



Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

A note on Carlitz Wieferich primes[☆]Alex Samuel Bamunoba^{a,b,*}^a Department of Mathematics, Stellenbosch University, South Africa^b Makerere University, Uganda

ARTICLE INFO

Article history:

Received 7 December 2013

Received in revised form 19 May 2016

Accepted 27 September 2016

Available online 14 December 2016

Communicated by F. Breuer

MSC:

11A99

11G09

Keywords:

The Carlitz module

Carlitz polynomials and c-Wieferich primes

ABSTRACT

In 1994, D. Thakur introduced the notion of Wieferich primes for the Carlitz module, hereafter called c-Wieferich primes. At almost the same time, L. Denis proved the Carlitz module analogue of the famous Fermat's Last Theorem. In this article, we relate Thakur's definition of c-Wieferich primes to Denis' result and state the necessary and sufficient condition for a monic irreducible (prime) polynomial P in $\mathbb{F}_q[T]$ to be c-Wieferich. We use this condition to give another proof for infinitude of c-Wieferich primes in $\mathbb{F}_2[T]$ and in addition construct two algorithms for computing c-Wieferich primes. With the help of the SAGE software, we compute several examples of c-Wieferich primes for the rings $\mathbb{F}_q[T]$, where $q \in \{3, 5, 7, 11, 13, 19, 29, 37\}$. Lastly, we unconditionally prove infinitude of non-c-Wieferich primes in $\mathbb{F}_q[T]$ for $q > 2$.

© 2016 Elsevier Inc. All rights reserved.

[☆] This work was carried out with financial support from the AIMS-DAAD Scholarship (A/13/90157), the University of Stellenbosch Postgraduate Merit Bursary Scheme, the Government of Canada's International Development Research Centre (IDRC) Grant number 107185-001, and within the framework of the AIMS Research for Africa Project.

* Correspondence to: Department of Mathematics, Makerere University, Uganda.

E-mail address: bamunoba@aims.ac.za.

1. Classical Wieferich primes

Fermat's Last Theorem (FLT) is the assertion that: for $n \in \mathbb{N}_{\geq 3}$, the equation $x^n + y^n = z^n$ has no integer solutions (x, y, z) with $xyz \neq 0$. This was proved by A. Wiles with help from R. Taylor. Now, P. Fermat had conjectured this result and only proved it for the case $n = 4$, (and as a corollary, FLT is true for any positive multiple of 4). Since every $n \in \mathbb{N}_{\geq 3}$ is either divisible by 4 or an odd prime, in order to prove Fermat's Conjecture, it remained to prove it for every odd prime. Two cases became distinguished: the first when the odd prime p does not divide xyz and the second when it does. A. Wieferich [19] proved [Theorem 1.1](#).

Theorem 1.1 (A. Wieferich). *If the first case of FLT is false for an odd prime p , then $2^{p-1} \equiv 1 \pmod{p^2}$.*

The prime numbers p that satisfy the congruence $2^{p-1} \equiv 1 \pmod{p^2}$ are called *Wieferich primes*. Early on, the search for these primes became important because of their connection to the first case of FLT. Despite the number of extensive searches, the only Wieferich primes known are 1093 and 3511 (sequence **A001220** in OEIS). We do not know whether there are finitely many Wieferich primes. However, there is a heuristic argument that asserts the number of Wieferich primes up to x to be $O(\log(\log(x)))$, [11, page 226].

A *non-Wieferich prime* is any prime number p satisfying $2^{p-1} \not\equiv 1 \pmod{p^2}$. Despite the overwhelming evidence for non-Wieferich primes, our best result is based on (a widely believed) conjecture. J. Silverman [13, [Theorem 1](#)] proved that: the *Masser–Oesterlé ABC – Conjecture* implies infinitude of non-Wieferich primes.

In [9], D. Mirimanoff showed that [Theorem 1.1](#) is true when the base 2 is replaced by 3. Currently, it is known that the base 2 can be replaced by any prime $a < 113$ [15] with the same conclusion as in [Theorem 1.1](#). In general, a Wieferich prime to base $a \in \mathbb{Z}_{\geq 2}$ is defined to be any prime p satisfying $a^{p-1} \equiv 1 \pmod{p^2}$. It is traditional to refer to “Wieferich primes to base 2” as Wieferich primes (without reference to the base).

So far, we have given a brief overview of the known results about classical Wieferich primes. In the proceeding sections, we shall discuss their Carlitz module analogues as well as some algorithms for their computation.

2. The Carlitz module and Carlitz polynomials

Let p be a prime number, q be a p -power, $A := \mathbb{F}_q[T]$, $k := \mathbb{F}_q(T)$ and K be a fixed algebraic closure of k . For each $a \in A - \{0\}$, the absolute value of a is defined to be $|a| := \#(A/aA) = q^{\deg(a)}$ and $|0| := 0$. By a prime P in A , we shall mean P is a monic irreducible polynomial in A . For the commutative A -algebra K , let τ be the q th-power Frobenius mapping, i.e., $x \mapsto x^q$ for all $x \in K$. Let $A\{\tau\}$ be an A -submodule generated by τ^i , $i = 0, 1, 2, \dots$. Then $A\{\tau\}$ forms a ring (the twisted polynomial ring with coefficients

in A) with usual addition and multiplication with commutation relation $\tau a = a^q \tau$ for all $a \in A$. In fact, $A\{\tau\}$ is equal to the endomorphism ring $\text{End}_{\mathbb{F}_q}(K)$ of the additive group K over $\mathbb{F}_q$. Through the endomorphism τ , the ring $A\{\tau\}$ is isomorphic to the ring of additive polynomials with coefficients in A . The $\mathbb{F}_q$ -linear ring homomorphism $\rho : A \rightarrow A\{\tau\}$ characterised by $1 \mapsto \tau^0$ and $T \mapsto \rho_T = \tau + T\tau^0$ is called the *Carlitz A -module homomorphism*. The pair $(K, \rho) =: \mathcal{C}$ with multiplication $m * w = \rho_m(w)$ for all $m \in A$ and $w \in K$ is called the *Carlitz A -module on K* . This is sometimes called the *Carlitzification of K* . To each $N \in A - \{0\}$, ρ associates an additive polynomial $\rho_N(x)$ given by $\rho_N(x) := \rho_N(\tau)(x)$ in $A[x]$, called the *Carlitz N -polynomial*.

Through the ring homomorphism ρ , K is endowed with a new A -module structure with multiplication defined as: for any $\alpha \in K$ and $N \in A$, we have $N * \alpha = \rho_N(\alpha)$. For any $N \in A - \{0\}$, $\Lambda_N := \{\lambda \in K : N * \lambda = 0\}$ is the set of *Carlitz N -torsion points*. It coincides with the set of zeros of $\rho_N(x)$. Through ρ , the set $\Lambda_N \subset K$ is endowed with an A -module structure (inherits an A -module structure from K) isomorphic to A/NA , a cyclic A -module (with usual multiplication) [12, Proposition 12.4]. Therefore, Λ_N is a cyclic A -module and its generators (as an A -module) are the *primitive Carlitz N -torsion points*. We define the Carlitz N th cyclotomic polynomial to be the polynomial $\Phi_N(x)$ whose roots are the primitive Carlitz N -torsion points. The polynomials $\rho_N(x)$ and $\Phi_N(x)$ have degrees $|N|$ and $\varphi(N)$ respectively, where $\varphi(N) := \#(A/NA)^\times$. From now on, we shall restrict N to prime polynomials in A . For details on the elementary properties of $\rho_N(x)$ and $\Phi_N(x)$, see [2] and [3]. For an explicit discussion of arithmetic in the Carlitz module, see [7, Chapter 3], [12, Chapter 12] and [4].

Lemma 2.1. *Let P be a prime in A . The coefficients of $\rho_P(x) - x^{|P|}$ are divisible by P .*

Proof. We have $\rho_P(x) = x \cdot \Phi_P(x)$ since $\rho_P(x)$ is separable over K and 0 is the only non-primitive Carlitz P -torsion point. [12, Corollary to Proposition 12.7] implies that $\Phi_P(x)$ is Eisenstein at P , hence the result. $\square$

Corollary 2.2 (*Carlitz–Fermat Theorem*). *Let P be a prime in A . For each $a \in A$, we have $\rho_{P-1}(a) \equiv 0 \pmod{P}$.*

3. Carlitz analogue of the first case of Fermat’s Last Theorem

Let $N \in A - \mathbb{F}_q$ ($\mathbb{F}_q$ considered as a subset of A). In [6, page 2], D. Goss defined the following polynomials,

$$\mathcal{P}_N(x, y) := y^{|N|} \rho_N\left(\frac{x}{y}\right), \quad (1)$$

$$\mathcal{P}_N(x, y, z) := \mathcal{P}_N(x, y) - z^{|N|}. \quad (2)$$

We call $\mathcal{P}_N(x, y, z) = 0$, the *homogeneous geometric Fermat equation*. In ([5], Theorems 1, 2, 3 and 4), L. Denis established Fermat's Last Theorem for this type of equation. From Denis' result, we extract [Statement 3.1](#).

Statement 3.1 (*Analogue of the first case of Fermat's Last Theorem*). Let $q > 2$ and P be a prime with $\deg(P) > 1$. For any $(x, y, z) \in A^3$ with $P \nmid xyz$, $\mathcal{P}_P(x, y, z) \neq 0$; (and for $q = 2$, we must have $\deg(P) > 2$).

Theorem 3.2. If [Statement 3.1](#) is false for the prime $P \in A$, then there exists an $a \in A$ coprime to P such that

$$\rho_P(a) \equiv a^{|P|} \pmod{P^2}.$$

Proof. If [Statement 3.1](#) is false for the prime $P \in A$, then there exists $(x, y, z) \in A^3$ with P coprime to xyz such that $\mathcal{P}_P(x, y, z) = 0$. It suffices to consider $x, y, z \not\equiv 0 \pmod{P}$. Let $x_1 = z^{-1}x$ and $y_1 = z^{-1}y \in k^\times$, then

$$\begin{aligned} 0 &= z^{-|P|} \mathcal{P}_P(x, y, z) = (z^{-1}y)^{|P|} \rho_P\left(\frac{x}{y}\right) - 1 = \mathcal{P}_P(z^{-1}x, z^{-1}y) - 1 \\ &= y_1^{|P|} \rho_{P^{-1}}\left(\frac{x_1}{y_1}\right) + x_1 y_1^{|P|-1} - 1 \equiv x_1 - 1 \pmod{P}. \end{aligned}$$

So $x_1 = 1 + cP$, the denominator of $c \in k^\times$ is coprime to P . Considering $\mathcal{P}_P(x, y, z) = 0$ modulo P^2 yields

$$\begin{aligned} \mathcal{P}_P(x_1, y_1) - 1 &= y_1^{|P|} \rho_P\left(\frac{1 + cP}{y_1}\right) - 1 \\ &\equiv y_1^{|P|} \rho_P\left(\frac{1}{y_1}\right) - 1 \pmod{P^2}. \end{aligned}$$

So $y_1^{|P|} \rho_P\left(\frac{1}{y_1}\right) \equiv 1 \pmod{P^2}$. Since y_1 has no factor of P either in numerator or denominator, so is $\frac{1}{y_1}$ which makes sense modulo P^2 . So a , (where a is a representative of the equivalence class of $\frac{1}{y_1}$ modulo P^2) is coprime to P , hence, $\rho_P(a) \equiv a^{|P|} \pmod{P^2}$. $\square$

Remark 3.3. [Theorem 3.2](#) is a weak analogue to the mixed bag of results due to A. Wieferich, D. Mirimanoff, etc. The classical results are stronger than [Theorem 3.2](#) because each of them implies a fixed base a .

Remark 3.4. If $a = 1$, then D. Thakur's definition of c -Wieferich primes [[16](#), page 6] is obtained.

4. Carlitz Wieferich primes in $\mathbb{F}_q[T]$

[Theorem 3.2](#) motivates the following definition for Carlitz Wieferich primes in $\mathbb{F}_q[T]$.

Definition 4.1. Let $a \in A - \{0\}$, a c-Wieferich prime (or Carlitz–Wieferich prime) to base a is a prime P in A coprime to a and satisfying $\rho_P(a) \equiv a^{|P|} \pmod{P^2}$. If $a \in \mathbb{F}_q^\times$, then P is called a c-Wieferich prime. A non-c-Wieferich prime to base a is any prime P that is not c-Wieferich to base a , i.e., $\rho_P(a) \not\equiv a^{|P|} \pmod{P^2}$.

We will often use the congruence $\rho_{P-1}(1) \equiv 0 \pmod{P^2}$ to define c-Wieferich primes in A . In general, D. Thakur proved that, if a is a p th power, then $\rho_P(a) \equiv a^{|P|} \pmod{P^2}$ is equivalent to $\rho_{P-1}(a) \equiv 0 \pmod{P^2}$, [\[18, Theorem 1\]](#). The congruence $\rho_{P-1}(1) \equiv 0 \pmod{P^2}$ is simple but messy when unpacked. It is for this reason, that we derive congruences easier to work with in order to study properties of c-Wieferich primes.

We shall use the following standard notation for A . For each $i \in \mathbb{Z}_{\geq 1}$, $[i] := T^{q^i} - T$, $L_i := [i][i-1] \cdots [1]$ and $D_i := [i][i-1]^q \cdots [1]^{q^{i-1}}$. The symbol $[i]$ represents the product of primes of degree dividing i , whereas L_i is the least common multiple of monic polynomials of degree i and D_i is the product of all monic polynomials of degree i . These follow from Carlitz’s results, the references [\[7, Proposition 3.1.6\]](#) and [\[17, page 44\]](#) are just convenient. We think of the symbol $[0]$ as an empty product and define it as $[0] := 1$. Similarly $L_0 = D_0 = 1$.

Let $i \in \mathbb{Z}_{\geq 1}$, define A_{i+} to be the set of monic polynomials of degree i and define $A_{0+} := \{1\}$, i.e., we consider the constant polynomial 1 to be a monic polynomial. Furthermore, for each $i \in \mathbb{Z}_{\geq 0}$, set

$$S_i := \frac{(-1)^i}{L_i} = \sum_{a \in A_{i+}} \frac{1}{a}. \quad (3)$$

The second equality in Equation [\(3\)](#) follows from Carlitz’s result. Define F_i as

$$\frac{F_i}{L_i} := \sum_{j=0}^i S_j.$$

Lemma 4.2. F_i satisfies the following recurrence relation; $F_0 = 1$ and $F_{i+1} = (-1)^{i+1} + [i+1]F_i$ for $i \in \mathbb{Z}_{\geq 0}$.

Proof. Since $L_0 = 1$, it follows from Equation [\(3\)](#) that $S_0 = 1$ and so $F_0 = 1$. For any $i \in \mathbb{Z}_{\geq 0}$, we have

$$\frac{F_{i+1}}{L_{i+1}} = \sum_{j=0}^{i+1} \frac{(-1)^j}{L_j} = \frac{(-1)^{i+1}}{L_{i+1}} + \sum_{j=0}^i \frac{(-1)^j}{L_j} = \frac{(-1)^{i+1}}{L_{i+1}} + \frac{F_i}{L_i}.$$

Multiplying both sides by L_{i+1} yields $F_{i+1} = (-1)^{i+1} + [i+1]F_i$. $\square$

It is not difficult to show that F_i is a monic polynomial in A and its degree is $\frac{q(q^i-1)}{q-1}$ (where $i \in \mathbb{Z}_{\geq 0}$).

Proposition 4.3. *Let P be a prime in A . P is a c -Wieferich prime if and only if $F_{\deg(P)-1} \equiv 0 \pmod{P}$.*

Proof. From [7, Proposition 3.3.10], we have that $\rho_P(1) = \sum_{i=0}^{\deg(P)} a_{P,i}$, where $a_{P,0} = P$, $a_{P,\deg(P)} = 1$ and $[i]a_{P,i} = a_{P,i-1}^q - a_{P,i-1}$ for $i = 1, \dots, \deg(P)$. This implies that $a_{P,i} \equiv 0 \pmod{P}$ for $i = 0, \dots, \deg(P) - 1$. For $i = 0, \dots, \deg(P) - 1$, we have $[i]a_{P,i} \equiv -a_{P,i-1} \pmod{P^2}$ and thence $L_i a_{P,i} \equiv (-1)^i a_{P,0} \pmod{P^2}$. So

$$\begin{aligned} \rho_{P-1}(1) &= \left(-1 + \sum_{i=0}^{\deg(P)} a_{P,i} \right) \equiv \left(a_{P,0} \sum_{i=0}^{\deg(P)-1} \frac{(-1)^i}{L_i} \right) \equiv P \sum_{i=0}^{\deg(P)-1} S_i \\ &\equiv P \frac{F_{\deg(P)-1}}{L_{\deg(P)-1}} \pmod{P^2}. \end{aligned}$$

Since $L_{\deg(P)-1} \not\equiv 0 \pmod{P}$, the proposition follows. $\square$

Remark 4.4. Proposition 4.3 is analogous to the following classical statement: “a prime p is a Wieferich prime if and only if it divides the numerator of $\frac{1}{2} \sum_{i=1}^{\frac{\varphi(p)}{2}} \frac{1}{i}$ ”, [11, page 216]. This is attributed to J. Sylvester.

Corollary 4.5. *There are no c -Wieferich primes in A of degree 1.*

Proof. Let P be an arbitrary prime in A of 1. Then $F_{\deg(P)-1} = F_0 = 1 \not\equiv 0 \pmod{P}$. It follows from Proposition 4.3 that P can not be a c -Wieferich prime in A . $\square$

Theorem 4.6. *Every c -Wieferich prime in A also satisfies the congruence $\rho_{P-1}(T) \equiv 0 \pmod{P^2}$.*

To prove Theorem 4.6, we shall need the following results.

Lemma 4.7 (Wilson’s Theorem, [12, Corollary 2, page 6]).

$$\prod_{\substack{a \in A - \{0\}, \\ \deg(a) < \deg(P)}} a \equiv -1 \pmod{P}. \quad (4)$$

Lemma 4.8. *Let P be a prime in A of degree n and P' denote its formal derivative with respect to T . Then*

$$P' \equiv (-1)^{n-1} L_{n-1} \pmod{P}.$$

Proof. To prove this congruence, we compute the derivative of D_n with respect to T , reduce it modulo P in two different ways and relate the results. Using the definition of D_n and reduction modulo P gives

$$P^{-1}D_n \equiv \prod_{\substack{a \in A - \{0\}, \\ \deg(a) < \deg(P)}} a \stackrel{\text{Lemma 4.7}}{\equiv} -1 \pmod{P}.$$

So $D_n \equiv -P \pmod{P^2}$. Differentiating $D_n \equiv -P \pmod{P^2}$ with respect to T yields $D'_n \equiv -P' \pmod{P}$. On the other hand, $D_n = [n][n-1]^q \cdots [1]^{q^{n-1}} = [n]D_{n-1}^q$. Differentiation with respect to T yields

$$\begin{aligned} D'_n &= -D_{n-1}^q = -[n-1]^q \cdots [1]^{q^{n-1}} = -([n] - [1]) \cdots ([n] - [n-1]) \\ &\equiv (-1)^n L_{n-1} \pmod{P}. \end{aligned}$$

Combining the two congruences, we get $-P' \equiv (-1)^n L_{n-1} \pmod{P}$ and we are done. $\square$

Proof of Theorem 4.6. Now $\rho_P(T) = \sum_{i=0}^n a_{P,i} T^{q^i}$, where $a_{P,0} = P, a_{P,n} = 1$ and $[i]a_{P,i} = a_{P,i-1}^q - a_{P,i-1}$. Differentiating $[i]a_{P,i} = a_{P,i-1}^q - a_{P,i-1}$, $i \leq i \leq n$ with respect to T , followed by reduction modulo P yields $[i]a'_{P,i} \equiv -a'_{P,i-1} \pmod{P}$. This implies $L_i a'_{P,i} \equiv (-1)^i a'_{P,0} \pmod{P}$ and $a'_{P,i} \equiv a'_{P,0} S_i \pmod{P}$. So,

$$\begin{aligned} (\rho_{P-1}(T))' &= \left(-T + \sum_{i=0}^n a_{P,i} T^{q^i} \right)' \equiv \left(-1 + \sum_{i=0}^{n-1} a'_{P,i} T^{q^i} \right) \equiv \left(-1 + P' \sum_{i=0}^{n-1} S_i T^{q^i} \right) \\ &\equiv \left(-1 + P'T + P' \left(\sum_{i=1}^{n-1} T S_i - S_{i-1} \right) \right) \\ &\equiv \left(-1 + P' \left(T S_{n-1} + (T-1) \sum_{i=0}^{n-2} S_i \right) \right) \\ &\equiv \left(-1 + P' \left(S_{n-1} + (T-1) \sum_{i=0}^{n-1} S_i \right) \right) \stackrel{\text{Lemma 4.8}}{\equiv} (T-1)P' \sum_{i=0}^{n-1} S_i \\ &\equiv 0 \pmod{P}, \end{aligned}$$

by assumption, and $\rho_{P-1}(T) \equiv 0 \pmod{P^2}$. $\square$

Remark 4.9. For any prime P in A , $\rho_{P-1}(T) \equiv 0 \pmod{P^2}$ if and only if $F_{\deg(P)-1} \equiv 0 \pmod{P}$.

Corollary 4.10. With the exception of T and $T+1$, all the primes in $\mathbb{F}_2[T]$ are c -Wieferich primes.

Proof. First, we show by induction on $n \in \mathbb{Z}$, that $[1]F_{n-1} = [n]$ for $n \geq 1$ and $q = 2$. For $n = 1$, we have $[1]F_0 = [1]$. Assume for $n = i \in \mathbb{Z}_{\geq 1}$, we have $[1]F_{i-1} = [i]$. We now show that $[1]F_i = [i+1]$. We have the following calculation,

$$[1]F_i = [1]((-1)^i + [i]F_{i-1}) = [1] + [1][i]F_{i-1} = [1] + [i]^2 = [1] + [i+1] + [1] = [i+1].$$

So $F_{n-1} \equiv [1]^{-1}[n] \equiv 0 \pmod{Q_n}$, where Q_n is an arbitrary monic irreducible polynomial of degree n . Therefore, all primes in $\mathbb{F}_2[T]$ of degree > 1 are c-Wieferich primes. $\square$

Remark 4.11. Corollary 4.10 was first observed and proved by D. Thakur [18, page 6].

5. Characterising c-Wieferich primes in $\mathbb{F}_p[T]$

Lemma 5.1. Let $\alpha \in \mathbb{F}_p^\times$ and $n \in \mathbb{Z}_{>0}$. Then $f = T^p - T - \alpha$ is a prime in $\mathbb{F}_p[T]$ and $[n] \equiv n\alpha \pmod{f}$.

Proof. f is an Artin Schreier polynomial for $\mathbb{F}_p[T]$, and these are well known for being irreducible over $\mathbb{F}_p$, [8, Corollary 3.79]. Lastly, we have $[n] = (T^p - T)^{p^{n-1}} + (T^p - T)^{p^{n-2}} + \dots + (T^p - T)^{p^0} \equiv n\alpha \pmod{f}$. $\square$

Let $n \in \mathbb{Z}_{\geq 0}$ and x be an indeterminate. Define $s_n(x) := \sum_{i=0}^n \frac{x^i}{i!}$. We have the following existence result.

Proposition 5.2 (*c-Wieferich primes horizontal existence criterion*). Let p be a prime. If there exists an $\alpha \in \mathbb{F}_p^\times$ such that $s_{p-1}(-\alpha^{-1}) = 0$, then $T^p - T - \alpha$ is a c-Wieferich prime in $\mathbb{F}_p[T]$.

Proof. Fix $\alpha \in \mathbb{F}_p^\times$ and define u_n by, $u_0 = 1$, $u_n = (-1)^n + n\alpha u_{n-1}$ for $1 \leq n < p$. Then,

$$\begin{aligned} \frac{u_n}{n!\alpha^n} &= \frac{(-1)^n}{n!\alpha^n} + \frac{u_{n-1}}{(n-1)!\alpha^{n-1}} = \frac{(-1)^n}{n!\alpha^n} + \frac{(-1)^{n-1}}{(n-1)!\alpha^{n-1}} + \frac{u_{n-2}}{(n-2)!\alpha^{n-2}} = \dots \\ &= \sum_{i=0}^n \frac{(-1)^i}{i!\alpha^i} = s_n(-\alpha^{-1}). \end{aligned}$$

So $u_{p-1} = -s_{p-1}(-\alpha^{-1})$. Now $F_n = (-1)^n + [n]F_{n-1} \equiv (-1)^n + n\alpha F_{n-1} \pmod{T^p - T - \alpha}$ for $n \geq 1$ and $F_0 = 1$. So $u_n \equiv F_n \pmod{T^p - T - \alpha}$. Therefore, if $s_{p-1}(-\alpha^{-1}) = 0$, then $u_{p-1} \equiv F_{p-1} \equiv 0 \pmod{T^p - T - \alpha}$, where $T^p - T - \alpha$ is an Artin Schreier prime in $\mathbb{F}_p[T]$. The result follows from Proposition 4.3. $\square$

Remark 5.3. Proposition 5.2 is a horizontal existence result because, we vary p to give a criterion for c-Wieferich primes in $\mathbb{F}_p[T]$, as opposed to searching c-Wieferich primes of higher degrees in $\mathbb{F}_p[T]$ for a fixed p . D. Thakur pointed out to the author that he had also discovered the same existence result [18, Pages 8, 11].

The description below is experimental and no proofs are available at the moment. Computations indicate that about 66% of the primes $p < 10^7$ satisfy the congruence in [Proposition 5.2](#). This motivates us to ask:

1. Are there infinitely many primes p_1 such that $s_{p_1-1}(\alpha) = 0$ for some $\alpha \in \mathbb{F}_{p_1}^\times$?
2. Are there infinitely many primes p_2 such that $s_{p_2-1}(\beta) \neq 0$ for all $\beta \in \mathbb{F}_{p_2}^\times$?

The examples of c-Wieferich primes obtained by the horizontal existence result above all have a property that they are invariant under the translation automorphisms of $\mathbb{F}_p[T]$. This turns out to be an important property characterising many c-Wieferich primes in $\mathbb{F}_p[T]$. In the subsequent results, we explore this in detail.

Suppose $m \in \mathbb{F}_p[T]$, we say m is an $\mathbb{F}_p$ -fixed ($\mathbb{F}_p$ -translation invariant) polynomial if $m(T+i) = m(T)$ for any $i \in \mathbb{F}_p$. Equivalently, m is $\mathbb{F}_p$ -fixed if $m(T+1) = m(T)$. Since $\#\mathbb{F}_p$ is a prime p , $\mathbb{F}_p$ is the only non-trivial subgroup of $\mathbb{F}_p$, the term *fixed polynomial* in $\mathbb{F}_p[T]$ will be used to mean $\mathbb{F}_p$ -fixed polynomials in $\mathbb{F}_p[T]$. On the other hand, we say $m \in \mathbb{F}_p[T]$ is non-fixed if $m(T+1) \neq m(T)$, for example $m = T$.

Proposition 5.4. *Let $f \in \mathbb{F}_p[T]$, then f is a fixed polynomial if and only if $f = g([1])$ for some $g \in \mathbb{F}_p[T]$.*

Proof. ($\Leftarrow$) This follows immediately from the fact that $[1]$ is fixed. ($\Rightarrow$) For the converse statement, assume f is a monic fixed polynomial of degree n and define $f_0 := f$. Then f_0 is fixed implies $g_1 = f_0 - f_0(0)$ is also fixed. Moreover, T divides g_1 since $g_1(0) = 0$. Since g_1 is fixed, g_1 is divisible by all the translates $T + \alpha$, $\alpha \in \mathbb{F}_p$ and so, $[1]$ divides g_1 . Let $f_1 = [1]^{-s}g_1$, where s is the number of times T divides g_1 , then repeat the procedure. Since f is a polynomial, this procedure terminates (after at most n steps). Looking at the sequence of operations in reverse reveals that f is a polynomial in $[1]$. $\square$

Remark 5.5. The precise formulation of [Proposition 5.4](#) is due to A. Keet and D. Thakur.

Corollary 5.6. *If m is a fixed polynomial in $\mathbb{F}_p[T]$, then its degree is divisible by p .*

A prime $P \in \mathbb{F}_p[T]$ is a fixed c-Wieferich prime if in addition to being a fixed polynomial, it is also a c-Wieferich prime (or vice versa). A non-fixed c-Wieferich prime in $\mathbb{F}_p[T]$ is a c-Wieferich prime that is not $\mathbb{F}_p$ -fixed.

Theorem 5.7. *There are infinitely many fixed prime polynomials in $\mathbb{F}_p[T]$.*

Proof. Let $m \in \mathbb{F}_p[T]$ and $\text{orb}(m) = \{m(T+i) : i \in \mathbb{F}_p\}$. Since $\mathbb{F}_p$ is a cyclic group of order p , where p is a prime, $|\text{orb}(m)|$ is either 1 or p . An $m \in \mathbb{F}_p[T]$ is fixed if and only if $\#\text{orb}(m) = 1$. Let $\pi_{\mathbb{F}_p[T]}(s)$ be the number of primes in $\mathbb{F}_p[T]$ of degree s . If $\pi_{\mathbb{F}_p[T]}(s) \not\equiv 0 \pmod{p}$, then there is a fixed prime $P \in \mathbb{F}_p[T]$. Let n be a positive integer, $w > 0$ and suppose that $p^w \parallel n$, say $n = p^w n_0$. By Gauss' formula, we have

$$\pi_{\mathbb{F}_p[T]}(n) = \frac{1}{n} \sum_{d|n} \mu(d) p^{\frac{n}{d}} = \frac{1}{n_0} \sum_{d|n} \mu(d) p^{\frac{n}{d}-w} \equiv -\frac{\mu(\frac{n}{w})}{n_0} \not\equiv 0 \pmod{p},$$

if and only if $\frac{n}{w}$ is a squarefree positive integer. We obtain fixed primes whenever p is odd, $w = 1$ and n_0 square-free or $p = 2$, n is $2n_0$ or $4n_0$ and n_0 is square-free. $\square$

For a generalised result of [Theorem 5.7](#) and count of fixed primes in $\mathbb{F}_p[T]$, refer to [\[10, Theorem 3.1.32\]](#).

Remark 5.8. Although $F_n \in \mathbb{F}_p[T]$ is an $\mathbb{F}_p$ -fixed polynomial, not all of its prime factors are actually fixed primes. Take for example, F_3 as an element of $\mathbb{F}_2[T]$ or as an element of $\mathbb{F}_3[T]$.

We also state and prove [Lemma 5.9](#) which will be important in the proof of [Theorem 5.10](#).

Lemma 5.9. *Every fixed prime in $\mathbb{F}_p[T]$ is a product of Artin Schreier primes in $\mathbb{F}_{p^s}[T]$ for some $s > 0$.*

Proof. Let $f \in \mathbb{F}_p[T]$ be a fixed prime of degree ps , where $s \geq 1$ and $\alpha \in \mathbb{F}_{p^{ps}}$ be a root of f but not in any $\mathbb{F}_{p^{ps}}$ sub-extensions. Since f is irreducible over $\mathbb{F}_p$ of degree ps , we have $\mathbb{F}_{p^{ps}} := \mathbb{F}_p(\alpha)$ is the splitting field of f over $\mathbb{F}_p$. Since f is fixed, for any chosen root $\alpha \in \mathbb{F}_{p^{ps}}^\times$, of f , $\alpha + \mathbb{F}_p$ is a subset of roots of f . Consider

$$g = \prod_{j \in \{0, 1, \dots, p-1\}} (T - (\alpha + j)) = (T - \alpha)^p - (T - \alpha) = T^p - T - \alpha^p + \alpha.$$

$\alpha^p - \alpha \in \mathbb{F}_{p^{ps}}^\times$ but is no longer primitive. This is because there is an automorphism σ of $\mathbb{F}_{p^{ps}}$ such that $\sigma(\alpha) = \alpha + 1$. The product is fixed by the action of the subgroup $\langle \sigma \rangle$ of $\text{Gal}(\mathbb{F}_{p^{ps}}/\mathbb{F}_{p^s})$, a subgroup which has p elements. Therefore, $\langle \sigma \rangle = \text{Gal}(\mathbb{F}_{p^{ps}}/\mathbb{F}_{p^s})$ and the result follows, i.e., $\text{Norm}_{\mathbb{F}_{p^{ps}}/\mathbb{F}_{p^s}}(\alpha) = (-1)^p \prod_{j=0}^{p-1} (\alpha + j) = -\alpha^p + \alpha \in \mathbb{F}_{p^s} \subset \mathbb{F}_{p^{ps}}$. Since $s \geq 1$ and $\mathbb{F}_{p^{ps}} = \mathbb{F}_p(\alpha)$, we have $\text{Tr}_{\mathbb{F}_{p^{ps}}/\mathbb{F}_p}(\alpha^p - \alpha) \neq 0$. This is because for g to be irreducible in $\mathbb{F}_{p^s}[T]$, we need $\alpha^p - \alpha \in \mathbb{F}_{p^s}^\times$, which follows from the norm above, and then the fact that g has no roots in $\mathbb{F}_{p^s}$, which is clear by construction. Therefore, g is an Artin Schreier polynomial (prime in $\mathbb{F}_{p^s}[T]$) dividing f . All the other roots yield the same conclusion, hence the required result. $\square$

Let E, F be finite fields. E/F is Galois and its Galois group $\text{Gal}(E/F)$ is cyclic with the Frobenius $(x \mapsto x^{\#F})$ as its generator. An $\alpha \in E$ is normal over F if $\{\sigma(\alpha) : \sigma \in \text{Gal}(E/F)\}$ is a basis of E as an F -vector space. [Theorem 5.10](#) shows that fixed c-Wieferich primes factor into Artin Schreier primes in $\mathbb{F}_{p^s}[T]$ for some $s > 0$.

Theorem 5.10. *Existence of a fixed c-Wieferich prime of degree ps in $\mathbb{F}_p[T]$ is equivalent to the existence of an element $\alpha \in \mathbb{F}_{p^s}$ normal over $\mathbb{F}_p$ with $\text{Tr}_{\mathbb{F}_{p^s}/\mathbb{F}_p}(\alpha) \neq 0$ such that $F_{ps-1} \equiv 0 \pmod{T^p - T - \alpha}$.*

Proof. ($\Leftarrow$) Given $F_{ps-1} \equiv 0 \pmod{T^p - T - \alpha}$, we have $F_{ps-1} = (T^p - T - \alpha)g$, for some monic polynomial $g \in \mathbb{F}_{p^s}[T]$. Since $\alpha \in \mathbb{F}_{p^s}$ is normal over $\mathbb{F}_p$, the absolute trace of α over $\mathbb{F}_p$ is nonzero. By [8, Corollary 3.79], $T^p - T - \alpha$ is irreducible over $\mathbb{F}_p$. For each automorphism $\sigma \in \text{Gal}(\mathbb{F}_{p^s}/\mathbb{F}_p)$, $\sigma(\alpha)$ is a conjugate to α , so

$$\begin{aligned} F_{ps-1} &= \sigma(F_{ps-1}) = \sigma(T^p - T - \alpha)\sigma(g) = (T^p - T - \sigma(\alpha))\sigma(g) \\ &\equiv 0 \pmod{T^p - T - \sigma(\alpha)}. \end{aligned}$$

Let $Q_{ps} = (T^p - T - \alpha_1) \cdots (T^p - T - \alpha_s)$, where α_i are α -conjugates; so $F_{ps-1} \equiv 0 \pmod{Q_{ps}}$. The coefficients of Q_{ps} are invariant under $\text{Gal}(\mathbb{F}_{p^s}/\mathbb{F}_p)$ which implies $Q_{ps} \in \mathbb{F}_p[T]$. Since the $\alpha_i \in \mathbb{F}_{p^s}$ are normal over $\mathbb{F}_p$, Q_{ps} is irreducible over $\mathbb{F}_p$ and has degree ps . By Proposition 4.3, Q_{ps} is a fixed c-Wieferich prime.

($\Rightarrow$) Let f be a fixed c-Wieferich prime of degree ps . By Lemma 5.9, f factors into s distinct polynomials $T^p - T - \alpha$, where $\text{Tr}_{\mathbb{F}_{p^s}/\mathbb{F}_p}(\alpha) \neq 0$ and $\alpha \in \mathbb{F}_{p^s}$ is normal over $\mathbb{F}_p$. So $F_{ps-1} \equiv 0 \pmod{T^p - T - \alpha}$. $\square$

We hope the above results can be extended to $\mathbb{F}_q$. However, preliminary results suggest that this comes at a cost, the notion of $\mathbb{F}_p$ -fixed is replaced by G -fixed polynomials, where G is a (non-trivial) subgroup of $\mathbb{F}_q$.

6. Computing Carlitz Wieferich primes in $\mathbb{F}_p[T]$

In this section, we present two algorithms for computing fixed c-Wieferich primes in $\mathbb{F}_p[T]$, highlight some new examples, open questions. We use Proposition 4.3 to develop Algorithm 1 which is used to compute the product of c-Wieferich primes to a prescribed degree. Algorithm 1 has an input as p – the number of elements in $\mathbb{F}_p$, (the algorithm works for general q) and n – the degree of the c-Wieferich primes; and outputs the product of c-Wieferich primes of degree dividing n . In step 1, F is initialised at $F_0 = 1$, in step 2, the algorithm recursively computes F_i up to F_{n-1} . In step 3, it computes the gcd of F_{n-1} and $[n]$.

Algorithm 1 Computing c-Wieferich primes I.

Input: p – the size of $\mathbb{F}_p$, and n – degree of the c-Wieferich prime required.

Output: Product of c-Wieferich primes of degree dividing n .

1. $F \leftarrow 1$ and $\mathcal{F}$ is an empty list.

2. for $i = 1$ to $n - 1$

$$F \leftarrow (-1)^i + (T^{p^i} - T)F$$

3. $\mathcal{F} \leftarrow (T^{p^n} - T, F) // \text{gcd of } [n] \text{ and } F_{n-1}, \text{ the product of c-Wieferich primes of degree dividing } n.$

Return: $\mathcal{F}$

Table 1
c-Wieferich primes in $\mathbb{F}_3[T]$ and $\mathbb{F}_5[T]$.

q	Degree bound	c-Wieferich primes P
3	18	$T^6 + T^4 + T^3 + T^2 + 2T + 2$, $T^9 + T^6 + T^4 + T^2 + 2T + 2$, $T^{12} + 2T^{10} + T^9 + 2T^4 + 2T^3 + T^2 + 1$
5	15	$T^5 + 4T + 1$ and $T^{10} + 3T^6 + 4T^5 + T^2 + T + 1$
7	10	$T^7 + 6T + 3$

Table 2
Elements in sub-extensions of $\overline{\mathbb{F}_3}$ normal over $\mathbb{F}_3$ and the corresponding c-Wieferich primes.

s	$f_{\min}^t(x)$	Non-conjugate elements of $\alpha \in \mathbb{F}_{3^s}$ normal over $\mathbb{F}_3$	c-Wieferich primes P
1	–	–	–
2	$x^2 + 2x + 2$	$\{2t, t + 2\}$	$T^6 + T^4 + T^3 + T^2 + 2T + 2$
3	$x^3 + 2x + 1$	$\{t^2, t^2 + t + 1, t^2 + 2t + 1\}$	$T^9 + T^6 + T^4 + T^2 + 2T + 2$
4	$x^4 + 2x^3 + 2$	$\{t^3 + t^2 + t + 2, 2t^3 + 2t^2 + 2t + 2,$ $t^3 + t^2 + 2, 2t^3 + 2t^2\}$	$T^{12} + 2T^{10} + T^9 + 2T^4 + 2T^3 + T^2 + 1$
5	$x^5 + 2x + 1$	$\{t^3 + 2t^2 + 2t + 1, 2t^4 + 2t^3 + 2t,$ $2t^4 + t^2, t^3 + t^2 + 1, 2t^4 + 2t^3 + 2t^2 + 2t\}$	$T^{15} + T^{13} + T^{12} + T^{11} + 2T^{10} + 2T^7$ $+ 2T^5 + 2T^4 + T^3 + T^2 + T + 1$
6	–	–	–

We implemented Algorithm 1 in SAGE [14] on a 32-bit duo-core Intel microprocessor with 2GB of RAM. We present our results in Table 1. We have highlighted (in blue) the examples of new c-Wieferich primes.

The first shortcoming of Algorithm 1 is that it requires a lot of computation memory due to the astronomical growth in the degrees of the polynomials involved. This makes gcd storage hard and computation very slow.

We used Theorem 5.10 to develop Algorithm 2, a better scheme for large degree c-Wieferich primes in $\mathbb{F}_p$.

Algorithm 2 Computing fixed c-Wieferich primes.

Input: p, s , and W , the list of non-conjugate elements of $\mathbb{F}_{p^s}$ normal over $\mathbb{F}_p$.
Output: List of fixed c-Wieferich primes of degree ps .
1. $F \leftarrow 1$, $\mathcal{F}$ and $\mathcal{W}$ are empty lists.
2. for α in W
 for $i = 1$ to $ps - 1$
 $F \leftarrow (-1)^i + i\alpha F$
 if $F = 0$
 $\mathcal{W} \leftarrow \alpha$
3. $w \leftarrow 1$.
4. for $i = 1$ to size of $\mathcal{W}$
 $w \leftarrow (T^p - T - W_i)w$ // W_i is the i th element in $\mathcal{W}$. (This computation occurs in $\mathbb{F}_{p^s}[T]$.)
5. $\mathcal{F} \leftarrow$ prime factors of w as an element in $\mathbb{F}_p[T]$. // (This computation occurs in $\mathbb{F}_p[T]$.)
Return: $\mathcal{F}$

Tables 2 and 3 show the first few fixed c-Wieferich primes in $\mathbb{F}_3[T]$ and $\mathbb{F}_5[T]$. In the third column(s) are the non-conjugate elements in subfields of $\overline{\mathbb{F}_p}$ normal over $\mathbb{F}_p$ that were used to compute c-Wieferich primes.

Table 3Elements in sub-extensions of $\mathbb{F}_5$ normal over $\mathbb{F}_5$ and the corresponding c-Wieferich primes.

s	$f_{\min}^t(x)$	Non-conjugate elements of $\alpha \in \mathbb{F}_{5^s}$ normal over $\mathbb{F}_5$	c-Wieferich primes P
1	$x + 1$	$\{4\}$	$T^5 + 4T + 1$
2	$x^2 + 4x + 2$	$\{2t + 2, 3t + 4\}$	$T^{10} + 3T^6 + 4T^5 + T^2 + T + 1$
3	$x^3 + 3x + 3$	—	—
4	$x^4 + 4x^2 + 4x + 2$	$\{t^3 + t^2 + 4, 3t^3 + 3t^2 + t + 4, t + 4, t^3 + t^2 + 3t + 4\}$	$T^{20} + T^{16} + 4T^{15} + T^{12} + 3T^{11} + T^8 + 2T^7 + T^5 + T^4 + T^3 + 4T + 1$
5,6	—	—	—

Table 4c-Wieferich primes in $\mathbb{F}_p[T]$ for small degree and $p \in \{3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37\}$.

p	Degree bound	Fixed c-Wieferich primes P
3	30	$T^6 + T^4 + T^3 + T^2 + 2T + 2, T^9 + T^6 + T^4 + T^2 + 2T + 2,$ $T^{12} + 2T^{10} + T^9 + 2T^4 + 2T^3 + T^2 + 1$ and $T^{15} + T^{13} + T^{12} + T^{11} + 2T^{10} + 2T^7 + 2T^5 + 2T^4 + T^3 + T^2 + T + 1$
5	30	$T^5 + 4T + 1, T^{10} + 3T^6 + 4T^5 + T^2 + T + 1$ and $T^{20} + T^{16} + 4T^{15} + T^{12} + 3T^{11} + T^8 + 2T^7 + T^5 + T^4 + T^3 + 4T + 1$
7	35	$T^7 + 6T + 3$ and $T^{14} + 5T^8 + 5T^7 + T^2 + 2T + 3$
11	44	$T^{11} + 10T + 4$ and $T^{33} + 8T^{23} + 4T^{22} + 3T^{13} + 3T^{12} + 10T^{11} + 10T^3 + 4T^2 + T + 4$
13	52	$T^{13} + 12T + 1$ and $T^{13} + 12T + 8,$
17	51	—
19	57	$T^{19} + 18T + 2$
23	69	—
29	87	$T^{58} + 27T^{30} + 15T^{29} + T^2 + 14T + 3$
31	93	$T^{31} + 30T + 20, T^{62} + 29T^{32} + 18T^{31} + T^2 + 13T + 2$ and $T^{93} + 28T^{63} + 16T^{62} + 3T^{33} + 30T^{32} + 24T^{31} + 30T^3 + 16T^2 + 7T + 30$
37	74	$T^{37} + 36T + 1, T^{37} + 36T + 7, T^{37} + 36T + 15, T^{37} + 36T + 21,$ $T^{74} + 35T^{38} + 12T^{37} + T^2 + 25T + 5$

We demonstrate how to compute the c-Wieferich prime $P = T^6 + T^4 + T^3 + T^2 + 2T + 2$ in $\mathbb{F}_3[T]$, (see line 2 of the Table 2). To determine fixed c-Wieferich primes of degree 6 in $\mathbb{F}_3[T]$ according to Theorem 5.10, we set the degree of the extension to be $s = 2$ and search all the elements of $\mathbb{F}_{3^2}$ normal over $\mathbb{F}_3$. For example, we used the quadratic field $\mathbb{F}_3(t)$ with $x^2 + 2x + 2$ as the minimal polynomial of t . Using SAGE [14], we found $\{2t, t + 2\}$ as the elements of $\mathbb{F}_{3^2}$ normal over $\mathbb{F}_3$ and satisfy the congruence in Theorem 5.10. Then $P = (T^3 - T - 2t)(T^3 - T - (t + 2)) = (T^3 - T)^2 - 2(T^3 - T) + 2t(t + 2) = T^6 + T^4 + T^3 + T^2 + 2T + 2$.

We implemented Algorithm 2 in SAGE [14] and our results are recorded in Table 4.

Question 6.1. Suppose $p > 2$. Are there finitely many fixed c-Wieferich primes in $\mathbb{F}_p[T]$?

Our calculations with Algorithms 1 and 2 show that for $p > 2$, many c-Wieferich primes in $\mathbb{F}_p[T]$ are fixed. The only examples of non-fixed c-Wieferich primes are in $\mathbb{F}_2[T]$. This motivates us to ask the following question.

Question 6.2. Suppose $q > 2$. Are there examples of non-fixed c-Wieferich primes in $\mathbb{F}_q[T]$?

The partial answer to [Question 6.2](#) is yes: for example, we considered the field $\mathbb{F}_{32}$ with a primitive element t such that $f_{\min}^t(x) = x^2 + 2x + 2$ is irreducible over $\mathbb{F}_3$. Using SAGE [\[14\]](#), we found that $P_0 = T^3 + (t+1)T + 1$ is one of the c-Wieferich primes in $\mathbb{F}_{32}[T]$. We let $G_1 = \{0, 1, 2\}$ and $G_2 = \{0, t+2, 2t+1\}$ both additive subgroups of $\mathbb{F}_{32}$ of order 3. It is easy to check that P_0 is invariant under translation by G_2 but not G_1 . So P_0 is a G_2 -fixed c-Wieferich prime. The prime polynomial P_0 is not invariant under translation by $\mathbb{F}_{32}$.

7. Non-c-Wieferich primes

Proposition 7.1. *Let P be a prime in A . If for some $m \in A_+$, $\rho_{m-1}(1) \equiv 0 \pmod{P}$ but $\rho_{m-1}(1) \not\equiv 0 \pmod{P^2}$, then P is a non-c-Wieferich prime in A .*

Proof. Let E be the Carlitz order of 1 modulo P , so $\rho_E(1) = PM$ for some $M \in A$. Since $\rho_{P-1}(1) \equiv 0 \pmod{P}$ and $\rho_{m-1} \equiv 0 \pmod{P}$ by hypothesis, it follows that $P \equiv 1 \pmod{E}$ and $m \equiv 1 \pmod{E}$. So

$$\rho_{m-1}(1) = \rho_{\frac{m-1}{E}}(\rho_E(1)) = \rho_{\frac{m-1}{E}}(PM) \equiv \frac{m-1}{E} \cdot PM \pmod{P^2}.$$

By hypothesis, $P \parallel \rho_{m-1}(1)$, so it follows that P does not divide M , hence,

$$\rho_{P-1}(1) = \rho_{\frac{P-1}{E}}(\rho_E(1)) = \rho_{\frac{P-1}{E}}(PM) \equiv \frac{P-1}{E} \cdot PM \not\equiv 0 \pmod{P^2}.$$

This shows that P is a non-c-Wieferich prime. $\square$

Lastly, we show that there are infinitely many non-c-Wieferich primes in A .

Theorem 7.2. *Let $q > 2$. There is at least a $(1 - \frac{1}{q-1})$ proportion of degree d non-c-Wieferich primes in A .*

Proof. The degree of the product of primes of degree d is asymptotically q^d whereas that of F_{d-1} is asymptotically $\frac{q^d}{q-1}$. So for large d , there is at least a $(1 - \frac{1}{q-1})$ proportion of degree d non-c-Wieferich primes. $\square$

Corollary 7.3. *For $q > 2$, there exist infinitely many non-c-Wieferich primes in A .*

Remark 7.4. Motivated by our proof of [Corollary 7.3](#), D. Thakur proposed [Theorem 7.2](#) to us.

Remark 7.5. In a recent email, D. Thakur has pointed out to the author that [Theorem 7.2](#) and subsequently [Corollary 7.3](#) have also been proved independently by B. Anglès and M. Duoh in [\[1\]](#) using similar arguments.

Remark 7.6. [Corollary 7.3](#) is the Carlitz module analogue of [\[13, Theorem 1\]](#).

Acknowledgments

I thank my advisor A. Keet, and D. Thakur for having read and improved the drafts of this manuscript. I also thank the editor and the anonymous referee for pointing out the many errors in the earlier manuscripts.

References

- [1] B. Anglès, M. Duoh, Arithmetic of “units” in $\mathbb{F}_q[T]$, arXiv:1210.1660, 2012.
- [2] S. Bae, The arithmetic of Carlitz polynomials, *J. Korean Math. Soc.* 35 (2) (1998) 341–360.
- [3] A. Bamunoba, On some properties of Carlitz cyclotomic polynomials, *J. Number Theory* 143 (2014) 102–108.
- [4] K. Conrad, Carlitz extensions, <http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/carlitz.pdf>.
- [5] L. Denis, Le théorème de Fermat–Goss, *Trans. Amer. Math. Soc.* 343 (2) (1994) 713–726.
- [6] D. Goss, On a Fermat equation arising in the arithmetic theory of function fields, *Math. Ann.* 261 (3) (1982) 269–286.
- [7] D. Goss, *Basic Structures of Function Field Arithmetic*, Springer-Verlag, Berlin, 1996.
- [8] R. Lidl, H. Niederreiter, *Introduction to Finite Fields and Their Applications*, Cambridge University Press, 1986.
- [9] D. Mirimanoff, Sur les dernier théorème de Fermat, *C. R. Acad. Sci. Paris* 150 (1910) 204–206.
- [10] G. Mullen, D. Panario, *Handbook of Finite Fields*, Chapman and Hall/CRC Press, 2013.
- [11] P. Ribenboim, *My Numbers, My Friends: Popular Lectures on Number Theory*, Springer, 2000.
- [12] M. Rosen, *Number Theory in Function Fields*, Springer-Verlag, Berlin, New York, 2002.
- [13] J. Silverman, Wieferich’s criterion and the *abc* – Conjecture, *J. Number Theory* 30 (2) (1988) 226–237.
- [14] W. Stein, et al., *Sage mathematics software*, version 5.6, The Sage Development Team, 2013.
- [15] J. Suzuki, On the generalized Wieferich criteria, *Proc. Japan Acad. Ser. A Math. Sci.* 70 (7) (1994) 230–234.
- [16] D. Thakur, Iwasawa theory and cyclotomic function fields, in: J. Jones, N. Childress (Eds.), *Proceedings of the Conference on Arithmetic Geometry*, Tempe, AZ 1993, in: *Contemp. Math.*, vol. 174, Amer. Math. Soc., 1994, pp. 157–165.
- [17] D. Thakur, *Function Field Arithmetic*, World Scientific Publishing Co. Pte. Ltd., 2004.
- [18] D. Thakur, Fermat vs Wilson congruences, arithmetic derivatives and zeta values, *Finite Fields Appl.* 32 (2015) 192–206.
- [19] A. Wieferich, Zum letzten Fermat’schen Theorem, *J. Reine Angew. Math.* 136 (1909) 293–302.