Let $D:=(P)+(Q)$.

Lemma 5. *If $D+\mathfrak{a}=R$, then either $(Q)+\mathfrak{a}=R$ or $\rho_U(\mathfrak{a})=+\infty$.*

Proof. If $(Q)+\mathfrak{a}\neq R$, then there exists a maximal ideal $\mathfrak{m}\subset R$ such that $(Q)+\mathfrak{a}\subset\mathfrak{m}$ and

$$U_{n+2}-PU_{n+1}=-QU_n\in\mathfrak{m},$$

for all $n\geq 0$. Thus, we have $U_{n+2}\equiv PU_{n+1}\equiv\cdots\equiv P^{n+1}\pmod{\mathfrak{m}}$, but $(Q)\subset\mathfrak{m}$ and $D+\mathfrak{m}=R$ imply that $(P)\not\subset\mathfrak{m}$. Hence $U_n\notin\mathfrak{m}$ for all $n\geq 2$. The case $n=1$ is easily verified. It follows that U_n does not belong to $\mathfrak{a}$ for all $n\geq 1$ and that $\rho_U(\mathfrak{a})=+\infty$. □

Throughout the rest of this paper, we let the letter $\mathfrak{p}$ denote a prime ideal in R. Next, we study properties analogous to well-known prime divisibility properties in the $R=\mathbb{Z}$ setting.

Lemma 6. *If $D\not\subset\mathfrak{p}$, then $(U_{n+1})+(U_n)\not\subset\mathfrak{p}$ for all $n\geq 0$.*

Proof. Let $\rho = \rho_U(\mathfrak{p})$. If $\rho = +\infty$, there is nothing to do. If $\rho < +\infty$, we proceed by induction on $n \geq 0$. If $n = 0$, then $(0) + (1) = R \not\subset \mathfrak{p}$. Assume the result holds for some $n \geq 0$ and that

$$(U_{n+2}) + (U_{n+1}) = (QU_n) + (U_{n+1}) \subset \mathfrak{p}, \tag{2}$$

by contradiction. We find that $(QU_n) \subset \mathfrak{p}$. Since $\mathfrak{p}$ is a prime ideal, $QU_n \in \mathfrak{p}$ implies that Q or U_n belongs to $\mathfrak{p}$. However, since the rank of $\mathfrak{p}$ exists, we must have $(Q) \not\subset \mathfrak{p}$ by Lemma 5. Thus we conclude that $(U_n) \subset \mathfrak{p}$. By (2), we have $(U_{n+1}) \subset \mathfrak{p}$ and therefore

$$(U_{n+1}) + (U_n) \subset \mathfrak{p},$$

contradicting the induction hypothesis. Hence $(U_{n+2}) + (U_{n+1}) \not\subset \mathfrak{p}$.

□

Proposition 3. *If $(Q) \not\subset \mathfrak{p}$, then $(U_n) \subset \mathfrak{p}$ if and only if $\rho_U(\mathfrak{p}) \mid n$.*

Proof. The "if" part follows from Lemma 2. Assume that $(U_n) \subset \mathfrak{p}$. By minimality of the rank, we must have $n \geq \rho := \rho_U(\mathfrak{p})$. Hence $n = q\rho + r$ for some $q \geq 1$ and $0 \leq r < \rho$. By Proposition 1, we have

$$U_n = U_{r+1}U_{q\rho} - QU_rU_{q\rho-1}.$$

By Lemma 2, this implies that $(QU_rU_{q\rho-1}) \subset \mathfrak{p}$. Since $(Q) \not\subset \mathfrak{p}$, we have $D \not\subset \mathfrak{p}$ and by Lemma 6, we find that $(U_{q\rho}) + (U_{q\rho-1}) \not\subset \mathfrak{p}$. Since $(U_{q\rho}) \subset \mathfrak{p}$, we obtain that $(U_{q\rho-1}) \not\subset \mathfrak{p}$. Thus, we have $QU_rU_{q\rho-1} \in \mathfrak{p}$ and $QU_{q\rho-1} \notin \mathfrak{p}$. Since $\mathfrak{p}$ is a prime ideal, we find that $U_r \in \mathfrak{p}$, so $(U_r) \subset \mathfrak{p}$. But $r < \rho$ implies that $r = 0$ and $n = q\rho$ by minimality of the rank. □

2.2. Unique factorization domains.

From now on, we assume that U is a regular Lucas sequence, i.e., it satisfies $(P)+(Q) = R$, and that R is a unique factorization domain with characteristic p. Hence irreducible elements $x \in R$ are prime elements, that we call primes. We denote both x and the prime ideal (x) by $\mathfrak{p}$ as a shorthand. We let $v_{\mathfrak{p}}$ denote the $\mathfrak{p}$-adic valuation, the function defined by

$$v_{\mathfrak{p}}(x) = \max\{n \geq 1 : \mathfrak{p}^n \mid x\},$$

for all non-zero $x \in R$, and $v_p(0) = -\infty$. Moreover, a valuation satisfies the following properties:

$$v_{\mathfrak{p}}(xy) = v_{\mathfrak{p}}(x) + v_{\mathfrak{p}}(y) \quad \text{and} \quad v_{\mathfrak{p}}(x + y) \geq \min(v_{\mathfrak{p}}(x), v_{\mathfrak{p}}(y)),$$

for all $x, y \in R$. We recall that a valuation and its properties can be extended to the field of fractions of R by $v_{\mathfrak{p}}(x/y) = v_{\mathfrak{p}}(x) - v_{\mathfrak{p}}(y)$ for all $x, y \in R$. By Proposition 3, we know that a prime $\mathfrak{p} \nmid Q$ divides a term U_n if and only if $\rho_U(\mathfrak{p})$ divides n. The aim of this subsection is to describe the behavior of $v_{\mathfrak{p}}(U_n)$ for all integers $n \geq 1$ divisible by $\rho_U(\mathfrak{p})$.

Lemma 7. *Assume $p > 0$. For all $i, n \geq 0$, we have $U_{p^i n} = \Delta^{\frac{p^i-1}{2}} U_n^{p^i}$.*

Proof. Since $a - b = \sqrt{\Delta}$, we have

$$U_{p^i n} = \frac{a^{p^i n} - b^{p^i n}}{a - b} = \frac{(a^n - b^n)^{p^i}}{a - b} = (a - b)^{p^i - 1} U_n^{p^i} = \Delta^{\frac{p^i-1}{2}} U_n^{p^i}.$$

□

Lemma 8. *Assume $p > 0$ and $\mathfrak{p} \nmid Q$. Then $\mathfrak{p} \mid \Delta$ if and only if $\rho_U(\mathfrak{p}) = p$.*

Proof. By Lemma 7, we have $U_p = \Delta^{(p-1)/2}$. (Note that $U_2 = P$ and $\Delta = P^2$ in characteristic 2.) Thus, all primes of rank p divide Δ. For the converse, we find that $\rho_U(\mathfrak{p}) \mid p$ by Proposition 3. Hence $\rho_U(\mathfrak{p}) = p$ since $U_1 = 1$. □

Theorem 2. *Assume $p > 0$ and $\mathfrak{p} \nmid Q$. Let $\rho = \rho_U(\mathfrak{p})$. Then*

$$v_{\mathfrak{p}}(U_{\rho n}) = p^{v_p(n)} v_{\mathfrak{p}}(U_\rho) + \frac{(p^{v_p(n)} - 1) v_{\mathfrak{p}}(\Delta)}{2}.$$

Proof. Write $n = \lambda p^u$ for some integers $\lambda \geq 1$, $p \nmid \lambda$, and $u \geq 0$. Since U is a regular sequence, by Proposition 2, we have $(U_n, U_{\rho p^{u+1}}) = U_{(n,\rho p^{u+1})} = U_{\rho p^u}$. The result follows by taking the $\mathfrak{p}$-adic valuation and using Lemma 7.

□

The next theorem deals with the case of a unique factorization domain and a polynomial ring R of characteristic zero. The key point is that R is a polynomial ring and we can use the notion of polynomial degree. In particular, any irreducible element $\mathfrak{p}$ is an irreducible polynomial with positive degree. Note that the theorem is not valid otherwise, as [1, Sect. 2.4, Lemma 11] shows for $R = \mathbb{Z}$.

Theorem 3. *Assume that R is a polynomial ring with $p = 0$. Let $\mathfrak{p} \nmid Q$ be a prime of rank ρ. Then, we have $v_{\mathfrak{p}}(U_{\rho n}) = v_{\mathfrak{p}}(U_\rho)$ for all $n \geq 1$.*

Proof. Following the method found in the book of Ballot and Williams [1, Section 2.2], we may prove the following formulas in any integral ring with zero characteristic:

$$2^{m-1} U_{mn} = \sum_{k=0}^{\lfloor (m-1)/2 \rfloor} \binom{m}{2k+1} \Delta^k U_n^{2k+1} V_n^{m-2k-1}, \tag{3}$$

for all $m, n \geq 0$, and $V_n^2 - \Delta U_n^2 = 4Q^n$ for all $n \geq 0$. It follows from the latter that (U_n, V_n) divides $4Q^n$ for all $n \geq 1$. Hence $\mathfrak{p}$ is not a divisor of V_ρ, since $\mathfrak{p} \nmid Q$ and $\mathfrak{p}$ has positive degree. Putting $n = \rho$ in (3), we obtain

$$2^{m-1} U_{m\rho} \equiv m U_\rho V_\rho^{m-1} \pmod{U_\rho^2}.$$

If $\lambda = v_{\mathfrak{p}}(U_\rho)$, then this implies

$$2^{m-1} U_{m\rho} \equiv m U_\rho V_\rho^{m-1} \pmod{\mathfrak{p}^{\lambda+1}},$$

but $\mathfrak{p}^\lambda \| m U_\rho V_\rho^{m-1}$ and we find that $v_{\mathfrak{p}}(U_{m\rho}) = \lambda$. □

3. The main theorem

Let $R = A[T]$ be the ring of polynomials with coefficients in A, where A is a field or a unique factorization domain with characteristic p equal to zero or a prime number. This makes R a unique factorization domain as well. We prove our main theorem on primitive prime divisors of Lucas sequences with parameters $P, Q \in R$. We assume that P and Q are non-zero, coprime and such that one of P or Q has positive polynomial degree. We follow a method of Yabuta [5].

Let $(Q_n)_{n \geq 0}$ be the sequence defined by $Q_0 = Q_1 = 1$ and for $n \geq 2$ by $Q_n := Q_n(a,b) = \Phi_n(a,b)$, where Φ_n is the n-th order homogeneous cyclotomic polynomial defined by

$$\Phi_n(X,Y) = \prod_{\substack{1 \leq k \leq n \\ (k,n)=1}} (X - \zeta_n^k Y),$$

for all $n \geq 1$. We have the following well-known identity:

$$X^n - Y^n = \prod_{d|n} \Phi_d(X,Y) = (X-Y) \prod_{\substack{d|n \\ d>1}} \Phi_d(X,Y),$$

which, applied to the Lucas sequence U, yields

$$U_n = \frac{a^n - b^n}{a-b} = \prod_{\substack{d|n \\ d>1}} \Phi_d(a,b) = \prod_{d|n} Q_d. \tag{4}$$

We want to study the prime divisors of U_n by looking at those of Q_d for all $d \mid n$. However, we first need to check that Q_n belongs to A for all $n \geq 1$. It is true for $n = 1$ and $n = 2$ since $Q_1 = 1$ and $Q_2 = P$. For $n \geq 3$, we first note that $\varphi(n)$ is even, where φ is Euler's totient function. Moreover, following the method used in [1, p. 89], we may prove that $Q_n(a,b) = Q_n(b,a)$. It follows that $Q_n \in K = \mathrm{Frac}(R)$. Indeed, let $L = K(a)$ be the splitting field of the characteristic polynomial of U, that is, $X^2 - PX + Q$. It is a Galois extension of K of degree 1 or 2. Hence $Q_n \in K$ if and only if $\sigma(Q_n) = Q_n$ for the non-trivial automorphism σ of L/K when it exists. If L is a quadratic extension of K, then

$$\sigma(Q_n(a,b)) = Q_n(\sigma(a), \sigma(b)) = Q_n(b,a) = Q_n(a,b),$$

because σ sends a to b. Thus $Q_n \in K$. To prove that Q_n is integral, we show that $v_{\mathfrak{p}}(Q_n) \geq 0$ for all irreducible elements $\mathfrak{p} \in R$. By (4), we have

$$v_{\mathfrak{p}}(U_n) = \sum_{d|n} v_{\mathfrak{p}}(Q_d),$$

and, using the Möbius inversion formula, we obtain

$$v_{\mathfrak{p}}(Q_n) = \sum_{d|n} \mu(n/d) v_{\mathfrak{p}}(U_d).$$

Note that in prime characteristic, Lemma 7 shows that it suffices to determine $v_{\mathfrak{p}}(Q_n)$ for all $n \geq 3$ not divisible by p. For simplification, we write $p \nmid n$ even in characteristic zero since it is equivalent to $n \geq 1$. If $\rho_U(\mathfrak{p}) \nmid n$, then $v_{\mathfrak{p}}(Q_n) = 0$ and we are done. Assume $\rho = \rho_U(\mathfrak{p}) \mid n$. By Theorem 2 if $p > 0$ and Theorem 3 if $p = 0$, we have

$$v_{\mathfrak{p}}(Q_n) = \sum_{d|n,\ \rho|d} \mu(n/d) v_{\mathfrak{p}}(U_d) = v_{\mathfrak{p}}(U_\rho) \sum_{d' | \frac{n}{\rho}} \mu(n/\rho d'),$$

for all $n \geq 3$, $p \nmid n$. The last sum is well-known to be equal to 1 if $n/\rho = 1$ and 0 if $n/\rho > 1$. Hence we just proved the following lemma:

Lemma 9. *We have $Q_n \in R$ for all $n \geq 1$. Moreover, if $p \nmid n$, then $\mathfrak{p} \mid Q_n$ if and only if $n = \rho_U(\mathfrak{p})$.*

Suppose $p \nmid n$. It follows from Lemma 9 that U_n has no primitive prime divisor if and only if Q_n is a constant in R, i.e., $Q_n \in A$. Now, assuming $n \geq 3$, we have $0 < k < n/2$ only if $n - k > n/2$. Therefore, using the identities $a^2 + b^2 = P^2 - 2Q$

and $ab = Q$, we may write

$$\begin{aligned} Q_n &= \prod_{\substack{0<k<n/2\\(k,n)=1}} (a-\zeta_n^k b)(a-\zeta_n^{n-k} b) \\ &= \prod_{\substack{0<k<n/2\\(k,n)=1}} (a^2+b^2-(\zeta_n^k+\zeta_n^{n-k})ab) \\ &= \prod_{\substack{0<k<n/2\\(k,n)=1}} (P^2-\theta_k Q), \end{aligned} \tag{5}$$

where $\theta_k = 2+\zeta_n^k+\zeta_n^{-k}$. We work on the above product formula for Q_n to prove our main theorem. Indeed, we prove that for all but finitely many $n \geq 3$, this product has a non-constant factor.

Lemma 10. *Let R be a commutative ring and $a, b \in R^\times$. We have equality $a + a^{-1} = b + b^{-1}$ if and only if $a = b$ or $a = b^{-1}$.*

Proof. The "if" part is trivial. For the converse, note that the polynomial $f(x) = x^2 - (a+a^{-1})x + 1$ annihilates both a and b because $a + a^{-1} = b + b^{-1}$. We have

$$\begin{aligned} f(a) = f(b) &\iff a^2 - a(a+a^{-1}) + 1 = b^2 - b(a+a^{-1}) + 1 \\ &\iff a^2 - b^2 = (a-b)(a+a^{-1}). \end{aligned}$$

If $a \neq b$, we may divide by $a - b$ and we obtain $a + b = a + a^{-1}$, or equivalently, $a = b^{-1}$. □

Theorem 4. *Assume $n \geq 2$ and $p \nmid n$. Then U_n has no primitive prime divisor if and only if there exists a non-zero constant $\lambda \in A$ such that one of the following holds:*

(1) $n = 2$, $P = \lambda$ and $\deg(Q) \geq 1$,
(2) $n = 3$ and $P^2 = Q + \lambda$,
(3) $n = 4$ and $P^2 = 2Q + \lambda$,
(4) $n = 6$ and $P^2 = 3Q + \lambda$.

In particular, we see that at most one of the above can hold.

Proof. The case $n = 2$ yields $U_2 = P = \lambda$. This is clearly sufficient. For $n \geq 3$, it suffices to check whether Q_n belongs to A by Lemma 9. By (5), we want to show that at least one of the $\varphi(n)/2$ factors $P^2 - \theta_k Q$ has positive degree, where $0 < k < n/2$ and $(k, n) = 1$. If $\deg(P^2) \neq \deg(Q)$, then $\deg(P^2 - \theta_k Q)$ is equal to the maximum of $\deg(P^2)$ and $\deg(Q)$, which is positive. Thus $Q_n \notin A$ and U_n has a primitive divisor by Lemma 9. Assume $2\deg(P) = \deg(Q)$ and $\varphi(n) > 2$. Then Q_n has a least two factors of the form $P^2 - \theta_k Q$. By contradiction, assume that there exist i and j, $i \neq j$, such that both

$$P^2 - \theta_i Q \quad \text{and} \quad P^2 - \theta_j Q$$

are constants, say λ_i and λ_j. We obtain $Q(\theta_j - \theta_i) = \lambda_i - \lambda_j$. However, we have $\deg(\lambda_i - \lambda_j) \leq 0$ and $\deg(Q) \geq 1$, since P and Q are not both constants by hypothesis. It follows that $\lambda_i = \lambda_j$ and $\theta_i = \theta_j$. The latter is equivalent to $\zeta_n^i + \zeta_n^{-i} = \zeta_n^j + \zeta_n^{-j}$. By Lemma 10, we either have $\zeta_n^i = \zeta_n^j$ or $\zeta_n^i = \zeta_n^{-j}$. Hence $n \mid i - j$ or $n \mid i + j$, but $0 < i, j < n/2$ implies that $i = j$, a contradiction. It follows that one and only one factor of Q_n in (5) can be constant. Since $\varphi(n) > 2$, $\varphi(n)$ is even and Q_n has $\varphi(n)/2$ factors in (5), we find that $\deg(Q_n) \geq 1$. The remaining cases for $2\deg(P) = \deg(Q)$ are integers $n \geq 3$ such that $\varphi(n) = 2$, that is, $n = 3, 4$ and 6. Note that we have the following:

$$U_3 = P^2 - Q, \quad U_4 = U_2(P^2 - 2Q), \quad \text{and} \quad U_6 = U_2U_3(P^2 - 3Q).$$

Using Proposition 2, we obtain that $Q_3 = P^2 - Q$, $Q_4 = P^2 - 2Q$, and $Q_6 = P^2 - 3Q$. The result follows. □

In conclusion, we obtained that the greatest integer $n \geq 1$ for which U_n has no primitive divisor is at most equal to 6. For each $1 \leq n \leq 6$, we found the conditions on P and Q for U_n not to have a primitive divisor. Note that the method we used is enough to obtain a similar result for sequences of the form $(a^n - b^n)_{n\geq 0}$, with $a, b \in R$, and for Lehmer sequences in R.

References

[1] C. Ballot and H. C. Williams, *The Lucas Sequences: Theory and Applications*, CMS/CAIMS Books Mathematics, Springer, 2023.

[2] Y. Bilu, G. Hanrot, and P. M. Voutier. Existence of primitive divisors of Lucas and Lehmer numbers. *J. Reine Angew. Math.*, **539** (2001), 75–122. With an appendix by M. Mignotte.

[3] 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, 49–70.

[4] M. Sha. Zsigmondy's theorem and primitive divisors of the Lucas and Lehmer sequences in polynomial rings. *J. Algebra*, **586** (2021), 830–843.

[5] M. Yabuta. A simple proof of Carmichael's theorem on primitive divisors. *Fibonacci Quart.*, **39** (2001), no. 5, 439–443.

[6] K. Zsigmondy. Zur Theorie der Potenzreste. Monatsh. *Math. Phys.*, **3** (1892), no. 1, 265–284.

Normandie Université, UNICAEN, CNRS, LMNO, 14000 Caen, France
Email address: `joaquim.cera-daconceicao@unicaen.fr`
URL: https://jceradaconceicao.github.io