



ELSEVIER

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt



On some properties of Carlitz cyclotomic polynomials



Alex Samuel Bamunoba

Department of Mathematical Sciences, University of Stellenbosch,
Stellenbosch 7602, South Africa

ARTICLE INFO

Article history:

Received 10 April 2013

Received in revised form 22 July 2013

2013

Accepted 13 March 2014

Available online 15 May 2014

Communicated by Florian Breuer

MSC:

11A99

11G09

Keywords:

Carlitz polynomials

Carlitz cyclotomic polynomials

ABSTRACT

Text. We consider the analogue, when $\mathbb{Z}$ is replaced with $\mathbb{F}_q[T]$ of the elementary cyclotomic polynomials and prove an analogue of Suzuki's Theorem.

Video. For a video summary of this paper, please visit <http://youtu.be/mVBw82N34NE>.

© 2014 Elsevier Inc. All rights reserved.

1. Introduction

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

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

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

where ζ_j are the n th roots of unity in $\mathbb{C}$ given by $\zeta_j = e^{\frac{2\pi i j}{n}}$. 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 n th roots of unity. The degree of $\Phi_n(x)$ is $\varphi(n)$, where φ is the Euler totient function. Since each n th root of unity is a primitive d th root of unity for a unique d dividing n (corollary to Lagrange's Theorem), we have the following fundamental relation involving cyclotomic polynomials (d runs over positive divisors):

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

We also have the following basic result (see [6] for several classical proofs of this result (certainly not all of them)).

Theorem 1.1. $\Phi_n(x)$ is monic, has integer coefficients and is irreducible over $\mathbb{Q}$.

Sketch proof. By construction $\Phi_n(x)$ is monic. To show that $\Phi_n(x)$ is an integral polynomial, we note that $\Phi_1(x) = x - 1 \in \mathbb{Q}[x]$. Now assume $\Phi_d(x) \in \mathbb{Q}[x]$ for all $d < n$, an induction on n shows that $\Phi_n(x) \in \mathbb{Q}[x]$. Since $\Phi_n(x)$ is monic and divides $x^n - 1 \in \mathbb{Z}[x]$, it follows from Gauss' lemma that $\Phi_n(x) \in \mathbb{Z}[x]$. To show irreducibility of $\Phi_n(x)$ over $\mathbb{Q}$, again with Gauss' lemma, it suffices to prove irreducibility over $\mathbb{Z}$. $\square$

Applying the (multiplicative form of the) Möbius inversion formula to Eq. (1),

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

Here μ is the Möbius function. Recall, this is the arithmetic function $\mu : \mathbb{N} \rightarrow \mathbb{C}$ defined as

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

Set

$$\Phi_n(x) = \sum_{i=0}^{\varphi(n)} c(n, i) x^i,$$

so $c(n, i) \in \mathbb{Z}$ for all $n \in \mathbb{Z}_+$ and $c(n, i) = 0$ for $i > \varphi(n)$. There is a lot of literature on the numbers $c(n, i)$, but of interest to us will be Suzuki's result. In 1987, J. Suzuki [5] showed that every integer appears as a coefficient in some elementary cyclotomic polynomial, i.e. $\{c(n, i) : n \in \mathbb{Z}_+, i \geq 0\} = \mathbb{Z}$. In 2009, Ji, Li and Moree [3] generalised this result by proving that $\{c(nn', i) : n' \in \mathbb{Z}_+, i \geq 0\} = \mathbb{Z}$ for any fixed $n \in \mathbb{Z}_+$.

Motivated by the beautiful number fields–function fields analogy, in particular the base case $\mathbb{Z} \leftrightarrow \mathbb{Q}$ and $\mathbb{F}_q[T] \leftrightarrow \mathbb{F}_q(T)$, the ground breaking work of L. Carlitz about the Carlitz module, Carlitz polynomials and the work of S. Bae [1],¹ we extend this analogy (of elementary cyclotomic polynomials) by proving versions of Suzuki, Ji, Li and Moree’s theorems in this setting. Here are some preliminary remarks.

Let p denote a prime number, $q = p^n$, $\mathbb{F}_q$ -finite field of q elements (characteristic p), T an indeterminate. Let $A := \mathbb{F}_q[T]$, $A_+ :=$ be monics in A , $k := \mathbb{F}_q(T)$, $k_\infty := \mathbb{F}_q((\frac{1}{T}))$, k_∞ has a non-archimedean valuation; $|T| := |T|_\infty = q$ and $\overline{k_\infty}$ be the algebraic closure of k_∞ . Let $\mathbb{C}_\infty$ be the completion of $\overline{k_\infty}$, with respect to the canonical extension of $|\cdot|_\infty$ in k_∞ . $\mathbb{C}_\infty$ is both complete and algebraically closed. Let τ be the Frobenius element defined by $\tau(x) = x^q$. We denote by $k\{\tau\}$ the ‘twisted polynomial ring’ whose multiplication is defined by $\tau\alpha = \alpha^q\tau$ for all $\alpha \in k$. The Carlitz A -module is the abelian group $\mathbb{C}_\infty$ together with the $\mathbb{F}_q$ -algebra homomorphism $\rho : A \rightarrow k\{\tau\}$ defined or characterised by $\rho_T = \tau + T$. To each $m \in A$ and $x \in \mathbb{C}_\infty$, we set $m * x := \rho_m(x)$ giving $\mathbb{C}_\infty$ a new A -module structure $\mathcal{C} := \rho(\mathbb{C}_\infty)$. So with each $m \in A_+$, we associate an additive (polynomial in x^{q^i} ’s), separable polynomial $\rho_m(x)$ called the m Carlitz polynomial.

Let $m \in A_+$, then $\mathbb{C}_\infty[m] := \{\lambda \in \mathbb{C}_\infty : \rho_m(\lambda) = 0\} = \Lambda_m$ is the set of Carlitz m -torsion or division points. As A -modules, $\mathbb{C}_\infty[m] \cong A/mA$ through the Carlitz module ρ . Now, $\lambda \in \mathbb{C}_\infty[m]$ is called a primitive torsion point of m 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 m Carlitz cyclotomic function field. This is to differentiate it from the classical cyclotomic extensions obtained by adjoining roots of unity to $\mathbb{Q}$.

Definition 1.2. Let $0 \neq m \in A_+$, the m Carlitz m cyclotomic polynomial over k is the polynomial,

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

The name m Carlitz cyclotomic polynomial to distinguish it from the elementary n th cyclotomic polynomial $\Phi_n(x)$. Like elementary cyclotomic polynomials, $\Phi_m(x)$ is a ‘monic’ integral polynomial irreducible over k and has degree $\varphi(m)$, where φ is the polynomial Euler totient function. It also satisfies nice relations, for example, the factorisation and composition identities in Propositions 1.3, 1.4, and 1.6. To prove all these properties, one simply imitates the classical arguments. This is a common phenomenon in this field.

¹ Who defined Carlitz cyclotomic polynomials (in the sense we use it in this article!) and even brought the analogy closer when he proved a series of properties analogous to the elementary cyclotomic polynomials by imitating classical proofs. One can argue that, all these properties follow trivially, from the fact that the multiplicative structures of the two rings $\mathbb{Z}$ and $\mathbb{F}_q[T]$ are almost identical.

Proposition 1.3. (See [2], Proposition 3.3.10.) Let $m \in A$, $\rho_m(x) = a(m, \deg(m))x^{q^{\deg(m)}} + \cdots + a(m, 0)x$;

$$a(m, 0) = m, \quad a(m, i) = \frac{(a(m, i-1))^q - a(m, i-1)}{T^{q^i} - T}, \quad i = 1, \dots, \deg(m).$$

Proposition 1.3 is important for two reasons; first, it is a recursive formula for computing coefficients of $\rho_m(x)$ and secondly, it will help in the extension the definition of cyclotomic polynomials to non-monic m .

Proposition 1.4. (See [1], Proposition 1.1.) Let $m \in A_+$, then

$$\rho_m(x) = \prod_{D|m} \Phi_D(x) \quad (2)$$

where D are monic divisors of m .

Proof. Since $\rho_m(x)$ is separable over $\mathbb{C}_\infty$, its roots are exactly the Carlitz m torsion points. On the other hand, if λ_D is a Carlitz m torsion point such that D is the monic polynomial in A with least degree such that $\rho_D(\lambda_D) = 0$, then λ_D is a primitive D torsion point, hence a root of $\Phi_D(x)$. But this implies that D divides m , so λ_D is also a root to the right hand side of Eq. (2). So the polynomials on left and right hand sides have the same roots. Equality of both polynomials on the left and right hand sides follows from the fact both polynomials (on right and left hand sides of (2)) are monic and separable over $\mathbb{C}_\infty$. $\square$

Applying the (multiplicative form of the) Möbius inversion formula to Eq. (2), we obtain

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

where μ is the polynomial Möbius function. This is defined as the function $\mu : A \rightarrow \mathbb{C}$ such that

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

If m is not monic, then there exists some unit $\alpha \neq 1$ in $\mathbb{F}_q^*$ and a polynomial $M \in A_+$ such that $m = \alpha M$. It follows from the fact that $\alpha^q = \alpha$ for all $\alpha \in \mathbb{F}_q$ and the recursive definition in Proposition 1.3 that $a(m, i) = \alpha a(M, i)$ and so $\rho_m(x) = \alpha \rho_M(x) = \alpha \prod_{D|M} \Phi_D(x)$. We conventionally set $\Phi_m(x) := \alpha \Phi_M(x)$.

Remark 1.5. The proof for $\mathbb{Z}$ does not work for $\mathbb{F}_q[T]$ but the first step of Proposition 1.6 is analogous.

Proposition 1.6. *Let m_0 be the ‘largest’ monic square free factor of $M \in A_+$, then $\Phi_M(x) = \Phi_{m_0}(\rho_{\frac{M}{m_0}}(x))$.*

Proof.

$$\begin{aligned}\Phi_M(x) &= \prod_{D|M} \rho_{\frac{M}{D}}(x)^{\mu(D)} = \prod_{\substack{D|M \\ D|m_0}} \rho_{\frac{M}{D}}(x)^{\mu(D)} \\ &= \prod_{D|m_0} \rho_{\frac{m_0}{D}}(\rho_{\frac{M}{m_0}}(x))^{\mu(D)} = \Phi_{m_0}(\rho_{\frac{M}{m_0}}(x)).\end{aligned}$$

The second equality follows from using the definition of Möbius function. $\square$

2. Statement of problem

Set

$$\Phi_m(x) = \sum_{i=0}^{\varphi(m)} c(m, i) x^i,$$

where $c(m, i) \in A$ and $c(m, i) = 0$ for $i > \varphi(m)$. We now focus on establishing the following theorem.

Theorem 2.1 (*Analogue of Suzuki’s Theorem*). *For any $a \in A$, $\exists m \in A$ and $i \in \mathbb{Z}_{\geq 0}$ such that $c(m, i) = a$.*

3. Main results

Like Ji, Li and Moree [3], let $T(m^*) = \{c(m^*m', i) : m' \in A, i \in \mathbb{Z}_{\geq 0}\}$, then we have the following result:

Theorem 3.1. *For any $m^* \in A_+$, we have $T(m^*) \supseteq \mathfrak{a}$, where $\mathfrak{a}$ is the principal ideal generated by $m_1 := \frac{m^*}{m_0}$.*

Proof. Let $m^* \in A_+$, with m_0^* as its square free part, so $T(m^*) = \{c(m^*m', i) : m' \in A, i \in \mathbb{Z}_{\geq 0}\}$, $\mathfrak{a} = m_1A$, $m_1 := \frac{m^*}{m_0^*}$. We will show that $\mathfrak{a} \subseteq T(m^*)$. To do this, let $0 \neq m \in \mathfrak{a}$, so $m = m_1N$ for some $N \in A$ and take $M := mm_0^*f_0$, where f_0 is the product of prime factors of N that do not divide m^* . So by Proposition 1.6 $\Phi_M(x) = \Phi_{m_0^*f_0}(\rho_m(x))$. It suffices to show that m is a coefficient in $\Phi_M(x)$, so $m \in T(m^*) \Rightarrow \mathfrak{a} \subseteq T(m^*)$.

Let m, M be as above, $m_0 := m_0^*f_0$ be the square free part of M , then $\varphi(m_0) \equiv (-1)^t \equiv \mu(m_0) \pmod{q}$, where t is the number of distinct prime factors of m_0 . We show that $\mu(m_0)m$ is a coefficient in $\Phi_M(x)$. By Proposition 1.6, $\Phi_M(x) = \Phi_{m_0}(\rho_m(x))$ so

we can write $\Phi_{m_0}(x) = x^{\varphi(m_0)} + g_{m_0}(x)$, where $g_{m_0}(x)$ is a polynomial in lower degree terms. So we search the coefficient of $x^{q^n(\varphi(m_0)-1)+1}$, (where $n := \deg(m)$) in

$$\Phi_M(x) = \Phi_{m_0}(\rho_m(x)) = (\rho_m(x))^{\varphi(m_0)} + g_{m_0}(\rho_m(x)).$$

The degree of $g_{m_0}(\rho_m(x))$ is at most $q^n(\varphi(m_0) - 1) < q^n(\varphi(m_0) - 1) + 1$, so no term in $g_{m_0}(\rho_m(x))$, contributes to the coefficient of $x^{q^n(\varphi(m_0)-1)+1}$. We concentrate on the first term, and split it into two terms as follows; $\rho_m(x) = mx + h_m(x)$, where $h_m(x)$ is a polynomial in higher degree terms. Expanding $(mx + h_m(x))^{\varphi(m_0)}$ using the binomial theorem, we get the following expressions;

$$\begin{aligned} \Phi_M(x) &= (h_m(x) + mx)^{\varphi(m_0)} + g_{m_0}(\rho_m(x)) \\ &= \sum_{j=0}^{\varphi(m_0)} \binom{\varphi(m_0)}{j} (mx)^j h_m(x)^{\varphi(m_0)-j} + g_{m_0}(\rho_m(x)) \\ &= [h_m(x)^{\varphi(m_0)} + \mu(m_0)mxh_m(x)^{\varphi(m_0)-1} + \dots + (mx)^{\varphi(m_0)}] + g_{m_0}(\rho_m(x)) \end{aligned}$$

Here we use a technical result which will be proved later in [Lemma 3.2](#) and [Remark 3.3](#). So we concentrate on the second term, that is, $\mu(m_0)mxh_m(x)^{\varphi(m_0)-1}$. We write $h_m(x) := x^{q^n} + i_m(x)$, where $i_m(x)$ is a polynomial in lower degree terms, but with the lowest term having degree q , that is $a(m, 1)x^q \neq 0$.

$$\begin{aligned} \Phi_M(x) &= h_m(x)^{\varphi(m_0)} + \mu(m_0)mx(x^{q^n} + i_m(x))^{\varphi(m_0)-1} + \dots \\ &\quad + (mx)^{\varphi(m_0)} + g_{m_0}(\rho_m(x)) \\ &= h_m(x)^{\varphi(m_0)} + [\mu(m_0)mx^{q^n(\varphi(m_0)-1)+1} + \dots] + \dots \\ &\quad + (mx)^{\varphi(m_0)} + g_{m_0}(\rho_m(x)). \end{aligned}$$

In general, to have the coefficient as m , for any $m \in A$, set $M = \mu(m_0)m_0m$, and use $\Phi_{\alpha m}(x) = \alpha\Phi_m(x)$. $\square$

Here are the technical details used in the proof of [Theorem 2.1](#).

Lemma 3.2. Let $w(x) = \sum_{i=1}^d w_i x^{q^i}$ be an additive polynomial in $k[x]$ of degree q^d with $w_d = 1$. Let $0 \leq j \leq s \leq q^d$ be integers. The term $x^{q^d(s-1)+1}$ occurs in $x^j w(x)^{s-j}$ if and only if $j = 1$ and the coefficient of $x^{q^d(s-1)+1}$ in $xw(x)^{s-1}$ is equal to 1.

Proof. A typical summand in $x^j w(x)^{s-j}$ is of the form $ax^j x^{q^{i_1}} \dots x^{q^{i_{s-j}}}$ with $1 \leq i_k \leq d$. We search exponents with $j + q^{i_1} + \dots + q^{i_{s-j}} = q^d(s-1) + 1$.

1. If $j \geq 2$, then $j + q^{i_1} + \cdots + q^{i_{s-j}} \leq s + q^d(s-2) < q^d(s-1) + 1$.
2. If $j = 0$, we want $q^{i_1} + \cdots + q^{i_{s-j}} = q^d(s-1) + 1$. If less than $s-1$ exponents are equal to d , we get $q^{i_1} + \cdots + q^{i_s} \leq q^d(s-2) + 2q^{d-1} < q^d(s-1) + 1$. If atleast $s-1$ exponents are equal to d , then we get $q^{i_1} + \cdots + q^{i_s} \geq q^d(s-1) + q > q^d(s-1) + 1$.
3. If $j = 1$, we get $1 + q^{i_1} + \cdots + q^{i_{s-1}} = q^d(s-1) + 1$ if and only if all the i_k are equal to d . There is exactly one summand with coefficient $w_d^{s-1} = 1$. $\square$

Remark 3.3. Let m be a monic in A and m_0 be its square free part. If in addition, the linear part (in x) of $w(x)$ above is mx , then there is no term of the form $bx^{q^d(\varphi(m_0)-1)+1}$ in $(mx)^j(w_m(x) - mx)^{\varphi(m_0)-j}$ except when $j = 1$.

Corollary 3.4. If m^* is a square free polynomial, then $T(m^*) = A$.

Proof. m^* -square free implies $m_1 = \frac{m^*}{m_0^*} = 1$ so $\mathfrak{a} = A$. By Theorem 3.1, $A \subseteq T(m^*) \subseteq A$, hence equality! $\square$

In particular, Theorem 2.1 is proved. It is worth mentioning, Theorem 2.1 was arrived at after a series of experiments done with Computer Algebra System of SAGE [4].

Acknowledgments

Thank you to Arnold Keet for supervising and reading the first versions of this work. Many thanks to the anonymous reviewer who suggested a precise formulation of Lemma 3.2 and other helpful comments.

References

- [1] S. Bae, The arithmetic of Carlitz polynomials, J. Korean Math. Soc. 35 (1998) 341–360.
- [2] D. Goss, Basic Structures of Function Field Arithmetic, vol. 35, Springer, 1998.
- [3] C. Ji, W. Li, P. Moree, Values of coefficients of cyclotomic polynomials II, Discrete Math. 309 (2009) 1720–1723.
- [4] W. Stein, et al., Sage Mathematics Software (version 5.6), The Sage Development Team, <http://www.sagemath.org/>, 2013.
- [5] J. Suzuki, On coefficients of cyclotomic polynomials, Proc. Japan Acad. Ser. A Math. Sci. 63 (1987) 279–280.
- [6] S.H. Weintraub, Several proofs of the irreducibility of the cyclotomic polynomials, Amer. Math. Monthly 120 (2013) 537–545.