Values of cyclotomic polynomials

Alex Samuel **BAMUNOBA**

(*bamunoba@aims.ac.za*)

Let $n \in \mathbb{Z}_+$ and $\mu_n := \{\zeta \in \mathbb{C} : \zeta^n = 1\}$, the n-torsion $\mathbb{Z}$-submodule of $\mathbb{C}^\times$. As $\mathbb{Z}$-modules, $\mu_n \cong \mathbb{Z}/n\mathbb{Z}$. The nth cyclotomic polynomial over $\mathbb{Q}$ is the monic polynomial $\Phi_n(x)$ whose zeroes are the primitive n-torsions of μ_n, i.e.,

$$\Phi_n(x) := \prod_{\zeta \in \mu_n,\ \text{primitive}} (x - \zeta).$$

$\Phi_n(x) \in \mathbb{Z}[x]$, is irreducible over $\mathbb{Z}$, and has degree $\varphi(n)$, where φ is the Euler totient function. Moreover,

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

"$d \mid n$ means: d runs over all the positive divisors of n".

Theorem 1.1 (V. Lebesque, (1859))

Let $s \in \mathbb{Z}_{+}$. Then $\Phi_1(1) = 0$ and for $n \geq 2$, we have

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

Equivalently, Theorem 1.1 asserts that: for $n \in \mathbb{Z}_{\geq 2}$, we have $\Phi_n(1) = e^{\Lambda(n)}$, where Λ is the von Mangoldt function:

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

Theorem 1.2 (D. H. Lehmer, (1966))

Let $m, n \in \mathbb{Z}_{\geq 2}$ and $\mathcal{A}_m := \{\Phi_n(1) : n \leq m\}$. As $m \to \infty$, the geometric mean of $\mathcal{A}_m$ tends to e, Euler's number.

Proof.

We have

$$\frac{1}{m-1}\sum_{1<n\leq m}\log(\Phi_n(1)) = \frac{1}{m-1}\sum_{1<n\leq m}\Lambda(n) = \frac{\psi(m)}{m-1} \sim 1.$$

□

- $\mathbb{Z} :=$ the ring of rational integers.
- $\mathbb{F}_q[t] :=$ the ring of polynomials in t defined over a finite field $\mathbb{F}_q$ of characteristic p, i.e., $q = p^s$ for some $s \in \mathbb{Z}_+$.

Let p be a prime number, $A := \mathbb{F}_q[t]$, where $q = p^s$, for some $s \in \mathbb{Z}_+$. Furthermore, let, $A_+ :=$ be the set of monic polynomials in A, P be a monic irreducible (prime) polynomial in A. We have the sequence of inclusions;

$$A \hookrightarrow k \hookrightarrow K := k_\infty \hookrightarrow \overline{K} \hookrightarrow \mathbb{C}_\infty := \widehat{\overline{K}}$$

Let τ be the qth power map $(x \mapsto x^q)$, $k\{\tau\}$ be the twisted polynomial ring in τ over k and $\rho : A \to k\{\tau\}$; $N \mapsto \rho_N$ be the Carlitz module, i.e., ρ is an $\mathbb{F}_q$-algebra homomorphism such that $\rho_t = t + \tau$. For each $N \in A$, we associate the additive polynomial $\rho_N(x)$, the Carlitz N polynomial.

Let $N \in A_+$ and $\mu_N := \{\zeta \in \mathbb{C}_\infty : [N] * \zeta = \rho_N(\zeta) = 0\}$, the Carlitz N-torsion A-submodule of $\mathbb{C}_\infty$. μ_N is isomorphic to A/NA as A-modules. The Carlitz N-cyclotomic polynomial over k is the monic polynomial $\Phi_N(x)$ whose zeroes are precisely the primitive Carlitz N-torsions, i.e.,

$$\Phi_N(x) := \prod_{\zeta \in \mu_N:\ \text{primitive}} (x - \zeta).$$

$\Phi_N(x) \in A[x]$, is irreducible over A, with degree $\varphi(N)$, where φ is the Euler function for A. Moreover,

$$\rho_N(x) = \prod_{D|N} \Phi_D(x). \tag{2}$$

"$D \mid N$ means; D runs over all monic divisors of N".

Theorem 3.1 ("Carlitz-Lebesque" Theorem)

Let $s \in \mathbb{Z}_+$, and $N \in A_+$. Then $\Phi_1(0) = 0$ and

$$\Phi_N(0) = \begin{cases} 1, & N \neq P^s, \\ P, & N = P^s. \end{cases}$$

Let $m \in \mathbb{Z}_+$, $\mathcal{A}_m := \{\Phi_N(0) : N \in A_+, 1 \leq \deg(N) \leq m\}$. The symbols $[i]$ and L_i for $i \in \mathbb{Z}_+$ shall denote $t^{q^i} - t$ and $[i][i-1]\cdots[1]$ respectively. For $i = 0$, we set $L_0 = [0] = 1$.

Theorem 3.2 (∞-adic topology)

The geometric mean of $\mathcal{A}_m$ tends to $[1]^{\frac{1}{q}}$ as $m \to \infty$.

Proof.

Let E_m be the geometric mean of $\mathcal{A}_m$. So

$$E_m = \left(\prod_{\substack{N \in A_+, \\ 1 \le \deg(N) \le m}} \Phi_N(0) \right)^{\frac{q-1}{q^{m+1}-q}} = \left(\prod_{1 \le \deg(P^s) \le m} P \right)^{\frac{q-1}{q^{m+1}-q}}.$$

The product $\prod_{1 \le \deg(P^s) \le m} P$ is the least common multiple of polynomials in A of degree m. This is precisely L_m. It is now clear that $E_m = (L_m)^{\frac{q-1}{q^{m+1}-q}}$. Set

$$\xi_m := \prod_{j=1}^{m-1} \left(1 - \frac{[j]}{[j+1]} \right) = \frac{[1]^{\frac{q^m-1}{q-1}}}{L_m}.$$

□

PROOF CONTINUED . . .

Since $\deg(L_m) = \frac{q^{m+1}-q}{q-1}$, it follows that $v_\infty(\xi_m) = 0$ for all $m \in \mathbb{Z}_+$, hence $\lim_{m\to\infty} \xi_m = \xi \in k_\infty =: K$. So

$$\lim_{m\to\infty} E_m = \lim_{m\to\infty} \left(\frac{[1]^{\frac{q^m-1}{q-1}}}{\xi_m} \right)^{\frac{q-1}{q^{m+1}-q}} = \frac{[1]^{\frac{1}{q}}}{\beta},$$

where $\beta = \lim_{m\to\infty} (\xi_m)^{\frac{q-1}{q(q^m-1)}}$. As $m \to \infty$, $\frac{q-1}{q^{m+1}-q} \to 0$ in the ∞-adic topology, hence $\beta = 1$ and $E_m \to E = [1]^{\frac{1}{q}}$. □

Proof of convergence in the p-adic topology.

Let $e_m = \frac{q-1}{q^{m+1}-q}$. As $m \to \infty$, we have $|q^{m+1}|_p \to 0$. So $\lim_{m\to\infty} e_m = \frac{1-q}{q}$, hence $\lim_{m\to\infty} E_m = E = [1]^{\frac{1}{q}}\xi^{1-\frac{1}{q}}$. □

Theorem 3.3 (p-adic topology)

The geometric mean of $\mathcal{A}_m$ tends to E as $m \to \infty$, where

$$E = [1]^{\frac{1}{q}}\xi^{1-\frac{1}{q}}, \text{ and } \xi = \lim_{m\to\infty}\prod_{j=1}^{m-1}\left(1 - \frac{[j]}{[j+1]}\right).$$

Remark 3.4

The limit E above is transcendental over k because $\overline{\pi}^{q-1} + (1 - \frac{1}{[1]})^{q-1}E^{q-1} = 0$, where $\overline{\pi}$ is the Carlitz period.

A. Bamunoba.

On coefficients of Carlitz cyclotomic polynomials.

Finite Fields Appl., 37:28–35, 2016.

D. Lehmer.

Some properties of the cyclotomic polynomial.

J. Math. Anal. Appl., 15(1):105–117, 1966.