Finite Fields and Their Applications 37 (2016) 28–35

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

On coefficients of Carlitz cyclotomic polynomials

Alex Samuel Bamunoba [a,b,*,1]

[a] *Department of Mathematics, Stellenbosch University, South Africa*
[b] *Department of Mathematics, Makerere University, Uganda*

ARTICLE INFO

Article history:
Received 24 May 2014
Accepted 31 August 2015
Available online 18 September 2015
Communicated by Gary L. Mullen

MSC:
11R60
11G09
11A99

Keywords:
Carlitz polynomials
Carlitz cyclotomic polynomials
Pillai function

ABSTRACT

Let $n \in \mathbb{Z}_+$, and $\Phi_n(x)$ be the nth classical cyclotomic polynomial. In [4, Theorem 1], D. Lehmer showed that the geometric mean of $\{\Phi_s(1) : s, n \in \mathbb{Z}_+, s \leq n\} \to e \approx 2.71828$, as $n \to \infty$. Replacing $\mathbb{Z}$ by $\mathbb{F}_q[T]$, and the nth elementary cylcotomic polynomial $\Phi_n(x)$ by the Carlitz m-cyclotomic polynomial $\Phi_m(x)$, where $m \in \mathbb{F}_q[T]$, we obtain an analogue to Lehmer's result. We also express $\Phi_m(0) \in \mathbb{F}_2[T]$ in terms of $\phi_*(\cdot)$, the Pillai polynomial function. The resulting expression is a function field analogue of Hölder's formula for $\Phi_n(1)$.

© 2015 Elsevier Inc. All rights reserved.

1. Introduction

Let n be a positive integer, the elementary nth cyclotomic polynomial is the polynomial

* Correspondence to: Department of Mathematics, Stellenbosch University, South Africa.
E-mail addresses: bamunoba@aims.ac.za, bamunoba@gmail.com.

[1] This work was carried out with financial support from the Stellenbosch Postgraduate Merit Bursary Scheme and the government of Canada's International Development Research Centre (IDRC) grant number SAMUG2009004S, and within the framework of the AIMS Research for Africa Project.

http://dx.doi.org/10.1016/j.ffa.2015.08.006
1071-5797/© 2015 Elsevier Inc. All rights reserved.

$$\Phi_n(x) = \prod_{j=1}^{n}{}'(x - \zeta_j),$$

where ζ_j are the nth roots of unity in $\mathbb{C}$ given by $\zeta_j = e^{\frac{2\pi ij}{n}}$. The prime in the product simply means that the product is taken over all positive integers less than n that are co-prime to n, i.e., the ζ_j's are the primitive nth roots of unity. The degree of $\Phi_n(x)$ is $\varphi(n)$, where $\varphi(n)$ is the Euler Totient function. Since each nth root of unity is a primitive dth root of unity for a unique d dividing n (corollary to Lagrange's Theorem), we have the following fundamental relation involving cyclotomic polynomials (as d runs over positive divisors of n),

$$x^n - 1 = \prod_{d|n} \Phi_d(x). \tag{1}$$

Applying the (multiplicative form of the) Möbius inversion formula to Equation (1), we get

$$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(\frac{n}{d})}. \tag{2}$$

Here μ is the Möbius function. Recall that this is the arithmetic function defined as

$$\mu(n) = \begin{cases} (-1)^s, & n \text{ is square free with } t \text{ distinct prime factors,} \\ 0, & \text{otherwise.} \end{cases} \tag{3}$$

The Möbius function satisfies the following identity [10, Theorem 2.1]

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & n = 1 \\ 0, & n \neq 1. \end{cases}$$

It is well known that $\Phi_n(x)$ is a monic polynomial, has integer coefficients and is irreducible over $\mathbb{Q}$, see [5]. There is enormous literature concerning properties and coefficients of cyclotomic polynomials, see [7,11,12] and a number of others focusing on the $\mathbb{F}_q[T]$ analogues of these objects, e.g., [2,8,9]. However, in all these resources, the analogues of the Theorems 1.1, 1.2 and 1.3 have not been explored. It is the analogues of these results that we attempt to prove in this article. To achieve this, let us first recall the classical situation.

The von Mangoldt function is an arithmetic function defined as follows:

$$\Lambda(n) := \begin{cases} 0, & n \neq p^s \\ \log(p), & n = p^s. \end{cases} \tag{4}$$

It satisfies the following identities: if n is a positive integer, then

$$\log(n) = \sum_{d|n} \Lambda(n), \tag{5}$$

$$\Lambda(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) \log(d). \tag{6}$$

For the proof of these results see [10, Theorems 2.10 and 2.11]. We have the following classical results.

Theorem 1.1. (*See V. Lebesque (1859) in [4].*) *Let $n, s \in \mathbb{Z}_+$. We have that*

$$\Phi_n(1) = \begin{cases} 0, & n = 1, \\ 1, & n \neq p^s, \\ p, & n = p^s. \end{cases}$$

Theorem 1.2. (*See [4, Theorem 1].*) *The geometric mean of $\{\Phi_n(1) : n, s \in \mathbb{Z}_+, s \leq n\} \to e \approx 2.71828$ as $n \to \infty$.*

Theorem 1.3. (*See O. Hölder (1936) in [4].*) *Let $n \in \mathbb{Z}_+$. We have that*

$$\Phi_n'(1) = \begin{cases} 1, & n = 1, \\ \frac{1}{2}\varphi(n)\Phi_n(1), & n \neq 1. \end{cases}$$

2. Function fields

Motivated by the beautiful number fields–function fields analogy; in particular the base case $\mathbb{Z} \leftrightarrow \mathbb{Q}$ and $\mathbb{F}_q[T] \leftrightarrow \mathbb{F}_q(T)$, we examine this analogy in the lens of cyclotomic polynomials. The first attempts were made by L. Carlitz [6] when he constructed an analogous class of polynomials parametrised by the elements $m \in \mathbb{F}_q[T]$. The zeroes of each such a polynomial, say $\rho_m(x)$ form an $\mathbb{F}_q[T]$-module. In addition, adjoining the zeroes of $\rho_m(x)$ to $\mathbb{F}_q(T)$ yields a Galois extension of $\mathbb{F}_q(T)$ whose Galois group is isomorphic to $(\mathbb{F}_q[T]/m\mathbb{F}_q[T])^*$. The closer analogy with elementary properties of cyclotomic polynomials was popularised by S. Bae [8]. We extend this analogy by proving $\mathbb{F}_q[T]$ versions of Theorems 1.1, 1.2 and 1.3. Here are some preliminary remarks.

Let p be a prime number, $q = p^s$ for some $s \in \mathbb{Z}_+$, $\mathbb{F}_q$ be finite field with q elements, T be an indeterminate. Let $A := \mathbb{F}_q[T]$, A_+ be the set of monics in A, $k := \mathbb{F}_q(T)$ be the fraction field of A, k_∞ and K be the algebraic closure of k_∞. k_∞ has a non-archimedean valuation given by $|T| := |T|_\infty = q$. Let $\mathbb{C}_\infty$ be the completion of K, with respect to the canonical extension of $|\cdot|_\infty$ in k_∞. $\mathbb{C}_\infty$ is both complete and algebraically closed.

Let τ be the qth power Frobenius map, then $K\{\tau\}$ is the non-commutative ring of polynomials in the variable τ with coefficients in k subject to the commutation relation $\tau w = w^q \tau$ for all $w \in K$. The ring $K\{\tau\}$ is called the ring of "twisted polynomials" in τ. It

is isomorphic to the ring of (additive) polynomials of the form $\sum_{i=0}^{n} a_i x^{q^i}$ where addition is defined as usual and multiplication is defined by composition of polynomials [3].

The Carlitz module homomorphism is the ring homomorphism $\rho : A \to K\{\tau\}$ characterised by $\rho_T = \tau + T$. Let $m \in A$ and $a \in \mathbb{C}_\infty$, we set $m * a := \rho_m(a)$ giving $\mathbb{C}_\infty$ a new A-module structure. We call the pair $\mathscr{C} := (\mathbb{C}_\infty, \rho)$, the Carlitz A-module, i.e., the abelian group $\mathbb{C}_\infty$ together with the ring homomorphism ρ. So, with each $m \in A$, we associate an additive (polynomial in x^{q^i}'s), separable polynomial $\rho_m(x)$ called the Carlitz m-polynomial.

As an example, we compute $\rho_{T^2+1}(x)$ in A. By definition of the ring homomorphism ρ, $\rho_1(x) = x$ and $\rho_T(x) = x^q + Tx$. Also $\rho_{T^2}(x) = \rho_T(\rho_T(x))$, since ρ is a ring homomorphism (composition of functions). So

$$\rho_{T^2}(x) = \rho_T(x^q + Tx) = x^{q^2} + (T^q + T)x^q + T^2 x.$$

Since ρ is additive, we have $\rho_{T^2+1}(x) = \rho_{T^2}(x) + \rho_1(x) = x^{q^2} + (T^q + T)x^q + (T^2 + 1)x$.

Let $m \in A$, then $\mathbb{C}_\infty[m] := \{\lambda \in \mathbb{C}_\infty : \rho_m(\lambda) = 0\}$ is the set of Carlitz m-torsion points. As A-modules, $\mathbb{C}_\infty[m] \cong A/mA$ through the Carlitz module homomorphism ρ. Now, $\lambda \in \mathbb{C}_\infty[m]$ is a primitive m-torsion point if and only if it generates $\mathbb{C}_\infty[m]$ as an A-module. Adjoining $\mathbb{C}_\infty[m]$ to k produces a Galois extension $K_m := k(\mathbb{C}_\infty[m])$ of degree $\varphi(m)$, called the Carlitz m-cyclotomic function field, see [3] and [9] for details.

Definition 2.1. Let $m \in A_+$, the Carlitz m-cyclotomic polynomial over k is the polynomial,

$$\Phi_m(x) = \prod_{\lambda:\text{primitive } m\text{-torsion}} (x - \lambda)$$

Remark 2.2. Definition 2.1 extends to A as follows: for any $m \in A_+$ and $\alpha \in \mathbb{F}_q$, $\Phi_{\alpha m}(x) := \alpha \Phi_m(x)$ [2].

Mimicking the proof in [5], it is easy to show that $\Phi_m(x)$ has integer coefficients (in the sense that they are elements of A), has degree $\varphi(m) := \#(A/mA)^*$ and is irreducible over k. In [8], S. Bae showed that these polynomials share many properties with the classical ones. For example, if $m \in A_+$, then

$$\rho_m(x) = \prod_{D|m} \Phi_D(x), \tag{7}$$

where the product runs over all monic divisors of m. Applying the Möbius inversion formula, we obtain

$$\Phi_m(x) = \prod_{D|m} \rho_D(x)^{\mu(\frac{m}{D})}, \tag{8}$$

where μ is the polynomial Möbius function defined as

$$\mu(m) = \begin{cases} (-1)^s, & m \text{ is square free with } s \text{ distinct prime factors,} \\ 0, & \text{otherwise.} \end{cases}$$

Moreover, μ satisfies the following identity [10, Theorem 2.1]

$$\sum_{D|m} \mu(D) = \begin{cases} 1, & m = 1 \\ 0, & m \neq 1. \end{cases}$$

The identity in Equation (8) helps us to study properties of $\Phi_m(x)$. Imitating classical construction, L. Carlitz defined more general absolute functions from A_+ to $\mathbb{C}_\infty$. In our case, let $\exp_A(\cdot)$ and $\mathrm{Log}_A(\cdot)$ be formal exponential and logarithm with the standard properties of the real exponential and logarithm functions. For example, for any $f, g \in A$, (i) $\exp_A(f+g) = \exp_A(f)\exp_A(g)$, (ii) $\exp_A(\mathrm{Log}_A(f)) = f$, (iii) $\mathrm{Log}_A(\exp_A(f)) = f$ and (iv) $\mathrm{Log}_A(fg) = \mathrm{Log}_A(f) + \mathrm{Log}_A(g)$. This yields two analogues of von Mangoldt functions, namely

$$\Lambda_0(m) = \begin{cases} \deg(P), & m = P^s, \\ 0, & \text{otherwise,} \end{cases} \quad \text{and} \quad \Lambda_1(m) = \begin{cases} \mathrm{Log}_A(P), & m = P^s, \\ 1, & \text{otherwise.} \end{cases} \tag{9}$$

These two von Mangoldt functions satisfy the following identities.

Proposition 2.3. *Let $m \in A_+$. We have that*

$$\begin{cases} \deg(m) &= \sum_{D|m} \Lambda_0(D), \\ \mathrm{Log}_A(m) &= \sum_{D|m} \Lambda_1(D), \end{cases} \quad \textit{and} \quad \begin{cases} \Lambda_0(m) &= \sum_{D|m} \deg(D), \\ \Lambda_1(m) &= \sum_{D|m} \mathrm{Log}_A(D). \end{cases}$$

Proof. Take $m = P_1^{e_1} \cdots P_s^{e_s}$ to be the prime factorisation of m. Then

$$\begin{cases} \sum_{D|m} \Lambda_0(D) = \sum_{i=1}^{s} \sum_{j=1}^{e_i} \Lambda_0(P_i^j) = \sum_{i=1}^{s} e_i \cdot \Lambda_0(P_i) = \sum_{i=1}^{s} \Lambda_0(P_i^{e_i}) = \deg(m), \\ \sum_{D|m} \Lambda_0(D) = \sum_{i=1}^{s} \sum_{j=1}^{e_i} \Lambda_1(P_i^j) = \sum_{i=1}^{s} e_i \cdot \Lambda_1(P_i) = \sum_{i=1}^{s} \Lambda_1(P_i^{e_i}) = \mathrm{Log}_A(m). \end{cases}$$

The second pair of equations follow by using the Möbius inversion formula for $\mathbb{F}_q[T]$. □

Proposition 2.4. *Let $m \in A_+$. We have that*

$$\Phi_m(0) = \begin{cases} 0, & m = 1, \\ P, & m = P^s,\ s \in \mathbb{Z}_+ \\ 1, & m \neq P^s. \end{cases}$$

Proof. If $m = 1$, then we have $\Phi_1(0) = 0$. For $m \neq 1$, it follows by Equations (7) and (8), that

$$\Phi_m(x) = \prod_{D|m} \rho_D(x)^{\mu(\frac{m}{D})} = x^{\sum_{D|m} \mu(\frac{m}{D})} \prod_{D|m} \rho_D^+(x)^{\mu(\frac{m}{D})} = \prod_{D|m} (\rho_D^+(x))^{\mu(\frac{m}{D})},$$

where $\rho_D^+(x) = x^{-1}\rho_D(x)$. Setting $x = 0$, and applying Proposition 2.3 and Equation (9) yields

$$\begin{aligned}\Phi_m(0) &= \prod_{D|m} D^{\mu(\frac{m}{D})} = \exp_A\left(\sum_{D|m} \mu\left(\frac{m}{D}\right) \mathrm{Log}_A(D)\right) \\ &= \exp_A(\Lambda_1(m)) = \begin{cases} P, & m = P^s,\ s \in \mathbb{Z}_+, \\ 1, & m \neq 1,\ P^s. \end{cases}\end{aligned}$$

□

Remark 2.5. Proposition 2.4 is analogous to Theorem 1.1, with 1 replaced by 0 and n by m.

Let us recall the fundamental numbers used in the arithmetic of A. We define the symbols $[0] := 1$ and for $i \in \mathbb{Z}_{\geq 1}$, $[i] = T^{q^i} - T$, $L_i = [i][i-1]\cdots[1]$ and $D_i = [i][i-1]^q \cdots [1]^{q^{i-1}}$, see [3]. We obtain the following result.

Theorem 2.6. *The geometric mean of* $\{\Phi_m(0) : m \in A_+, \deg(m) \leq n\} \to [1]^{\frac{1}{q}}$ *as* $\deg(m) \to \infty$.

Proof. Let E_n be the geometric mean of $\{\Phi_m(0) : m \in A_+, \deg(m) \leq n\}$. By Proposition 2.4 we have

$$E_n = \left(\prod_{m \in A_+, 1 \leq \deg(m) \leq n} \Phi_m(0)\right)^{\frac{q-1}{q^{n+1}-q}} = \left(\prod_{1 \leq \deg(P^s) \leq n} P\right)^{\frac{q-1}{q^{n+1}-q}} = (L_n)^{\frac{q-q}{q^{n+1}-q}},$$

where $L_n = [n][n-1]\cdots[1]$. The product $\prod_{1 \leq \deg(P^s) \leq n} P$ is the least common multiple of the nonzero polynomials in A of degree less or equal to n. By [3, Proposition 3.1.6], this is L_n which has degree $\frac{q^n-1}{q-1}$. Set

$$\xi_n = \prod_{j=1}^{n-1} \left(1 - \frac{[j]}{[j+1]}\right) = \frac{[1]^{\frac{q^n-1}{q-1}}}{L_n}, \qquad n \geq 1.$$

Since $v_\infty(\xi_n) = 0$ for all $n \in \mathbb{Z}_+$, it is clear, the sequence $\{\xi_n\}$ has a limit in $\xi \in k_\infty$. So

$$\lim_{n\to\infty} E_n = \lim_{n\to\infty} (L_n)^{\frac{q-1}{q^{n+1}-q}} = \lim_{n\to\infty} \left(\frac{[1]^{\frac{q^n-1}{q-1}}}{\xi_n}\right)^{\frac{q-1}{q^{n+1}-q}} = \alpha[1]^{\frac{1}{q}},$$

where $\alpha = (1)^{\frac{1}{q}} \in \overline{\mathbb{F}_q}$. Since $\alpha^q = 1$, its order in $\mathbb{F}_q^*$ is 1, and so $\alpha = 1$. □

Remark 2.7. The classical geometric mean tends to the transcendental number e (Theorem 1.2), whereas the Carlitz geometric mean tends to an "algebraic number" in k_∞.

Although a great deal is known about $\Phi_m(x)$, some properties of its coefficients are still imperfectly understood. In the propositions below, we study some of these special properties over $\mathbb{F}_2[T]$. We shall need the following arithmetic functions, the Euler Totient function and the absolute Pillai arithmetic function. Over $\mathbb{F}_q[T]$, the Euler Totient function φ is defined as $\varphi(m) := \#(A/mA)^*$ for any $m \in A_+$. Its properties are analogous to those of the classical Euler Totient function and follow almost trivially from counting principles in A, for example, $\varphi(1) = 1$, $\varphi(P^s) = |P|^{s-1}(|P| - 1)$ and $\varphi(m_1 m_2) = \varphi(m_1)\varphi(m_2)$ if $(m_1, m_2) = 1$, i.e., multiplicativity. The absolute Pillai arithmetic function is the mapping $\phi_* : A \to A$ given by $\phi_*(m) = \sum_{a \in A_m}(a, m)$, where $A_m := \{a \in A : |a| < |m|\}$ and (a, m) is the greatest common divisor (gcd) of D and m.

Proposition 2.8. *ϕ_* is a multiplicative function.*

Proof. By grouping the terms according to the gcd we have $\phi_*(m) = \sum_{a \in A_m}(a, m) = \sum_{D|m} \varphi(\frac{m}{D})(D, m)$. Since the gcd function and $\varphi(m)$ are multiplicative, so is their Dirichlet product which in this case is ϕ_*. □

We have $\phi_*(1) = 1$, $\phi_*(P^s) = P^{s-1}(P - 1)$ and $\phi_*(m_1 m_2) = \phi_*(m_1)\phi_*(m_2)$ if $(m_1, m_2) = 1$. Although the properties of ϕ_* are analogous to those of φ, the function ϕ_* is analogous to the gcd sum. We also have that

$$m = \sum_{D|m} \phi_*(D) \qquad \text{and} \qquad \phi_*(m) = \sum_{D|m} D\mu\left(\frac{m}{D}\right).$$

Theorem 2.9. *Let $q = 2$ and $m \in A_+$. We have that $\Phi_1'(0) = 1$ and if $\deg(m) \geq 1$ then*

$$\Phi_m'(0) = \frac{\Phi_m(0)\phi_*(m)}{T(T+1)},$$

where $\phi_*(m)$ is the analogue of Pillai arithmetical function.

Proof. It is trivial, when $m = 1$, as $\Phi_m(x) = x$ and so $\Phi_m'(1) = 1$. Let $m \in A_+ - \{1\}$, then

$$\Phi_m(x) = \prod_{D|m} \rho_D(x)^{\mu(\frac{m}{D})} = \prod_{D|m} \rho_D^+(x)^{\mu(\frac{m}{D})},$$

where $\rho_D^+(x) = \frac{\rho_D(x)}{x}$, so $\rho_D^+(0) = D$. Taking logarithmic derivatives on both sides yields

$$\frac{\Phi'_m(x)}{\Phi_m(x)} = \sum_{D|m} \mu\left(\frac{m}{D}\right) \frac{(\rho_D^+(x))'}{\rho_D^+(x)}.$$

So, we have

$$\begin{aligned}\Phi'_m(0) &= \left(\Phi_m(x) \sum_{D|m} \mu\left(\frac{m}{D}\right) \frac{(\rho_D^+(x))'}{\rho_D^+(x)}\right)\Big|_{x=0} = \sum_{D|m} \mu\left(\frac{m}{D}\right) \left\{\Phi_m(x) \frac{(\rho_D^+(x))'}{\rho_D^+(x)}\right\}\Big|_{x=0} \\ &= \sum_{D|m} \mu\left(\frac{m}{D}\right) \Phi_m(0) \left\{\frac{\frac{D^2-D}{T^2-T}}{D}\right\} = \Phi_m(0) \sum_{D|m} \mu\left(\frac{m}{D}\right) \frac{D-1}{T^2-T} \\ &= \frac{\Phi_m(0)}{T(T+1)} \sum_{D|m} \mu\left(\frac{m}{D}\right)(D-1) = \frac{\Phi_m(0)}{T(T+1)} \sum_{D|m} D\mu\left(\frac{m}{D}\right) = \frac{\Phi_m(0)\phi_*(m)}{T(T+1)},\end{aligned}$$

where $\phi_*(m)$ is the analogue of Pillai arithmetical function. □

Remark 2.10. Theorem 2.9 is analogous to Theorem 1.3 with $\varphi(n)$ replaced by $\phi_*(m)$ and $\Phi_n(1)$ by $\Phi_m(0)$.

Notes added to the proof: All the above discussed old and new results form part of the author's PhD thesis [1].

Acknowledgment

I thank Dr. Arnold Keet (my advisor), Professor Florian Breuer and Professor Barry Green (AIMS Director) for the continued encouragement while writing up this work.

References

[1] A. Bamunoba, Arithmetic of Carlitz polynomials, PhD thesis, Stellenbosch University, 2014.
[2] A. Bamunoba, On some properties of Carlitz cyclotomic polynomials, J. of Number Theory 143 (2014) 102–108.
[3] D. Goss, Basic Structures of Function Field Arithmetic, vol. 35, Springer-Verlag, 1998.
[4] D. Lehmer, Some properties of the cyclotomic polynomial, J. Math. Anal. Appl. 15 (1) (1966) 105–117.
[5] K. Ireland, M. Rosen, A Classical Introduction to Modern Number Theory, Springer, 1990.
[6] L. Carlitz, A class of polynomials, Trans. Amer. Math. Soc. 43 (1938) 167–182.
[7] R. Thangadurai, On the coefficients of cyclotomic polynomials, in: Cyclotomic Fields and Related Topics, Pune, 1999, Bhaskaracharya Pratishthana, Pune, 2000, pp. 311–322.
[8] S. Bae, The arithmetic of Carlitz polynomials, J. Korean Math. Soc. 35 (2) (1998) 341–360.
[9] S. Bae, S. Hahn, On the Carlitz module, J. Chungcheong Math. Soc. 4 (1991) 85–90.
[10] T. Apostol, Introduction to Analytic Number Theory, Springer-Verlag, 1976.
[11] V. Prasolov, Polynomials, Springer-Verlag, Berlin, Heidelberg, 2004.
[12] Y. Gallot, P. Moree, H. Hommersom, Value distribution of cyclotomic polynomial coefficients, Unif. Distrib. Theory 6 (2011) 177–206.