FUNCTION FIELD ANALOGUES OF BANG–ZSIGMONDY’S THEOREM AND FEIT’S THEOREM

NGUYEN NGOC DONG QUAN

CONTENTS

1. Introduction 1
   1.1. A Carlitz module analogue of Bang–Zsigmondy’s theorem 2
   1.2. A Carlitz module analogue of Feit’s theorem 4
   1.3. Notation 5
2. Cyclotomic polynomials over function fields 5
3. A Carlitz module analogue of Zsigmondy primes 12
4. Bang–Zsigmondy’s theorem in characteristic $p \neq 2$ 16
5. Bang–Zsigmondy’s theorem in characteristic two 20
6. An analogue of large Zsigmondy primes, and Feit’s theorem in positive characteristic 24
Acknowledgements 46
References 46

1. INTRODUCTION

In the number field setting, Bang–Zsigmondy’s theorem [15] states that for any integers $u, m > 1$, there exists a prime divisor $\varphi$ of $u^m - 1$ such that $\varphi$ does not divide $u^n - 1$ for every integer $n$ with $0 < n < m$, except exactly in the following cases:

(i) $m = 2$, and $u = 2^s - 1$ for some integer $s \geq 2$; or
(ii) $m = 6$, and $u = 2$.

A prime $\varphi$ satisfying the conditions in Bang–Zsigmondy’s theorem is called a Zsigmondy prime for $(u, m)$. Bang–Zsigmondy’s theorem has many applications; for example, the existence of Zsigmondy primes was used in the original proof of Wedderburn’s theorem [19]. See also [1] for applications of Zsigmondy primes in theory of finite groups.

If $\varphi$ is a Zsigmondy prime for $(u, m)$ for some integers $u, m > 1$, then the multiplicative order of $u$ modulo $\varphi$ is exactly $m$, which implies that Zsigmondy primes are associated to the multiplicative group $\mathbb{G}_m(Q)$.

Feit [9] observed that if $\varphi$ is a Zsigmondy prime for $(u, m)$, then $\varphi \equiv 1 \pmod{m}$ since the multiplicative order of $u$ modulo $\varphi$ is exactly $m$. The last congruence implies that $\varphi \geq m + 1$, which in turn motivated Feit to introduce the following notion of a large Zsigmondy prime: a prime $\varphi$ is called a large Zsigmondy prime for $(u, m)$ if $\varphi$ is a Zsigmondy prime for $(u, m)$ such that either $\varphi > m + 1$ or $\varphi^2$ divides $u^m - 1$.

In [9], Feit proved a refinement of Bang–Zsigmondy’s theorem. He showed that for any integers $u, m > 1$, there exists a large Zsigmondy prime for $(u, m)$ except exactly in the following cases:

(i) $m = 2$ and $u = 2^s3^t - 1$ for some positive integer $s$, and either $t = 0$ or 1.
(ii) $u = 2$ and $m = 4, 6, 10, 12, 18$.
(iii) $u = 3$ and $m = 4, 6$.
(iv) $u = 5$ and $m = 6$.  

Date: March 6, 2015.
It is obvious that Bang–Zsigmondy’s theorem follows immediately from Feit’s theorem.

There are many strong analogies [11] [15] [17] between number fields and function fields. It is well-known (see [11] Chapter 3) that the Carlitz module is an analogue of the multiplicative group \( \mathbb{G}_m \).

The aim of this paper is to search for new analogous phenomena between the Carlitz module and the multiplicative group \( \mathbb{G}_m \). We will introduce notions of Zsigmondy primes and large Zsigmondy primes for the Carlitz module, and prove a Carlitz module analogue of Bang–Zsigmondy’s theorem and an analogue of Feit’s theorem in the Carlitz module context.

Throughout the paper, let \( q = p^s \), where \( p \) is a prime and \( s \) is a positive integer. Let \( \mathbb{F}_q \) be the finite field of \( q \) elements. Let \( A = \mathbb{F}_q[T] \), and let \( k = \mathbb{F}_q(T) \). Let \( \tau \) be the mapping defined by \( \tau(x) = x^q \), and let \( k(\tau) \) denote the twisted polynomial ring. Let \( C : A \to k(\tau) (a \mapsto C_a) \) be the Carlitz module, namely, \( C \) is an \( \mathbb{F}_q \)-algebra homomorphism such that \( C_T = T + \tau \).

1.1. A Carlitz module analogue of Bang–Zsigmondy’s theorem. The main ingredient in the notion of Zsigmondy primes in the number field context is the notion of the multiplicative order of an integer modulo a prime. Hence in order to define a Carlitz module analogue of Zsigmondy primes, we need to find a function field replacement for the notion of the multiplicative order of an integer modulo a prime.

In \([3]\), we introduced the notion of the Carlitz annihilator of a monic prime \( \varphi \in A \), which is a function field replacement for the multiplicative order of 2 modulo a prime. In Section 2 of the present paper, we will prove a result (see Proposition 3.1) that motivates a generalization of the Carlitz annihilator of a monic prime to a couple \( (u, \varphi) \), where \( u \) is a nonzero polynomial in \( A \) and \( \varphi \) is a monic prime. If \( \varphi \) does not divide \( u \), the Carlitz annihilator of a couple \( (u, \varphi) \), denoted by \( P_{u, \varphi} \), is the unique monic polynomial in \( A \) of least positive degree such that \( C_{P_{u, \varphi}}(u) \equiv 0 \pmod{\varphi} \), i.e., \( P_{u, \varphi} \) divides \( m \) for any nonzero polynomial \( m \in A \) with \( C_m(u) \equiv 0 \pmod{\varphi} \). If \( \varphi \) divides \( u \), we simply let \( P_{u, \varphi} = 1 \).

The Carlitz annihilator of a couple \( (u, \varphi) \) can be viewed as a replacement in the function field setting for the multiplicative order of an integer \( u \) modulo a prime \( \varphi \) in the number field setting. This analogy is crucial throughout the current work. The basic analogy between the multiplicative group \( \mathbb{G}_m \) and the Carlitz module \( C \) that will be used throughout this paper is illustrated in Table 1.

| The multiplicative group \( \mathbb{G}_m \) | The Carlitz module \( C \) |
|-------------------------------------------|-----------------------------|
| \( u^m - 1 \) for \( u, m \in \mathbb{Z}_{>0} \) | \( C_m(u) \) for \( m, u \in A \) |

Table 1: The analogy between the multiplicative group \( \mathbb{G}_m \) and the Carlitz module \( C \)

In the number field context, recall that a prime \( \varphi \) is a Zsigmondy prime for \( (u, m) \) if the multiplicative order of \( u \) modulo \( \varphi \) is exactly \( m \). The analogy in Table 1 suggests that one can define a Carlitz module analogue of Zsigmondy primes as follows. For any nonzero polynomials \( u, m \in A \), a monic prime \( \varphi \) is called a Zsigmondy prime for \( (u, m) \) if the Carlitz annihilator of \( (u, \varphi) \) is \( m \). In more concrete terms, this means that \( \varphi \) divides \( C_m(u) \), and \( C_{n}(u) \not\equiv 0 \pmod{\varphi} \) for any nonzero polynomial \( n \in A \) with \( \deg(n) < \deg(m) \).

It is natural to ask whether there exists a Zsigmondy prime for a given couple \( (u, m) \), where \( u, m \) are nonzero polynomials in \( A \). Note that if \( \deg(m) = \deg(u) = 0 \), then \( C_m(u) = mu \in \mathbb{F}_q^* \), and thus there exists no Zsigmondy primes for \( (u, m) \). Therefore without loss of generality, one can modify the last question by adding the assumption that at least one of \( m, u \) is of positive degree.

Determining when there exists no Zsigmondy primes for a given couple \( (u, m) \) is a Carlitz module analogue of the classical theorem of Bang–Zsigmondy. The first main result in this paper asserts that there exists a Zsigmondy prime for a given couple \( (u, m) \), except exactly in some exceptional cases that can be explicitly determined; more precisely, we obtain the following theorem.
**Theorem 1.1** (See Theorem 4.1 and Theorem 5.2). Assume that \( q > 2 \). Let \( m, u \) be monic polynomials in \( A \) such that at least one of them is of positive degree. Then there exists a Zsigmondy prime for \((u, m)\) except exactly in the following cases:

(i) \( q = 3, u = 1, \) and \( m = (\varphi - 1)\varphi \), where \( \varphi \) is an arbitrary monic prime of degree 1 in \( \mathbb{F}_3[T] \).

(ii) \( q = 2^2, u = 1, \) and \( m = (\varphi - 1)\varphi \), where \( \varphi \) is an arbitrary monic prime of degree 1 in \( \mathbb{F}_{2^2}[T] \).

Theorem 1.1 will be split into two parts. The first part is Theorem 1.2 that considers the case when \( p \neq 2 \). The second part is Theorem 5.2 that treats Theorem 1.1 in the case when \( p = 2 \).

A Carlitz module analogue of the classical Bang–Zsigmondy theorem was first considered by Bae in [3]. In fact, Bae considered a more general analogue of the classical Bang–Zsigmondy theorem, which can be viewed as a function field analogue of the classical Zsigmondy theorem. (See [20] or [4] for an account of the classical Bang–Zsigmondy theorem. Note that Birkhoff and Vandiver [6] independently discovered Zsigmondy’s theorem in 1904 after the theorem was first proved by Zsigmondy [21] in 1892.) It seems that the main result in Bae [3] (see [3] Theorem 4.10) is erroneous. Before pointing out the error in [3] Theorem 4.10, let us recall the statement of Theorem 4.10 in [3].

Let \( u, v \) be relatively prime elements in \( A \), and let \( m \) be a monic polynomial in \( A \). Set

\[
Z_m(u, v) = v^{\deg(m)} C_m(u/v).
\]

Following Bae [3], a monic prime \( \varphi \) is called a primitive factor of \( Z_m(u, v) \) if \( Z_m(u, v) \equiv 0 \pmod{\varphi} \), and \( Z_m(u, v) \not\equiv 0 \pmod{\varphi} \) for any monic divisor \( n \) of \( m \) with \( n \neq m \). Note that when \( v = 1 \), the notion of primitive factors in [3] agrees with that of Zsigmondy primes introduced in this paper.

Theorem 4.10 in Bae [3] states that if \( q > 2 \) and \( \deg(m) > 0 \), then \( Z_m(u, v) \) has at least one primitive factor except exactly in the following case:

(PF) \( q = 3, u = \pm 1, v = \pm 1, \) and \( m = (\varphi - 1)\varphi \), where \( \varphi \) is an arbitrary monic prime of degree one in \( \mathbb{F}_3[T] \).

We now provide a counterexample to Theorem 4.10 in Bae [3]. Indeed, if one takes \( q = 2^2, u = v = 1, \) and \( m = (\varphi - 1)\varphi \), where \( \varphi \) is an arbitrary monic prime of degree one in \( \mathbb{F}_{2^2}[T] \), then Table 3 in the proof of Lemma 5.4 shows that there exits no Zsigmondy prime for \((u, m)\), i.e., \( Z_m(u, v) \) has no primitive factors in this case, which provides a counterexample to Theorem 4.10 in Bae [3].

We should also note that in his Ph.D. thesis (see [1] Theorem 4.2.10), Bamunoba, following closely the techniques in Bae [3], attempted to give a different proof to Theorem 4.10 in Bae [3]. Due to the counterexample to Theorem 4.10 in Bae [3] that we pointed out above, it seems that the proof of Theorem 4.2.10 in Bamunoba [4] is also erroneous.

Note that the techniques that Bae exploited in [3] are based on the work of Birkhoff and Vandiver [6]. We, however, use completely different arguments from Bae [3] to prove Theorem 1.1 and the strategy of our proof is similar to the work of Roitman [16]. Let us now describe the strategy of our proof of Theorem 1.1 in detail.

In Section 4 we obtain a function field analogue of L¨uneburg’s theorem (see L¨uneburg [13] Satz 1 or Roitman [16] Proposition 2) for an account of L¨uneburg’s theorem in the number field context that describes a sufficient and necessary condition under which a prime \( \varphi \) is a non-Zsigmondy prime for \((u, m)\).

**Theorem 1.2.** (See Theorem 4.7 or Corollary 5.8)

Assume that \( q > 2 \). Let \( m, u \) be monic polynomials in \( A \) such that \( m \) is of positive degree. Let \( \varphi \) be a monic prime dividing \( \Psi_m(u) \), where \( \Psi_m(x) \in A[x] \) denotes the \( m \)-th cyclotomic polynomial (that will be reviewed in Section 2). Let \( P_{u, \varphi} \) be the Carlitz annihilator of \((u, \varphi)\). Then

(i) \( \varphi \) is a non-Zsigmondy prime for \((u, m)\) if and only if \( \varphi \) divides \( m \).

(ii) if \( \varphi \) is a non-Zsigmondy prime for \((u, m)\), then \( m = P_{u, \varphi} \varphi^s \) for some positive integer \( s \). Furthermore \( \varphi^s \) does not divide \( \Psi_m(u) \).

**Remark 1.3.** In his Ph.D. thesis, Bamunoba (see [4] Corollary 4.1.5) independently obtained part (i) of Theorem 1.2 with a slightly different proof. Bamunoba (see [4] Lemma 4.1.6) also independently proved part (ii) of Theorem 1.2 under the more restrictive assumption that \( \gcd(u, m) = 1 \). We should note that Bae (see [3] Proposition 4.4) also obtained a more general version of part (i) of Theorem 1.2.
Using Theorem 1.2 and under the assumption that there are no Zsigmondy primes for a pair \((u, m)\), we deduce that the prime factorization of \(\Psi_m(u)\) in \(A\) is of very special form. If the characteristic \(p\) of \(k\) is not equal to 2, then \(\Psi_m(u)\) is a prime dividing \(m\) (see Corollary 1.3). If \(p = 2\), then either \(\Psi_m(u)\) is a prime dividing \(m\) or \(\Psi_m(u) = \epsilon \varphi(u) - 1\), where \(\epsilon \in \mathbb{F}_q^*\) and both \(\varphi\) and \(\varphi - 1\) are monic prime divisors of \(m\) (see Lemma 5.1). In either case, by deriving several lower bounds for \(\deg(\Psi_m(u))\), we show that except the exceptional cases (i), (ii) in Theorem 1.1, the prime factorization of \(\Psi_m(u)\) can not fall into these forms, and of course this proves that there must exist a Zsigmondy prime for \((u, m)\).

Theorem 1.4 can also be interpreted in terms of divisibility sequences and Zsigmondy sets in \(A\).

A sequence \((a_m)_{m \in A} \subset A\) is called a divisibility sequence in \(A\) if \(a_{mn} \equiv 0 \pmod{a_m}\) for all \(m, n \in A\). For a given nonzero polynomial \(u\) in \(A\), we see that the sequence \(S_C = (C_m(u))_{m \in A}\) is a divisibility sequence in \(A\).

Let \(S = (a_n)_{n \in A}\) be a sequence of polynomials in \(A\), and let \(m\) be a polynomial in \(A\). A monic prime \(\varphi\) in \(A\) is called a Zsigmondy prime for \(a_m\) if \(\varphi\) divides \(a_m\), and \(a_n \not\equiv 0 \pmod{\varphi}\) for any nonzero polynomial \(n\) with \(\deg(n) < \deg(m)\). The notion of a Zsigmondy prime for a given term \(a_m\) in a sequence \(S = (a_n)_{n \in A}\) agrees with that of a Zsigmondy prime for a given couple \((u, m)\) when \(S = S_C\).

The Zsigmondy set of \(S\) is defined by

\[
Z_q(S) = \{ m \in A \mid a_m \text{ has no Zsigmondy primes} \}.
\]

Note that we also include \(q\) as a subscript in the notation of the Zsigmondy set of \(S\) to indicate that the set \(Z_q(S)\) might depend on \(q\) for some sequence \(S\). We now recast Theorem 1.1 in terms of divisibility sequences and Zsigmondy sets as follows.

**Theorem 1.4.** Assume that \(q > 2\). Let \(u\) be a monic polynomial in \(A\), and let \(S_C = (C_m(u))_{m \in A}\) be the divisibility sequence in \(A\) as above. Then

1. if \(\deg(u) = 0\), then
   \[
   Z_q(S_C) \subseteq \{ \mathbb{F}_q^* \} \cup \{ m = (\varphi - 1)\varphi, \text{ where } \varphi \text{ is an arbitrary monic prime of degree 1 in } A \},
   \]
   with equality if \(q = 3\) or \(q = 2^2\). Furthermore, if \(q > 4\), then \(Z_q(S_C) = \mathbb{F}_q^*\).
2. if \(\deg(u) > 0\), then \(Z_q(S_C)\) is empty.

To end this subsection, let us remark that although it seems possible that one could, with a little more effort, exploit the techniques in this paper to obtain a function field analogue of Zsigmondy’s theorem in full generality, we decided not to further pursue in this direction for several reasons. First, Theorem 1.4 viewed as the function field analogue of Bang—Zsigmondy’s theorem, is sufficient for our purpose to prove a function field analogue of Feit’s theorem. Second, we want to prove function field analogues of Bang—Zsigmondy’s theorem and Feit’s theorem in a unified manner, and third, we want to keep the exposition as simple as possible.

1.2. A Carlitz module analogue of Feit’s theorem. Before stating a Carlitz module analogue of Feit’s theorem—our most important result in this paper, let us recall a function field analogue of Fermat’s little theorem, which is a direct consequence of [13 Proposition 2.4].

**Lemma 1.5.** Let \(u\) be a nonzero polynomial in \(A\), and let \(\varphi\) be a monic prime in \(A\). Then

\[
C_{\varphi - 1}(u) \equiv 0 \pmod{\varphi}.
\]

Now let \(\varphi\) be a Zsigmondy prime for \((u, m)\), where \(u, m\) are monic polynomials in \(A\). Then the Carlitz annihilator of \((u, \varphi)\) is \(m\), i.e., \(m\) is the unique monic polynomial of least positive degree such that \(C_m(u) \equiv 0 \pmod{\varphi}\). Hence it follows from Lemma 1.5 that \(m\) divides \(\varphi - 1\), which implies that \(\deg(\varphi) = \deg(\varphi - 1) \geq \deg(m)\). The last inequality and the notion of large Zsigmondy primes introduced in Feit [9] motivate a notion of a function field analogue of large Zsigmondy primes as follows: A Zsigmondy prime \(\varphi\) for \((u, m)\) is called a large Zsigmondy theorem for \((u, m)\) if either \(\deg(\varphi) > \deg(m)\) or \(\varphi^2\) divides \(C_m(u)\).

Classifying all pairs \((u, m)\) such that there does not exist a large Zsigmondy prime for \((u, m)\) can be viewed as a function field analogue of Feit’s theorem. We are now in a position to state our most important result in this paper, a function field analogue of Feit’s theorem.
Theorem 1.6 (See Theorem 6.10). Assume that \( q > 2 \). Let \( m, u \) be monic polynomials in \( A \) such that at least one of them is of positive degree. Then there exists a large Zsigmondy prime for \((u, m)\) except in some exceptional cases that can be explicitly determined. (Theorem 6.10 explicitly lists all triples \((q, u, m)\) in the exceptional cases.)

We will prove Theorem 1.6 in Section 6. It is obvious that Theorem 1.1 follows immediately from Theorem 1.6.

The strategy of the proof of Theorem 1.6 is as follows. Under the assumption that there exists a Zsigmondy prime for a pair \((u, m)\), but there are no large Zsigmondy primes for \((u, m)\), we deduce (see Corollary 6.3) that the following are true:

(i) \( m + 1 \) is the only Zsigmondy prime for \((u, m)\);
(ii) either \( \Psi_m(u) = \epsilon(m + 1) \) or \( \Psi_m(u) = \epsilon q(m + 1) \) for some unit \( \epsilon \in \mathbb{F}_q^* \) and some monic prime \( q \) dividing \( m \).

The next step is to show that \( \deg(\Psi_m(u)) \) is sufficiently large so that at least one of (i) and (ii) above cannot be satisfied except in some exceptional cases that can be explicitly determined. This implies that there exists a large Zsigmondy prime for \((u, m)\) except in some exceptional cases, and hence Theorem 1.6 follows. In many cases in the proof of Theorem 1.6, we need a sharper lower bound for \( \deg(\Psi_m(u)) \) when \( m = \varphi^s \) for some monic prime \( \varphi \) and \( s \geq 2 \), or \( m \) is a monic prime of degree \( \geq 2 \). Here \( \Phi(\cdot) \) is a function field analogue of the classical Euler \( \phi \)-function whose definition will be reviewed in the next subsection.

1.3. Notation. Every nonzero element \( m \in A \) is of the form

\[
m = \alpha_n T^n + \cdots + \alpha_1 T + \alpha_0,
\]

where the \( \alpha_i \) are elements in \( \mathbb{F}_q \) and \( \alpha_n \neq 0 \). When \( m \) is of the form as above, we say that the degree of \( m \) is \( n \). In notation, we write \( \deg(m) = n \). We use the standard convention that \( \deg(0) = -\infty \). With this convention, one obtains the degree function \( \deg : A \to \mathbb{Z} \cup \{-\infty\} \) in an obvious way.

With \( m \) of the above form, we say that the leading coefficient of \( m \) is \( \alpha_n \).

For a polynomial \( m \in A \) of positive degree, we define \( \Phi(m) \) to be the number of nonzero polynomials of degree less than \( \deg(m) \) and relatively prime to \( m \). The function \( \Phi(\cdot) \) is a function field analogue of the classical Euler \( \phi \)-function.

Let

\[
m = \alpha \varphi_1^{s_1} \cdots \varphi_h^{s_h}
\]

be the prime factorization of \( m \), where \( \alpha \in \mathbb{F}_q^* \), the \( \varphi_i \) are monic primes in \( A \), and the \( s_i \) are positive integers. It is well-known (see [15] Proposition 1.7) that

\[
\Phi(m) = \prod_{i=1}^h \Phi(\varphi_i^{s_i}) = \prod_{i=1}^h \left( q^{\deg(\varphi_i^{s_i})} - q^{\deg(\varphi_i^{s_i-1})} \right).
\]

In particular, this implies that when \( m = \varphi^s \) for some monic prime \( \varphi \) and some positive integer \( s \), then

\[
\Phi(\varphi^s) = q^{\deg(\varphi^s)} - q^{\deg(\varphi^{s-1})}.
\]

2. Cyclotomic polynomials over function fields

In this section, we study cyclotomic polynomials over function fields. Using well-known basic properties of cyclotomic polynomials in function fields, we derive many results about cyclotomic polynomials in function fields that will be used in subsequent sections to study Carlitz module analogues of Zsigmondy primes and large Zsigmondy primes. We begin by recalling the definition of cyclotomic polynomials in function fields, and some well-known results of cyclotomic polynomials in function fields whose proofs can be found, for example, in [2] or [18].

Fix an algebraic closure \( \bar{k} \) of \( k \), and let \( m \) be a polynomial of positive degree. Set \( \Lambda_m := \{ \lambda \in \bar{k} \mid C_m(\lambda) = 0 \} \). We define a primitive \( m \)-th root of \( C \) to be a root of the polynomial \( C_m(x) \in A[x] \) that generates the \( A \)-module \( \Lambda_m \). We fix a primitive \( m \)-th root of \( C \), and denote it by \( \lambda_m \).
Recall that the $m$-th cyclotomic polynomial, denoted by $\Psi_m(x)$, is the minimal polynomial of $\lambda_m$ over $k$, i.e., $\Psi_m(x) \in k[x]$ is the monic irreducible polynomial of least degree such that $\Psi_m(\lambda_m) = 0$. It is well-known that $\Psi_m(x) \in A[x]$. When $m = \varphi^s$ for some monic prime $\varphi$ and some positive integer $s$, we know from Proposition 2.4 of [13] that

$$\Psi_{\varphi^s}(x) = C_{\varphi^s}(x)/C_{\varphi^{s-1}}(x). \tag{1}$$

The next two results are well-known.

**Proposition 2.1.** (See part (2) in Proposition 12.3.13)

Let $m$ be a monic polynomial in $A$. Then

$$C_m(x) = \prod_{\substack{b|m, \ b \text{ monic}}} \Psi_b(x). \tag{2}$$

**Proposition 2.2.** (See Proposition 1.2(c))

Let $\varphi$ be a monic prime in $A$, and let $m$ be a monic polynomial in $A$ such that $\gcd(m, \varphi) = 1$. Let $h$ be a positive integer. Then

$$\Psi_m(C_{\varphi^h}(x)) = \Psi_{m\varphi^h}(x)\Psi_m(C_{\varphi^{h-1}}(x)).$$

Using Proposition 2.2, we prove the following result that will be useful in the proof of a Carlitz module analogue of L"uneburg’s theorem.

**Lemma 2.3.** Let $m$ be a monic polynomial in $A$ of positive degree, and let $\varphi$ be a monic prime in $A$ such that $\varphi$ divides $m$. Then $\Psi_m(x)$ divides $C_m(x)/C_{m/q}(x)$ in the polynomial ring $A[x]$.

**Proof.** We first prove Lemma 2.3 in the case when $m = \varphi^s$ for some monic prime $\varphi$ and some positive integer $s$. In this case, we see that $\varphi = \varphi$, and thus

$$\Psi_m(x) = \Psi_{\varphi^s}(x) = \frac{C_{\varphi^s}(x)}{C_{\varphi^{s-1}}(x)} = \frac{C_m(x)}{C_{m/\varphi}(x)} = \frac{C_m(x)}{C_{m/q}(x)},$$

which prove Lemma 2.3 for $m = \varphi^s$.

Set $d = \deg(m) \geq 1$. We prove Lemma 2.3 by induction on $d$.

If $d = 1$, then $m = \varphi$ for some monic prime $\varphi$ of degree $1$. Thus Lemma 2.3 holds for $d = 1$.

Assume that Lemma 2.3 holds for any monic polynomial $m$ of degree less than $d$. We prove that Lemma 2.3 is true for $d$. Indeed, take any monic polynomial $m$ of degree $d$. If $m$ has exactly one monic prime factor $\varphi$, then $m = \varphi^s$ for some positive integer $s$, and we already prove that Lemma 2.3 is true in this case.

If $m$ has at least two distinct prime factors, then there exists another monic prime $\varphi$ with $\varphi \neq \varphi$. Write $m = n\varphi^s$ for some positive integer $s$, where $n$ is a monic polynomial such that $\gcd(n, \varphi) = 1$. Since $\varphi$ divides $m$ and $\varphi \neq \varphi$, we deduce that $\varphi$ divides $n$. Note that $1 \leq \deg(n) < \deg(m) = d$.

By the induction hypothesis, we know that $\Psi_n(x)$ divides $C_n(x)/C_{n/q}(x)$, and thus there exists a polynomial $\Gamma(x) \in A[x]$ such that

$$\Psi_n(x)\Gamma(x) = \frac{C_n(x)}{C_{n/q}(x)}.$$.

Substituting $C_{\varphi^s}(x)$ for $x$ in the above equation, we deduce that

$$\Psi_n(C_{\varphi^s}(x))\Gamma(C_{\varphi^s}(x)) = \frac{C_n(C_{\varphi^s}(x))}{C_{n/q}(C_{\varphi^s}(x))} = \frac{C_{n\varphi^s}(x)}{C_{(n\varphi^s)/q}(x)} = \frac{C_m(x)}{C_{m/q}(x)}. \tag{2}$$

Using equation (2) and applying Proposition 2.2 with $n, \varphi^s$ in the roles of $m, \varphi^s$, respectively, we deduce that

$$\Psi_m(x)\Psi_n(C_{\varphi^{s-1}}(x)) = \Psi_{n\varphi^s}(x)\Psi_n(C_{\varphi^{s-1}}(x)) = \Psi_n(C_{\varphi^s}(x)) = \left(\frac{C_m(x)}{C_{m/q}(x)}\right)\frac{1}{\Gamma(C_{\varphi^s}(x))}.$$
and thus
\[ \Psi_m(x)\Psi_n(C_{\psi^r}(x))\Gamma(C_{\psi^r}(x)) = \frac{C_m(x)}{C_{m/q}(x)}. \]

Thus Lemma 2.3 follows immediately.

The next two results, i.e., Propositions 2.4 and 2.5 are already well-known (see Bae [3], Lemma 4.6). The proofs of these two results presented below are different from Bae [3], and use mainly the classical inequality of Bernoulli.

**Proposition 2.4.** Let \( m \) be an element in \( A \), and let \( u \) be a polynomial in \( A \) of positive degree. Assume that the following condition is true:

(D) if \( \deg(u) = 1 \), then \( q > 2 \).

Then
\[ \deg(C_m(u)) = \begin{cases} -\infty & \text{if } m = 0, \\ \deg(u)q^{\deg(m)} & \text{if } m \neq 0. \end{cases} \]

**Proof.** It is easy to see that if \( m = 0 \) or \( \deg(m) = 0 \), then Proposition 2.4 follows immediately.

Assume that \( m \) is of positive degree. By [12, Proposition 12.11], \( C_m(u) \) is of the form
\[ C_m(u) = mu + [m, 1]u^q + \ldots + [m, \deg(m) - 1]u^{q^{\deg(m)-1}} + [m, \deg(m)]u^{q^{\deg(m)}}, \]
where \([m, i]\) is a polynomial of degree \( q^{i}(\deg(m) - i) \) for each \( 1 \leq i \leq \deg(m) - 1 \), and \([m, d] \in \mathbb{F}_q^* \) is the leading coefficient of \( m \). We prove that
\[ \deg(u^{q^{\deg(m)}}) > \deg([m, i]u^q) \]
for every \( 1 \leq i \leq \deg(m)-1 \). Indeed, take any integer \( i \) such that \( 1 \leq i \leq \deg(m)-1 \). Using Bernoulli's inequality [12, Theorem 42] and noting that \( \deg(m) - i \geq 1 \), we deduce that
\[ q^{\deg(m)-i} = (1 + (q-1))^{\deg(m)-i} \geq 1 + (q-1)(\deg(m) - i). \]

Assumption (D) implies that \( \deg(u)(q-1) > 1 \). Thus we deduce that
\[ \deg(u)q^{\deg(m)-i} \geq \deg(u)(1 + (q-1)(\deg(m) - i)) \]
\[ = \deg(u) + \deg(u)(q-1)(\deg(m) - i) \]
\[ > \deg(u) + (\deg(m) - i). \]

Therefore
\[ \deg(u^{q^{\deg(m)}}) = \deg(u)q^{\deg(m)} > \deg(u)q^i + q^i(\deg(m) - i) = \deg([m, i]u^q) \]
for every \( 1 \leq i \leq \deg(m)-1 \).

Using Bernoulli’s inequality and similar arguments as above, one sees that
\[ \deg(mu) = \deg(m) + \deg(u) < \deg(u)q^{\deg(m)} = \deg(u^{q^{\deg(m)}}). \]

Therefore by (3), (4), we deduce that
\[ \deg(C_m(u)) = \deg(u^{q^{\deg(m)}}) = \deg(u)q^{\deg(m)}. \]

**Proposition 2.5.** Let \( m \) be an element in \( A \), and let \( u \) be a unit in \( \mathbb{F}_q^* \). Assume that \( q > 2 \). Then the degree of \( C_m(u) \) satisfies
\[ \deg(C_m(u)) = \begin{cases} -\infty & \text{if } m = 0, \\ 0 & \text{if } \deg(m) = 0, \\ q^{\deg(m)}-1 & \text{otherwise}. \end{cases} \]
Proof. The proof presented here is very similar to that of Proposition 2.4 and so we only sketch the main ideas of the proof.

The case when \( m = 0 \) or \( \deg(m) = 0 \) is trivial. Suppose now that \( \deg(m) > 0 \). Since \( \deg(C_m(u)) = \deg(uC_m(1)) = \deg(C_m(1)) \), it suffices to compute the degree of \( C_m(1) \). Using the same arguments as in Proposition 2.4, we can write \( C_m(1) \) in the form

\[
C_m(1) = [m, 0] + [m, 1] + \ldots + [m, \deg(m) - 1] + [m, \deg(m)],
\]

where \([m, 0] = m\), \([m, i] \) is a polynomial of degree \( q^i(\deg(m) - i) \) for each \( 1 \leq i \leq \deg(m) - 1 \), and \([m, \deg(m)] \) in \( \mathbb{P}^n_\mathbb{F} \) is the leading coefficient of \( m \). Repeating the same arguments as in Proposition 2.4 and using Bernoulli’s inequality, we can show that

\[
\deg([m, \deg(m) - 1]) = q^{\deg(m) - 1} > q^i(\deg(m) - i) = \deg([m, i])
\]

for every \( 0 \leq i \leq \deg(m) - 2 \). Thus Proposition 2.5 follows immediately.

The following elementary result will be used at many times in proofs of some subsequent results.

**Corollary 2.6.** Let \( m \) be a nonzero polynomial in \( A \), and let \( u \) be a polynomial in \( A \). Assume that the following is true:

- \( (D)\) if \( \deg(u) = 0 \) or \( \deg(u) = 1 \), then \( q > 2 \).

Then \( C_m(u) \neq 0 \) if and only if \( u \neq 0 \).

Proof. If \( u = 0 \), then \( C_m(u) = 0 \). If \( u \neq 0 \), then either \( \deg(u) = 0 \) or \( \deg(u) \geq 1 \). If \( \deg(u) = 0 \), it follows from \( (D)\) that \( q > 2 \). Since \( u \neq 0 \), we know that \( u \) is a unit in \( \mathbb{F}_q^* \), and it thus follows from Proposition 2.4 that \( C_m(u) \neq 0 \).

If \( \deg(u) \geq 1 \), we deduce from \( (D)\) that condition \( (D) \) in Proposition 2.4 is satisfied, and it thus follows from Proposition 2.4 that \( C_m(u) \neq 0 \).

In the number field context, Roitman [16] obtained several lower bounds for the value of \( \Psi_m(u) \), where \( \Psi_m(x) \in \mathbb{Z}[x] \) is the classical \( m \)-th cyclotomic polynomial and \( u \) is a positive integer. These lower bounds play a significant role in the proofs of the classical Bang-Zsigmondy theorem and the classical Feit theorem that are given in Roitman [16]. In the function field context, in order to measure how large a polynomial in \( A \) is, one can use the degree function \( \deg : A \to \mathbb{Z} \cup \{-\infty\} \) in place of the usual absolute value \( |\cdot| \) of \( \mathbb{R} \). The aim of the next two lemmas is to compute the value of \( \deg(\Psi_m(u)) \), where \( \Psi_m(x) \in A[x] \) is the \( m \)-th cyclotomic polynomial over function fields, and \( m, u \) are polynomials in \( A \). In contrast to the classical case, we can obtain an exact formula for \( \deg(\Psi_m(u)) \). The next two lemmas will be crucial in the proofs of our main results.

We first prove an exact formula for \( \deg(\Psi_m(u)) \) in the case when \( u \) is of positive degree.

**Lemma 2.7.** Let \( m \) be a monic polynomial in \( A \) of positive degree, and let \( u \) be a polynomial of positive degree. Assume that \( (D) \) in Proposition 2.4 is true. Then

\[
\deg(\Psi_m(u)) = \deg(u)\Phi(m),
\]

where \( \Phi(\cdot) \) is the function field analogue of the classical Euler \( \phi \)-function (see Subsection 1.3 for its definition).

Proof. Let us first consider the case when \( m = P^s \) for some monic prime \( P \in A \) and some positive integer \( s \). By Corollary 2.6, we see that \( C_{P^{s-1}}(u) \neq 0 \), and it thus follows from [11] that

\[
\Psi_m(u) = \Psi_{P^s}(u) = \frac{C_{P^s}(u)}{C_{P^{s-1}}(u)}.
\]

Applying Proposition 2.4 with \( P^{s-1}, u \) in the roles of \( m, u \), respectively, we see that

\[
\deg(C_{P^{s-1}}(u)) = \deg(u)q^{\deg(P^{s-1})}.
\]
Using Proposition 2.4 with $P^s, u$ in the roles of $m, u$, respectively, we deduce that
\[
\deg(C_{P^s}(u)) = \deg(u)q^{\deg(P^s)}.
\]
Thus
\[
\deg(\Psi_m(u)) = \deg(C_{P^s}(u)) - \deg(C_{P^{s-1}}(u))
= \deg(u)(q^{\deg(P^s)} - q^{\deg(P^{s-1})})
= \deg(u)\Phi(P^s) = \deg(u)\Phi(m),
\]
which proves Lemma 2.7 for $m = P^s$.

Now let $m$ be a monic polynomial in $A$ of positive degree. We can write $m$ in the form $m = n\varphi^h$ for some positive integer $h$, where $n$ is a monic polynomial and $\varphi$ is a monic polynomial such that $\gcd(m, \varphi) = 1$. If $n = 1$, then $m = \varphi^h$, and we already show that Lemma 2.7 holds in this case.

If $n$ is of positive degree, then by the induction hypothesis, we know that Lemma 2.7 is true for $n$, that is, for any polynomial $v$ of positive degree, we have
\[
\deg(\Psi_n(v)) = \deg(v)\Phi(n).
\]
Using this fact and Proposition 2.4 and noting that $\deg(C_{\varphi^r}(u)) \geq 1$ and $\deg(C_{\varphi^{r-1}}(u)) \geq 1$, we deduce that
\[
\deg(\Psi_n(C_{\varphi^r}(u))) = \deg(C_{\varphi^r}(u))\Phi(n) = \deg(u)q^{\deg(\varphi^r)}\Phi(n),
\]
and
\[
\deg(\Psi_n(C_{\varphi^{r-1}}(u))) = \deg(C_{\varphi^{r-1}}(u))\Phi(n) = \deg(u)q^{\deg(\varphi^{r-1})}\Phi(n).
\]
Therefore it follows from Proposition 2.2 that
\[
\deg(\Psi_m(u)) = \deg(\Psi_{n\varphi^h}(u))
= \deg(\Psi_n(C_{\varphi^r}(u)) - \deg(\Psi_n(C_{\varphi^{r-1}}(u))
= \deg(u)q^{\deg(\varphi^r)}\Phi(n) - \deg(u)q^{\deg(\varphi^{r-1})}\Phi(n)
= \deg(u)\Phi(n)(q^{\deg(\varphi^r)} - q^{\deg(\varphi^{r-1})})
= \deg(u)\Phi(n)\Phi(\varphi)
= \deg(u)\Phi(m),
\]
which proves our contention.

We now prove a formula for $\deg(\Psi_m(u))$, where $u$ is a unit in $F_q^\times$.

**Lemma 2.8.** Let $m$ be a monic polynomial in $A$ of positive degree, and let $u$ be a unit in $F_q^\times$. Assume that $q > 2$. Then the degree of $\Psi_m(u)$ satisfies
\[
\deg(\Psi_m(u)) = \begin{cases} 
\frac{\Phi(m) + (-1)^{h+1}}{q} & \text{if } m = \varphi_1\varphi_2\cdots\varphi_h, \text{ where the } \varphi_i \text{ are distinct monic primes}, \\
\frac{\Phi(m)}{q} & \text{if there exists a monic prime } \varphi \text{ such that } \varphi^2 \text{ divides } m.
\end{cases}
\]

**Proof.** We see that either $m$ is square-free or there exists a monic prime $\varphi$ such that $\varphi^2$ divides $m$. We consider the cases:

* Case 1. $m$ is square-free.

Since $m$ is square-free, one can write $m$ in the form
\[
m = \varphi_1\varphi_2\cdots\varphi_h,
\]
where the $\varphi_i$ are distinct monic primes and $h$ is a positive integer. By induction on $h$, we prove that if $m$ is of the form (6), then Lemma 2.8 holds for $m$. 


Assume that \( h = 1 \). Then \( m = \varphi \) for some monic prime \( \varphi \). We know from (1) that

\[
\Psi_m(u) = \Psi_{\varphi}(u) = \frac{C_{\varphi}(u)}{u}
\]

We know from Proposition 2.5 that

\[
\deg(C_{\varphi}(u)) = q^{\deg(\varphi) - 1},
\]

and thus

\[
\deg(\Psi_m(u)) = \deg(C_{\varphi}(u)) - \deg(u) = q^{\deg(\varphi) - 1} = \frac{\Phi(\varphi) + 1}{q} = \frac{\Phi(m) + (-1)^{h+1}}{q},
\]

which proves Lemma 2.8 for \( h = 1 \).

Assume that Lemma 2.8 is true for \( h - 1 \) with \( h \geq 2 \). We now prove that Lemma 2.8 is true for \( h \).

Indeed, take any polynomial \( m \in A \) of the form

\[
m = \varphi_1\varphi_2\cdots\varphi_h,
\]

where the \( \varphi_i \) are distinct monic primes. Set

\[
n = \varphi_2\cdots\varphi_h.
\]

One sees that \( \deg(n) \geq 1 \), and \( m = \varphi_1 n \).

By Proposition 2.5, we know that

\[
\deg(C_{\varphi_1}(u)) = q^{\deg(\varphi_1) - 1} \geq 1,
\]

and it thus follows from Lemma 2.7 that

\[
(7) \quad \deg(\Psi_n(C_{\varphi_1}(u))) = \deg(C_{\varphi_1}(u)) \Phi(n) = q^{\deg(\varphi_1) - 1} \Phi(n).
\]

By the induction hypothesis, we know that

\[
\deg(\Psi_n(u)) = \deg(\Psi_{\varphi_2\cdots\varphi_h}(u)) = \frac{\Phi(n) + (-1)^h}{q}.
\]

In particular, this implies that \( \Psi_n(u) \neq 0 \).

Applying Proposition 2.2 with \( 1, \varphi_1, n \) in the roles of \( h, \varphi, m \), respectively, and noting that \( \Psi_n(u) \neq 0 \), we deduce that

\[
\Psi_m(u) = \Psi_{\varphi_1 n}(u) = \frac{\Psi_n(C_{\varphi_1}(u))}{\Psi_n(C_{\varphi_1}(u))} = \frac{\Psi_n(C_{\varphi_1}(u))}{\Psi_n(C_{\varphi_1}(u))} = \frac{\Psi_n(C_{\varphi_1}(u))}{\Psi_n(u)}.
\]

Thus we deduce from (7) and (8) that

\[
\deg(\Psi_m(u)) = \deg(\Psi_n(C_{\varphi_1}(u))) - \deg(\Psi_n(u)) = q^{\deg(\varphi_1) - 1} \Phi(n) - \frac{\Phi(n) + (-1)^h}{q} = \frac{\Phi(n)q^{\deg(\varphi_1) - 1} + (-1)^{h+1}}{q} = \frac{\Phi(m) + (-1)^{h+1}}{q},
\]

which proves that Lemma 2.8 holds for any monic polynomial \( m \) of the form \( m = \varphi_1\varphi_2\cdots\varphi_h \), where \( h \) is a positive integer, and the \( \varphi_i \) are distinct monic primes.

\( \star \) Case 2. \( m \) is a monic polynomial such that \( \varphi^2 \) divides \( m \) for some monic prime \( \varphi \).

Write

\[
m = n\varphi^s,
\]

where \( s \) is an integer such that \( s \geq 2 \), \( \varphi \) is a monic prime, and \( n \) is a monic polynomial such that \( \gcd(n, \varphi) = 1 \).
By Proposition 2.5 and since \( s \geq 2 \), we see that
\[
\deg(C_{\varphi^s}(u)) = q^{\deg(\varphi^s) - 1} = q^s \deg(\varphi) - 1 \geq q, \tag{10}
\]
and
\[
\deg(C_{\varphi^{s-1}}(u)) = q^{\deg(\varphi^{s-1}) - 1} \geq 1. \tag{11}
\]
In particular, the last equality implies that \( C_{\varphi^{s-1}}(u) \neq 0 \).

We first consider the case when \( n = 1 \). In this case, we see that \( m = \varphi^{s} \). From (11), and noting that \( C_{\varphi^{s-1}}(u) \neq 0 \), we deduce that
\[
\Psi_m(u) = \Psi_{\varphi^{s}}(u) = \frac{C_{\varphi^{s}}(u)}{C_{\varphi^{s-1}}(u)},
\]
and thus
\[
\deg(\Psi_m(u)) = \deg(C_{\varphi^{s}}(u)) - \deg(C_{\varphi^{s-1}}(u)) = q^{\deg(\varphi^{s}) - 1} - q^{\deg(\varphi^{s-1}) - 1} = \frac{q^{\deg(\varphi^{s})} - q^{\deg(\varphi^{s-1})}}{q} = \frac{\Phi(\varphi^{s})}{q} = \frac{\Phi(m)}{q}.
\]
Therefore Lemma 2.8 is true when \( n = 1 \).

Suppose now that \( n \) is of positive degree. Applying Proposition 2.2 with \( s, \varphi, n \) in the roles of \( h, \varphi, m \), respectively, we deduce that
\[
\Psi_n(C_{\varphi^s}(u)) = \Psi_n(\varphi^s)(u)\Psi_n(C_{\varphi^{s-1}}(u)) = \Psi_m(u)\Psi_n(C_{\varphi^{s-1}}(u)),
\]
and thus
\[
\deg(\Psi_m(u)) = \deg(\Psi_n(C_{\varphi^s}(u))) - \deg(\Psi_n(C_{\varphi^{s-1}}(u))). \tag{12}
\]
Since \( n \) is of positive degree, it follows from (10), (11), and Lemma 2.7 that
\[
\deg(\Psi_n(C_{\varphi^s}(u))) = \deg(C_{\varphi^s}(u))\Phi(n) = q^{\deg(\varphi^s)-1}\Phi(n),
\]
and
\[
\deg(\Psi_n(C_{\varphi^{s-1}}(u))) = \deg(C_{\varphi^{s-1}}(u))\Phi(n) = q^{\deg(\varphi^{s-1})-1}\Phi(n).
\]
Therefore we deduce from (12) that
\[
\deg(\Psi_m(u)) = q^{\deg(\varphi^s)-1}\Phi(n) - q^{\deg(\varphi^{s-1})-1}\Phi(n) = \frac{\Phi(n)(q^{\deg(\varphi^s)} - q^{\deg(\varphi^{s-1})})}{q} = \frac{\Phi(n)\Phi(\varphi^{s})}{q} = \frac{\Phi(m)}{q},
\]
which proves that Lemma 2.8 is true when \( n \) is of positive degree.

From Cases 1 and 2, our contention follows. \( \square \)
3. A Carlitz module analogue of Zsigmondy primes

In this section, we introduce a Carlitz module analogue of Zsigmondy primes for a pair of monic polynomials. We then prove a function field analogue of L"uneburg’s theorem which is crucial in the proofs of our main results. We begin by proving a result that motivates a notion of the Carlitz annihilators of a pair consisting of a polynomial and a monic prime. This notion plays a key role in the study of Zsigmondy primes for the Carlitz module. In comparison, the notion of Carlitz annihilators is a function field analogue of that of the multiplicative order of an integer modulo a prime in the number field context.

**Proposition 3.1.** Let $u$ be a nonzero polynomial in $A$, and let $\varphi$ be a monic prime in $A$ such that $\varphi$ does not divide $u$. Then there exists a unique monic polynomial $q$ of positive degree satisfying the following two conditions.

(CA1) $C_\varphi(u) \equiv 0 \pmod{\varphi}$; and
(CA2) for any nonzero polynomial $m$ in $A$, $q$ divides $m$ if and only if $C_m(u) \equiv 0 \pmod{\varphi}$.

**Proof.** By Lemma [1.5], we know there exists a monic polynomial of positive degree, say $C$, satisfying (CA1), that is, $C_\varphi(u) \equiv 0 \pmod{\varphi}$; for example, one can take $a = \varphi - 1$. Take a monic polynomial of least degree satisfying (CA1), say $q$. Such a monic polynomial exists since for a given positive integer $h$, there are finitely many monic polynomials in $A$ of degree $h$. We prove that $q$ is the unique monic polynomial satisfying (CA1) and (CA2). By the choice of $q$, we know that $q$ satisfies (CA1).

We now prove that $q$ satisfies (CA2). Indeed take any nonzero polynomial $m$ such that $C_m(u) \equiv 0 \pmod{\varphi}$. We know that there exist polynomials $n, r \in A$ such that

$$m = nq + r$$

and $r$ is either 0 or $0 \leq \deg(r) < \deg(q)$. We see that

$$0 \equiv C_m(u) = C_{nq+r}(u) = C_n(C_q(u)) + C_r(u) \pmod{\varphi}.$$  

By [1.5] Proposition 12.11, one can write $C_n(x) \in A[x]$ in the form

$$C_n(x) = nx + \left[n,1\right]x^q + \ldots + \left[n,\deg(n) - 1\right]x^{\deg(n) - 1} + \left[n,\deg(n)\right]x^{\deg(n)},$$

where the $\left[n,i\right]$ are elements in $A$. Since $C_q(u) \equiv 0 \pmod{\varphi}$, we deduce from the above equation that $C_n(C_q(u)) \equiv 0 \pmod{\varphi}$. Therefore it follows from [1.4] that

$$C_r(u) \equiv 0 \pmod{\varphi}.$$  

Since $q$ is the monic polynomial of least degree satisfying (CA1), we deduce from [1.5] that $\deg(r) = 0$ or $r = 0$. If $\deg(r) = 0$, then $r$ is a unit in $F_q^\times$. We deduce from [1.5] that

$$ru = C_r(u) \equiv 0 \pmod{\varphi},$$

and thus $\varphi$ divides $u$, which is a contradiction. Therefore $r = 0$, and hence by [1.5] we deduce that $m = nq$. Thus $q$ divides $m$.

Conversely suppose that $q$ divides $m$. Then there exists a nonzero polynomial, say $n$, such that $m = nq$. By [1.5] Proposition 12.11, one can write $C_n(x) \in A[x]$ in the form

$$C_n(x) = nx + \left[n,1\right]x^q + \ldots + \left[n,\deg(n) - 1\right]x^{\deg(n) - 1} + \left[n,\deg(n)\right]x^{\deg(n)},$$

where the $\left[n,i\right]$ are elements in $A$. Since $C_q(u) \equiv 0 \pmod{\varphi}$, we deduce that

$$C_m(u) = C_{nq}(u) = C_n(C_q(u)) = nC_q(u) + \left[n,1\right](C_q(u))^q + \ldots + \left[n,\deg(n)\right](C_q(u))^\deg(n) \equiv 0 \pmod{\varphi}.$$  

Thus $q$ satisfies (CA2).

Finally we prove that $q$ is unique. Indeed, assume there exists a monic polynomial of positive degree $P$ satisfying (CA1) and (CA2). By (CA2), we know that $q$ divides $P$, and $P$ divides $q$. Since $q, P$ are monic, we deduce that $q = P$, which proves our contention.
In [8], I introduced the notion of the Carlitz annihilator of a monic prime to study congruences of primes dividing a Mersenne number in the function field setting. The following definition is a generalization of the notion of the Carlitz annihilator of a monic prime to a couple \((u, \wp)\), where \(u\) is a nonzero polynomial and \(\wp\) is a monic polynomial.

**Definition 3.2.** Let \(u\) be a nonzero polynomial in \(A\), and let \(\wp\) be a monic prime in \(A\). Let \(P_{u,\wp}\) be the unique monic polynomial satisfying (CA1) and (CA2) in Proposition 3.1 if \(\wp\) does not divide \(u\), and let \(P_{u,\wp} = 1\) if \(\wp\) divides \(u\). The monic polynomial \(P_{u,\wp}\) is called the Carlitz annihilator of \((u, \wp)\).

For the rest of this paper, we always denote by \(P_{u,\wp}\) the Carlitz annihilator of a couple \((u, \wp)\). The following result is immediate from Lemma 1.5, Proposition 3.1, and Definition 3.2.

**Proposition 3.3.** Let \(u\) be a nonzero polynomial in \(A\), and let \(\wp\) be a monic prime in \(A\). Let \(P_{u,\wp}\) be the Carlitz annihilator of \((u, \wp)\). Then

1. \(P_{u,\wp}\) divides \(\wp - 1\);
2. \(P_{u,\wp} = 1\) if and only if \(\wp\) divides \(u\);
3. for any nonzero polynomial \(m\) in \(A\), \(P_{u,\wp}\) divides \(m\) if and only if \(C_m(u) \equiv 0 \pmod{\wp}\);
4. \(C_n(u) \not\equiv 0 \pmod{\wp}\) for every nonzero polynomial \(n \in A\) with \(\deg(n) < \deg(P_{u,\wp})\).

**Proof.** Only part (iv) needs a proof. If \(P_{u,\wp} = 1\), then part (iii) is trivial. Assume that \(P_{u,\wp}\) is of positive degree, and take any nonzero polynomial \(n \in A\) with \(\deg(n) < \deg(P_{u,\wp})\). If \(C_n(u) \equiv 0 \pmod{\wp}\), then we see from Proposition 3.1 that \(P_{u,\wp}\) divides \(n\). This implies that \(\deg(P_{u,\wp}) \leq \deg(n)\), which is a contradiction. Hence \(C_n(u) \not\equiv 0 \pmod{\wp}\), and therefore our contention follows immediately.

The analogy between the multiplicative group \(G_m\) and the Carlitz module \(C\) that is explained in Section 1 (see Table 1) motivates the following notion.

**Definition 3.4.** Let \(m, u\) be nonzero polynomials in \(A\). A Zsigmondy prime for \((u, m)\) is a monic prime \(\wp\) such that \(C_m(u) \equiv 0 \pmod{\wp}\) and \(C_n(u) \not\equiv 0 \pmod{\wp}\) for every nonzero polynomial \(n \in A\) with \(\deg(n) < \deg(m)\).

If a monic prime \(\wp\) is not a Zsigmondy prime for \((u, m)\), we say that \(\wp\) is a non-Zsigmondy prime for \((u, m)\).

**Remark 3.5.**

1. Write \(m = \epsilon m_0\), where \(\epsilon \in \mathbb{F}_q^\times\) is the leading coefficient of \(m\) and \(m_0\) is a monic polynomial in \(A\). By Proposition 3.3(iv), one sees that Definition 3.4 is equivalent to the following notion: A monic prime \(\wp\) is a Zsigmondy prime for a pair \((u, m)\) if the Carlitz annihilator of \((u, \wp)\) is exactly \(m_0\). In particular, when \(m\) is monic, this means that the Carlitz annihilator of \((u, \wp)\) is exactly \(m\).

2. For any nonzero polynomials \(m, u \in A\), write \(m = \epsilon m_0\) and \(u = \delta u_0\), where \(\epsilon, \delta \in \mathbb{F}_q^\times\), and \(m_0, u_0\) are monic polynomials. We see that \(C_m(u) = \epsilon \delta C_{m_0}(u_0)\), and \(C_n(u) = \delta C_{m_0}(u_0)\) for any polynomial \(n \in A\). Thus we deduce that a prime \(\wp\) is a Zsigmondy prime for \((u, m)\) if and only if it is a Zsigmondy prime for \((u_0, m_0)\).

3. Assume that \(m, u\) are nonzero polynomials in \(A\) such that \(\deg(m) = \deg(u) = 0\). Then \(m, u\) are units in \(\mathbb{F}_q^\times\). Hence \(C_m(u) = mu \in \mathbb{F}_q^\times\). Thus there exist no Zsigmondy primes for \((u, m)\).

By Remark 3.5 it suffices to study Zsigmondy primes for pairs \((u, m)\), where \(m, u\) are monic polynomials such that at least one of them is of positive degree. Throughout this paper, in order to rule out the trivial cases, whenever we study Zsigmondy primes for a pair \((u, m)\), we will always assume that \(m, u\) are monic polynomials such that at least one of them is of positive degree.

**Remark 3.6.**
(i) If $\wp$ is a Zsigmondy prime for $(u, m)$, then we know from Proposition 2.1 that $\wp$ divides $C_m(u) = \prod_{n|m} \Psi_n(u)$. If $\wp$ divides $\Psi_n(u)$ for some monic polynomial $n$ dividing $m$ with $n \neq m$, then we deduce from Proposition 2.1 that

$$C_n(u) = \prod_{b|n \text{ monic}} \Psi_b(u) \equiv 0 \pmod{\wp}.$$ 

Since $n \neq m$, $n$ divides $m$, and both of $n, m$ are monic, we deduce that $\deg(n) < \deg(m)$. Thus the above congruence implies that $\wp$ is not a Zsigmondy prime for $(u, m)$, which is a contradiction. Hence $\gcd(\wp, \Psi_n(u)) = 1$ for any monic polynomial $n$ dividing $m$ with $n \neq m$. Therefore $\wp$ divides $\Psi_m(u)$.

(ii) The above remark also implies that if $\wp$ does not divide $\Psi_m(u)$, then $\wp$ is a non-Zsigmondy prime for $(u, m)$. Hence in order to show whether a monic prime $\wp$ is a Zsigmondy prime for $(u, m)$, it suffices to consider the case when $\wp$ divides $\Psi_m(u)$. The next result gives a simple criterion for testing whether a monic prime $\wp$ is a non-Zsigmondy prime for a given pair $(u, m)$. This is a function field analogue of L"uneburg’s theorem (see L"uneburg [13] Satz 1 or Roitman [14 Proposition 2]) which we will need in the proof of our first main result, the function field analogue of Bang–Zsigmondy’s theorem.

Theorem 3.7. Let $m, u$ be monic polynomials in $A$ such that $m$ is of positive degree. Let $\wp$ be a monic prime dividing $\Psi_m(u)$, and let $P_{u, \wp}$ be the Carlitz annihilator of $(u, \wp)$. Assume that condition $(D^*)$ in Corollary 2.4 is satisfied. Then

(i) $\wp$ is a non-Zsigmondy prime for $(u, m)$ if and only if $\wp$ divides $m$.

(ii) if $\wp$ is a non-Zsigmondy prime for $(u, m)$, then $m = P_{u, \wp} \wp^s$ for some positive integer $s$. Furthermore $\wp^2$ does not divide $\Psi_m(u)$ unless $q = 2$ and $\deg(\wp) = 1$.

Proof. Since $\wp$ divides $\Psi_m(u)$, it follows from Proposition 2.1 that $\wp$ divides $C_m(u)$. Thus we deduce from Proposition 3.3 (iv) that $P_{u, \wp}$ divides $m$.

We now prove part (i). We first show that the “only if” part of (i) is true. Indeed assume that $\wp$ is a non-Zsigmondy prime for $(u, m)$. We know from Remark 3.3 that $m \neq P_{u, \wp}$. Since both of $P_{u, \wp}, m$ are monic, and $P_{u, \wp}$ divides $m$, we deduce that $\deg(P_{u, \wp}) < \deg(m)$.

Write

(16) $$m = P_{u, \wp}^r n,$$

where $r$ is a positive integer, and $n$ is a monic element in $A$ such that $\gcd(P_{u, \wp}, n) = 1$. Since $\deg(P_{u, \wp}) < \deg(m)$, it follows that $r \geq 2$ or $\deg(n) \geq 1$.

Let $l$ be a monic prime of positive degree such that $l$ divides $m$ and $P_{u, \wp}$ divides $m/l$. Then we see from Proposition 3.3 (iii) that

(17) $$C_{m/l}(u) \equiv 0 \pmod{\wp}.$$ 

By Lemma 2.3, we know that $\Psi_m(x)$ divides $C_m(x)/C_{m/l}(x)$ in the polynomial ring $A[x]$. By Corollary 2.6 one sees that $C_{m/l}(u) \neq 0$, and it thus follows that $\Psi_m(u)$ divides $C_m(u)/C_{m/l}(u)$. Since $\wp$ divides $\Psi_m(u)$, we deduce that

(18) $$\frac{C_m(u)}{C_{m/l}(u)} \equiv 0 \pmod{\wp}.$$ 

By [15 Proposition 12.11], one can write $C_l(x) \in A[x]$ in the form

$$C_l(x) = lx + [l, 1]x^q + \ldots + [l, \deg(l) - 1]x^{q^{\deg(l)} - 1} + x^{q^{\deg(l)}},$$
where $[l, i]$ is a polynomial of degree $q^i (\deg(l) - i)$ for each $1 \leq i \leq \deg(l) - 1$. By (17), we deduce that

$$ \frac{C_m(u)}{C_{m/l}(u)} = \frac{C_l(C_{m/l}(u))}{C_{m/l}(u)} = l + [l, 1]C_{m/l}(u)^q - 1 + \ldots + [l, \deg(l) - 1]C_{m/l}(u)^{q^{\deg(l) - 1}} - 1 + (C_{m/l}(u))^{q^{\deg(l) - 1}} $$

$$ \equiv l \pmod{\varphi}, $$

and therefore it follows from (18) that $l \equiv 0 \pmod{\varphi}$. Since $l, \varphi$ are monic primes, we deduce that $l = \varphi$.

In summary, we have proved that if $l$ is a monic prime of positive degree such that $l$ divides $m$, and $P_{u, \varphi}$ divides $m/l$, then $l = \varphi$.

We now prove that $r = 1$ and $n = \varphi^s$ for some positive integer $s$ in the equation (16) of $m$. Indeed if $r \geq 2$, then letting $l = P_{u, \varphi}$, we see that

$$ \frac{m}{l} = \frac{m}{P_{u, \varphi}} = P_{u, \varphi}^{-1} n \equiv 0 \pmod{P_{u, \varphi}}. $$

Thus repeating the same arguments as before, we deduce that $P_{u, \varphi} = l = \varphi$, which is a contradiction since Proposition 3.3 (i) tells us that $P_{u, \varphi}$ divides $\varphi - 1$. Thus $r = 1$.

Now take any monic prime $l$ dividing $n$. In particular, this implies that $l$ divides $m$. We know from (19) that

$$ \frac{m}{l} = P_{u, \varphi}(n/l) \equiv 0 \pmod{P_{u, \varphi}}. $$

Thus using the same arguments as before, we deduce that $l = \varphi$. Since $n$ is a monic polynomial, we see that $n = \varphi^s$ for some positive integer $s$. Therefore

$$ m = P_{u, \varphi} \varphi^s. $$

In particular, this implies that $\varphi$ divides $m$, which establishes the “only if” part of (i).

We now prove the “if” part of (i). Assume that $\varphi$ divides $m$. Assume the contrary, i.e., $\varphi$ is a Zsigmondy prime for $(u, m)$. By Remark 3.3 (i), we know that $m = P_{u, \varphi}$. Since $\varphi$ divides $m$, we deduce that

$$ \deg(\varphi) \leq \deg(m) = \deg(P_{u, \varphi}). $$

On the other hand, we know from Proposition 3.3 (i) that $P_{u, \varphi}$ divides $\varphi - 1$, and thus

$$ \deg(P_{u, \varphi}) \leq \deg(\varphi - 1) = \deg(\varphi). $$

Therefore $\deg(P_{u, \varphi}) = \deg(\varphi) = \deg(\varphi - 1)$, and hence $P_{u, \varphi} = \varphi - 1$. This implies that $m = P_{u, \varphi} = \varphi - 1$, which is a contradiction since $\varphi$ divides $m$. Thus $\varphi$ is a non-Zsigmondy prime for $(u, m)$, which proves the “if” part of (i).

We now prove part (ii). In the proof of the “only if” part of (i) above, we have showed that if $\varphi$ is a non-Zsigmondy prime for $(u, m)$, then $m$ is of the form (19), and thus the first part of (ii) follows immediately.

For the last part of (ii), using Proposition 12.11, one can write $C_{\varphi}(x) \in \mathbb{A}[x]$ in the form

$$ C_{\varphi}(x) = \varphi x + [\varphi, 1]x^q + \ldots + [\varphi, d - 1]x^{q^{d-1}} + x^{q^d}, $$

where $d = \deg(\varphi)$, and $[\varphi, i]$ is a polynomial of degree $q^i (d - i)$ in $\mathbb{A}$ for each $1 \leq i \leq d - 1$. It is well-known Proposition 2.4 that $C_{\varphi}(x)$ is an Eisenstein polynomial, that is, $[\varphi, i]$ is divisible by $\varphi$ for each $1 \leq i \leq d - 1$.

By the first part of (ii) and (19), we know that $P_{u, \varphi}$ divides the polynomial $m/\varphi$, and it thus follows from Proposition 3.3 (iii) that

$$ C_{m/\varphi}(u) \equiv 0 \pmod{\varphi}. $$

If $d = \deg(\varphi) > 1$, then we know that $q^i - 1 \geq 1$ for every $1 \leq i \leq d - 1$, and thus

$$ [\varphi, i]C_{m/\varphi}(u)q^{i-1} \equiv 0 \pmod{\varphi^2} $$
for every $1 \leq i \leq d - 1$. Furthermore since $q^i - 1 \geq q^2 - 1 \geq 3$, we deduce that $(C_{m/\varphi}(u))^{q^i-1} \equiv 0 \mod \varphi^2$. By Corollary 2.6 one knows that $C_{m/\varphi}(u) \neq 0$, and therefore we deduce from (20) that
\[
\frac{C_m(u)}{C_{m/\varphi}(u)} = \frac{C_{\varphi}(C_{m/\varphi}(u))}{C_{m/\varphi}(u)} = \varphi + [q, 1](C_{m/\varphi}(u))^{q-1} + \ldots + [\varphi, d-1](C_{m/\varphi}(u))^{q^d-1} + (C_{m/\varphi}(u))^{q^d-1} \equiv \varphi \mod \varphi^2.
\]

Since $C_{m/\varphi}(u) \neq 0$, we deduce from Lemma 2.6 that $\Psi_m(u)$ divides $C_m(u)/C_{m/\varphi}(u)$. If $\varphi^2$ divides $\Psi_m(u)$, then
\[
\varphi \equiv \frac{C_m(u)}{C_{m/\varphi}(u)} \equiv 0 \mod \varphi^2,
\]
which is a contradiction. Therefore $\varphi^2$ does not divide $\Psi_m(u)$.

If $q > 2$, then we see that $q^i - 1 \geq 2$ for every $1 \leq i \leq d$, and thus $(C_{m/\varphi}(u))^{q^i-1} \equiv 0 \mod \varphi^2$ for every $1 \leq i \leq d$. Repeating in the same arguments as above, we deduce that
\[
\frac{C_m(u)}{C_{m/\varphi}(u)} \equiv \varphi \mod \varphi^2,
\]
and thus $\varphi^2$ does not divide $\Psi_m(u)$. Therefore the last part of (ii) follows.

When $q > 2$, we see that condition $(D*)$ in Corollary 2.6 is trivially satisfied. For the rest of this paper, we will always assume that $q > 2$, and thus it is worth restating Theorem 3.7 with the assumption $q > 2$ in place of $(D*)$.

**Corollary 3.8.** Assume that $q > 2$. Let $m, u$ be monic polynomials in $A$ such that $m$ is of positive degree. Let $\varphi$ be a monic prime dividing $\Psi_m(u)$, and let $P_{u,\varphi}$ be the Carlitz annihilator of $(u, \varphi)$. Then
(i) $\varphi$ is a non-Zsigmondy prime for $(u, m)$ if and only if $\varphi$ divides $m$.
(ii) If $\varphi$ is a non-Zsigmondy prime for $(u, m)$, then $m = P_{u,\varphi}\varphi^s$ for some positive integer $s$. Furthermore $\varphi^2$ does not divide $\Psi_m(u)$.

4. Bang–Zsigmondy’s theorem in characteristic $p \neq 2$

In this section, we prove a function field analogue of Bang–Zsigmondy’s theorem in the case when $p \neq 2$ (see Theorem 4.1 below). The strategy of the proof of Theorem 4.1 is as follows. We first assume that there are no Zsigmondy primes for $(u, m)$. Using Corollary 3.8, we show that $\Psi_m(u)$ is a prime in $A$, and in fact it divides $m$. In comparing the degree of $\Psi_m(u)$ with that of $m$, we reach a contradiction except for some exceptional cases that will be explicitly determined.

We begin by proving an elementary but very useful result that will play a key role in the proofs of Theorem 4.1 and Theorem 5.2.

**Lemma 4.1.** Assume that $q > 2$. Let $m$ be a polynomial in $A$ of positive degree. Then $\Phi(m) \geq (q - 1)\deg(m)$, where $\Phi(\cdot)$ denotes the function field analogue of the Euler $\phi$-function (see Subsection 1.3 for its definition).

**Proof.** Since $\Phi(m) = \Phi(\epsilon m)$ for any unit $\epsilon \in \mathbb{F}_q^\times$, we can, without loss of generality, assume throughout the proof that $m$ is a monic polynomial.

We first prove a special case of Lemma 4.1 when $m = P^s$, where $P$ is a monic prime and $s$ is a positive integer. Indeed, set $d = \deg(P) \geq 1$. If $s = 1$, using Bernoulli’s inequality (see 124 Theorem 42), we deduce that
\[
\Phi(m) = \Phi(P) = q^d - 1 = (1 + (q - 1))^d - 1 \geq 1 + (q - 1)d - 1 = (q - 1)d = (q - 1)\deg(m).
\]
If $s > 1$, then we see from Bernoulli’s inequality that
\[
q^{s(d-1)} - 1 \geq (q - 1)d(s - 1).
\]
Since \( q > 2 \) and \( d \geq 1 \), we deduce that
\[
q^{d(s-1)} \geq 1 + (q-1)d(s-1) > 1 + (s-1) = s.
\]
Therefore
\[
\Phi(m) = \Phi(P^s) = q^{\deg(P^s)} - q^{\deg(P^{s-1})} = q^{d(s-1)}(q^d - 1) > s((q-1)d) = (q-1)ds = (q-1)d\deg(P^s) = (q-1)\deg(m).
\]
Therefore Lemma 4.1 holds for \( m = P^s \), where \( P \) is a monic prime and \( s \) is a positive integer.

Let \( m \) be any monic polynomial, and let \( r = \deg(m) \geq 1 \). We now prove Lemma 4.1 by induction on \( r \).

If \( r = \deg(m) = 1 \), then \( m \) is a monic prime of degree 1, and we have already proved that Lemma 4.1 is true in this case. Now take any integer \( r \geq 2 \), and assume that Lemma 4.1 is true for any monic polynomial of degree less than \( r \). We prove that Lemma 4.1 holds for any monic polynomial of degree \( r \) in this case. If \( \deg(n) \geq 1 \), we see that \( 1 \leq \deg(n) < \deg(m) = r \). By the induction hypothesis, and since \( q > 2 \), we deduce that
\[
\Phi(n) \geq (q-1)\deg(n) \geq 2\deg(n) \geq 2.
\]
Since Lemma 4.1 holds for the polynomial \( P^s \), we deduce from the above inequality that
\[
\Phi(P^s)(\Phi(n) - 1) \geq (q-1)\deg(P^s)(\Phi(n) - 1) \geq 2(\Phi(n) - 1) \geq \Phi(n),
\]
and thus
\[
(21) \quad \Phi(m) = \Phi(n)\Phi(P^s) \geq \Phi(n) + \Phi(P^s).
\]
Since Lemma 4.1 holds for \( P^s \), we deduce that
\[
\Phi(n) + \Phi(P^s) \geq (q-1)\deg(n) + (q-1)\deg(P^s) = (q-1)\deg(nP^s) = (q-1)\deg(m).
\]
Thus we deduce from (21) that
\[
\Phi(m) = \Phi(n)\Phi(P^s) \geq \Phi(n) + \Phi(P^s) \geq (q-1)\deg(m),
\]
which proves our contention.

**Lemma 4.2.** Assume that \( q > 2 \). Let \( m, u \) be monic polynomials such that \( m \) is of positive degree. Then \( \Psi_m(u) \) is of positive degree.

**Proof.** If \( u \) is of positive degree, we see from Lemmas 2.7 and 3.1 that
\[
\deg(\Psi_m(u)) = \deg(u)\Phi(m) \geq (q-1)\deg(m) \geq q-1 \geq 2,
\]
and thus \( \Psi_m(u) \) is of positive degree.

If \( u \) is a unit in \( \mathbb{F}_q^* \), we see from Lemma 2.8 that either \( \deg(\Psi_m(u)) = \Phi(m)/q \) or \( \deg(\Psi_m(u)) = \Phi(m) + \delta \)
for some \( \delta \in \{ \pm 1 \} \). In either case, we deduce from Lemmas 2.7 that
\[
\deg(\Psi_m(u)) \geq \frac{\Phi(m) - 1}{q} \geq \frac{(q-1)\deg(m) - 1}{q} \geq \frac{q-2}{q} \geq 1/q > 0,
\]
and therefore \( \Psi_m(u) \) is of positive degree.

The next result is crucial in the proof of Theorem 4.4.
Corollary 4.3. Assume that $p \neq 2$ (recall that $p$ is the characteristic of $\mathbb{F}_q$). Let $m, u$ be monic polynomials in $A$ such that $m$ is of positive degree. Assume that there are no Zsigmondy primes for $(u, m)$. Then $\Psi_m(u) = \epsilon \varphi$ for some unit $\epsilon \in \mathbb{F}_q^\times$ and some monic prime $\varphi$.

Proof. Note that since $p \neq 2$, we know that $q > 2$. By Lemma 4.2, we know that $\Psi_m(u)$ is of positive degree. Hence there exists a monic prime $\varphi$ dividing $\Psi_m(u)$. Since $\varphi$ is a non-Zsigmondy prime for $(u, m)$, applying Corollary 3.8(ii), we see that $m = P_{u, \varphi} s$ for some positive integer $s$, where $P_{u, \varphi}$ is the Carlitz annihilator of $(u, \varphi)$.

We now prove that $\varphi$ is the only monic prime factor of $\Psi_m(u)$. Indeed, assume the contrary, that is, there exists a monic prime $P$ dividing $\Psi_m(u)$ such that $P \neq \varphi$. By assumption, we know that $P$ is a non-Zsigmondy prime for $(u, m)$. Hence we know from Corollary 3.8 that $P$ divides $m$. Since $\gcd(P, \varphi) = 1$ and $m = P_{u, \varphi} s$, we see that $P$ divides $P_{u, \varphi}$. Therefore by Proposition 3.3(i), we deduce that

$$\varphi - 1 \equiv 0 \pmod{P}.$$  

In particular, this implies that $\deg(P) \leq \deg(\varphi - 1) = \deg(\varphi)$.

Exchanging the roles of $\varphi$ and $P$ and using the same arguments as above, we deduce that

$$P - 1 \equiv 0 \pmod{\varphi}.$$  

Furthermore this implies that $\deg(\varphi) \leq \deg(P - 1) = \deg(P)$, and it thus follows that $\deg(P) = \deg(\varphi)$. Since $P, \varphi$ are monic, we deduce from (22) and (23) that $P = \varphi - 1$ and $P - 1 = \varphi$, respectively. Hence $P = \varphi - 1 = P - 2$, and thus $2 = 0$, which is a contradiction since $p \neq 2$. This contradiction establishes that $\varphi$ is the only monic prime factor of $\Psi_m(u)$, and thus

$$\Psi_m(u) = \epsilon \varphi^e$$  

for some unit $\epsilon \in \mathbb{F}_q^\times$ and some positive integer $e$.

By Corollary 3.8(ii), we deduce that $\varphi^2$ does not divide $\Psi_m(u)$, and therefore $e = 1$. Thus Corollary 4.3 follows immediately.

The following result is a Carlitz module analogue of Bang–Zsigmondy’s theorem in characteristic $p \neq 2$. An analogue of Bang–Zsigmondy’s theorem in characteristic two will be proved in Section 5.

Theorem 4.4. Assume that $p \neq 2$. Let $m, u$ be monic polynomials in $A$ such that at least one of them is of positive degree. Then there exists a Zsigmondy prime for $(u, m)$ except exactly in the following case:

(EC1) $q = 3$, $u = 1$, and $m = (\varphi - 1)\varphi$, where $\varphi$ is an arbitrary monic prime of degree 1 in $\mathbb{F}_3[T]$.

We will prove Theorem 4.4 at the end of this section. The proof of Theorem 4.4 will follow immediately from the next two lemmas.

Lemma 4.5. Assume that $p \neq 2$. Let $m, u$ be monic polynomials in $A$ such that $u$ is of positive degree. Then there exists a Zsigmondy prime for $(u, m)$.

Proof. Since $p \neq 2$, we see that $q > 2$. If $\deg(m) = 0$, we deduce that $m = 1$. Hence it is easy to see that $\varphi$ is a Zsigmondy prime for $(u, m)$ for each monic prime $\varphi$ dividing $u$.

Suppose now that $\deg(m) > 0$. Assume the contrary, that is, there exist no Zsigmondy primes for $(u, m)$. It then follows from Corollary 4.3 that $\Psi_m(u) = \epsilon \varphi$ for some unit $\epsilon \in \mathbb{F}_q^\times$ and some monic prime $\varphi$.

Since $u$ is of positive degree, we know from Lemma 2.6 that

$$\deg(\Psi_m(u)) = \deg(u) \Phi(m),$$  

where we recall that $\Phi(\cdot)$ denotes the function field analogue of the Euler $\phi$-function. Thus

$$\deg(\varphi) = \deg(\Psi_m(u)) = \deg(u) \Phi(m).$$
Since \( \varphi \) is a non-Zsigmondy prime for \((u, m)\), we deduce from Corollary 5.3(i) that \( \varphi \) divides \( m \), and thus \( \deg(\varphi) \leq \deg(m) \). Therefore

\[
\deg(u)\Phi(m) \leq \deg(m).
\]

On the other hand, Lemma 4.1 tells us that \( \Phi(m) \geq (q - 1)\deg(m) \), and therefore

\[
\deg(m) \geq \deg(u)\Phi(m) \geq \Phi(m) \geq (q - 1)\deg(m) \geq 2\deg(m).
\]

Hence \( \deg(m) = 0 \), which is a contradiction. Thus there exists a Zsigmondy prime for \((u, m)\).

\[\Box\]

**Lemma 4.6.** Assume that \( p \neq 2 \). Let \( m \) be a monic polynomial in \( A \) such that \( m \) is of positive degree. Then there exists a Zsigmondy prime for \((1, m)\) except exactly in the following case:

(EC1) \( q = 3 \), and \( m = (\varphi - 1)\varphi \), where \( \varphi \) is an arbitrary monic prime of degree 1 in \( \mathbb{F}_3[T] \).

**Proof.** Assume first that \( q = 3 \), and \( m = (\varphi - 1)\varphi \), where \( \varphi \) is an arbitrary monic prime of degree 1 in \( \mathbb{F}_3[T] \). Table 2 tells us that there exist no Zsigmondy primes for \((1, m)\).

Suppose now that we are not in the exceptional case (EC1) in Lemma 4.6, that is, either \( q = 3 \) and \( m \neq (\varphi - 1)\varphi \) for any monic prime \( \varphi \) of degree 1 in \( \mathbb{F}_3[T] \) or \( q \neq 3 \).

Assume the contrary, that is, there exist no Zsigmondy primes for \((1, m)\). It then follows from Corollary 4.3 that

\[
\Psi_m(1) = \epsilon\varphi
\]

for some unit \( \epsilon \in \mathbb{F}_q^\times \) and some monic prime \( \varphi \). Since \( \varphi \) is a non-Zsigmondy prime for \((1, m)\), we know from Corollary 3.3(i) that

\[
m = P_{1,\varphi}\varphi^s,
\]

where \( P_{1,\varphi} \) is the Carlitz annihilator of \((1, \varphi)\), and \( s \) is a positive integer. Note that by Proposition 3.3(i), we know that \( P_{1,\varphi} \) is of positive degree.

By Lemma 2.8 we see that

\[
\deg(\Psi_m(1)) = \frac{\Phi(m) + \delta}{q},
\]

where \( \delta \) is an integer in \( \{0, \pm 1\} \). Recall from Proposition 3.3(i) that \( P_{1,\varphi} \) divides \( \varphi - 1 \), and thus \( \gcd(P_{1,\varphi}, \varphi) = 1 \). Since \( p \neq 2 \), we know that \( q > 2 \), and it thus follows from Lemma 2.8 that

\[
\Phi(m) = \Phi(P_{1,\varphi})\Phi(\varphi^s) \geq (q - 1)\deg(P_{1,\varphi})(q - 1)^2\deg(\varphi) \geq s(q - 1)^2\deg(P_{1,\varphi})\deg(\varphi).
\]

Since \( \deg(P_{1,\varphi}) \geq 1 \) and \( s \geq 1 \), it follows from the above inequalities that

\[
\Phi(m) \geq (q - 1)^2\deg(\varphi).
\]

### Table 2: Nonexistence of Zsigmondy primes for \((1, m)\), where \( m = (\varphi - 1)\varphi \) for some monic prime \( \varphi \) of degree 1 in \( \mathbb{F}_3[T] \).

| \( \varphi \) | \( m = (\varphi - 1)\varphi \) | The prime factorization of \( C_m(1) \) | Nonexistence of Zsigmondy primes for \((1, m)\) |
| --- | --- | --- | --- |
| \( T \) | \((T - 1)T\) | \( C_m(1) = \varphi_1^2\varphi_2 \), where \( \varphi_1 = T \) and \( \varphi_2 = T + 1 \). | There are no Zsigmondy primes for \((1, m)\) since \( \varphi_1 = C_{T-1}(1) \) and \( C_T(1) = \varphi_2 \). |
| \( T + 1 \) | \( T(T + 1) \) | \( C_m(1) = \varphi_1\varphi_2^2 \), where \( \varphi_1 = T + 1 \) and \( \varphi_2 = T + 2 \). | There are no Zsigmondy primes for \((1, m)\) since \( \varphi_1 = C_T(1) \) and \( C_{T+1}(1) = \varphi_2 \). |
| \( T + 2 \) | \((T + 1)(T + 2)\) | \( C_m(1) = \varphi_1\varphi_2^2 \), where \( \varphi_1 = T \) and \( \varphi_2 = T + 2 \). | There are no Zsigmondy primes for \((1, m)\) since \( \varphi_1 = C_{T-1}(1) \) and \( C_{T+1}(1) = \varphi_2 \). |
Note that if equality in (27) occurs, then \( \deg(P_{1,\wp}) = s = 1 \).
Since \( \delta \geq -1 \), we deduce from (26) and (27) that
\[
\deg(\Psi_m(1)) \geq \frac{(q - 1)^2\deg(\wp) - 1}{q}.
\]
From (27) and the remark following (27), we see that if equality in (28) occurs, then \( \deg(P_{1,\wp}) = s = 1 \).
By (24), (28), we deduce that
\[
(q - 1)^2\deg(\wp) - 1 \leq \deg(\Psi_m(1)) = \deg(\wp),
\]
and thus
\[
((q - 1)^2 - q)\deg(\wp) \leq 1.
\]
Note that equality in (30) occurs if and only if equality in (29) occurs.
On the other hand, since \( q > 2 \), we see that
\[
(q - 1)^2 - q \geq 1
\]
with equality if and only if \( q = 3 \). Since \( \deg(\wp) \geq 1 \), we deduce from (30) that
\[
1 \leq ((q - 1)^2 - q)\deg(\wp) \leq 1,
\]
and therefore
\[
((q - 1)^2 - q)\deg(\wp) = 1.
\]
Equation (31) implies that equality in (30) occurs, and thus \( q = 3 \) and \( \deg(\wp) = 1 \). Furthermore since equality in (30) occurs, equality in (29) also occurs, which in turns implies that equality in (28) occurs. Therefore by the remark following (28), we see that \( \deg(P_{1,\wp}) = s = 1 \). Thus it follows from (25) that
\[
m = P_{1,\wp}\wp,
\]
where \( \deg(P_{1,\wp}) = \deg(\wp) = 1 \). Since \( P_{1,\wp}, \wp - 1 \) are monic primes and \( P_{1,\wp} \) divides \( \wp - 1 \), we deduce that \( P_{1,\wp} = \wp - 1 \). Therefore \( q = 3 \) and \( m = (\wp - 1)\wp \), where \( \wp \) is a monic prime of degree 1 in \( \mathbb{F}_3[T] \).
This implies that we are in the exceptional case (EC1), which is a contradiction. Thus there exists a Zsigmondy prime for \((1, m)\).

We now prove Theorem 4.4.

**Proof of Theorem 4.4.** If \( u \) is of positive degree, we see from Lemma 4.5 that there exists a Zsigmondy primes for \((u, m)\).

If \( m \) is of positive degree and \( \deg(u) = 0 \), we see that \( u = 1 \). By Lemma 4.6 we know that there exists a Zsigmondy primes for \((1, m) = (u, m)\) except in the exceptional case (EC1). Therefore Theorem 4.4 follows.

5. Bang–Zsigmondy’s theorem in characteristic two

In this section, we will prove an analogue of Bang–Zsigmondy’s theorem in characteristic two. Throughout this section, we assume that \( p = 2 \) and \( q > 2 \). We first prove a basic result that describes the prime factorizations of polynomials \( \Psi_m(u) \), where \( m, u \) are monic polynomials such that there exist no Zsigmondy primes for \((u, m)\).

**Lemma 5.1.** Let \( m, u \) be monic polynomials in \( A \) such that \( m \) is of positive degree. Assume that there are no Zsigmondy primes for \((u, m)\).

Then either of the following is true:

(i) \( \Psi_m(u) = \epsilon\wp \) for some unit \( \epsilon \in \mathbb{F}_q^\times \) and some monic prime \( \wp \);

(ii) \( \Psi_m(u) = \epsilon\wp(\wp - 1) \), where \( \epsilon \in \mathbb{F}_q^\times \) and \( \wp \) is a monic prime such that \( \wp - 1 \) is also a prime.
Proof. By Lemma 5.2, we know that $\Psi_m(u)$ is of positive degree. Hence there exists a monic prime $\varphi$ dividing $\Psi_m(u)$. Since $\varphi$ is a non-Zsigmondy prime for $(u, m)$, applying Corollary 3.8(ii), we deduce that

$$m = P_{u, \varphi} \varphi^s$$

for some positive integer $s$, where $P_{u, \varphi}$ is the Carlitz annihilator of $(u, \varphi)$.

If $\varphi$ is the only prime factor of $\Psi_m(u)$, then we see that $\Psi_m(u) = \epsilon \varphi^e$ for some unit $\epsilon \in \mathbb{F}_q^\times$ and some positive integer $e$. Since $q > 2$, we deduce from Corollary 3.8(ii) that $\varphi^2$ does not divide $\Psi_m(u)$, and therefore $e = 1$. Thus $\Psi_m(u) = \epsilon \varphi$.

If $\Psi_m(u)$ has at least two distinct prime factors, let $P$ be an arbitrary monic prime dividing $\Psi_m(u)$ such that $P \neq \varphi$. We contend that $P = \varphi - 1$. Indeed, by assumption, we know that $P$ is a non-Zsigmondy prime for $(u, m)$. Hence Corollary 3.8(ii) tells us that $P$ divides $m$. Since $\gcd(P, \varphi) = 1$, we deduce from (32) that $P$ divides $P_{u, \varphi}$. Therefore by Proposition 3.3(i), we deduce that

$$\varphi - 1 \equiv 0 \pmod{P}.$$ 

In particular, this implies that $\deg(P) \leq \deg(\varphi - 1) = \deg(\varphi)$.

Exchanging the roles of $\varphi$ and $P$ and using the same arguments as above, we deduce that

$$P - 1 \equiv 0 \pmod{\varphi}.$$ 

Furthermore this implies that $\deg(\varphi) \leq \deg(P - 1) = \deg(P)$, and it thus follows that $\deg(P) = \deg(\varphi)$. Since $P, \varphi$ are monic, we deduce from (33) that $P = \varphi - 1$.

Thus we have proved that if $P$ is an arbitrary monic prime dividing $\Psi_m(u)$ such that $P \neq \varphi$, then $P = \varphi - 1$. In particular, this implies that $\varphi - 1$ is prime, and $\varphi, \varphi - 1$ are the only monic prime factors of $\Psi_m(u)$. Therefore $\Psi_m(u)$ is of the form

$$\Psi_m(u) = (\varphi - 1)^r \varphi^e$$

for some positive integers $r, e$ and some $\epsilon \in \mathbb{F}_q^\times$. Corollary 3.8(ii) tells us that $\varphi^2$ does not divide $\Psi_m(u)$, and therefore $e = 1$. Similarly since $\varphi - 1$ is a non-Zsigmondy prime for $(u, m)$, Corollary 3.8(ii) implies that $(\varphi - 1)^2$ does not divide $\Psi_m(u)$, and thus $r = 1$. Hence

$$\Psi_m(u) = \epsilon (\varphi - 1)\varphi,$$

which proves our contention.  

We now state an analogue of Bang–Zsigmondy’s theorem in characteristic two.

**Theorem 5.2.** Let $m, u$ be monic polynomials in $A$ such that at least one of them is of positive degree. Then there exists a Zsigmondy prime for $(u, m)$ except exactly in the following case:

(EC2) $q = 2^2$, $u = 1$, and $m = (\varphi - 1)\varphi$, where $\varphi$ is an arbitrary monic prime of degree 1 in $\mathbb{F}_2[T]$.

We will prove Theorem 5.2 at the end of this section. We first show that if $u$ is of positive degree, then Theorem 5.2 is true.

**Lemma 5.3.** Let $m, u$ be monic polynomials in $A$ such that $u$ is of positive degree. Then there exists a Zsigmondy prime for $(u, m)$.

*Proof.* If $\deg(m) = 0$, we deduce that $m = 1$. Hence it is easy to see that $\varphi$ is a Zsigmondy prime for $(u, m)$ for each monic prime $\varphi$ dividing $u$.

We now consider the case when $\deg(m) > 0$. Assume the contrary, that is, there exist no Zsigmondy primes for $(u, m)$. Then by Lemma 5.1, we know that either of the following is true:

(i) $\Psi_m(u) = \epsilon \varphi$ for some unit $\epsilon \in \mathbb{F}_q^\times$ and some monic prime $\varphi$;

(ii) $\Psi_m(u) = \epsilon (\varphi - 1)\varphi$ for some unit $\epsilon \in \mathbb{F}_q^\times$, where $\varphi$ is a monic prime such that $\varphi - 1$ is also a prime.
If $\Psi_m(u) = \epsilon \varphi$ for some unit $\epsilon \in \mathbb{F}_q^\times$ and some monic prime $\varphi$, repeating the same arguments as in the proof of Lemma 3.3, we deduce that there exists a Zsigmondy prime for $(u, m)$.

Suppose now that $\Psi_m(u) = \epsilon (\varphi - 1)\varphi$ for some unit $\epsilon \in \mathbb{F}_q^\times$, where $\varphi$ is a monic prime such that $\varphi - 1$ is also a prime. Since $\varphi$ divides $\Psi_m(u)$ and $\varphi$ is a non-Zsigmondy prime for $(u, m)$, we deduce from Corollary 3.8(ii) that

$$m = P_{u, \varphi} \varphi^s,$$

where $P_{u, \varphi}$ is the Carlitz annihilator of $(u, \varphi)$ and $s$ is a positive integer. By Proposition 3.3(i), we know that $P_{u, \varphi}$ divides $\varphi - 1$.

Since $\varphi - 1$ is a monic prime and divides $m$, we deduce from Corollary 3.8(ii) that

$$m = P_{u, \varphi - 1} (\varphi - 1)^r,$$

where $P_{u, \varphi - 1}$ is the Carlitz annihilator of $(u, \varphi - 1)$ and $r$ is a positive integer. Since $(\varphi - 1) - 1 = \varphi$, we deduce from Proposition 3.3(i) that $P_{u, \varphi - 1}$ divides $\varphi$.

From (35), (36), we get

$$m = P_{u, \varphi} \varphi^s = P_{u, \varphi - 1} (\varphi - 1)^r.$$

By Proposition 3.3(i), we know that $P_{u, \varphi}$ divides $\varphi - 1$. In particular this implies that $\deg(P_{u, \varphi}) \leq \deg((\varphi - 1)) = \deg(\varphi)$. From 37 and since $\gcd((\varphi - 1)^r, \varphi^s) = 1$, we deduce that $(\varphi - 1)^r$ divides $P_{u, \varphi}$. Hence

$$\deg(P_{u, \varphi}) \leq \deg(\varphi) \leq r \deg(\varphi) = r \deg(\varphi - 1) = \deg((\varphi - 1)^r) \leq \deg(P_{u, \varphi}),$$

which in turn implies that

$$\deg(P_{u, \varphi}) = \deg(\varphi) = r \deg(\varphi) = \deg((\varphi - 1)^r).$$

Since $P_{u, \varphi}, \varphi - 1$ are monic, we deduce that $(\varphi - 1)^r = P_{u, \varphi}$, and it thus follows from the above identities that $r = 1$ and $P_{u, \varphi} = \varphi - 1$. Exchanging the roles of $\varphi$ and $\varphi - 1$, one can show that $s = 1$ and $P_{u, \varphi - 1} = (\varphi - 1) - 1 = \varphi$, and thus

$$m = (\varphi - 1)\varphi.$$

Therefore $\Psi_m(u) = \epsilon (\varphi - 1)\varphi = \epsilon m$.

By Lemma 2.7, we deduce that

$$\deg(\Psi_m(u)) = \deg(u) \Phi(m) = \deg(m).$$

By Lemma 4.1 and the above equation, we deduce that

$$\deg(m) \geq \deg(u)(q - 1) \deg(m) \geq (q - 1) \deg(m) > \deg(m),$$

which is a contradiction. Thus there exists a Zsigmondy prime for $(u, m)$.

We now consider Theorem 5.2 in the case when $m$ is of positive degree and $\deg(u) = 0$.

**Lemma 5.4.** Let $m$ be a monic polynomial in $A$ such that $m$ is of positive degree. Then there exists a Zsigmondy prime for $(1, m)$ except exactly in the following case:

(EC2) $q = 2^2$, and $m = (\varphi - 1)\varphi$, where $\varphi$ is an arbitrary monic prime of degree 1 in $\mathbb{F}_{2^2}[T]$.

**Proof.** Assume that we are in the exceptional case (EC2), that is, $q = 2^2$ and $m = (\varphi - 1)\varphi$ for a monic prime $\varphi$ of degree 1 in $\mathbb{F}_{2^2}[T]$. We see that $\mathbb{F}_{2^2} = \mathbb{F}_2(\omega)$, where $\omega$ is an element in the algebraic closure of $\mathbb{F}_2$ such that $\omega^2 + \omega + 1 = 0$. We know that $\{1, T, T + 1, T + \omega, T + \omega^2\}$ consists of all monic primes of degree 1 in $\mathbb{F}_{2^2}[T]$.

Table 3 tells us that there are no Zsigmondy primes for $(1, m)$ in the exceptional case (EC2).

Suppose now that we are not in the exceptional case (EC2) in Lemma 5.3, that is, either $q = 2^2$ and $m \neq (\varphi - 1)\varphi$ for any monic prime $\varphi$ of degree 1 in $\mathbb{F}_{2^2}[T]$ or $q \neq 2^2$. Assume the contrary, that is, there exist no Zsigmondy primes for $(1, m)$. Then by Lemma 5.1, we know that either of the following is true:

(i) $\Psi_m(1) = \epsilon \varphi$ for some unit $\epsilon \in \mathbb{F}_q^\times$ and some monic prime $\varphi$;
\begin{table}[h]
\centering
\begin{tabular}{|c|c|c|c|}
\hline
\(\varphi\) & \(m = (\varphi - 1)\varphi\) & The prime factorization of \(C_m(1)\) & Nonexistence of Zsigmondy primes for \((1, m)\) \\
\hline
\(T\) & \((T-1)T\) & \(C_m(1) = \varphi_1^2\varphi_2^2\), where \(\varphi_1 = T\) and \(\varphi_2 = T + 1\). & There are no Zsigmondy primes for \((1, m)\) since \(\varphi_1 = C_{T-1}(1)\) and \(\varphi_2 = C_T(1)\). \\
\hline
\(T + 1\) & \((T + 1)\) & \(C_m(1) = \varphi_1^2\varphi_2^2\), where \(\varphi_1 = T\) and \(\varphi_2 = T + 1\). & There are no Zsigmondy primes for \((1, m)\) since \(\varphi_1 = C_{T-1}(1)\) and \(\varphi_2 = C_T(1)\). \\
\hline
\(T + \omega\) & \((T + \omega - 1)(T + \omega)\) & \(C_m(1) = \varphi_1^2\varphi_2^2\), where \(\varphi_1 = T + \omega\) and \(\varphi_2 = T + \omega^2\). & There are no Zsigmondy primes for \((1, m)\) since \(\varphi_1 = C_{T+\omega-1}(1)\) and \(\varphi_2 = C_{T+\omega^2-1}(1)\). \\
\hline
\(T + \omega^2\) & \((T + \omega^2 - 1)(T + \omega^2)\) & \(C_m(1) = \varphi_1^2\varphi_2^2\), where \(\varphi_1 = T + \omega\) and \(\varphi_2 = T + \omega^2\). & There are no Zsigmondy primes for \((1, m)\) since \(\varphi_1 = C_{T+\omega-1}(1)\) and \(\varphi_2 = C_{T+\omega^2-1}(1)\). \\
\hline
\end{tabular}
\caption{Nonexistence of Zsigmondy primes for \((1, m)\), where \(m = (\varphi - 1)\varphi\) for a monic prime \(\varphi\) of degree 1 in \(\mathbb{F}_2[T]\).}
\end{table}

(ii) \(\Psi_m(1) = \epsilon(\varphi - 1)\varphi\) for some unit \(\epsilon \in \mathbb{F}_q^\times\), where \(\varphi\) is a monic prime such that \(\varphi - 1\) is also a prime.

Repeating the same arguments as in the proof of Lemma 4.6, we deduce that there exists a Zsigmondy prime for \((1, m)\) if \(\Psi_m(1) = \epsilon \varphi\) for some unit \(\epsilon \in \mathbb{F}_q^\times\) and some monic prime \(\varphi\).

Suppose now that \(\Psi_m(1) = \epsilon(\varphi - 1)\varphi\) for some unit \(\epsilon \in \mathbb{F}_q^\times\), where \(\varphi\) is a monic prime such that \(\varphi - 1\) is also a prime. Using the same arguments as in Lemma 5.3, we deduce that \(m = (\varphi - 1)\varphi\) and hence \(\Psi_m(1) = \epsilon m\). By Lemma 2.3, we see that

\[\deg(\Psi_m(1)) = \frac{\Phi(m) + \delta}{q},\]

where \(\delta\) is an integer in \(\{0, \pm 1\}\). Since \(\varphi - 1, \varphi\) are primes such that \(\gcd(\varphi - 1, \varphi) = 1\), we deduce from Lemma 4.1 that

\[\Phi(m) = \Phi((\varphi - 1)\varphi) = \Phi(\varphi - 1)\Phi(\varphi) \geq (q - 1)\deg(\varphi - 1)(q - 1)\deg(\varphi) = (q - 1)^2\deg(\varphi)^2.\]

Since \(\delta \geq -1\) and \(\deg(\varphi) \geq 1\), we get

\[2\deg(\varphi) = \deg(m) = \deg(\Psi_m(1)) \geq \frac{(q - 1)^2\deg(\varphi)^2 - 1}{q} \geq \frac{(q - 1)^2\deg(\varphi) - 1}{q},\]

and therefore

\[(38) \quad \deg(\varphi)((q - 1)^2 - 2q) \leq 1.

Since \(p = 2, q > 2,\) and \(q\) is a power of 2, we deduce that \(q \geq 4\). Thus

\[(39) \quad (q - 1)^2 - 2q = q^2 - 4q + 1 \geq 1\]

with equality if and only if \(q = 4 = 2^2\). Since \(\deg(\varphi) \geq 1\), we deduce that

\[1 \leq \deg(\varphi)((q - 1)^2 - 2q) \leq 1,\]

and hence

\[\deg(\varphi)((q - 1)^2 - 2q) = 1.\]

By (39), we deduce that \(\deg(\varphi) = 1\) and \(q = 2^2\). Hence \(q = 2^2\), and \(m = (\varphi - 1)\varphi\) for some monic prime \(\varphi\) of degree 1 in \(\mathbb{F}_2[T]\). Thus we are in the exceptional case (EC2), which is a contradiction. Therefore there exists a Zsigmondy prime for \((1, m)\). \(\square\)
We now prove Theorem 5.2.

**Proof of Theorem 5.2.** If \( u \) is of positive degree, Theorem 5.2 follows immediately from Lemma 5.3.

If \( m \) is of positive degree and \( \deg(u) = 0 \), we see that \( u = 1 \), and thus Theorem 5.2 follows from Lemma 5.4.

\[ \square \]

6. AN ANALOGUE OF LARGE ZSIGMONDY PRIMES, AND FEIT’S THEOREM IN POSITIVE CHARACTERISTIC

In this section, we introduce a notion of large Zsigmondy primes in the function field context, and prove a function field analogue of Feit’s theorem (see Theorem 6.16) which assures the existence of a large Zsigmondy prime for a pair \((u, m)\) of monic polynomials except some exceptional cases. The strategy of the proof of Theorem 6.16 is similar to that of Theorem 4.4. More precisely, take a pair \((u, m)\) of monic polynomials such that at least one of them is of positive degree. If we assume that there are no large Zsigmondy primes for \((u, m)\), we show that the prime factorization of \( \Psi_m(u) \) is of very special form, and that \( m+1 \) is the only Zsigmondy prime for \((u, m)\). In comparing the degree of \( \Psi_m(u) \) with the degrees of the prime factors of \( \Psi_m(u) \), one reaches a contradiction except some exceptional cases that will be explicitly determined. The contradiction in turn implies that there exists a large Zsigmondy prime for \((u, m)\), which is exactly a function field analogue of Feit’s theorem.

We begin by recalling the notion of large Zsigmondy primes that was already mentioned in the introduction.

**Definition 6.1.** Let \( u, m \) be monic polynomials in \( A = \mathbb{F}_q[T] \). A monic prime \( \wp \) is called a **large Zsigmondy prime for** \((u, m)\) if \( \wp \) is a Zsigmondy prime for \((u, m)\), and either \( \deg(\wp) > \deg(m) \) or \( \wp^2 \) divides \( C_m(u) \).

**Remark 6.2.** Let \( \wp \) be a Zsigmondy prime for \((u, m)\). We know from Remark 3.3(i) that \( m \) is the Carlitz annihilator of \((u, \wp)\). By Proposition 3.3(i), we deduce that \( \deg(m) \leq \deg(\wp - 1) = \deg(\wp) \).

Thus \( \wp \) is not a large Zsigmondy prime for \((u, m)\) if and only if the following are true:

1. \( \deg(\wp) = \deg(m) \); and
2. \( \wp^2 \) does not divide \( C_m(u) \).

The next result plays a central role in the proof of Theorem 6.16.

**Corollary 6.3.** Assume that \( q > 2 \). Let \( u, m \) be monic polynomials in \( A \) such that at least one of them is of positive degree. Assume that there exists no large Zsigmondy prime for \((u, m)\), and that there exists a Zsigmondy prime for \((u, m)\). Then

1. \( m + 1 \) is the unique Zsigmondy prime for \((u, m)\);
2. either \( \Psi_m(u) = \epsilon(m + 1) \) or \( \Psi_m(u) = \epsilon q(m + 1) \) for some unit \( \epsilon \in \mathbb{F}_q^\times \) and some monic prime \( q \) dividing \( m \).

**Proof.** We contend that \( m \) is of positive degree. Indeed, assume the contrary, i.e., \( \deg(m) = 0 \), and hence \( m = 1 \). By assumption, we deduce that \( \deg(u) \geq 1 \). It is not difficult to show that any monic prime \( \wp \) dividing \( u \) is a large Zsigmondy prime for \((u, m)\), which is a contradiction. Thus \( \deg(m) \geq 1 \).

Let \( q \) be any Zsigmondy prime for \((u, m)\). By Corollary 3.3(i), we see that \( q \) does not divide \( m \). Since \( q \) is not a large Zsigmondy prime for \((u, m)\), we know from Remark 6.2 that \( \deg(q) = \deg(m) \). Since \( q \) is a Zsigmondy prime for \((u, m)\), we see from Remark 3.3(i) that \( m = P_{u,q} \). Hence it follows from Proposition 3.3(i) that \( m \) divides \( q - 1 \), and thus \( m = q - 1 \) since \( \deg(q - 1) = \deg(q) = \deg(m) \). Hence \( q = m + 1 \), which proves part (i) of Corollary 6.3.

By Remark 6.3(i), we deduce from part (i) that \( m + 1 \) divides \( \Psi_m(u) \). We see that \((m + 1)^2 \) does not divide \( \Psi_m(u) \); otherwise, it follows from Proposition 2.4 that \((m + 1)^2 \) divides \( C_m(u) \), and hence \( m + 1 \) is a large Zsigmondy prime for \((u, m)\), which is a contradiction. Therefore we can write \( \Psi_m(u) \) in the form

\[
\Psi_m(u) = \epsilon Q(m + 1),
\]

where \( Q \) is a monic polynomial in \( \mathbb{F}_q[T] \) and \( \epsilon \in \mathbb{F}_q^\times \).
where $\epsilon \in \mathbb{F}_q^*$ and $Q$ is a monic polynomial such that $\gcd(Q, m+1) = 1$. If $\deg(Q) = 0$, or equivalently $Q = 1$, we see that $\Psi_m(u) = \epsilon(m+1)$, and part (ii) follows.

Suppose now that $\deg(Q) \geq 1$. Then there is a monic prime $q$ of positive degree such that $q$ divides $Q$. By part (i) and since $\gcd(q, m+1) = 1$, we know that $q$ is a non-Zsigmondy prime for $(u, m)$, and it thus follows from Corollary 3.8(i) that $m$ can be written in the form

$$m = P_{u,q}q^s$$

for some positive integer $s$, where $P_{u,q}$ is the Carlitz annihilator of $(u, q)$.

By Proposition 3.8(i), we know that $P_{u,q}$ divides $q - 1$. In particular, this implies that $\deg(P_{u,q}) \leq \deg(q - 1) = \deg(q)$.

We now prove that $Q = q$. Assume the contrary, that is, $Q \neq q$. By Corollary 3.8(ii), $q^2$ does not divide $\Psi_m(u)$, and thus $Q/q$ is not divisible by $q$. Since $q, Q$ are monic, we see that $Q/q$ is a monic polynomial in $A$. Since $Q/q \neq 1$, we deduce that $\deg(Q/q) > 0$, and thus there is a monic prime, say $p$, dividing $Q/q$. Since $\gcd(q, Q/q) = 1$, we deduce that $\gcd(q, q) = 1$.

We will prove that $\varphi = q - 1$ and $p = 2$ (recall that $p$ is the characteristic of $\mathbb{F}_q$). Indeed since $\varphi$ divides $Q/q$, we deduce that $\gcd(q, m + 1) = 1$, and thus part (i) tells us that $\varphi$ is a non-Zsigmondy prime for $(u, m)$. Following the same arguments as above, we see that $m = P_{u,\varphi}q^r$ for some positive integer $r$, where $P_{u,\varphi}$ is the Carlitz annihilator of $(u, \varphi)$. Thus

$$m = P_{u,q}q^s = P_{u,\varphi}q^r.$$

By Proposition 3.8(i), $P_{u,\varphi}$ divides $\varphi - 1$, and thus $\deg(P_{u,\varphi}) \leq \deg(\varphi - 1) = \deg(\varphi)$. Since $\gcd(\varphi, q) = 1$, we deduce that $\varphi^r$ divides $P_{u,q}$, which in turn implies that $\varphi^r$ divides $q - 1$, and hence $r\deg(\varphi) \leq \deg(q - 1) = \deg(q)$. Similarly, $q^s$ divides $\varphi - 1$, and $s\deg(q) \leq \deg(q - 1) = \deg(q)$. Therefore

$$\deg(\varphi) \leq r\deg(\varphi) \leq \deg(q) \leq s\deg(q) \leq \deg(\varphi),$$

and thus

$$\deg(\varphi) = r\deg(\varphi) = \deg(q) = s\deg(q) = \deg(\varphi).$$

Hence $r = s = 1$, and $\deg(q) = \deg(\varphi)$. Since $\varphi, q$ are monic, we deduce that

$$\varphi = q - 1,$$

and

$$q = \varphi - 1.$$

Therefore $q = \varphi - 1 = q - 2$, and hence $-2 = 0$, which implies that $p = 2$, where recall $p$ is the characteristic of $\mathbb{F}_q$.

Furthermore, since $\varphi$ divides $P_{u,q}$, and $P_{u,q}$ divides $q - 1$, we deduce from (42) that

$$P_{u,q} = \varphi = q - 1,$$

and thus

$$m = P_{u,q}q = (q - 1)q.$$

In summary, we have shown that if $\varphi$ is any monic prime dividing $Q/q$, then $\varphi = q - 1$. In particular, this implies that $q - 1$ is a prime. Hence $Q/q$ is of the form

$$Q/q = (q - 1)^{s_1}$$

for some positive integer $s_1$. Since $\gcd(Q, m + 1) = 1$, we deduce from part (i) that $q - 1$ is a non-Zsigmondy prime for $(u, m)$, and Corollary 3.8(ii) tells us that $s_1 = 1$. Hence $Q = q(q - 1)$, and it therefore follows from (40) and (44) that

$$\Psi_m(u) = cQ(m + 1) = cq(q - 1)(m + 1) = cm(m + 1).$$

We consider two cases:

* Case 1. $\deg(u) = 0$. 

Since $u$ is monic, we deduce that $u = 1$. From (44) and (45), we see that
\[
\Psi_m(u) = \epsilon(q-1)q(q-1) + 1,
\]
and thus
\[
\deg(\Psi_m(u)) = 4\deg(q).
\] (46)

On the other hand, since $\deg(u) = 0$, we know from Lemma 2.8 that
\[
\deg(\Psi_m(u)) = \Phi(m) + \delta
\] for some integer $\delta \in \{-1, 0, 1\}$.

Applying Lemma 4.1 and noting that $\gcd(q, q - 1) = 1$, we see from (44) that
\[
\Phi(m) = \Phi(q(q - 1)) = \Phi(q)\Phi(q - 1) \geq (q - 1)^2\deg(q)\deg(q - 1) = (q - 1)^2\deg(q)^2.
\]
Since $\delta \geq -1$, we deduce from (46) and (47) that
\[
4\deg(q) = \deg(\Psi_m(u)) \geq \frac{\Phi(m) - 1}{q} \geq \frac{(q - 1)^2\deg(q)^2 - 1}{q},
\] and thus
\[
\deg(q)((q - 1)^2\deg(q) - 4q) \leq 1.
\] (48)

Note that $q \geq 4$ since $q$ is a power of 2 and $q > 2$. If $\deg(q) \geq 2$, then we see that
\[
2(q - 1)^2 - 4q = 2(q^2 - 4q + 1) = 2(q(q - 4) + 1) \geq 2,
\]
and thus
\[
\deg(q)((q - 1)^2\deg(q) - 4q) \geq 4,
\]
which is a contradiction to (48).

We now consider the case when $\deg(q) = 1$. Since $q$ is a power of 2 and $q > 2$, either $q \geq 8$ or $q = 4$. If $q = 4$, then we see from (44) that $m = q(q - 1)$, where $q$ is a monic prime of degree 1 in $\mathbb{F}_{2^2}[T]$. Since $u = 1$, Theorem 5.2 tells us that there exist no Zsigmondy primes for $(u, m)$ in $\mathbb{F}_{2^2}[T]$, which is a contradiction. This contradiction establishes that $q \geq 8$.

Now we see that
\[
\deg(q)((q - 1)^2\deg(q) - 4q) = q^2 - 6q + 1 = q(q - 6) + 1 \geq 17,
\]
which is a contradiction to (48).

* Case 2. $\deg(u) > 0$.

By Lemma 2.7, (44), and (45), we deduce that
\[
\deg(\Psi_m(u)) = \Phi(m)\deg(u) = 2\deg(m),
\]
and it thus follows from Lemma 4.1 that
\[
2\deg(m) = \Phi(m)\deg(u) \geq \Phi(m) \geq (q - 1)\deg(m).
\]
Therefore
\[
(q - 3)\deg(m) \leq 0,
\]
which is a contradiction since $q \geq 4$ and $\deg(m) \geq 1$.

By Cases 1 and 2, we conclude that $Q = q$, and it thus follows from (44) that $\Psi_m(u) = \epsilon q(m + 1)$. Therefore part (ii) follows.

We now prove several lemmas (see Lemmas 6.4, 6.5, 6.6, 6.7, 6.8, 6.9, 6.10, and 6.11) that we need in the proof of Theorem 6.16. These lemmas rule out the exceptional cases in Theorem 6.16 that naturally appear in the proof of Theorem 6.16. The proofs of the lemmas are purely computational, and the reader can skip them for a first reading.
Lemma 6.4. Let \( q = 3 \). Let \( X_3 \) be the set of all monic polynomials \( m \in \mathbb{F}_3[T] \) satisfying the following conditions:

(i) \( m = (\varphi - 1)\varphi^s \) for some monic prime \( \varphi \) of degree one in \( \mathbb{F}_3[T] \) and some integer \( 2 \leq s \leq 7 \);

(ii) \( m + 1 \) is the only Zsigmondy prime for \((1, m)\);

(iii) there are no large Zsigmondy primes for \((1, m)\).

Then

\[
X_3 = \{(T - 1)T^2, T(T + 1)^2, (T + 1)(T + 2)^2\}.
\]

Proof. We prove Lemma 6.4 by computation. Let \( Y_3 \) be the set of all monic polynomials \( m \in \mathbb{F}_3[T] \) satisfying the following two conditions:

(I) \( m = (\varphi - 1)\varphi^s \) for some monic prime \( \varphi \) of degree one in \( \mathbb{F}_3[T] \) and some integer \( 2 \leq s \leq 7 \); and

(II) \( m + 1 \) is a prime in \( \mathbb{F}_3[T] \).

We see that \( X_3 \subset Y_3 \). We know that \( \{T, T + 1, T + 2\} \) is the set of all monic primes of degree one in \( \mathbb{F}_3[T] \). In order to find all elements of \( Y_3 \), we search for all monic polynomials \( m \) in \( \mathbb{F}_3[T] \) satisfying (I), (II) above, where \( \varphi \) ranges over the set of all monic primes of degree one in \( \mathbb{F}_3[T] \). Table 4 tells us that

\[
Y_3 = \{(T - 1)T^2, (T - 1)T^4, T(T + 1)^2, T(T + 1)^4, (T + 1)(T + 2)^2, (T + 1)(T + 2)^4\}.
\]

| \( \varphi \) | \( s \) | \( m = (\varphi - 1)\varphi^s \) | \( m + 1 \) is a prime |
|------------|--------|-----------------|------------------|
| \( T \)    | 2      | \((T - 1)T^2\)   | \( T^3 + 2T^2 + 1 \) |
| \( T \)    | 4      | \((T - 1)T^4\)   | \( T^3 + 2T^4 + 1 \) |
| \( T + 1 \)| 2      | \((T + 1)(T + 2)^2\) | \( T^3 + 2T^2 + T + 1 \) |
| \( T + 1 \)| 4      | \((T + 1)(T + 2)^4\) | \( T^3 + 2T^4 + 2T + 1 \) |
| \( T + 2 \)| 2      | \((T + 1)(T + 2)^2\) | \( T^3 + 2T^2 + 2T + 2 \) |
| \( T + 2 \)| 4      | \((T + 1)(T + 2)^4\) | \( T^3 + 2T^4 + 2T + 2 \) |

Table 4: The list of all polynomials \( m \) of the form \( m = (\varphi - 1)\varphi^s \) for some monic prime \( \varphi \) of degree one in \( \mathbb{F}_3[T] \) and some integer \( 2 \leq s \leq 7 \) such that \( m + 1 \) is a prime in \( \mathbb{F}_3[T] \).

In order to find all elements of \( X_3 \), we only need to find all polynomials \( m \in Y_3 \) such that there are no large Zsigmondy primes for \((1, m)\). Indeed, for any \( m \in Y_3 \), we know that \( m = (\varphi - 1)\varphi^s \) for some integer \( 2 \leq s \leq 7 \) and some monic prime \( \varphi \) of degree one in \( \mathbb{F}_3[T] \). Hence we are not in the exceptional case (EC1) in Theorem 4.4, which implies that there exists a Zsigmondy prime for \((1, m)\) for any \( m \in Y_3 \).

If there exists a large Zsigmondy primes for \((1, m)\), then \( m \) does not satisfy (iii) in Lemma 6.4 and thus \( m \notin X_3 \). If there are no large Zsigmondy primes for \((1, m)\), then Corollary 6.3 tells us that \( m + 1 \) is the only Zsigmondy prime for \((1, m)\). Therefore \( m \) satisfies (i), (ii) in Lemma 6.4 and hence \( m \in X_3 \).

In summary, we have shown that an element \( m \in Y_3 \) belongs to \( X_3 \) if and only if there are no large Zsigmondy primes for \((1, m)\). In what follows, we verify whether each element \( m \in Y_3 \) satisfies this requirement.

\* Case 1. \( m = (T - 1)T^2 \).

We see that

\[
C_m(1) = \varphi_1^3\varphi_2\varphi_3(m + 1),
\]

where \( \varphi_1 = T, \varphi_2 = T + 1, \) and \( \varphi_3 = T^2 + 1 \). Since \( \deg(\varphi_3) = 2 < \deg(m) = 3 \) and \( \varphi_2^2 \) does not divide \( C_m(1) \), we see that \( \varphi_3 \) is not a large Zsigmondy prime for \((1, m)\). Since \( \deg(m + 1) = \deg(m) \) and \( (m + 1)^2 \) does not divide \( C_m(1) \), we see that \( m + 1 \) is not a large Zsigmondy prime for \((1, m)\). On the other hand, \( C_{T^2-1}(1) \equiv 0 \mod(\varphi_1) \) and \( C_T(1) \equiv 0 \mod(\varphi_2) \), and thus \( \varphi_1, \varphi_2 \) are not Zsigmondy primes for \((1, m)\). Therefore \( \varphi_1, \varphi_2 \) are not large Zsigmondy primes for \((1, m)\). Hence there are no large Zsigmondy primes for \((1, m)\), and thus \( m \in X_3 \).

\* Case 2. \( m = (T - 1)T^4 \).
We see that
\[ C_m(1) = \varphi_1^5 \varphi_2 \varphi_3 \varphi_4 (m + 1)^{\varphi_5 \varphi_6 \varphi_7 \varphi_8}, \]
where
\[
\begin{align*}
\varphi_1 &= T, \\
\varphi_2 &= T + 1, \\
\varphi_3 &= T^2 + 1, \\
\varphi_4 &= T^3 + 2T^2 + 1, \\
\varphi_5 &= T^6 + 2T^5 + T^3 + 1, \\
\varphi_6 &= T^{11} + T^{10} + T^9 + 2T^8 + T^7 + 2T^6 + 2T^5 + 2T^3 + 1, \\
\varphi_7 &= T^{18} + 2T^{15} + 2T^{13} + 2T^{12} + 2T^{11} + T^{10} + 2T^6 + T^4 + 1, \\
\varphi_8 &= T^{30} + T^{20} + T^{23} + 2T^{20} + 2T^{19} + 2T^{22} + 2T^{21} + T^{18} \\
&\quad+ 2T^{17} + T^{16} + T^{15} + 2T^{14} + 2T^{11} + T^{10} + T^7 + T^6 + 2T^5 + 1.
\end{align*}
\]

We prove that \( \varphi_8 \) is a large Zsigmondy prime for \((1, m)\). Take any nonzero polynomial \( n \in F_4[T] \) of degree less than \( \deg(m) = 5 \), that is, \( n \in F_3[T] \) such that \( 0 \leq \deg(n) \leq 4 \). By Proposition 2.5, we know that either \( \deg(C_n(1)) = 0 \) or \( \deg(C_n(1)) = 3^{\deg(n)} - 1 \leq 3^3 = 27 \). Either case implies that \( \deg(C_n(1)) < 30 = \deg(\varphi_8) \), and thus \( C_n(1) \not\equiv 0 \mod \varphi_8 \) for any any nonzero polynomial \( n \in A \) with \( \deg(n) < \deg(m) \). Hence \( \varphi_8 \) is a Zsigmondy prime for \((1, m)\), and since \( \deg(\varphi_8) = 30 > 5 = \deg(m) \), \( \varphi_8 \) is a large Zsigmondy prime for \((1, m)\). Therefore \( m \not\in \mathcal{X}_3 \).

* Case 3. \( m = T(T + 1)^2 \).

We see that
\[ C_m(1) = \varphi_1^3 \varphi_2 \varphi_3 (m + 1), \]
where \( \varphi_1 = T + 1, \varphi_2 = T + 2, \) and \( \varphi_3 = T^2 + 2T + 2 \). Using the same arguments as in Case 1, we can prove that \( \varphi_2, \varphi_3, m + 1 \) are not large Zsigmondy primes for \((1, m)\). Furthermore \( C_T(1) = T + 1 \equiv 0 \mod \varphi_1 \), and thus \( \varphi_1 \) is not a Zsigmondy prime for \((1, m)\). Therefore \( \varphi_1 \) is not a large Zsigmondy prime for \((1, m)\), and hence there are no large Zsigmondy primes for \((1, m)\). Thus \( m \not\in \mathcal{X}_3 \).

* Case 4. \( m = T(T + 1)^4 \).

We see that
\[ C_m(1) = \varphi_1^5 \varphi_2 \varphi_3 \varphi_4 (m + 1)^{\varphi_5 \varphi_6 \varphi_7 \varphi_8}, \]
where
\[
\begin{align*}
\varphi_1 &= T + 1, \\
\varphi_2 &= T + 2, \\
\varphi_3 &= T^2 + 2T + 2, \\
\varphi_4 &= T^3 + 2T^2 + T + 1, \\
\varphi_5 &= T^6 + 2T^5 + T^4 + 2T^3 + 2T^2 + T + 2, \\
\varphi_6 &= T^{11} + 2T^8 + 2T^7 + 2T^6 + 2T^4 + 2T^3 + 2T^2 + 1, \\
\varphi_7 &= T^{18} + 2T^{15} + 2T^{13} + 2T^{12} + 2T^{11} + T^{10} + 2T^9 + T^6 + T^3 + 2T^2 + 2T + 2, \\
\varphi_8 &= T^{30} + T^{29} + 2T^{27} + 2T^{26} + 2T^{24} + T^{23} + 2T^{22} + 2T^{20} + 2T^{19} \\
&\quad+ 2T^{18} + 2T^{14} + T^{12} + T^{11} + T^8 + T^6 + 2T^4 + 2T^3 + 2T^2 + 1.
\end{align*}
\]

Using the same arguments as in Case 2, one can show that \( \varphi_8 \) is a large Zsigmondy prime for \((1, m)\), and thus \( m \not\in \mathcal{X}_3 \).

* Case 5. \( m = (T + 1)(T + 2)^2 \).
We see that

\[ C_m(1) = \varphi_1 \varphi_2^3 \varphi_3(m + 1), \]

where \( \varphi_1 = T \), \( \varphi_2 = T + 2 \), and \( \varphi_3 = T^2 + T + 2 \). Using the same arguments as in Case 1, we can prove that \( \varphi_1, \varphi_3, m + 1 \) are not large Zsigmondy primes for \( (1, m) \). Furthermore \( C_{T+1}(1) = T + 2 = 0 \pmod{\varphi_2} \), and thus \( \varphi_2 \) is not a Zsigmondy prime for \( (1, m) \). Therefore \( \varphi_2 \) is not a large Zsigmondy prime for \( (1, m) \), and hence there are no large Zsigmondy primes for \( (1, m) \). Thus \( m \in \mathcal{X}_3 \).

* Case 6. \( m = (T + 1)(T + 2)^4 \).

We see that

\[ C_m(1) = \varphi_1 \varphi_2^2 \varphi_3 \varphi_4(m + 1) \varphi_5 \varphi_6 \varphi_7 \varphi_8, \]

where

\[
\begin{align*}
\varphi_1 &= T, \\
\varphi_2 &= T + 2, \\
\varphi_3 &= T^2 + T + 2, \\
\varphi_4 &= T^3 + 2T^2 + 2T + 2, \\
\varphi_5 &= T^6 + 2T^5 + 2T^4 + T^3 + T^2 + T + 2, \\
\varphi_6 &= T^{11} + 2T^{10} + T^9 + 2T^8 + T^5 + 2T^4 + T^3 + 2T^2 + 2T + 2, \\
\varphi_7 &= T^{18} + 2T^{15} + 2T^{13} + 2T^{12} + 2T^{11} + T^{10} + T^9 + 2T^4 + 2T^3 + T^2 + T + 2, \\
\varphi_8 &= T^{30} + 2T^{29} + 2T^{28} + T^{27} + 2T^{26} + T^{25} + 2T^{23} + 2T^{20} + 2T^{19} + T^{18} + T^{17} + T^{16} + 2T^{15} + 2T^{13} + T^{12} + T^{11} + 2T^9 + 2T^7 + T^6 + T^4 + T + 1.
\end{align*}
\]

Using the same arguments as in Case 2, one can show that \( \varphi_8 \) is a large Zsigmondy prime for \( (1, m) \), and thus \( m \not\in \mathcal{X}_3 \).

By what we have showed in Cases 1–6, we see that

\[ \mathcal{X}_3 = \{(T - 1)T^2, T(T + 1)^2, (T + 1)(T + 2)^2\}. \]

\[ \square \]

**Lemma 6.5.** Let \( q = 3 \). Let \( \mathcal{X}_4 \) be the set of all polynomials \( m \in \mathbb{F}_3[T] \) satisfying the following conditions:

(i) \( m \) is a monic prime of degree one in \( \mathbb{F}_3[T] \);

(ii) \( m + 1 \) is the only Zsigmondy prime for \( (m, m) \);

(iii) there are no large Zsigmondy primes for \( (m, m) \).

Then

\[ \mathcal{X}_4 = \{T, T + 1, T + 2\}. \]

**Proof.** Let \( \mathcal{Y}_4 \) be the set of all monic primes of degree one in \( \mathbb{F}_3[T] \). It is clear that \( \mathcal{X}_4 \subseteq \mathcal{Y}_4 \).

We now prove that \( \mathcal{X}_4 = \mathcal{Y}_4 \). Indeed, take any element \( m \in \mathcal{Y}_4 \). Since \( m \) is a monic prime of degree one in \( \mathbb{F}_3[T] \), we see that \( m = T + \alpha \), where \( \alpha \in \mathbb{F}_3 \). It is not difficult to see that

\[ C_m(m) = m^2(m + 1), \]

where \( m + 1 = T + \alpha + 1 \) is a monic prime in \( \mathbb{F}_3[T] \). Since \( C_1(m) = m \equiv 0 \pmod{m} \), we see that \( m \) is not a Zsigmondy prime for \( (m, m) \), and thus not a large Zsigmondy prime for \( (m, m) \).

Since \( \deg(m + 1) = \deg(m) \), and \( (m + 1)^2 \) does not divide \( C_m(m) \), we deduce that \( m + 1 \) is not a large Zsigmondy prime for \( (m, m) \). Thus there are no large Zsigmondy primes for \( (m, m) \), and thus \( m \) satisfies (iii) in Lemma 6.3.

Applying Theorem 4.3 with \( 3, m, m \) in the roles of \( q, u, m \), we know that there exists a Zsigmondy prime for \( (m, m) \). Thus Corollary 6.3 tells us that \( m + 1 \) is the only Zsigmondy prime for \( (m, m) \), and
Table 5: The list of all polynomials \( m \) in \( \mathbb{F}_3[T] \) of the form \( m = P_{1,q} \), where \( q \) ranges over the set of all monic primes in \( \mathbb{F}_3[T] \) of degree 2.

\[
\begin{array}{|c|c|c|c|}
\hline
q & P_{1,q} = q - 1 & m = P_{1,q} & \text{Is } m + 1 \text{ a prime?} \\
\hline
T^2 + 1 & T^2 & m = T^4 + T^2 & \text{Since } m + 1 = \varphi_1^2 \varphi_2^2, \text{ where } \varphi_1 = T + 1 \text{ and } \varphi_2 = T + 2, \text{ we see that } m + 1 \text{ is not a prime.} \\
T^2 + T + 2 & T^2 + T + 1 & m = T^4 + 2T^3 + T^2 + 2 & \text{Since } m + 1 = \varphi_1^2 \varphi_2^2, \text{ where } \varphi_1 = T \text{ and } \varphi_2 = T + 1, \text{ we see that } m + 1 \text{ is not a prime.} \\
T^2 + 2T + 2 & T^2 + 2T + 1 & m = T^4 + T^3 + T^2 + 2 & \text{Since } m + 1 = \varphi_1^2 \varphi_2^2, \text{ where } \varphi_1 = T \text{ and } \varphi_2 = T + 2, \text{ we see that } m + 1 \text{ is not a prime.} \\
\hline
\end{array}
\]

Therefore \( m \) satisfies \((ii)\) in Lemma 6.5. Therefore \( m \in \mathcal{X}_3 \), and hence \( \mathcal{X}_4 = \mathcal{Y}_4 = \{T, T + 1, T + 2\} \).

\[\Box\]

Lemma 6.6. Let \( q = 3 \). Let \( \mathcal{X}_3 \) be the set of all monic polynomials \( m \in \mathbb{F}_3[T] \) satisfying the following two conditions:

(i) there exists a monic prime \( q \) of degree 2 or 3 in \( \mathbb{F}_3[T] \) such that the Carlitz annihilator \( P_{1,q} \) of \((1, q)\) is of degree 2 and \( m = P_{1,q} \);

(ii) \( m + 1 \) is a prime in \( \mathbb{F}_3[T] \).

Then \( \mathcal{X}_3 = \emptyset \).

Proof. Let \( \mathcal{Y}_3 \) be the set of all monic polynomials \( m \in \mathbb{F}_3[T] \) satisfying condition \((i)\) in Lemma 6.6. We will prove that if \( m \in \mathcal{Y}_3 \), then \( m + 1 \) is not a prime, and it thus follows immediately that \( \mathcal{X}_3 = \emptyset \).

Take an arbitrary monic polynomial \( m \in \mathcal{Y}_3 \). By condition \((i)\) in Lemma 6.6 we see that there exists a monic prime \( q \) of degree either 2 or 3 in \( \mathbb{F}_3[T] \) such that the Carlitz annihilator \( P_{1,q} \) of \((1, q)\) is of degree 2 and

\[m = P_{1,q} \tag{50}\]

We consider the cases:

\* Case 1. \( \deg(q) = 2 \).

By parts \((i), (ii)\) in Proposition 3.3 we know that \( P_{1,q} \) divides \( q - 1 \), and is of positive degree. Hence the degree of \( P_{1,q} \) is either 1 or 2. If \( \deg(P_{1,q}) = 1 \), then we see from Proposition 2.6 that

\[\deg(C_{P_{1,q}}(1)) = q^{\deg(P_{1,q})-1} = 3^0 = 1,\]

which is a contradiction since \( q \) divides \( C_{P_{1,q}}(1) \). Thus \( \deg(P_{1,q}) = 2 \), and since \( \deg(q - 1) = 2 \) and \( P_{1,q} \) divides \( q - 1 \), we deduce that \( P_{1,q} = q - 1 \). Thus we see from \((50)\) that

\[m = (q - 1)q.\]

Note that the set of all monic primes of degree 2 in \( \mathbb{F}_3[T] \) is \( \{T^2 + 1, T^2 + T + 2, T^2 + 2T + 2\} \). In Table 4, letting \( q \) range over the set of all monic primes in \( \mathbb{F}_3[T] \) of degree 2, we find all the polynomials \( m \in \mathbb{F}_3[T] \) of the form \((50)\). Examining the table, one sees that \( m + 1 \) is not a prime.

\* Case 2. \( \deg(q) = 3 \).

Using the same arguments as in Case 1, we see that \( P_{1,q} \) is of degree 2 or 3. Since \( P_{1,q} \) divides \( q - 1 \), one needs to test whether there exists a monic polynomial of degree 2 dividing \( q - 1 \), say \( \Gamma \), such that \( C_{\Gamma}(1) \equiv 0 \pmod{q} \). If this is the case, then Proposition 3.3 \((iii)\) tells us that \( P_{1,q} = \Gamma \); otherwise \( \deg(P_{1,q}) = \deg(q - 1) = 3 \), and thus \( P_{1,q} = q - 1 \). In Table 4 we use this argument to find the Carlitz annihilator \( P_{1,q} \) of \((1, q)\), where \( q \) ranges over the set of all monic primes of degree 3 in \( \mathbb{F}_3[T] \). Examining
The prime factorization of \( P \) is closely Table 6, one can easily find all the monic primes in \( \mathbb{F}_3[T] \) for which the Carlitz annihilator \( P_{1,q} \) of \((1,q)\) is of degree 2.

From Table 6, we see the only pairs \((q,P_{1,q})\) for which \( m = P_{1,q}q \) satisfies (i) in Lemma 6.6 are the following:
\[(q,P_{1,q}) = (T^3 + T^2 + T + 2, T^2 + 1), (T^3 + T^2 + 2, T^2 + 2T + 2), (T^3 + T^2 + 2T + 1, T^2 + T + 2).\]

We consider the subcases:

* **Subcase 2A.** \((q,P_{1,q}) = (T^3 + T^2 + T + 2, T^2 + 1)\).
  
  We see that
  \[ m = P_{1,q}q = T^5 + T^4 + 2T^3 + T + 2.\]

  Thus \( m + 1 \) is not a prime since
  \[ m + 1 = T(T + 1)(T^3 + 2T + 1).\]

* **Subcase 2B.** \((q,P_{1,q}) = (T^3 + T^2 + 2, T^2 + 2T + 2)\).
  
  We see that
  \[ m = P_{1,q}q = T^5 + T^3 + T^2 + T + 1.\]

  Thus \( m + 1 \) is not a prime since
  \[ m + 1 = (T + 1)(T + 2)(T^3 + 2T + 1).\]

Table 6: The Carlitz annihilators \( P_{1,q} \) of \((1,q)\), where \( q \) ranges over the set of all monic primes of degree 3 in \( \mathbb{F}_3[T] \).
\* Subcase 2C. \((q,P_{1,q}) = (T^3 + T^2 + 2T + 1, T^2 + T + 2)\).

We see that

\[ m = P_{1,q}q = T^5 + 2T^4 + 2T^3 + 2T^2 + 2T + 2. \]

Thus \(m + 1\) is not a prime since

\[ m + 1 = T(T + 2)(T^3 + 2T + 1). \]

In conclusion, we have showed in Cases 1 and 2 that if \(m \in \mathcal{Y}_5\), then \(m + 1\) is not a prime, i.e., \(m\) does not satisfy (ii) in Lemma 6.7. Therefore \(\mathcal{X}_5 = \emptyset\) as desired.

\[ \Box \]

**Lemma 6.7.** Let \(\mathcal{X}_6\) be the set of all monic polynomials \(m \in F_5[T]\) satisfying the following conditions:

(i) \(m = (\varphi - 1)\varphi\) for some monic prime \(\varphi\) of degree one in \(F_5[T]\);

(ii) \(m + 1\) is the only Zsigmondy prime for \((1,m)\); and

(iii) there are no large Zsigmondy primes for \((1,m)\).

Then

\[ \mathcal{X}_6 = \{m = (T + \alpha - 1)(T + \alpha) \mid \alpha \in F_5\}. \]

**Proof.** Since every element \(m\) in \(\mathcal{X}_6\) satisfies (i) in Lemma 6.7, it is clear that \(\mathcal{X}_6\) is a subset of the set \(\{m = (T + \alpha - 1)(T + \alpha) \mid \alpha \in F_5\}\). Conversely, take any element \(m = (T + \alpha - 1)(T + \alpha)\) for some \(\alpha \in F_5\). Then \(m\) satisfies condition (i) in Lemma 6.7, with \(\varphi = T + \alpha\).

It is not difficult to see that

\[ m + 1 = (T + \alpha - 1)(T + \alpha) + 1 = T^2 + (2\alpha - 1)T + \alpha^2 - \alpha + 1 \]

is a prime in \(F_5[T]\). We see that

\[ C_m(1) = C_{(T + \alpha - 1)(T + \alpha)}(1) = \varphi_1^2\varphi_2(m + 1), \]

where \(\varphi_1 = T + \alpha\) and \(\varphi_2 = T + \alpha + 1\). Since \(C_{T + \alpha - 1}(1) = \varphi_1 \equiv 0 \pmod{\varphi_1}\) and \(C_{T + \alpha}(1) = \varphi_2 \equiv 0 \pmod{\varphi_2}\), we deduce that \(\varphi_1, \varphi_2\) are not Zsigmondy primes for \((1,m)\). In particular, this implies that \(\varphi_1, \varphi_2\) are not large Zsigmondy primes for \((1,m)\).

Since \(\deg(m + 1) = \deg(m)\), and \((m + 1)^2\) does not divide \(C_m(1)\), we see that \(m + 1\) is not a large Zsigmondy prime for \((1,m)\), and hence (iii) in Lemma 6.7 is satisfied. By Theorem 4.1, we know that there exists a Zsigmondy prime for \((1,m)\), and it thus follows from Corollary 6.3 that \(m + 1\) is the only Zsigmondy prime for \((1,m)\). Therefore \(m\) satisfies (ii) in Lemma 6.7, and thus \(m \in \mathcal{X}_6\). Hence

\[ \mathcal{X}_6 = \{m = (\varphi - 1)\varphi \mid \varphi \text{ is a monic prime of degree one in } F_5[T]\} = \{m = (T + \alpha - 1)(T + \alpha) \mid \alpha \in F_5\}. \]

\[ \Box \]

**Lemma 6.8.** Assume that \(q > 2\). Let \(\mathcal{X}_7\) be the set of all monic primes of degree one in \(F_q[T]\). Then there are no large Zsigmondy primes for \((1,m)\) for any \(m \in \mathcal{X}_7\).

**Proof.** Take any element \(m \in \mathcal{X}_7\). Then \(m\) is a monic prime of degree one in \(F_q[T]\), and thus is of the form \(m = T + \alpha\) for some \(\alpha \in F_q\). It is easy to see that

\[ C_m(1) = C_{T + \alpha}(1) = T + \alpha + 1. \]

Thus \(\varphi = T + \alpha + 1\) is the only monic prime dividing \(C_m(1)\). Since \(\deg(\varphi) = 1 = \deg(m)\), and \(\varphi^2\) does not divide \(C_m(1)\), we deduce that \(\varphi\) is not a large Zsigmondy prime for \((1,m)\). Therefore there are no large Zsigmondy primes for \((1,m)\), which proves our contention.

\[ \Box \]

**Lemma 6.9.** Let \(q = 3\). Let \(\mathcal{X}_8\) be the set of all monic polynomials \(m \in F_3[T]\) satisfying the following conditions:

1. \(m = (\varphi - 1)\varphi\) for some monic prime \(\varphi\) of degree one in \(F_3[T]\);
2. \(m + 1\) is the only Zsigmondy prime for \((1,m)\);
3. there are no large Zsigmondy primes for \((1,m)\).
(i) \( m = \phi^2 \) for some monic prime \( \phi \) of degree one in \( \mathbb{F}_3[T] \);
(ii) \( m + 1 \) is the only Zsigmondy prime for \((1, m)\);
(iii) there are no large Zsigmondy primes for \((1, m)\).

Then
\[
\mathcal{X}_8 = \{T^2, (T + 1)^2, (T + 2)^2\}.
\]

**Proof.** Note that any monic prime \( \phi \) of degree one in \( \mathbb{F}_3[T] \) is of the form \( \phi = T + \alpha \) for some \( \alpha \in \mathbb{F}_3 \). Hence it is easy to see that
\[
\mathcal{X}_8 \subset \{T^2, (T + 1)^2, (T + 2)^2\}.
\]

Now take any element \( m = (T + \alpha)^2 \) for some \( \alpha \in \mathbb{F}_3 \). It is not difficult to see that
\[
m + 1 = (T + \alpha)^2 + 1 = T^2 + 2\alpha T + \alpha^2 + 1,
\]
which is a prime in \( \mathbb{F}_3[T] \). Furthermore
\[
C_m(1) = C_{(T+\alpha)^2}(1) = \phi(m + 1),
\]
where \( \phi = T + \alpha + 1 \).

Since \( \deg(\phi) = 1 < 2 = \deg(m) \), and \( \phi^2 \) does not divide \( m \), we deduce that \( \phi \) is not a large Zsigmondy prime for \((1, m)\). Similarly one can show that \( m + 1 \) is not a large Zsigmondy prime for \((1, m)\), and therefore there are no large Zsigmondy primes for \((1, m)\). Hence \( m \) satisfies (iii).

On the other hand, Theorem 4.4 tells us that there exists a Zsigmond y prime for \((1, m)\), and it follows from Corollary 6.3 that \( m + 1 \) is the only Zsigmondy prime for \((1, m)\). Thus \( m \) satisfies (ii), and hence \( m \in \mathcal{X}_8 \). Therefore our contention follows. \( \square \)

**Lemma 6.10.** Let \( q = 4 \), and write \( \mathbb{F}_4 = \mathbb{F}_2(w) \), where \( w \) is an element in the algebraic closure of \( \mathbb{F}_2 \) such that \( w^2 + w + 1 = 0 \). Let \( \mathcal{X}_9 \) be the set of all monic polynomials \( m \in \mathbb{F}_4[T] \) satisfying the following conditions:

(i) \( m = m_1 m_2 \), where \( m_1, m_2 \) are monic polynomials in \( \mathbb{F}_4[T] \) such that \( \deg(m_1) = \deg(m_2) = 1 \) and \( \gcd(m_1, m_2) = 1 \);
(ii) \( m + 1 \) is the only Zsigmondy prime for \((1, m)\);
(iii) there are no large Zsigmondy primes for \((1, m)\).

Then
\[
\mathcal{X}_9 = \{T(T + w), T(T + w^2), (T + 1)(T + w), (T + 1)(T + w^2)\}.
\]

**Proof.** We know that the set \( \{T, T + 1, T + w, T + w^2\} \) consists of all monic primes of degree one in \( \mathbb{F}_4[T] \). Now let \( \mathcal{Y}_9 \) be the set of all monic polynomials \( m \in \mathbb{F}_4[T] \) such that \( m \) satisfies (i) in Lemma 6.10 and \( m + 1 \) is a prime in \( \mathbb{F}_4[T] \). By computation, one sees that
\[
\mathcal{Y}_9 = \{T(T + w), T(T + w^2), (T + 1)(T + w), (T + 1)(T + w^2)\}.
\]
We should note that \( \mathcal{X}_9 \subset \mathcal{Y}_9 \), and that an element \( m \) in \( \mathcal{Y}_9 \) belongs to \( \mathcal{X}_9 \) if and only if it satisfies both conditions (ii) and (iii) in Lemma 6.10.

Take any element \( m \in \mathcal{Y}_9 \). Examining closely (51), one sees that
\[
m = (T + \alpha)(T + \beta),
\]
where \( \alpha \in \{0, 1\} \) and \( \beta \in \{w, w^2\} \). We deduce that
\[
C_m(1) = \varphi_1 \varphi_2 (m + 1),
\]
where \( \varphi_1 = T + \alpha + 1 \) and \( \varphi_2 = T + \beta + 1 \). Since \( \deg(m + 1) = \deg(m) = 2 \) and \( (m + 1)^2 \) does not divide \( C_m(1) \), we find that \( m + 1 \) is not a large Zsigmondy prime for \((1, m)\). Furthermore since \( C_{T+\alpha}(1) = \varphi_1 \equiv 0 \pmod{\varphi_1} \) and \( C_{T+\beta}(1) = \varphi_2 \equiv 0 \pmod{\varphi_2} \), one sees that \( \varphi_1, \varphi_2 \) are non-Zsigmondy primes for \((1, m)\). In particular, this implies that \( \varphi_1, \varphi_2 \) are not large Zsigmondy primes for \((1, m)\). Thus there are no large Zsigmondy primes for \((1, m)\), and hence (iii) in Lemma 6.10 is satisfied.
We should also note that no elements in \( \mathcal{Y}_3 \) are in the exceptional case (EC2) of Theorem 5.2. Thus there exists a Zsigmondy prime for \((1, m)\), and therefore, we, by appealing to Corollary 6.3, deduce that \( m + 1 \) is the only Zsigmondy prime for \((1, m)\). This proves that \( m \in \mathcal{X}_9 \), which proves our contention. 

\[ \square \]

**Lemma 6.11.** Let \( q = 3 \). Let \( \mathcal{X}_{10} \) be the set of all monic polynomials \( m \in \mathbb{F}_3[T] \) satisfying the following conditions:

(i) \( m \) is square-free, i.e., \( \phi^2 \) does not divide \( m \) for any monic prime \( \phi \);

(ii) \( m = m_1m_2 \), where \( m_1, m_2 \) are monic polynomials in \( \mathbb{F}_3[T] \) such that \( \gcd(m_1, m_2) = 1 \), \( \deg(m_1) \in \{1, 2\} \), and \( \deg(m_2) = 1 \);

(iii) \( m + 1 \) is the only Zsigmondy prime for \((1, m)\);

(iv) there are no large Zsigmondy primes for \((1, m)\).

Then

\[ \mathcal{X}_{10} = \{T^3 + 2T\}. \]

**Proof.** Let \( \mathcal{Y}_{10} \) be the set of all monic polynomials \( m \in \mathbb{F}_3[T] \) such that \( m + 1 \) is a prime, and both conditions (i), (ii) in Lemma 6.11 are satisfied. By computation, one sees that

\[ \mathcal{Y}_{10} = \{T^3 + T^2 + 1, T^3 + T^2 + 2T, T^3 + 2T, T^3 + T^2 + T + 1\}. \]

We should note that \( \mathcal{X}_{10} \subset \mathcal{Y}_{10} \), and that an element \( m \in \mathcal{Y}_{10} \) belongs to \( \mathcal{X}_{10} \) if and only if it satisfies both conditions (iii) and (iv) in Lemma 6.11.

We first prove that for an element \( m \in \mathcal{Y}_{10} \), if there exists a monic prime \( P \) of degree 5 such that \( P \) divides \( C_m(1) \), but \( P^2 \) does not divide \( C_m(1) \), then \( P \) is a large Zsigmondy prime for \((1, m)\). In particular, this implies that such an element \( m \) does not belong to \( \mathcal{X}_{10} \). Indeed, take such an element \( m \in \mathcal{Y}_{10} \), and let \( n \) be any nonzero polynomial such that \( \deg(n) < \deg(m) \). Since \( \deg(m) = 3 \), we deduce that \( \deg(n) \leq 2 \), and thus \( \deg(n) \in \{0, 1, 2\} \).

If \( \deg(n) = 0 \), then \( n \in \mathbb{F}_q^* \), and thus \( C_n(1) = n \equiv 0 \pmod{P} \) since \( \deg(P) = 5 \).

If \( 1 \leq \deg(n) \leq n \), we, by appealing to Proposition 2.6, find that

\[ \deg(C_n(1)) = 3^{\deg(n) - 1} \leq 3 < 5 = \deg(P), \]

which proves that \( C_n(1) \equiv 0 \pmod{P} \).

Thus \( P \) is a Zsigmondy prime for \((1, m)\), and since \( \deg(P) = 5 > 3 = \deg(m) \), we deduce that \( P \) is a large Zsigmondy prime for \((1, m)\). In particular, since \( m \) does not satisfy condition (iv) in Lemma 6.11, we see that \( m \) does not belong to \( \mathcal{X}_{10} \).

Now we see that

\[
\begin{align*}
C_{T^3+T^2+1}(1) &= T(T^3 + T^2 + 2)P_1, \\
C_{T^3+T^2+2T}(1) &= (T + 1)(T^3 + T^2 + 2T + 1)P_2, \\
C_{T^3+T^2+T+1}(1) &= (T + 2)(T^3 + T^2 + T + 2)P_3, \\
\end{align*}
\]

where

\[
\begin{align*}
P_1 &= T^5 + 2T^4 + T^3 + 2T^2 + T + 1, \\
P_2 &= T^5 + T^4 + T^3 + 2T^2 + T + 1, \\
P_3 &= T^5 + 2T + 1. \\
\end{align*}
\]

Since the \( P_i \) are monic primes of degree 5, we deduce from the fact above that \( T^3 + T^2 + 1, T^3 + T^2 + 2T, T^3 + T^2 + T + 1 \) do not belong to \( \mathcal{X}_{10} \).

We now prove that \( T^3 + 2T \) belongs to \( \mathcal{X}_{10} \). Indeed, setting \( m = T^3 + 2T \), we see that

\[ C_m(1) = \phi_1^2 \phi_2^2 \phi_3^2 (m + 1), \]

where \( \phi_1 = T, \phi_2 = T + 1, \) and \( \phi_3 = T + 2 \). Since \( C_{T^{-1}}(1) = \phi_1, C_T(1) = \phi_2, \) and \( C_{T+1}(1) = \phi_3, \) we see that \( \phi_1, \phi_2, \phi_3 \) are not Zsigmondy primes for \((1, m)\). In particular, this implies that \( \phi_1, \phi_2, \phi_3 \) are not large Zsigmondy primes for \((1, m)\).
On the other hand, since \( \deg(m + 1) = \deg(m) \) and \((m + 1)^2 \) does not divide \( C_m(1) \), we deduce that \( m + 1 \) is not a large Zsigmondy prime for \((1, m)\), which in turn implies that condition \((iv)\) in Lemma 6.11 is satisfied. Furthermore Theorem 4.4 tells us that there exists a Zsigmondy prime for \((1, m)\), and it thus follows from Corollary 6.3 that \( m + 1 \) is the only Zsigmondy prime for \((1, m)\). Therefore condition \((iii)\) in Lemma 6.11 is satisfied, and hence \( m = T^3 + 2T \in X_{10} \). Thus \( X_{10} = \{T^3 + 2T\} \).

In order to rule out some exceptional cases in the proof of Theorem 6.16, we need to strengthen Lemma 4.1, and obtain a sharper lower bound for \( \Phi(m) \) in the case when \( m \) is a power of a monic prime, or \( m \) is a monic prime of degree at least two. The next four results are devoted to obtaining a sharper lower bound for \( \Phi(m) \) in these special cases.

Lemma 6.12. Assume that \( q > 2 \). Let \( \wp \) be a monic prime of degree \( \geq 2 \). Then

\[
\Phi(\wp) - q\deg(\wp) \geq q^2 - 2q - 1.
\]

Furthermore equality in (53) occurs if and only if \( \deg(\wp) = 2 \).

Proof. Let \( H(\alpha) \) be the function defined by

\[
H(\alpha) = q\alpha - 1 - q\alpha,
\]

where \( \alpha \) ranges over the set \([2, \infty)\). Note that (53) is equivalent to the inequality

\[
H(\deg(\wp)) \geq q^2 - 2q - 1.
\]

We prove that \( H \) is a strictly increasing function over the interval \([2, \infty)\). Indeed, the derivative of \( H \) is equal to

\[
H'(\alpha) = \ln(q)q^\alpha - q,
\]

and since \( q \geq 3 \) and \( \alpha \geq 2 \), we deduce that

\[
H'(\alpha) \geq \ln(3)q^2 - q > q^2 - q = q(q - 1) \geq 6 > 0.
\]

Thus \( H \) is a strictly increasing function over the interval \([2, \infty)\), and therefore

\[
H(\deg(\wp)) \geq H(2) = q^2 - 2q - 1.
\]

Note that equality in (53) occurs if and only if \( \alpha = 2 \).

Now replacing \( \alpha \) by \( \deg(\wp) \) in (53), Lemma 6.12 follows immediately.

Since \( q^2 - 2q - 1 = q(q - 2) - 1 \geq 2 \), the next result follows immediately from Lemma 6.12.

Corollary 6.13. Assume that \( q > 2 \). Let \( \wp \) be a monic prime of degree \( \geq 2 \). Then

\[
\Phi(\wp) > q\deg(\wp).
\]

Lemma 6.14. Assume that \( q > 2 \). Let \( \wp \) be a monic prime, and let \( s \) be an integer such that \( s \geq 2 \). Then

\[
\Phi(\wp^s) - q\deg(\wp^s) \geq q(q - 3)
\]

Furthermore equality in (56) occurs if and only if \( \deg(\wp) = 1 \) and \( s = 2 \).

Proof. Let \( F(\alpha) \) be the function defined by

\[
F(\alpha) = q^{s\alpha} - q^{(s-1)\alpha} - sq\alpha,
\]

where \( \alpha \) ranges over the set \([1, \infty)\). Note that (56) is equivalent to the inequality

\[
F(\deg(\wp)) \geq q(q - 3).
\]
We prove that $F$ is a strictly increasing function over the interval $[1, \infty)$. Indeed, the derivative of $F$ is equal to
\[
F'(\alpha) = s \ln(q)q^{s\alpha} - (s-1) \ln(q)q^{(s-1)\alpha} - sq
\]
(58)
\[
= q(\ln(q)q^{(s-1)\alpha-1}(sq^\alpha - s + 1) - s).
\]
Since $q \geq 3$, $s \geq 2$, and $\alpha \geq 1$, we deduce that $\ln(q) \geq \ln(3) > 1$, $q^{(s-1)\alpha-1} \geq q^0 = 1$, and thus
\[
\ln(q)q^{(s-1)\alpha-1} > 1.
\]
(59)
On the other hand, since $q^\alpha \geq 3$, we deduce that
\[
sq^\alpha - s + 1 \geq 3s - s + 1 = 2s + 1.
\]
(60)
Combining (59), (60), and noting that $2s + 1 \geq 5$, we deduce from (59) that
\[F'(\alpha) > q(2s + 1 - s) = q(s + 1) \geq 9 > 0,
\]
which proves that $F$ is a strictly increasing function over the interval $[1, \infty)$. Therefore
\[F(\alpha) \geq F(1) = q^s - q^{s-1} - sq
\]
(61)
for any $\alpha \geq 1$. We should note that equality in (61) occurs if and only if $\alpha = 1$.

Now consider the function $G(\beta)$ of the form
\[G(\beta) = q^\beta - q^{\beta-1} - \beta q,
\]
where $\beta$ ranges over the set $[2, \infty)$. Note that
\[G(s) = q^s - q^{s-1} - sq = F(1).
\]
(62)
We prove that $G$ is a strictly increasing function over the interval $[2, \infty)$. Indeed, the derivative of $G$ is equal to
\[
G'(\beta) = \ln(q)q^\beta - \ln(q)q^{\beta-1} - q = q(\ln(q)(q^{\beta-1} - q^{\beta-2}) - 1).
\]
(63)
Since $q \geq 3$ and $\beta \geq 2$, we deduce that
\[\ln(q)(q^{\beta-1} - q^{\beta-2}) - 1 = \ln(q)q^{\beta-2}(q - 1) - 1 \geq \ln(3)q^0(q - 1) - 1 > q - 2 \geq 1,
\]
and thus
\[G'(\beta) > q \geq 3 > 0,
\]
Therefore $G$ is a strictly increasing function over the interval $[2, \infty)$. Hence
\[
G(\beta) \geq G(2) = q^2 - q - 2q = q(q - 3)
\]
(64)
for any $\beta \geq 2$. We should also note that equality in (64) occurs if and only if $\beta = 2$.

Replacing $\alpha, \beta$ by $\deg(\varphi), s$ in (61), (65), respectively, we deduce from (63) that
\[\Phi(\varphi^s) - q\deg(\varphi^s) = F(\beta) \geq F(1) = G(s) \geq G(2) = q(q - 3),
\]
(65)
which proves (66).

Note that equality in (66) occurs if and only both equalities in (61), (65) occur. By the remarks following (61), (65), we deduce that equality in (66) occurs if and only $\deg(\varphi) = 1$ and $s = 2$.

\[\square\]

**Corollary 6.15.** Assume that $q > 2$. Let $\varphi$ be a monic prime, and let $s$ be an integer such that $s \geq 2$. Then
\[
\Phi(\varphi^s) \geq q\deg(\varphi^s).
\]
(67)
Furthermore equality in (67) occurs if and only if $q = 3$, $\deg(\varphi) = 1$, and $s = 2$. \[\square\]
Proof. By Lemma 6.14, we deduce that
\[ \Phi(\wp^s) \geq q \deg(\wp^s) + q(q - 3). \]  
(68)

Since \( q \geq 3 \), we deduce that
\[ q(q - 3) \geq 0. \]  
(69)

Note that equality in (69) occurs if and only if \( q = 3 \).

By (68), (69), we deduce that
\[ \Phi(\wp^s) \geq q \deg(\wp^s) + q(q - 3) \geq q \deg(\wp^s), \]  
(70)

which proves (67).

Now we see that equality in (70) occurs if and only if both equalities in (68) and (69) occurs. By Lemma 6.14 and the remark following (69), we deduce that equality in (70) occurs if and only if \( q = 3 \), \( \deg(\wp) = 1 \), and \( s = 2 \). \qed

The following theorem is the second main result of this paper that can be viewed as a function field analogue of Feit’s theorem (see Feit \([9, \text{Theorem A}] \)). Corollary 6.3 plays a key role in the proof of the next theorem.

**Theorem 6.16.** Assume that \( q > 2 \). Let \( m, u \) be monic polynomials in \( A \) such that at least one of them is of positive degree. Then there exists a large Zsigmondy prime for \((u,m)\) except exactly in the following cases:

- **(EC-I)** \( q = 3 \), \( u = 1 \), and \( m = (\wp - 1)\wp \), where \( \wp \) is an arbitrary monic prime of degree one in \( \mathbb{F}_3[T] \);
- **(EC-II)** \( q = 2^2 \), \( u = 1 \), and \( m = (\wp - 1)\wp \), where \( \wp \) is an arbitrary monic prime of degree one in \( \mathbb{F}_{2^2}[T] \);
- **(EC-III)** \( q = 3 \), \( u = 1 \), and \( m \in \mathcal{X}_3 = \{ (T - 1)T^2, T(T + 1)^2, (T + 1)(T + 2)^2 \} \), where \( \mathcal{X}_3 \) is the set in Lemma 6.4.
- **(EC-IV)** \( q = 3 \), \( u = m \in \mathcal{X}_4 = \{ T, T + 1, T + 2 \} \), where \( \mathcal{X}_4 \) is the set in Lemma 6.5.
- **(EC-V)** \( q = 5 \), \( u = 1 \), and
  \[ m \in \mathcal{X}_6 = \{ T(T + 1), (T + 1)(T + 2), (T + 2)(T + 3), (T + 3)(T + 4), (T + 4)T \}, \]
  where \( \mathcal{X}_6 \) is the set in Lemma 6.7.
- **(EC-VI)** \( u = 1 \), and \( m \in \mathcal{X}_7 \), i.e., \( m \) is a monic prime of degree one in \( \mathbb{F}_q[T] \), where \( \mathcal{X}_7 \) is the set in Lemma 6.8. (Note that there is no restriction on \( q \) in this exceptional case.)
- **(EC-VII)** \( q = 3 \), \( u = 1 \), and
  \[ m \in \mathcal{X}_8 = \{ T^2, (T + 1)^2, (T + 2)^2 \}, \]
  where \( \mathcal{X}_8 \) is the set in Lemma 6.9.
- **(EC-VIII)** \( q = 4 \), \( u = 1 \), and
  \[ m \in \mathcal{X}_9 = \{ T(T + w), T(T + w^2), (T + 1)(T + w), (T + 1)(T + w^2) \}, \]
  where \( \mathcal{X}_9 \) is the set in Lemma 6.10. (Note that \( \mathbb{F}_4 = \mathbb{F}_2(w) \), where \( w \) is an element in the algebraic closure of \( \mathbb{F}_2 \) such that \( w^2 + w + 1 = 0 \).)
- **(EC-IX)** \( q = 3 \), \( u = 1 \), and
  \[ m \in \mathcal{X}_{10} = \{ T^3 + 2T \}, \]
  where \( \mathcal{X}_{10} \) is the set in Lemma 6.11.
Proof. If \( \deg(m) = 0 \), then \( m = 1 \), and it thus follows from the assumption that \( u \) is of positive degree. It is easy to see that any monic prime \( \wp \) dividing \( u \) is a large Zsigmondy prime for \( (u, m) = (u, 1) \). For the rest of the proof, without loss of generality, one can assume that \( m \) is of positive degree.

We first consider the cases when we are in one of the exceptional cases (EC-I)–(EC-IX). If we are in the exceptional case (EC-I) or the exceptional case (EC-II), then Theorem 4.4 and Theorem 5.2 tell us that there are no Zsigmondy primes for \( (u, m) \), and thus there are no large Zsigmondy primes for \( (u, m) \).

On the other hand, Lemmas 6.4, 6.5, 6.7, 6.8, 6.9, 6.10, and 6.11 tell us that there are no large Zsigmondy primes for \( (u, m) \).

Suppose, for the rest of the proof, that we are not in any of the exceptional cases (EC-I)–(EC-IX).

We prove that there exists a large Zsigmondy prime for \( (u, m) \). Assume the contrary, that is, (LZP0) there exist no large Zsigmondy primes for \( (u, m) \).

By Theorem 4.4 and Theorem 5.2 we know that there exists a Zsigmondy prime for \( (u, m) \), and it thus follows from Corollary 6.3 that the following are true:

(LZP1) \( m + 1 \) is the only Zsigmondy prime for \( (u, m) \); and

(LZP2) either \( \Psi_m(u) = \epsilon(m + 1) \) for some unit \( \epsilon \in \mathbb{F}_q \) or \( \Psi_m(u) = \epsilon q(m + 1) \) for some unit \( \epsilon \in \mathbb{F}_q \) and some monic prime \( q \) dividing \( m \).

We consider the following two cases:

* Case 1. \( \Psi_m(u) = \epsilon(m + 1) \) for some unit \( \epsilon \in \mathbb{F}_q \) and some monic prime \( q \) dividing \( m \).

Since \( \gcd(m, m + 1) = 1 \) and \( q \) divides \( m \), we deduce that \( \gcd(q, m + 1) = 1 \). Hence we, by appealing to (LZP1), find that \( q \) is a non-Zsigmondy prime for \( (u, m) \). Since \( q \) divides \( \Psi_m(u) \), it follows from Corollary 3.8(ii) that \( m \) is of the form

\[
m = P_{u,q} q^s,
\]

where \( P_{u,q} \) is the Carlitz annihilator of \( (u, q) \) and \( s \) is a positive integer.

We consider the following two subcases, according as to whether \( \deg(u) \geq 1 \) or \( \deg(u) = 0 \).

* Subcase 1A. \( \deg(u) \geq 1 \).

Since \( \deg(P_{u,q}) \geq 0 \), we consider the following two subsubcases, according as to whether \( \deg(P_{u,q}) = 0 \) or \( \deg(P_{u,q}) \geq 1 \).

• Subsubcase 1A(i). \( \deg(P_{u,q}) = 0 \).

By Definition 3.2, we see that \( P_{u,q} = 1 \). From (71), we find that

\[
m = q^s.
\]

Since \( \deg(u) \geq 1 \), we deduce from (72), Lemma 2.7 and Lemma 4.1 that

\[
\deg(\Psi_m(u)) = \Phi(m) \deg(u) \geq (q - 1) \deg(m) = s(q - 1) \deg(q).
\]

Note that equality in (73) occurs if and only if \( \deg(u) = 1 \) and \( \Phi(m) = (q - 1) \deg(m) \).

On the other hand, we see from (72) that

\[
\deg(\Psi_m(u)) = \deg(\epsilon q(m + 1)) = \deg(q) + \deg(m + 1) = \deg(q) + \deg(m) = (s + 1) \deg(q).
\]

Combining (73) and (74), we find that

\[
(s + 1) \deg(q) = \deg(\Psi_m(u)) \geq s(q - 1) \deg(q),
\]

and thus

\[
(s(q - 1) - (s + 1)) \deg(q) \leq 0.
\]

By the remark following (73), note that equality in (75) occurs if and only if \( \deg(u) = 1 \) and \( \Phi(m) = (q - 1) \deg(m) \).

Furthermore since \( s \geq 1 \) and \( q \geq 3 \), we find that

\[
s(q - 1) - (s + 1) \geq 2s - (s + 1) = s - 1 \geq 0,
\]

and since \( \deg(q) \geq 1 \), we deduce that

\[
(s(q - 1) - (s + 1)) \deg(q) \geq 0.
\]
Note that equality in (70) occurs if and only if \( s = 1 \) and \( q = 3 \).

Combining (74), (76), we deduce that
\[
(s(q - 1) - (s + 1))\deg(q) = 0.
\]

Hence by appealing to the remarks following (75), (76), we deduce that \( s = 1 \), \( q = 3 \), \( \deg(u) = 1 \) and \( \Phi(m) = (q - 1)\deg(m) \). It then follows from (72) that \( m = q \), and
\[
\Phi(q) = \Phi(m) = 2\deg(m) = 2\deg(q).
\]

If \( \deg(q) \geq 2 \), then we deduce from Corollary 6.13 that
\[
\Phi(q) > q\deg(q) = 3\deg(q),
\]
which is a contradiction to (77). Hence we deduce that \( \deg(q) = 1 \).

Recall that \( \gcd(q, q - 1) = 1 \), and since \( \deg(u) = \deg(q) = 1 \) and \( q, u \) are monic polynomials, we deduce that \( q = u \).

In summary, we have showed that
\[
\lambda = \deg(P_{u,q}) \geq 1.
\]

Set
\[
(78) \quad \gamma = \deg(q) \geq 1.
\]

and
\[
(79) \quad \lambda = \deg(P_{u,q}) \geq 1.
\]

Recall from Proposition 3.3 (i) that \( P_{u,q} \) divides \( q - 1 \), and since \( \gcd(q, q - 1) = 1 \), we deduce that \( \gcd(P_{u,q}, q) = 1 \). Hence by appealing to Lemma 1.1 we deduce from (71) that
\[
(80) \quad \Phi(m) = \Phi(P_{u,q}q^s) = \Phi(P_{u,q})\Phi(q^s) \geq (q - 1)^2\deg(P_{u,q})\deg(q^s) = (q - 1)^2\deg(P_{u,q})\deg(q).
\]

Since \( \deg(u) \geq 1 \), we deduce from Lemma 2.7 and (80) that
\[
(81) \quad \deg(\Psi_m(u)) = \deg(u)\Phi(m) \geq \Phi(m) \geq (q - 1)^2\deg(P_{u,q})\deg(q) = (q - 1)^2\lambda \gamma.
\]

Recall that \( \Psi_m(u) = eq(m + 1) \), and it thus follows from (71) that
\[
\deg(\Psi_m(u)) = \deg(q) + \deg(m + 1) = \deg(q) + \deg(m) = (s + 1)\deg(q) + \deg(P_{u,q})
\]
\[
= (s + 1)\gamma + \lambda.
\]

Combining (81) and (82), we find that
\[
(s + 1)\gamma + \lambda = \deg(\Psi_m(u)) \geq (q - 1)^2\lambda \gamma,
\]
and thus
\[
(83) \quad (q - 1)^2\lambda \gamma - (s + 1)\gamma - \lambda \leq 0.
\]

Since \( \lambda \geq 1 \), \( \gamma \geq 1 \), and \( s \geq 1 \), we deduce that
\[
(84) \quad 2s\lambda \gamma - (s + 1)\gamma \geq 2s\gamma - (s + 1)\gamma = (s - 1)\gamma \geq 0.
\]

On the other hand, since \( \lambda \geq 1 \), \( \gamma \geq 1 \), and \( s \geq 1 \), we see that
\[
(85) \quad 2s\lambda \gamma - \lambda \geq 2\lambda - \lambda = \lambda \geq 1.
\]

Combining (84) and (85), and note that \( (q - 1)^2 \geq 4 \), we deduce that
\[
(86) \quad (q - 1)^2\lambda \gamma - (s + 1)\gamma - \lambda \geq 4s\lambda \gamma - (s + 1)\gamma - \lambda
\]
\[
= (2s\lambda \gamma - (s + 1)\gamma) + (2s\lambda \gamma - \lambda)
\]
\[
\geq 0 + 1 = 1,
\]
which is a contradiction to (83).
* Subcase 1B. \( \deg(u) = 0 \), i.e., \( u = 1 \).

Note that in this subcase, \( P_u, q = P_{1, q} \) since \( u = 1 \). Recall from Proposition 3.3(i) that \( P_{1, q} \) divides \( q - 1 \), and since \( \gcd(q, q - 1) = 1 \), we deduce that \( \gcd(P_{1, q}, q) = 1 \). We should also note from Proposition 3.3(ii) that \( \deg(P_{1, q}) \geq 1 \), and that

\[
(86) \quad \deg(P_{1, q}) \leq \deg(q - 1) = \deg(q).
\]

We see from Lemma 4.1 and (71) that

\[
(87) \quad \Phi(m) = \Phi(P_{1, q}q^*) = \Phi(P_{1, q})\Phi(q^*) \geq (q - 1)^2 \deg(P_{1, q}) \deg(q^*) = s(q - 1)^2 \deg(P_{1, q}) \deg(q).
\]

By Lemma 2.8 we know that

\[
(88) \quad \deg(\Psi_m(u)) = \deg(\Psi_m(1)) = \frac{\Phi(m) + \delta}{q}
\]

for some integer \( \delta \in \{-1, 0, 1\} \).

Since \( u = 1 \), we see that

\[
\Psi_m(1) = \Psi_m(u) = \epsilon q(m + 1).
\]

Since \( \delta \geq -1 \), it thus follows from (87) and (88) that

\[
(89) \quad \deg(q) + \deg(m) = \deg(q) + \deg(m + 1) = \deg(\Psi_m(1)) \geq \frac{s(q - 1)^2 \deg(P_{1, q}) \deg(q) - 1}{q}.
\]

By (88), we deduce that

\[
\deg(m) = \deg(P_{1, q}q^*) = \deg(P_{1, q}) + s \deg(q) \leq (s + 1) \deg(q),
\]

and it thus follows from (89) that

\[
q(s + 2) \deg(q) \geq q(\deg(q) + \deg(m)) \geq s(q - 1)^2 \deg(P_{1, q}) \deg(q) - 1.
\]

Therefore

\[
(90) \quad \deg(q)(s(q - 1)^2 \deg(P_{1, q}) - q(s + 2)) \leq 1.
\]

We consider the following three subsubcases, according as to whether \( \deg(P_{1, q}) \geq 3 \), \( \deg(P_{1, q}) = 2 \), or \( \deg(P_{1, q}) = 1 \).

• Subcase 1B(i). \( \deg(P_{1, q}) \geq 3 \)

By (88), we see that

\[
\deg(q) \geq \deg(P_{1, q}) \geq 3.
\]

Since \( q \geq 3 \) and \( s \geq 1 \), we deduce that

\[
3sq - (7s + 2) \geq 9s - (7s + 2) = 2s - 2 \geq 0,
\]

and thus

\[
s(q - 1)^2 \deg(P_{1, q}) - q(s + 2) \geq 3s(q - 1)^2 - q(s + 2) = q(3sq - (7s + 2)) + 3s \geq 3.
\]

Therefore

\[
\deg(q)(s(q - 1)^2 \deg(P_{1, q}) - q(s + 2)) \geq 9,
\]

which is a contradiction to (90).

• Subcase 1B(ii). \( \deg(P_{1, q}) = 2 \)

We, by appealing to (88), find that

\[
\deg(q) \geq \deg(P_{1, q}) = 2.
\]

If \( q \geq 4 \), we see that

\[
2sq - (5s + 2) \geq 8s - (5s + 2) = 3s - 2 \geq 1,
\]

and thus

\[
s(q - 1)^2 \deg(P_{1, q}) - q(s + 2) = 2s(q - 1)^2 - q(s + 2) = q(2sq - (5s + 2)) + 2s \geq 4 + 2 = 6.
\]
Hence
\[
deg(q)(s(q - 1)^2 \deg(P_{1,q}) - q(s + 2)) \geq 12,
\]
which is a contradiction to (90).

Suppose now that \( q = 3 \). By (90), and since \( \deg(q) \geq \deg(P_{1,q}) = 2 \), we see that
\[
\frac{1}{2} \geq \frac{1}{\deg(q)} \geq s(q - 1)^2 \deg(P_{1,q}) - q(s + 2) = 8s - 3(s + 2) = 5s - 6,
\]
and thus
\[
s \leq \frac{13}{10}.
\]
Since \( s \) is a positive integer, we deduce from the last inequality that \( s = 1 \).

By Proposition 2.5 we know that
\[
\deg(C_{P_{1,q}}(1)) = q^{\deg(P_{1,q})-1} = 3^{2-1} = 3,
\]
and since \( C_{P_{1,q}}(1) \equiv 0 \pmod{q} \) (recall that \( P_{1,q} \) is the Carlitz annihilator of \((1, q)\)), and \( \deg(q) \geq 2 \), we deduce that either \( \deg(q) = 2 \) or \( \deg(q) = 3 \).

In summary, by appealing to (LZP1), we find that the following are true:

(i) \( q = 3, u = 1, \) and \( m = P_{1,q}q; \) where \( q \) is a monic prime in \( \mathbb{F}_3[T] \) of degree 2 or 3 such that the Carlitz annihilator \( P_{1,q} \) of \((1, q)\) is of degree 2;
(ii) \( m + 1 \) is a prime in \( \mathbb{F}_3[T] \);

This, in particular, implies \( m \in \mathcal{X}_5 \), where \( \mathcal{X}_5 \) is the set in Lemma 6.6. Hence \( \mathcal{X}_5 \neq \emptyset \), which is absurd since we know from Lemma 6.6 that \( \mathcal{X}_5 = \emptyset \).

- **Subsubcase 1B(iii).** \( \deg(P_{1,q}) = 1 \)

By Proposition 2.5 we know that
\[
\deg(C_{P_{1,q}}(1)) = q^{\deg(P_{1,q})-1} = q^0 = 1,
\]
and since \( C_{P_{1,q}}(1) \equiv 0 \pmod{q} \) and \( \deg(q) \geq 1 \), we deduce that \( \deg(q) = 1 \). Since \( P_{1,q}, q - 1 \) are monic polynomials, \( P_{1,q} \) divides \( q - 1 \) (see Proposition 2.3(i)), and \( \deg(P_{1,q}) = \deg(q - 1) = \deg(q) = 1 \), we deduce that
\[
P_{1,q} = q - 1.
\]

If \( q \geq 5 \), we see that
\[
sq - (3s + 2) \geq 5s - (3s + 2) = 2s - 2 \geq 0.
\]

Note that equality in (91) occurs if and only if \( q = 5 \) and \( s = 1 \).

By (91), we see that
\[
\deg(q)(s(q - 1)^2 \deg(P_{1,q}) - q(s + 2)) = s(q - 1)^2 - q(s + 2) = q(sq - (3s + 2)) + s \geq 1.
\]

Note that equality in (92) occurs if and only if \( s = 1 \) and equality in (91) occurs.

Combining (91) and (92), we find that
\[
\deg(q)(s(q - 1)^2 \deg(P_{1,q}) - q(s + 2)) = 1,
\]
which implies that equality in (92) occurs. By appealing to the remarks following (91) and (92), we find that \( q = 5 \) and \( s = 1 \).

By appealing to (LZP0) and (LZP1), we find that the following are true:

(i) \( q = 5, u = 1, \) and \( m = P_{1,q}q = (q - 1)q, \) where \( q \) is a monic prime of degree one in \( \mathbb{F}_5[T] \);
(ii) \( m + 1 \) is the only Zsigmondy prime for \((1, m)\);
(iii) there are no large Zsigmondy primes for \((1, m)\).
This, in particular, implies that \( m \in X_6 \), where \( X_6 \) is the set in Lemma 6.7. This is equivalent to saying that we are in the exceptional case (EC-V), which is a contradiction.

For the rest of Subsubcase 1B(iii), it remains to consider the case when \( q = 3 \) or \( q = 4 \).

If \( q = 4 \), recall that \( \deg(q) = \deg(P_{1, q}) = 1 \), and thus we see from (90) that
\[
1 \geq \deg(q)(s(q - 1)^2\deg(P_{1, q}) - q(s + 2)) = 5s - 8.
\]
Hence
\[
s \leq \frac{9}{5},
\]
and since \( s \) is a positive integer, we deduce from the last inequality that \( s = 1 \). Thus
\[
m = P_{1, q}q^s = (q - 1)q,
\]
where \( q \) is a monic prime of degree one in \( \mathbb{F}_{2^e}[T] \). This implies that we are in the exceptional case (EC-II), which is a contradiction.

If \( q = 3 \), we see from (90) that
\[
1 \geq \deg(q)(s(q - 1)^2\deg(P_{1, q}) - q(s + 2)) = s - 6,
\]
and thus
\[
s \leq 7.
\]
Hence
\[
s \in \{1, 2, 3, 4, 5, 6, 7\}.
\]
Thus
\[
m = P_{1, q}q^s = (q - 1)q^s,
\]
where \( q \) is a monic prime of degree one in \( \mathbb{F}_3[T] \) and \( s \in \{1, 2, 3, 4, 5, 6, 7\} \).

If \( s = 1 \), we deduce that \( m = (q - 1)q \). Since \( q = 3 \), \( u = 1 \), and \( q \) is a monic prime of degree one in \( \mathbb{F}_3[T] \), we see that we are in the exceptional case (EC-I), which is a contradiction.

If \( 2 \leq s \leq 7 \), we, by appealing to (LZP0) and (LZP1), find that \( m \in X_3 \), where \( X_3 \) is the set in Lemma 6.4. This, in turn, is equivalent to saying that we are in the exceptional case (EC-III), which is a contradiction.

\* Case 2. \( \Psi_m(u) = \epsilon(m + 1) \) for some unit \( \epsilon \in \mathbb{F}_q^\times \).

If \( \deg(u) \geq 1 \), we deduce from Lemma 2.7 and Lemma 4.1 that
\[
\deg(m) = \deg(m + 1) = \deg(\Psi_m(u)) = \Phi(m)\deg(u) \geq (q - 1)\deg(m).
\]
Thus
\[
(q - 2)\deg(m) \leq 0,
\]
which is a contradiction since \( \deg(m) \geq 1 \) and \( q > 2 \).

If \( \deg(u) = 0 \), then \( u = 1 \), and hence
\[
\Psi_m(1) = \epsilon(m + 1).
\]
Since \( m \) is of positive degree, there exists a monic prime \( \wp \) of positive degree dividing \( m \). Then one can write
\[
m = n\wp^s,
\]
where \( s \) is a positive integer, and \( n \) is a monic polynomial such that \( \gcd(n, \wp) = 1 \).

We consider the following subcases, according as to whether \( \deg(n) = 0 \) or \( \deg(n) \geq 1 \).

\* Subcase 2A. \( \deg(n) = 0 \).

In this subcase, since \( n \) is monic, we see that \( n = 1 \), and thus
\[
m = \wp^s.
\]
We first consider the case when \( s = 1 \). If \( \deg(q) = 1 \), then \( m = q \) is a monic prime of degree one in \( \mathbb{F}_q[T] \). This implies that \( m \in \mathcal{X}_2 \), where \( \mathcal{X}_2 \) is the set in Lemma 6.8. Recall that \( u = 1 \). Hence we are in the exceptional case (EC-VI), which is a contradiction.

Suppose now that \( \deg(q) \geq 2 \). Since \( m = q \) is a monic prime, we deduce from Lemma 2.8 that
\[
\deg(\Psi_m(1)) = \deg(\Psi_q(1)) = \frac{\Phi(q) + (-1)^2}{q} = \frac{\Phi(q) + 1}{q},
\]
and it therefore follows from (93) that
\[
(96) \quad \deg(q) = \deg(m) = \deg(\epsilon(m + 1)) = \deg(\Psi_m(1)) = \frac{\Phi(q) + 1}{q}.
\]
By Corollary 6.13 we know that \( \Phi(q) > q\deg(q) \), and thus
\[
\frac{\Phi(q) + 1}{q} > \frac{\Phi(q)}{q} > \deg(q),
\]
which is a contradiction to (96).

We now consider the case when \( s \geq 2 \). By (93), we know from Lemma 2.8 that
\[
(97) \quad \deg(q^s) = \deg(m) = \deg(\epsilon(m + 1)) = \deg(\Psi_m(1)) = \frac{\Phi(q^s)}{q},
\]
and it thus follows from Corollary 6.15 that
\[
(98) \quad \deg(q^s) = \frac{\Phi(q^s)}{q} \geq \frac{q\deg(q^s)}{q} = \deg(q^s).
\]
Therefore equality in (98) occurs, and hence we deduce from Corollary 6.15 that \( q = 3, \deg(q) = 1, \) and \( s = 2 \). Then \( q = 3, u = 1, \) and \( m = q^2 \), where \( q \) is a monic prime of degree one in \( \mathbb{F}_3[T] \). By (LZP0), (LZP1), we deduce that \( m \in \mathcal{X}_s \), where \( \mathcal{X}_s \) is the set in Lemma 6.9. This implies that we are in the exceptional case (EC-VII), which is a contradiction.

* Subcase 2B. \( \deg(n) \geq 1 \).

We first prove that the following is true:

(LZP3) \( m \) is square-free, that is, \( q^2 \) does not divide \( m \) for any monic prime \( q \).

Assume that (LZP3) does not hold, i.e., there exists a monic prime \( q \) such that \( q^2 \) divide \( m \). Then one can write \( m \) in the form
\[
m = uq^r,
\]
where \( r \geq 2, \) and \( u \) is a monic polynomial such that \( \gcd(u, q) = 1 \). Note that since \( m = nq^s \) (see 91), \( \gcd(n, q) = 1, \deg(n) \geq 1, \) and \( \deg(q^s) \geq 1, \) we deduce that \( \deg(u) > 0 \).

Applying Lemma 4.1 for \( u, \) and applying Corollary 6.15 for \( q^s, \) we deduce that
\[
(100) \quad \Phi(m) = \Phi(uq^s) = \Phi(u)\Phi(q^s) \geq (q - 1)\deg(u)\deg(q^s) = q(q - 1)\deg(u)\deg(q^s).
\]
We deduce from (93), (99), (100), and Lemma 2.8 that
\[
\deg(u) + \deg(q^s) = \deg(uq^s) = \deg(m) = \deg(\epsilon(m + 1)) = \deg(\Psi_m(1)) = \frac{\Phi(m)}{q} \geq (q - 1)\deg(u)\deg(q^s),
\]
and thus
\[
(101) \quad (q - 2)\deg(u)\deg(q^s) + \deg(u)\deg(q^s) - (\deg(u) + \deg(q^s)) \leq 0.
\]
Since \( r \geq 2, \) we see that \( \deg(q^s) = r\deg(q) \geq 2, \) and thus
\[
(102) \quad (q - 2)\deg(u)\deg(q^s) \geq 2(q - 2) \geq 2.
\]
On the other hand, since \( \deg(u) \geq 1 \) and \( \deg(q^s) \geq 2, \) we know that
\[
\deg(u)\deg(q^s) - (\deg(u) + \deg(q^s)) + 1 = (\deg(u) - 1)(\deg(q^s) - 1) \geq 0,
\]
and therefore equality in (100) occurs, and hence we deduce from Corollary 6.15 that \( q = 3, \deg(q) = 1, \) and \( s = 2 \). Then \( q = 3, u = 1, \) and \( m = q^2 \), where \( q \) is a monic prime of degree one in \( \mathbb{F}_3[T] \). By (LZP0), (LZP1), we deduce that \( m \in \mathcal{X}_s \), where \( \mathcal{X}_s \) is the set in Lemma 6.9. This implies that we are in the exceptional case (EC-VII), which is a contradiction.
and thus
\[(103) \quad \deg(u)\deg(q^r) - (\deg(u) + \deg(q^r)) \geq -1.\]

From (102) and (103), we deduce that
\[(q - 2)\deg(u)\deg(q^r) + \deg(u)\deg(q^r) - (\deg(u) + \deg(q^r)) \geq 1,
\]
which is a contradiction to (101). Thus (LZP3) is true, i.e., \(m\) is square-free.

In order to get a contradiction in this subcase, we use another representation of \(m\). By (94), and since \(\gcd(n, \varphi) = 1\), we deduce that \(m\) can be written in the form
\[(104) \quad m = m_1m_2,
\]
where \(m_1, m_2\) are monic polynomials of positive degrees such that \(\gcd(m_1, m_2) = 1\). (For example, one can take \(m_1 = n\) and \(m_2 = \varphi^r\).) Set
\[(105) \quad \alpha = \deg(m_1) \geq 1,
\]
and
\[(106) \quad \beta = \deg(m_2) \geq 1.
\]
Without loss of generality, one can further assume that
\[(107) \quad \alpha = \deg(m_1) \geq \deg(m_2) = \beta.
\]
Since \(\deg(m_1) \geq 1\) and \(\deg(m_2) \geq 1\), we deduce from (104) and Lemma 4.1 that
\[(108) \quad \Phi(m) = \Phi(m_1m_2) = \Phi(m_1)\Phi(m_2) \geq (q - 1)^2\deg(m_1)\deg(m_2) = (q - 1)^2\alpha\beta.
\]
Since \(m\) is square-free, we deduce from (93) and Lemma 2.8 that there exists an integer \(\delta \in \{-1, 1\}\) such that
\[(109) \quad \alpha + \beta = \deg(m_1) + \deg(m_2) = \deg(m) = \deg(\epsilon(m + 1)) = \deg(\Psi_m(1)) = \frac{\Phi(m) + \delta}{q}.
\]
Since \(\delta \geq -1\), we deduce from (108) and (109) that
\[(110) \quad \alpha + \beta \geq \frac{(q - 1)^2\alpha\beta - 1}{q}.
\]
Inequality (110) is equivalent to the inequality
\[(111) \quad q((\alpha\beta)q - (2\alpha\beta + \alpha + \beta)) + \alpha\beta = (\alpha\beta)q^2 - (2\alpha\beta + \alpha + \beta)q + \alpha\beta \leq 1.
\]
Note that equality in (110) occurs if and only if \(\delta = -1\) and equality in (108) occurs. Since inequality (111) is equivalent to inequality (110), we should also note that the following is true:

(ELZP) **Equality in (110) occurs if and only if \(\delta = -1\) and equality in (108) occurs.**

Since \(\alpha \geq 1\) and \(\beta \geq 1\), we deduce that
\[\alpha\beta - (\alpha + \beta) + 1 = (\alpha - 1)(\beta - 1) \geq 0,
\]
and thus
\[(112) \quad \alpha\beta \geq \alpha + \beta - 1.
\]
Note that equality in (112) occurs if and only if \(\alpha = 1\) or \(\beta = 1\).

Since \(q \geq 3\), we deduce from (112) that
\[(113) \quad (\alpha\beta)q - (2\alpha\beta + \alpha + \beta) \geq 3\alpha\beta - (2\alpha\beta + \alpha + \beta) = \alpha\beta - (\alpha + \beta) \geq -1.
\]
Since \((\alpha\beta)q - (2\alpha\beta + \alpha + \beta)\) is an integer, we deduce from the above inequality that either
\[(114) \quad (\alpha\beta)q - (2\alpha\beta + \alpha + \beta) \geq 0
\]
or
\[(115) \quad (\alpha\beta)q - (2\alpha\beta + \alpha + \beta) = -1.
\]
Note that (115) holds if and only if equalities in (113) occur at the same time. This of course implies that (115) holds if and only if \( q = 3 \), and \( \alpha = 1 \) or \( \beta = 1 \).

We consider the following subsubcases:

- **Subsubcase 2B(i).** (114) holds, i.e., \((\alpha \beta)q - (2\alpha \beta + \alpha + \beta) \geq 0\).

  In this subsubcase, since \( \alpha \geq 1 \) and \( \beta \geq 1 \), we see that
  \[
  (116) \quad q((\alpha \beta)q - (2\alpha \beta + \alpha + \beta)) + \alpha \beta \geq 1. 
  \]

  Note that equality in (116) occurs if and only if
  \[
  (117) \quad (\alpha \beta)q - (2\alpha \beta + \alpha + \beta) = 0, 
  \]
  and \( \alpha = \beta = 1 \).

  From (111) and (116), we deduce that equality in (116) occurs, and it thus follows from the above remark that \( \alpha = \beta = 1 \), and
  \[
  (118) \quad (\alpha \beta)q - (2\alpha \beta + \alpha + \beta) = 0. 
  \]

  Since \( \alpha = \beta = 1 \), equation (118) implies that \( q = 4 \).

  In summary, we have showed in this subsubcase that \( q = 4 \), \( u = 1 \), and \( m = m_1m_2 \), where \( m_1, m_2 \) are monic polynomials in \( \mathbb{F}_4[T] \) such that \( \deg(m_1) = \deg(m_2) = 1 \) and \( \gcd(m_1, m_2) = 1 \). It then follows from (LZP0) and (LZP1) that \( m \in X_9 \), where \( X_9 \) is the set in Lemma 6.10. This implies that we are in the exceptional case (EC-VIII), which is a contradiction.

- **Subsubcase 2B(ii).** (112) holds, i.e., \((\alpha \beta)q - (2\alpha \beta + \alpha + \beta) = -1\).

  The remark following (115) tells us that in this subsubcase, \( q = 3 \), and \( \alpha = 1 \) or \( \beta = 1 \). If \( \alpha = 1 \), we see from (117) that \( \beta = 1 \). Thus, in any event, \( q = 3 \) and \( \beta = 1 \).

  Since \( q = 3 \) and \( \beta = 1 \), we deduce from (111) and (115) that \( \alpha \leq 4 \), and therefore \( \alpha \in \{1, 2, 3, 4 \} \).

  We contend that \( \alpha = 1 \) or \( \alpha = 2 \). Indeed, if \( \alpha = 4 \), then one sees that equality in (111) occurs, and it thus follows from (ELZP) that equality in (108) occurs. This implies that
  \[
  (119) \quad \Phi(m) = \Phi(m_1)\Phi(m_2) = (q - 1)^2\alpha \beta = 16. 
  \]

  Since \( \deg(m_2) = \beta = 1 \), we see that \( m_2 \) is a monic prime of degree one in \( \mathbb{F}_3[T] \). Hence \( \Phi(m_2) = 3^{\deg(m_2)} - 1 = 3 - 1 = 2 \), and thus
  \[
  (120) \quad \Phi(m_1) = 8. 
  \]

  We should note that \( m_1 \) is square-free since \( m \) is square-free. Since \( \alpha = \deg(m_1) = 4 \), either all monic prime factors of \( m_1 \) are of degree one or there exists a monic prime, say \( P \), of degree at least 2 such that \( P \) divides \( m_1 \). If the former holds, then \( m_1 \) is of the form
  \[
  m_1 = P_1P_2P_3P_4, 
  \]
  where the \( P_i \) are distinct monic primes of degree one in \( \mathbb{F}_3[T] \). Then
  \[
  \Phi(m_1) = \Phi(P_1)\Phi(P_2)\Phi(P_3)\Phi(P_4) = (3^{\deg(P_1)} - 1)(3^{\deg(P_2)} - 1)(3^{\deg(P_3)} - 1)(3^{\deg(P_4)} - 1) = 16, 
  \]
  which is a contradiction to (120).

  Suppose now that there exists a monic prime \( P \) of degree at least 2 such that \( P \) divides \( m_1 \). Write
  \[
  m_1 = Pm_*, 
  \]
  where \( m_* \) is a monic polynomial such that \( \gcd(m_*, P) = 1 \). Since \( \deg(m_1) = \alpha = 4 \), we see that
  \[
  2 \leq \deg(P) \leq 4. 
  \]

  If \( \deg(P) = 4 \), then \( m_1 = P \), and thus
  \[
  \Phi(m_1) = \Phi(\alpha_*P) = 3^{\deg(P)} - 1 = 3^4 - 1 = 80, 
  \]
  which is a contradiction to (120).

  If \( 2\deg(P) \leq 3 \), then \( \deg(m_*) \geq 1 \). We see from Lemma 3.1 that
  \[
  \Phi(m_*) \geq (q - 1)\deg(m_*) \geq 2. 
  \]
On the other hand, since \(2\deg(P) \leq 3\), we deduce that 
\[
\Phi(P) = 3^{\deg(P)} - 1 \geq 3^2 - 1 = 8.
\]

Therefore 
\[
\Phi(m) = \Phi(P)\Phi(m_+) \geq 16,
\]
which is a contradiction to \([120]\). Thus, by what we have showed above, we deduce that \(\alpha \in \{1, 2, 3\}\).

Suppose now that \(\alpha = 3\). Recall that \(q = 3\) and \(\beta = 1\). We now deduce from \([109]\) that 
\[
4 = \alpha + \beta = \frac{\Phi(m) + \delta}{q} = \frac{\Phi(m) + \delta}{3}.
\]

Since \(\delta = \pm 1\), we find from \([124]\) that either \(\Phi(m) = 11\) or \(\Phi(m) = 13\). On the other hand, since \(\beta = \deg(m_2) = 1\), we deduce that \(m_1\) is a monic prime of degree one, and it thus follows from \([104]\) that 
\[
\Phi(m) = \Phi(m_1)\Phi(m_2) = \Phi(m_1)(\beta^{\deg(m_2)} - 1) = 2\Phi(m_1) \equiv 0 \pmod{2},
\]
which is a contradiction to the fact that either \(\Phi(m) = 11\) or \(\Phi(m) = 13\). This contradiction implies that \(\alpha = 1\) or \(\alpha = 2\).

In summary, we have showed in Subsubcase 2B(ii) that \(q = 3\), \(u = 1\), and \(m = m_1m_2\), where \(m_1, m_2\) are monic polynomials in \(\mathbb{F}_3[T]\) such that \(\gcd(m_1, m_2) = 1\), \(\alpha = \deg(m_1) \in \{1, 2\}\), and \(\beta = \deg(m_2) = 1\). We therefore, by appealing to (LZP0), (LZP1), and (LZP3), find that \(m \in \mathcal{X}_{10}\), where \(\mathcal{X}_{10}\) is the set in Lemma \([6,11]\). This implies that we are in the exceptional case (EC-IX), which is a contradiction.

In any event, by all of what we have showed above, we deduce that there exists a large Zsigmondy prime for \((u, m)\), and therefore Theorem \([6,10]\) follows immediately.

\[\Box\]

Acknowledgements

All the calculations in this paper were performed using the computational algebra software MAGMA (see \([7]\)).

References

[1] E. Artin, The orders of the linear groups, Comm. Pure Appl. Math. 8 (1955), 355–365.
[2] S. Bae and S.-G. Hahn, On the ring of integers of cyclotomic function fields, Bull. Korean Math. Soc. 29 (1992), no. 1, 153–163. Available at \[\text{http://pdf.medrang.co.kr/kms01/BKMS/29/BKMS-29-1-153-163.pdf}\]
[3] S. Bae, The arithmetic of Carlitz polynomials, J. Korean Math. Soc. 35 (1998), no. 2, 341–360. Available at \[\text{http://www.mathnet.or.kr/mathnet/kms_tex/33383.pdf}\]
[4] A.S. Banumoba, Arithmetic of Carlitz polynomials, Ph.D. Thesis–Stellenbosch University (2014). Available at \[\text{http://scholar.sun.ac.za/handle/10019.1/95850}\]
[5] A.S. Bang, Taltheoretiske undersøgelser, Tidsskrift f. Math. 4, (1886), no. 5, 70–80, 130–137.
[6] G.D. Birkhoff and H.S. Vandiver, On the integral divisors of \(a^n - b^n\), Ann. of Math. 2 (5) (1904), no. 4, 173–180.
[7] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system. I. The user language, Computational algebra and number theory (London, 1993), J. Symbolic Comput. 24 (1997), no. 3–4, 235–265.
[8] N.N. Dong Quan, Carlitz module analogues of Mersenne primes, Wieferich primes, and certain prime elements in cyclotomic function fields, Journal of Number Theory 145 (2014), 181–193.
[9] W. Feit, On large Zsigmondy primes, Proc. Amer. Math. Soc. 102 (1988), no. 1, 29–36.
[10] W. Feit and G. Seitz, On finite rational groups and related topics, Illinois J. Math. 33 (1989), no. 1, 103–131.
[11] D. Goss, Basic structures of function field arithmetic, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], 35, Springer-Verlag, Berlin, (1996).
[12] G.H. Hardy, J.E. Littlewood and G. Pólya, Inequalities, Cambridge University Press, Cambridge, UK, (1952).
[13] D.R. Hayes, Explicit class field theory for rational function fields, Trans. Amer. Math. Soc. 189 (1974), 77–91.
[14] H. Lüneburg, Ein einfacher Beweis für den Satz von Zsigmondy über primitive Primteiler von \(A^N - 1\). (German) [A simple proof of Zsigmondy’s theorem on primitive prime divisors of \(A^N - 1\)]. Geometries and groups (Berlin, 1981), pp. 219–222, Lecture Notes in Math., 893, Springer, Berlin-New York, 1981.
[15] M. Rosen, Number theory in function fields, Graduate Texts in Mathematics, 210. Springer-Verlag, New York (2002).
[16] M. Roitman, On Zsigmondy primes, Proc. Amer. Math. Soc. 125 (1997), no. 7, 1913–1919.
[17] D.S. Thakur, Function Field Arithmetic, World Scientific Publishing Co., Inc., River Edge, NJ, (2004).
[18] G.D. Villa Salvador, *Topics in the theory of algebraic function fields*, Mathematics: Theory & Applications. Birkhäuser Boston, Inc., Boston, MA (2006).

[19] A.H. Wedderburn, *A theorem on finite algebras*, Trans. Amer. Math. Soc. 6 (1905), 349–352.

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

Department of Mathematics, The University of Texas at Austin, Austin, TX 78712, USA
E-mail address: dongquan.ngoc.nguyen@gmail.com