ON THE LUCAS AND LEHMER SEQUENCES IN POLYNOMIAL RINGS

MIN SHA

ABSTRACT. In this paper, we obtain analogues of Zsigmondy's theorem and the primitive divisor results for the Lucas and Lehmer sequences in polynomial rings of several variables.

1. INTRODUCTION

1.1. **Background and motivation.** Given a sequence $(a_n)_{n\geq 1}$ of the rational integers $\mathbb{Z}$, a prime divisor of a term a_n is called *primitive* if it divides no earlier term. The sequence is a *divisibility sequence* if $a_m \mid a_n$ whenever $m \mid n$, and it is a *strong divisibility sequence* if $\gcd(a_m, a_n) = a_d$ with $d = \gcd(m, n)$ for any positive integers m, n. These notions apply to any sequence of a unique factorization domain.

It is a classical and still very active topic in number theory to study primitive prime divisors of an integer sequence. The classical Zsigmondy theorem [22] in 1892, extending earlier work of Bang [2] in the case $b = 1$, says that every term beyond the sixth in the sequence $(a^n - b^n)_{n\geq 1}$ has a primitive prime divisor, where a, b are positive coprime integers. This theorem was independently rediscovered by Birkhoff and Vandiver [4]. Results of this form are often useful in group theory and in the theory of recurrence sequences (see [8, Section 6.3] for a discussion and references).

In 1913, Carmichael [5] showed that each term of the Lucas sequence $((a^n - b^n)/(a - b))_{n\geq 1}$ beyond the twelfth has a primitive prime divisor, where a, b are real algebraic integers such that a/b is not a root of unity, and $a + b$ and ab are coprime integers in $\mathbb{Z}$. In 1955, Ward [19] obtained a similar result for the Lehmer sequence $(s_n)_{n\geq 1}$ with $s_n = (a^n - b^n)/(a - b)$ for odd n and $s_n = (a^n - b^n)/(a^2 - b^2)$ for even n, where a, b are real, and $(a + b)^2$ and ab are coprime integers in $\mathbb{Z}$. All these results, including Zsigmondy's theorem, were extended to any number field (that is, a, b do not need to be real) by Schinzel [15]

in an effective but not explicit manner (see [12] for an earlier work), which was first made explicitly by Stewart [18]. Furthermore, in 2001, Bilu, Hanrot and Voutier [3] listed all the Lucas and Lehmer numbers without primitive prime divisor.

So far, the above classical results have various extensions in different settings. For example, the extensions to elliptic divisibility sequence [7, 16], to dynamical sequences [11, 14], to function fields defined over number fields [10], to Drinfeld modules [1, 13, 21]. Recently, Flatters and Ward [9] found an analogue of Zsigmondy's theorem for a polynomial sequence $(f^n - g^n)_{n \geq 1}$, where f, g are two coprime polynomials in a polynomial ring $K[X]$ (K is a field).

In this paper, we want to establish analogues of Zsigmondy's theorem and the primitive divisor results for the Lucas and Lehmer sequences in polynomial rings of several variables. The approach is essentially the same as in [9]. It in fact follows the classical one with some modifications needed to avoid terms in the sequence where the Frobenius automorphism precludes primitive divisors. However, for analogues of polynomial Lucas and Lehmer sequences, it indeed needs some more considerations.

Throughout the paper, let K be a field, and $R = K[X_1, \ldots, X_r]$ the ring of polynomials in varibales $X_1, \ldots, X_r$. Let p be the characteristic of K. Note that R is a unique factorization domain. Besides, a *prime divisor* of a polynomial h in R means a monic irreducible polynomial in R dividing h.

We state the main results in the rest of Section 1, and then prove them later on.

1.2. **Main results.** Let λ, η be non-zero algebraic elements over R such that λ/η is not a root of unity. Assume that $(\lambda + \eta)^2$ and $\lambda\eta$ are non-zero coprime polynomials in R which are not both in K. Define the *Lehmer sequence* of R:

$$
U_n = \begin{cases}
\frac{\lambda^n - \eta^n}{\lambda - \eta} & \text{if } n \text{ is odd,} \\[2ex]
\frac{\lambda^n - \eta^n}{\lambda^2 - \eta^2} & \text{if } n \text{ is even.}
\end{cases}
$$

We remark that the Lehmer sequence $(U_n)_{n \geq 1}$ satisfies the following recurrence relation over R:

$$
U_{n+4} = (\lambda^2 + \eta^2)U_{n+2} - \lambda^2\eta^2 U_n, \quad n = 1, 2, \ldots.
$$

The following two theorems are about the strong divisibility property and the primitive prime divisors of the sequence $(U_n)_{n \geq 1}$, respectively.

Theorem 1.1. *The sequence $(U_n)_{n \geq 1}$ is a strong divisibility sequence.*

Theorem 1.2. *Suppose the characteristic $p > 0$ and let U' be the sequence obtained from $(U_n)_{n \geq 1}$ by deleting the terms U_n with $p \mid n$, then each term of U' beyond the second has a primitive prime divisor. If $p = 0$, then each term of $(U_n)_{n \geq 1}$ beyond the second has a primitive prime divisor.*

Applying Theorems 1.1 and 1.2, we can obtain the strong divisibility property and the primitive divisor result for polynomial Lucas sequences.

Let α, β be non-zero algebraic elements over R such that the quotient α/β is not a root of unity. Assume that $\alpha + \beta$ and $\alpha\beta$ are coprime polynomials in R which are not both in K. Define the *Lucas sequence* of R:

$$L_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \quad n = 1, 2, \dots.$$

We remark that the Lucas sequence $(L_n)_{n \geq 1}$ satisfies the following recurrence relation over R:

$$L_{n+2} = (\alpha + \beta)L_{n+1} - \alpha\beta L_n, \quad n = 1, 2, \dots.$$

Theorem 1.3. *The sequence $(L_n)_{n \geq 1}$ is a strong divisibility sequence.*

Theorem 1.4. *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.*

Theorem 1.4 in fact implies an analogue of Zsigmondy's theorem in R. Let f, g be non-zero coprime polynomials in R such that f and g are not both in K and the quotient f/g is not a root of unity. Define the sequence of R:

$$F_n = f^n - g^n, \quad n = 1, 2, \dots.$$

Theorem 1.5. *The sequence $(F_n)_{n \geq 1}$ is a strong divisibility sequence.*

Theorem 1.6. *Suppose the characteristic $p > 0$ and let F' be the sequence obtained from $(F_n)_{n \geq 1}$ by deleting the terms F_n with $p \mid n$, then each term of F' beyond the second has a primitive prime divisor. If $p = 0$, then each term of $(F_n)_{n \geq 1}$ beyond the second has a primitive prime divisor.*

For f, g as the above, define the sequence:

$$S_n = f^n + g^n, \quad n = 1, 2, \dots.$$

If $p \neq 2$, then $(S_n)_{n \geq 1} \neq (F_n)_{n \geq 1}$. Note that $F_{2n} = F_n S_n$, which implies that each primitive prime divisor of F_{2n} comes from S_n. Then, the following corollary is a direct consequence of Theorem 1.6.

Corollary 1.7. *Suppose $p > 0$, and let S' be the sequence obtained from $(S_n)_{n \geq 1}$ by deleting the terms S_n with $p \mid n$, then each term of S' beyond the second has a primitive prime divisor. If $p = 0$, then each term of $(S_n)_{n \geq 1}$ beyond the second has a primitive prime divisor.*

2. Preliminaries

Although the sequences we consider are defined over R, we prefer to establish some results in a more general setting. Throughout this section, let D be a unique factorization domain.

Recall that the resultant of two homogeneous polynomials in variables X and Y is defined to the determinant of their Sylvester matrix. Some basic properties of this resultant are listed in the following lemma; see [17, Proposition 2.3].

Lemma 2.1. *For two non-constant homogeneous polynomials defined over a field*

$$A(X,Y) = a_0 X^m + a_1 X^{m-1} Y + \ldots + a_m Y^m = a_0 \prod_{i=1}^{m} (X - \alpha_i Y)$$

and

$$B(X,Y) = b_0 X^n + b_1 X^{n-1} Y + \ldots + b_n Y^n = b_0 \prod_{j=1}^{n} (X - \beta_j Y),$$

their resultant is

$$\mathrm{Res}(A,B) = a_0^n b_0^m \prod_{i=1}^{m} \prod_{j=1}^{n} (\alpha_i - \beta_j) \in \mathbb{Z}[a_0, \ldots, a_m, b_0, \ldots, b_n].$$

Moreover, there exist $G_1, H_1, G_2, H_2 \in \mathbb{Z}[a_0, \ldots, a_m, b_0, \ldots, b_n][X,Y]$ homogeneous in X and Y such that

$$G_1 A + H_1 B = \mathrm{Res}(A,B) X^{m+n-1},$$
$$G_2 A + H_2 B = \mathrm{Res}(A,B) Y^{m+n-1}.$$

For any integer $n \geq 1$, the n-th homogeneous cyclotomic polynomial is defined by

$$\Phi_n(X,Y) = \prod_{k=1,\, \gcd(k,n)=1}^{n} (X - \zeta_n^k Y) \in \mathbb{Z}[X,Y],$$

where ζ_n is a primitive n-th root of unity, and we also define the polynomial

$$P_n(X,Y) = \frac{X^n - Y^n}{X - Y} = \sum_{k=0}^{n-1} X^{n-1-k} Y^k = \prod_{k=1}^{n-1} (X - \zeta_n^k Y).$$

Then, it is easy to see that

$$X^n - Y^n = \prod_{d|n} \Phi_d(X,Y), \qquad P_n(X,Y) = \prod_{d|n,\, d\geq 2} \Phi_d(X,Y).$$

The following result is [9, Lemma 2.4] about the resultant of $P_m(X,Y)$ and $P_n(X,Y)$.

Lemma 2.2. *For any positive coprime integers m and n, we have* $\mathrm{Res}(P_m, P_n) = \pm 1$.

We now want to establish some results about coprime elements in D. First, we prove a general result.

Lemma 2.3. *Let a, b be algebraic elements over D. Assume that $(a + b)^2$ and ab are coprime elements in D. Let $A(X,Y), B(X,Y) \in \mathbb{Z}[X,Y]$ be non-constant homogeneous polynomials with resultant $\mathrm{Res}(A,B) = \pm 1$. Assume that both $A(a,b)$ and $B(a,b)$ are in D. Then, $A(a,b)$ and $B(a,b)$ are coprime in D.*

Proof. Let $m = \deg A$ and $n = \deg B$. By assumption, $a^2 + b^2$ and ab are also coprime in D. Note that for any integer $k \geq 1$, $a^{2k} + b^{2k}$ is in D. Using Lemma 2.1 and noticing $\mathrm{Res}(A,B) = \pm 1$, we obtain that there exist $u_1, w_1, u_2, w_2 \in \mathbb{Z}[a,b]$ such that

$$u_1 A(a,b) + w_1 B(a,b) = a^{2(m+n-1)} + b^{2(m+n-1)} \in D$$

and

$$u_2 A(a,b) + w_2 B(a,b) = a^{2(m+n-1)} b^{2(m+n-1)} \in D.$$

By contradiction, suppose that $A(a,b)$ and $B(a,b)$ are not coprime in D. Then, there is a prime element $\pi \in D$ such that $\pi \mid A(a,b)$ and $\pi \mid B(a,b)$ in D.

By the above discussion, we obtain that both

$$\frac{u_1 A(a,b) + w_1 B(a,b)}{\pi}, \quad \frac{u_2 A(a,b) + w_2 B(a,b)}{\pi}$$

are in the fraction field of D and integral over D (because a, b are integral over D satisfying the equation $X^4 - (a^2 + b^2)X^2 + a^2 b^2 = 0$). Note that D is an integrally closed domain, so these two quotients are both in D. Hence, we have $\pi \mid a^{2(m+n-1)} + b^{2(m+n-1)}$ and $\pi \mid a^{2(m+n-1)} b^{2(m+n-1)}$ in D. So, $\pi \mid ab$ in D.

Let $k = m + n - 1$. We have known that $\pi \mid a^{2k} + b^{2k}$ and $\pi \mid ab$ in D. Consider

$$(a^2 + b^2)^k = a^{2k} + b^{2k} + \sum_{i=1}^{k-1} \binom{k}{i}(a^2)^i(b^2)^{k-i}$$

$$= a^{2k} + b^{2k} + a^2 b^2 \sum_{i=1}^{k-1} \binom{k}{i}(a^2)^{i-1}(b^2)^{k-1-i}.$$

Note that $\sum_{i=1}^{k-1} \binom{k}{i}(a^2)^{i-1}(b^2)^{k-1-i}$ is also in D, because it is symmetric in a^2 and b^2. Hence, we have $\pi \mid (a^2 + b^2)^k$, and then $\pi \mid a^2 + b^2$, so $\pi \mid (a+b)^2$ in D (because $\pi \mid ab$). This leads to a contradiction with the assumption that $(a + b)^2$ and ab are coprime in D. Therefore, $A(a, b)$ and $B(a, b)$ are coprime in D. $\qquad\square$

Based on Lemma 2.3, we can derive several results about coprime elements in R in the sequel.

Lemma 2.4. *Let a, b be two algebraic elements over D. Assume that $a+b$ and ab are coprime elements in D. Then, for any positive coprime integers m, n, $P_m(a, b)$ and $P_n(a, b)$ are coprime in D.*

Proof. Without loss of generality, we can assume $m \geq 2, n \geq 2$. Clearly, both $P_m(a, b)$ and $P_n(a, b)$ are in D. Because both $P_m(X, Y)$ and $P_n(X, Y)$ are symmetric in X and Y.

By assumption, $(a + b)^2$ and ab are coprime elements in D. Then, the desired result follows from Lemmas 2.2 and 2.3. $\qquad\square$

Lemma 2.5. *Let a, b be defined as in Lemma 2.3. Let m, n be two positive coprime integers such that both m and n are odd. Then, $P_m(a, b)$ and $P_n(a, b)$ are coprime in D.*

Proof. Without loss of generality, we can assume $m \geq 3, n \geq 3$. Since both $(a+b)^2$ and ab are in D, we have $a^2 + b^2 \in D$. Moreover, we have that for any integer $k \geq 1$, $a^{2k} + b^{2k} \in D$.

Note that $P_m(X, Y)$ is homogeneous of even degree $m - 1$ and symmetric in X and Y. So, if $X^i Y^j$ is a term in $P_m(X, Y)$, then $X^j Y^i$ is also a term in $P_m(X, Y)$, and then assuming $i \leq j$, we have

$$a^i b^j + a^j b^i = (ab)^i(a^{j-i} + b^{j-i}) \in D,$$

where we use the fact that $j - i$ is even (because $i + j = m - 1$ is even). Hence, we have that $P_m(a, b)$ is in D. Similarly, $P_n(a, b)$ is also in D. Now, the desired result follows directly from Lemmas 2.2 and 2.3. $\qquad\square$

Lemma 2.6. *Let a, b be defined as in Lemma 2.3. Let m, n be two positive coprime integers such that m is odd and n is even. Then, $P_m(a, b)$ and $P_n(a, b)/(a + b)$ are coprime in D.*

Proof. Without loss of generality, we can assume $m \geq 3, n \geq 4$ (because $P_2(a, b)/(a + b) = 1$). Since m is odd, as in the proof of Lemma 2.5 $P_m(a, b)$ is in D. For any odd integer $k \geq 1$, note that

$$\frac{a^k + b^k}{a + b} = a^{k-1} - a^{k-2}b + \ldots - ab^{k-2} + b^{k-1}$$

is homogeneous of even degree $k - 1$ and is symmetric in a and b, so it is in D. Hence, for even n, since

$$\frac{P_n(a, b)}{a + b} = \frac{a^{n-1} + b^{n-1}}{a + b} + ab \cdot \frac{a^{n-3} + b^{n-3}}{a + b} + \ldots + a^{\frac{n-2}{2}} b^{\frac{n-2}{2}} \cdot \frac{a + b}{a + b},$$

we have that $P_n(a, b)/(a + b)$ is in D.

Denote $T_n(X, Y) = P_n(X, Y)/(X + Y)$, which can be viewed as a polynomial over $\mathbb{Z}$. Using Lemma 2.1 and applying the same arguments as in the proof of [9, Lemma 2.4], we obtain that the resultant of $P_m(X, Y)$ and $T_n(X, Y)$ is equal to ± 1.

Hence, by Lemma 2.3, $P_m(a, b)$ and $T_n(a, b)$ are coprime in D. $\qquad\square$

Lemma 2.7. *Let a, b be defined as in Lemma 2.3. Let m, n be two positive integers such that both m and n are odd. Then, $P_m(a^n, b^n)$ and $(a^n + b^n)/(a + b)$ are coprime in D.*

Proof. Without loss of generality, we can assume $m \geq 3, n \geq 3$. As before, since m and n are odd, both $P_m(a^n, b^n)$ and $(a^n + b^n)/(a + b)$ are indeed in D.

Define

$$V_m(X, Y) = P_m(X^n, Y^n), \qquad W_n(X, Y) = \frac{X^n + Y^n}{X + Y}.$$

Both V_m and W_n can be viewed as polynomials over $\mathbb{Z}$. So, we first compute their resultant over $\mathbb{Z}$. Note that

$$V_m(X, Y) = \prod_{i=1}^{m-1}(X^n - \zeta_m^i Y^n) = \prod_{i=1}^{m-1}\prod_{j=1}^{n}(X - \zeta_n^j \zeta_{mn}^i Y),$$

and

$$W_n(X, Y) = \frac{X^n - (-Y)^n}{X + Y} = \prod_{k=1}^{n-1}(X + \zeta_n^k Y).$$

By Lemma 2.1, the resultant

$$\text{Res}(V_m, W_n) = \prod_{i=1}^{m-1} \prod_{j=1}^{n} \prod_{k=1}^{n-1} (\zeta_{mn}^i \zeta_n^j + \zeta_n^k) \in \mathbb{Z}.$$

For each factor $\zeta_{mn}^i \zeta_n^j + \zeta_n^k$ in the resultant, we have $\zeta_{mn}^i \zeta_n^j \neq \zeta_n^k$ (because otherwise we would have $\zeta_{mn}^i \zeta_{mn}^{mj} = \zeta_{mn}^{mk}$, and then $m \mid i$, but $1 \leq i \leq m-1$), and so $\zeta_{mn}^i \zeta_n^j + \zeta_n^k = \zeta_{m'}(1 - \zeta_2 \zeta_{n'})$ for some odd integer m' and odd integer $n' \geq 3$ (noticing both m, n are odd), and thus it is a unit by [20, Proposition 2.8]. Hence, $\text{Res}(V_m, W_n)$ is a unit in $\mathbb{Z}$, that is, $\text{Res}(V_m, W_n) = \pm 1$.

Therefore, as polynomials over D, we also have $\text{Res}(V_m, W_n) = \pm 1$. Then, by Lemma 2.3, $V_m(a, b)$ and $W_n(a, b)$ are coprime in D. □

Lemma 2.8. *Let a, b be defined as in Lemma 2.3. Then, for any odd integer $n \geq 1$, $(a^n - b^n)/(a - b)$ and $(a + b)^2$ are coprime in D.*

Proof. Without loss of generality, we fix an odd integer $n \geq 3$. As before, both $(a^n - b^n)/(a - b)$ and $(a + b)^2$ are in D.

As in the proof of Lemma 2.7, we deduce that the resultant of the homogeneous polynomials $(X^n - Y^n)/(X - Y)$ and $(X + Y)^2$ is equal to ± 1. Hence, using Lemma 2.3, we obtain that $(a^n - b^n)/(a - b)$ and $(a + b)^2$ are coprime in D. □

3. Proofs of Theorems 1.1 and 1.2

We need to make one more preparation.

Recall that p is the characteristic of the field K. As usual, denote by $v_\pi(h)$ the maximal power to which an irreducible polynomial π divides $h \in R$.

Let M be the fraction field of R. By assumption, $M(\lambda)$ is a field extension over M having degree at most four. Note that $\eta \in M(\lambda)$. For any irreducible polynomial $\pi \in R$, as usual v_π induces a valuation of M. It is well-known that the valuation v_π in M can be extended to the field $M(\lambda)$; see, for instance, [6, Theorem 3.1.2]. Without confusion, we still denote by v_π the corresponding extension of valuation in $M(\lambda)$.

Lemma 3.1. *Let $\pi \in R$ be an irreducible polynomial dividing U_n for some $n \geq 3$. Then, for any $m \geq 1$ with $p \nmid m$ (including the case $p = 0$), we have $v_\pi(U_{mn}) = v_\pi(U_n)$.*

Proof. First, since λ, η are both integral over the ring R, we have that $v_\pi(\lambda) \geq 0$ and $v_\pi(\eta) \geq 0$.

Suppose that $v_\pi(\eta) > 0$. Note that we have either $\lambda^n = \eta^n + (\lambda - \eta)U_n$, or $\lambda^n = \eta^n + (\lambda^2 - \eta^2)U_n$. Then, since $v_\pi(\eta) > 0$ and $v_\pi(U_n) > 0$,

we have $v_\pi(\lambda^n) > 0$. So, $v_\pi(\lambda) > 0$. Thus,

$$v_\pi(\lambda + \eta) > 0, \qquad v_\pi(\lambda\eta) > 0,$$

which contradicts the assumption that $(\lambda + \eta)^2$ and $\lambda\eta$ are coprime in R. Hence, we must have $v_\pi(\eta) = 0$. Similarly, we must have $v_\pi(\lambda) = 0$.

Assume that n is odd. Then, $U_n = (\lambda^n - \eta^n)/(\lambda - \eta)$. So, we have

$$\lambda^n = \eta^n + (\lambda - \eta)U_n.$$

Then, we obtain

$$\lambda^{mn} = \left(\eta^n + (\lambda - \eta)U_n\right)^m = \eta^{mn} + \sum_{i=1}^{m} \binom{m}{i}(\lambda - \eta)^i U_n^i \eta^{n(m-i)}.$$

So

$$\frac{\lambda^{mn} - \eta^{mn}}{\lambda - \eta} = m\eta^{n(m-1)}U_n + \sum_{i=2}^{m} \binom{m}{i}(\lambda - \eta)^{i-1}\eta^{n(m-i)}U_n^i.$$

Hence, we obtain that for odd m

$$U_{mn} = m\eta^{n(m-1)}U_n + \sum_{i=2}^{m} \binom{m}{i}(\lambda - \eta)^{i-1}\eta^{n(m-i)}U_n^i,$$

and for even m

$$(\lambda + \eta)U_{mn} = m\eta^{n(m-1)}U_n + \sum_{i=2}^{m} \binom{m}{i}(\lambda - \eta)^{i-1}\eta^{n(m-i)}U_n^i.$$

We also note that since n is odd and $v_\pi(U_n) > 0$, by Lemma 2.8 we have $v_\pi(\lambda + \eta) = 0$. Then, the desired result follows.

Finally, assume that n is even. Then, as the above, for any integer $m \geq 1$ we obtain

$$U_{mn} = m\eta^{n(m-1)}U_n + \sum_{i=2}^{m} \binom{m}{i}(\lambda^2 - \eta^2)^{i-1}\eta^{n(m-i)}U_n^i.$$

The desired result now follows. $\square$

Now, we are ready to prove the theorems.

Proof of Theorem 1.1. Let $d = \gcd(m, n)$.

First, we assume that both m and n are even. Then, d is also even. By definition, we obtain

$$U_m = U_d P_{m/d}(\lambda^d, \eta^d), \quad U_n = U_d P_{n/d}(\lambda^d, \eta^d).$$

By assumption, it is easy to see that $\lambda^d + \eta^d$ and $\lambda^d\eta^d$ are coprime in R (as in the last paragraph of the proof of Lemma 2.3). Hence, by

Lemma 2.4, we know that $P_{m/d}(\lambda^d, \eta^d)$ and $P_{n/d}(\lambda^d, \eta^d)$ are coprime in R, and so we have $\gcd(U_m, U_n) = U_d$ in this case.

Now, we assume that both m and n are odd. Then, d is also odd. By definition, we have

$$U_m = U_d P_{m/d}(\lambda^d, \eta^d), \quad U_n = U_d P_{n/d}(\lambda^d, \eta^d).$$

We also note that $(\lambda^d + \eta^d)^2$ and $\lambda^d \eta^d$ are coprime in R. Then, by Lemma 2.5 we know that $P_{m/d}(\lambda^d, \eta^d)$ and $P_{n/d}(\lambda^d, \eta^d)$ are coprime in R, and so we have $\gcd(U_m, U_n) = U_d$.

Finally, when m and n do not have the same parity, without loss of generality, we assume that m is odd and n is even. Then, d is odd. By definition, we have

$$U_m = U_d P_{m/d}(\lambda^d, \eta^d),$$

and

$$U_n = U_d \cdot \frac{P_{n/d}(\lambda^d, \eta^d)}{\lambda^d + \eta^d} \cdot \frac{\lambda^d + \eta^d}{\lambda + \eta}.$$

Then, by Lemma 2.6 we know that $P_{m/d}(\lambda^d, \eta^d)$ and $P_{n/d}(\lambda^d, \eta^d)/(\lambda^d + \eta^d)$ are coprime in R. Besides, by Lemma 2.7 we obtain that $P_{m/d}(\lambda^d, \eta^d)$ and $(\lambda^d + \eta^d)/(\lambda + \eta)$ are coprime in R. Hence, we have $\gcd(U_m, U_n) = U_d$. This completes the proof.   □

Proof of Theorem 1.2. As in [19], we define the sequence $(Q_n)_{n \geq 1}$ of polynomials by $Q_1 = 1, Q_2 = 1$, and

$$Q_n(X, Y) = \Phi_n(X, Y), \quad n = 3, 4, \ldots.$$

Then, it is easy to see that for any integer $n \geq 1$ we have

$$U_n = \prod_{d|n} Q_d(\lambda, \eta).$$

By the Möbius inversion, we have

$$Q_n(\lambda, \eta) = \prod_{d|n} U_d^{\mu(n/d)}.$$

So, for any irreducible polynomial π in R we have

$$v_\pi(Q_n(\lambda, \eta)) = \sum_{d|n} \mu(n/d) v_\pi(U_d).$$

Now, assume the characteristic $p > 0$. suppose that π is a prime divisor of U_n which is not primitive, where $p \nmid n$. Let m be the minimal positive integer such that $\pi \mid U_m$. Automatically, $p \nmid m$. Then, by Theorem 1.1 we have $m \mid n$, and by Lemma 3.1, for any positive integer k with $p \nmid k$

$$v_\pi(U_{mk}) = v_\pi(U_m).$$

Hence, if $m < n$, noticing $p \nmid n$ we obtain

$$
\begin{aligned}
v_\pi(Q_n(\lambda, \eta)) &= \sum_{d|n/m} \mu(n/(dm)) v_\pi(Q_{dm}) \\
&= \sum_{d|n/m} \mu(n/(dm)) v_\pi(Q_m) \\
&= v_\pi(Q_m) \sum_{d|n/m} \mu(n/(dm)) = 0.
\end{aligned}
$$

So, any non-primitive prime divisor of U_n (in the sequence U') does not divide $Q_n(\lambda, \eta)$. It is easy to see that when $n > 2$, $Q_n(\lambda, \eta) = \Phi_n(\lambda, \eta)$ is non-constant (because at least one of λ and η is transcendental over K), and so $Q_n(\lambda, \eta)$ has a prime divisor in R. Thus, when $n > 2$, any prime divisor of $Q_n(\lambda, \eta)$ is primitive, and so each term in the sequence U' beyond the second has a primitive prime divisor.

The proof for the case $p = 0$ follows exactly the same way. $\qquad\square$

Remark 3.2. In the proof of Theorem 1.2, we obtain more: the *primitive part* (that is, the product of all the primitive prime divisors to their respective powers) of U_n is $Q_n(\lambda, \eta) = \Phi_n(\lambda, \eta)$, where $n \geq 3$, and $p \nmid n$ if $p > 0$.

4. Proofs of Theorems 1.3 and 1.4

The proofs follow easily from Theorems 1.1 and 1.2.

Proof of Theorem 1.3. Fix positive integers m, n with $d = \gcd(m, n)$. If either both m, n are odd, or both m, n are even, it follows directly from Theorem 1.1 that $\gcd(L_m, L_n) = L_d$ (setting $\lambda = \alpha, \eta = \beta$).

Now, without loss of generality, assume that m is even and n is odd. By Theorem 1.1, we have

$$
\gcd\left(\frac{\alpha^m - \beta^m}{\alpha^2 - \beta^2}, \frac{\alpha^n - \beta^n}{\alpha - \beta}\right) = \frac{\alpha^d - \beta^d}{\alpha - \beta}.
$$

Using Lemma 2.8 we know that $(\alpha^n - \beta^n)/(\alpha - \beta)$ and $\alpha + \beta$ are coprime in R. Hence, we obtain $\gcd(L_m, L_n) = L_d$. This completes the proof. $\qquad\square$

Proof of Theorem 1.4. Assume that the characteristic $p = 0$. First, by Lemma 2.8, we have that for any odd $n \geq 3$, $\Phi_n(\alpha, \beta)$ and $\alpha + \beta$ are coprime in R.

Now, fix an even integer $n \geq 4$. Suppose that there exists an irreducible polynomial, say π, in R dividing both $\Phi_n(\alpha, \beta)$ and $\alpha + \beta$. This means that the polynomial $X^n - Y^n$, defined over the fraction field of

the ring $R \pmod{\pi}$, has a multiple root (that is, (α, β)). However, this fraction field has characteristic zero (because it contains the field K), which implies that $X^n - Y^n$ is in fact a simple polynomial. Hence, this leads to a contradiction, and so $\Phi_n(\alpha, \beta)$ and $\alpha + \beta$ are coprime in R.

Therefore, by constructions we directly obtain from Remark 3.2 that the primitive part of L_n is $\Phi_n(\alpha, \beta)$, where $n \geq 3$.

Finally, if the characteristic $p > 0$, then by contruction the above arguments still work (because in the sequence L' we have deleted those terms L_n with $p \mid n$). $\qquad\square$

Remark 4.1. In the proof of Theorem 1.4, we obtain more: the primitive part of L_n is $\Phi_n(\alpha, \beta)$, where $n \geq 3$, and $p \nmid n$ if $p > 0$.

5. PROOFS OF THEOREMS 1.5 AND 1.6

Clearly, Theorem 1.5 follows directly from Theorem 1.3.

Proof of Theorem 1.6. Assume that the characteristic $p = 0$. Fix an integer $n \geq 3$. Taking $\alpha = f$ and $\beta = g$ in Theorem 1.4 and noticing Remark 4.1, we know that the primitive part of the term $(f^n - g^n)/(f - g)$ is $\Phi_n(f, g)$. As the above, we obtain that $\Phi_n(f, g)$ and $f - g$ are coprime in R. Hence, the primitive part of the term $F_n = f^n - g^n$ is $\Phi_n(f, g)$.

Finally, if the characteristic $p > 0$, then by contruction the above arguments still work (because in the sequence F' we have deleted those terms F_n with $p \mid n$). $\qquad\square$

Remark 5.1. In the proof of Theorem 1.6, we obtain more: the primitive part of F_n is $\Phi_n(f, g)$, where $n \geq 3$, and $p \nmid n$ if $p > 0$.

6. COMMENTS

In this section, we make some remarks about extending our results to unique factorization domains.

Note that all the lemmas used in proving the strong divisibility property are valid for any unique factorization domain. So, we have the following result.

Theorem 6.1. *The strong divisibility properties in Theorems 1.1, 1.3 and 1.5 still hold when we replace the ring R by a unique factorization domain D.*

In order to extend fully all our results on primitive divisors to a unique factorization domain D, we need to assure two properties. One

is about the valuation similar as in Lemma 3.1. The other is to assure that $\Phi_n(f, g), \Phi_n(\alpha, \beta)$ and $\Phi_n(\lambda, \eta)$ are all non-zero and non-unit whenever $n \geq 3$.

If D contains a field, then any integer as an element in D is either zero or a unit, and so the valuation result holds in this case by following the same arguments as Lemma 3.1. Hence, in this case, if one can show that $\Phi_n(f, g)$ is non-unit whenever $n > n_0$ for some integer n_0, then one in fact prove the result in Theorem 1.6 by replacing "beyond the second" with "beyond the n_0-th". Similar things apply to Theorems 1.2 and 1.4.

We present an example here. Let $D = K[[X]]$ be the formal power series ring defined over a field K in one variable X. Then, an element $\sum_{n=0}^{\infty} a_n X^n$ in D is a unit if and only if $a_0 \neq 0$. Let f and g be non-zero, non-unit and coprime in D such that f/g is not a root of unity. Then, $\Phi_n(f, g)$ is non-zero and non-unit for any $n \geq 1$, and so Theorem 1.6 holds in this case. In addition, if let f be non-unit and g a unit in D, then $\Phi_n(f, g)$ is a unit for any $n \geq 1$,

Acknowledgement

References

[1] A.S. Bamunoba, *On the integral divisors of the Carlitz analogue of $a^n - b^n$*, Acta Arith., 190 (2019), 317–337.

[2] A.S. Bang, *Taltheoretiske undersølgelser*, Tidskrifft Math., 5 (1886), 70–80, 130–137.

[3] Y. Bilu, G. Hanrot and P.M. Voutier, *Existence of primitive divisors of Lucas and Lehmer numbers*, J. Riene Angew. Math., 539 (2001), 75–122.

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

[5] R.D. Carmichael, *On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$*, Ann. Math., 15 (1913), 30–70.

[6] A.J. Engler and A. Prestel, *Valued fields*, Springer, Berlin, 2005.

[7] G.R. Everest, G. Mclaren and T. Ward, *Primitive divisors of elliptic divisibility sequences*, J. Number Theory, 118 (2006), 71–89.

[8] G. Everest, A. van der Poorten, I. Shparlinski and T. Ward, *Recurrence sequences*, Amer. Math. Soc., Providence, RI, 2003.

[9] A. Flatters and T. Ward, *A polynomial Zsigmondy theorem*, J. Algebra, 343 (2011), 138–142.

[10] P. Ingram, V. Mahé, J.H. Silverman, K.E. Stange and M. Streng, *Algebraic divisibility sequences over function fields*, J. Aust. Math. Soc., 92 (2012), 99–126.

[11] P. Ingram and J.H. Silverman, *Primitive divisors in arithmetic dynamics*, Math. Proc. Cambridge Philos. Soc., 146 (2009), 289–302.

[12] L.P. Postnikova and A. Schinzel, *Primitive divisors of the expression $a^n - b^n$ in algebraic number fields*, Math. USSR Sb., 4 (1968), 153–159.

[13] N.N.D. Quan, *Function–field analogues of Bang–Zsigmondy's theorem and Feit's theorem*, Indiana Univ. Math. J., 65 (2016), 2081–2124.

[14] B. Rice, *Primitive prime divisors in polynomial arithmetic dynamics*, Integers, 7 (2007), A16.

[15] A. Schinzel, *Primitive divisors of the expression $A^n - B^n$ in algebraic number fields*, J. Riene Angew. Math., 268/269 (1974), 27–33.

[16] J.H. Silverman, *Wieferich's criterion and the abc-conjecture*, J. Number Theory, 30 (1988), 226–237.

[17] J.H. Silverman, *The arithmetic of dynamical systems*, Grad. Texts in Math., vol. 241, Springer, New York, 2007.

[18] C.L. Stewart, *Primitive divisors of Lucas and Lehmer sequences*, Transcendence Theory: Advances and Applications (A. Baker and D.W. Masser, eds.), Academic Press, New York, 1977, 79–92.

[19] M. Ward, *The intrinsic divisors of Lehmer numbers*, Ann. Math., 62 (1955), 230–236.

[20] L.C. Washington, *Introduction to cyclotomic fields*, Grad. Texts in Math., vol. 83, Springer, New York, 1982.

[21] Z. Zhao and Q. Ji, *Zsigmondy theorem for arithmetic dynamics induced by a drinfeld module*, Int. J. Number Theory, 15 (2019), 1111–1125.

[22] K. Zsigmondy, *Zur Theorie der Potenzreste*, Monatsh. Math., 3 (1892), 265–284.

School of Mathematics and Statistics, University of New South Wales, Sydney, NSW 2052, Australia

E-mail address: shamin2010@gmail.com