ECONSPEAK: A Journal of Advances in Management IT & Social Sciences,
Vol. 7, Issue 2, February 2017 Impact Factor 5.132 ISSN: (2231-4571)
www.skirec.org Email Id: skirec.org@gmail.com

A NUMERICAL STUDY OF CYCLOTOMIC POLYNOMIALS & ITS PROPERTIES AND THEOREMS

Renu Priya[1], Dr. Ashwini Kumar Nagpal[2]

Department of Mathematics

[1,2]OPJS University, Churu (Rajasthan)

ABSTRACT

In this paper we give a brief however solid foundation to the number fields-function fields analogy. In here, we state numerous properties of the ring **A** and delineate how they are butt-centric ogous to those in **Z**. With the assistance of the Chinese leftover portion hypothesis, we might depict the structure of (A/f A), the gathering of units of the remainder ring A/f A, and additionally express the polynomial variants of some vital arithmetic functions. Specifically, the Möbius-m function, the Euler-totient function and their critical relationships, as a use of these properties, we state and demonstrate the analogs of Fermat's and Euler's little hypotheses. We should likewise give a short prologue to the Riemann zeta function for the ring A.

1. INTRODUCTION

The nth cyclotomic polynomial, $\Phi_n(z)$ is the insignificant polynomial of the nth primitive underlying foundations of solidarity. It is a polynomial over Z with commonly little integer coefficients. We let the request of $\Phi_n(z)$ be the number of unmistakable odd prime divisors of n. We are keen on the properties of the coefficients of $\Phi_n(z)$ and specifically the stature of $\Phi_n(z)$ which we signify by A(n) 2 N. There are a number of open issues concerning A(n) ∈ N that are liable to dynamic research [1].

One such open issue is to totally portray flat cyclotomic polynomials. $\Phi_n(z)$ is said to be flat if A(n) = 1. Cyclotomic polynomials of request 1 are inconsequentially flat and Bang demonstrated that each one of those of request two are flat too. Late endeavors by Bachman, Elder, and Kaplan have grouped vast groups of flat $\boldsymbol{\Phi_n(z)}$ of request three.

All the more as of late Kaplan has discovered an endless group of flat cyclotomic polynomials of request. It stays open, be that as it may, regardless of whether these families envelop all flat $\Phi_n(z)$ of requests three and four. In addition, we as of now don't know whether there exists a flat cyclotomic polynomial of request five or more prominent.

We are similarly keen on cyclotomic polynomials of expansive tallness. Erdos˝ first demonstrated that the statures of cyclotomic polynomials can be subjectively extensive. Erdos demonstrated that, given c > 0, that there exist unendingly numerous n with the end goal that A(n) > n^c; Maier demonstrated what's more that the arrangement of such n 2 N has positive lower thickness. We looked to reply: what is minimal n for which A(n) > n? n^2? n^3? And so forward [2].

2. THE MÖBIUS FUNCTION AND EULER'S FUNCTION

We define the number-theoretic functions and, which appear often in our discussion of cyclotomic polynomials.

Definition 1.1: The Möbius function is the function: N → f{- 1; 0; 1}g fulfilling (n) = 1 for square free n with a considerably number of prime factors, (n) = 1 for square free n with an odd number of prime factors, and μ (n) = 0 for non-square free n [3].

E.g. μ (6) = 1. We note that is a multiplicative function. That is, if gcd(a; b) = 1, then μ (ab) = μ (a) (b).

Definition 1.2: The totient of a natural number n,φ (n), is the number of integers j such that 0≤ j < n such that gcd(j; n) = 1.

Given n = p^{e1} 1 p^{e2} 2 . . . p^{ek}_k , an integer with k distinct prime factors p_1, p_2, . . . , p_k, it is well known that

$$\Phi() = \prod_{i=1}^{k} p^{e_{k-1}} (p-1) = n \prod_{p|n} (1 - \frac{1}{p})$$

3. CYCLOTOMIC POLYNOMIALS

Definition 1.3: A component ω of a field F is said to be a nth root of unity if $\omega^n = 1$; besides, we say such a root of unity is primitive if ω n = 1 and ω k 6= 1 for 0 < k < n.

That is, the nth primitive roots of unity are the nth roots of unity with multiplicative request n [4]. The nth complex roots of unity in C are the values the intricate primitive roots of unity are precisely those for which gcd(j, n) = 1.

$$e^{2\pi ij/n} \text{ for } 0 \leq j < n;$$

Definition 1.4: The nth cyclotomic polynomial, $\Phi_n(z) \in C[z]$, is the monic polynomial whose roots are the nth primitive roots of unity.

$$\Phi_n(Z) = (z - e^{2\pi ij/n}).$$

We could also characterize $\Phi_n(z)$ over any field F containing nth primitive roots of unity. "Cyclotomic" is Latin in starting point, signifying "circle isolating". In reality, every one of the roots of $\Phi_n(z)$ lie on the unit circle [5]. The level of $\Phi_n(z)$ is the totient of n, ϕ(n). As each nth root of unity has multiplicative request d for some one of a kind positive d isolating n, it takes after that

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

Where the item is assumed control over all positive d separating n

We let the file of $\Phi_n(z)$ be n, and the request of $\Phi_n(z)$ be the number of particular odd prime divisors partitioning n. What's more we characterize $\Psi_n(z)$ the nth backwards cyclotomic polynomial

Definition 1.5: The nth inverse cyclotomic polynomial, $_n(z)$, is the polynomial satisfying $_n(z)$ $_n(z) = z^n$ 1.

It is immediate from definitions 1.4 and 1.5 that $_n(z)$ is the monic polynomial whose n (n) roots are the nth non-primitive roots of unity. We note that both $_n(z)$ andΦ $_n(z)$ Ψ $_n(z)$ have no repeated roots, a fact we use in some proofs.

$$\psi_n(z) = \prod_{\substack{0\le j<n \\ \gcd(j,n)>1}} (z - e^{2\pi ij/n}).$$

More introduced inverse cyclotomic polynomials and was the first to study their properties. As we see that the coefficients of $\Psi_n(z)$ happen in the power arrangement extension of $1/\Phi_n(z)$.

$$\frac{1}{\Phi_n(z)} = \psi_n(z)(1 + z^n + z^{2n} + \dots.),$$

The initial six cyclotomic and backwards cyclotomic polynomials are as per the following:

$$\boldsymbol{\Phi_1(z) = z - 1,} \qquad \boldsymbol{\psi_1(z) = 1}$$

$$\boldsymbol{\Phi_2(z) = z + 1,} \qquad \boldsymbol{\psi_2(z) = z - 1}$$

$$\boldsymbol{\Phi_3(z) = z^2 + z + 1,} \qquad \boldsymbol{\psi_3(z) = z - 1}$$

$$\boldsymbol{\Phi_4(z) = z^2 + 1,} \qquad \boldsymbol{\psi_4(z) = z^2 - 1}$$

$$\boldsymbol{\Phi_5(z) = z^4 + z^3 + z^2 + z + 1,} \qquad \boldsymbol{\psi_5(z) = z - 1}$$

$$\boldsymbol{\Phi_6(z) = z^2 - z + 1} \qquad \boldsymbol{\psi_6(z) = z^4 + z^3 - z - 1}$$

CYCLOTOMIC POLYNOMIALS OF LARGE HEIGHT

Definition 1.6: We denote by A(n) and S(n) the height and length of Φn(z), respectively. That is, for

$$\Phi_n(z) = \sum_{k=0}^{\phi(n)} a_n(k),$$

$$A(n) = \max_{0\le k\le \phi(n)} |a_n(k)|, \quad \text{and} \quad S(n) = \sum_{k=0}^{\phi(n)} |a_n(k)|.$$

We similarly let $A^-(n)$ and $S^-(n)$ be the height and length of Ψn(z). We see that A(n) = 1 for the first six cyclotomic polynomials. The least n for which A(n) > 1 is n = 105. A(n) = 2, as

$$\Phi_{105}(z) = z^{48} + z^{47} + z^{46} - z^{43} - z^{42} - z^{41} - z^{40} - z^{39} + z^{36} + z^{35} + z^{34} + z^{33} + z^{32} + z^{31} - z^{28} - z^{26} - z^{24} - z^{22} - z^{20} + z^{17} + z^{16} + z^{15} + z^{14} + z^{13} + z^{12} - z^{9} - z^{8} - z^{7} - z^{6} - z^{5} + z^{2} + z^{1} + 1$$

Paul Erdos demonstrated that ″ A(n) isn't limited by n^c for any c > 0; in any case, his verification does not recommend, given c, precisely how extraordinary must n be for A(n) to be more prominent than n^c ? This was the first rousing inquiry that impelled the creator and Monagan to create and execute calculations to register cyclotomic polynomials. We were occupied with concentrate the development of $\max_{m\le n}$ A(m) regarding n. Φn(z) of little request and record ordinarily have little coefficients [6]. These, shockingly, are precisely the cyclotomic polynomials that are anything but difficult to register. Koshiba figured the initial 10% of the terms of $\Phi_n(z)$ for n = 111546435 and in doing as such demonstrated that A(n) > n, the principal such case as far as anyone is concerned. Monagan discovered A(1181895) = 14102773, and confirmed this was minimal n for which A(n) > n. Monagan, additionally, discovered cases of n fulfilling A(n) > n^2 and A(n) > n^4 . He discovered such cases by processing $\Phi_n(z)$ for n which were distinct by 1181895. By actualizing new calculations we have since demonstrated that Monagan figured minimal n for which A(n) > n2 and A(n) > n^4 separately. We, in addition, found minimal n for which A(n) > n^k for k = 3, 5, 6, and 7.

FLAT CYCLOTOMIC POLYNOMIALS

$\Phi_n(z)$ is said to be flat if A(n) = 1. All cyclotomic polynomials of request 1 or 2 are flat; in any case, this not valid all in all for $\Phi_n(z)$ of higher request. The primary non-flat cyclotomic polynomial, $\Phi_{105}(z)$, is in certainty the first of request no less than three, as 105 = 3•5•7. Bachman, Kaplan, and all the more as of late Elder have discovered interminable groups of flat $\Phi_n(z)$ of request three [7]. Noe processed various flat $\Phi_n(z)$ of request 4 . Kaplan first built an unbounded group of flat $\Phi_n(z)$ of request four. Senior has since discovered a more extensive such family. Regardless of whether this family envelops all flat cyclotomic polynomials of request four is obscure. We don't yet know, notwithstanding, regardless of whether there exist any flat cyclotomic polynomials of request five or more noteworthy. For $\Phi_n(z)$ of request five with n < 6.5 • 10^8 , A(n) is no less than 4.

The creator looked for flat cyclotomic polynomials of request five among candidate $\Phi_n(z)$ for n of the frame n = $p_1p_2p_3p_4p_5$, a result of five odd primes fulfilling $p_k \equiv \pm 1 \mod \prod_{i=1}^{k-1} Pi$ for 1 < k ≤ 5. The littlest such n is n=746,443,728,915=3·5 31· 929· 1727939 for which the level of $\Phi_n(z)$ is ϕ(n) = 384, 846, 351, 360. Notwithstanding putting away the coefficients of $\Phi_n(z)$ to any exactness, in memory, isn't

conceivable with most current PCs. The enormous prime calculation, depicted in detail in Chapter 4, enables us to figure A(n) in a way which does not expect us to store every one of the coefficients of $\Phi_n(z)$ on the double. With this calculation, we could discover several cases of $\Phi_n(z)$ of request five and tallness 2. We were not able, in any case, to discover $\Phi_n(z)$ of request 5 and tallness 1 [8].

FUNDAMENTAL PROPERTIES OF CYCLOTOMIC POLYNOMIALS

We see in (1.7) that $\Phi_n(z)$ and $\Psi_n(z)$ are in Z[z] for $n \leq 6$. It is not immediate from their definitions whether this is true for all n. We show that it is.

Theorem 1.7: $\Phi_n(z)$ is in Z[z].

Before a proof of Theorem 1.7, we need to define the content of a polynomial.

Definition 1.8: Let $f(z) = a_k Z^k + \cdots + a_1 z + a_0$ be a polynomial of degree k in Z[z]. The content of f, denoted by cont (f), is defined as

$$\text{cont}(f) = \gcd(a_0, a_1 \ldots, a_k).$$

At the end of the day, cont(f) is the best integer l for which f/l is over the integers. Gauss initially demonstrated the accompanying result about substance, which we will use in the confirmation of 1.7. We allude to for a proof of Lemma 1.9.

Lemma 1.9: (Gauss's lemma). Let $f, g \in Z[z]$. Then cont(fg) = cont(f)cont(g).

We also use the following theorem.

Theorem 1.10: Let F be a field. Then F[z] forms a Euclidean domain with the valuation function v: F[z] \ {0} → $Z_{\geq}0$ defined by v(f(z)) = deg(f).

In other words, if F is a field and f(z), g(z) ∈ F[z] are nonzero polynomials, then there exist Q(z) and R(z) in F[z] such that f(z) = Q(z)g(z) + R(z) and either R(z) = 0 or deg(R) < deg(f). We refer to for a proof.

THE PALINDROMIC PROPERTY OF THE CYCLOTOMIC COEFFICIENTS

Lemma 1.11: Let n > 1 and let $a_n(k)$ and $c_n(k)$ be the coefficients of the z^k zerm of $\Phi_n(z)$ and $\Psi_n(z)$ respectively, so that

$$\Phi_n(z) = \sum_{k=0}^{\phi(n)} a_n(k) z^k, \text{ and } \Psi_n(z) = \sum_{k=0}^{n-\phi(n)} c_n(k) z^k.$$

Then $a_n(k) = a_n(\phi(n) - k)$ and $c_n(k) = -c_n(n - \phi(n) - k)$.

To prove Lemma 1.11, we use a complete characterization of $a_n(0) = \Phi_n(0)$.

Lemma 1.12

$$\Phi_n(0) = \begin{cases} -1: & \text{if } n = 1 \\ 1: & \text{otherwise} \end{cases}$$

ECONSPEAK: A Journal of Advances in Management IT & Social Sciences,
Vol. 7, Issue 2, February 2017 Impact Factor 5.132 ISSN: (2231-4571)
www.skirec.org Email Id: skirec.org@gmail.com

Proof: Our proof is by strong induction on n. Certainly as $\Phi 1(z) = z-1$, $\Phi_1(0) = 0-1 = 1$. Fix $n > 0$ and suppose, for $1 \le d < n$, that (1.18) holds for $\Phi_d(0)$. Evaluating both sides of the identity $z^n - 1 = \prod_{d|n} \Phi_d(z)$ at $z = 0$, we have

$$-1 = \prod_{d|n} \Phi_d(0)$$

$$= \Phi_1(0)\Phi_n(0) \prod_{d|n,1<d<n} \Phi_d(0)$$

$$= -\Phi_n(0) \prod_{d|n,1<d<n} \Phi_d(0)$$

By our induction hypothesis, $\Phi_d(0) = 1$ for any $d|n$, $1 < d < n$. It follows that $\Phi_n(0) = 1$.

A NAIVE ALGORITHM FOR COMPUTING $\Phi_N(Z)$

In this segment we depict an essential calculation for registering $\Phi_n(z)$. With that in mind, we demonstrate the accompanying basic result, which will be valuable in the evidence of a couple of cyclotomic polynomial characters from that point.

Lemma 1.13: Give ω a chance to be a nth primitive root of unity and let $k > 0$ and $m = n/\gcd(k, n)$. At that point ω^k is a mth primitive root of unity [9].

Confirmation: On the off chance that ω is a nth primitive root of unity, at that point.

$\omega^j = 1$ if and just if $n|j$. Let $d = \gcd(k, n)$, in which case $(\omega^k)^m = \omega^{k(n/d)} = (\omega^n)^{k/d} = 1$. Along these lines ω^k is a mth root of unity. It stays to be demonstrated that ω^k is, what's more, primitive. Assume then that $0 < j < m = n/d$ and $(\omega^k) j = 1$. In which case $n|jk$, consequently $\left(\frac{n}{d} \middle| j\frac{k}{d}\right)$ and, as $\frac{n}{d}$ and $\frac{k}{d}$ are coprime, this thus suggests n/d isolates j, repudiating our decision of j.

4. IMPLEMENTING MODULAR ARITHMETIC

In a considerable lot of our usage of the algorithms portrayed in this postulation we figure $\Phi_n(z)$ modulo a prime q. How we execute modular arithmetic is along these lines imperative to the performance of our algorithms.

Diminishing integers modulo q (i.e. the "%" binary administrator in C code) is costly contrasted with other integer arithmetic operations on a cutting edge PC processor. Commonly, for the motivations behind our arithmetic, we store an integer modulo a prime q in the nonnegative range [0, q). On the off chance that $0 \le u, v < q$, at that point $0 \le u + v < 2q$ and $-q < u - v < q$. Therefore to diminish $u + v$ modulo q, it gets the job done to take $u + v - q$ if $u + v$ surpasses q. Correspondingly, to lessen $u \ge v$ then $u - v \bmod q$ is precisely $u - v$, else it is $u - v + q$. Along these lines both expansion and subtraction in Zq

require at most one integer expansion, one subtraction and one examination [10]. We incline toward that 2q can fit in one machine word (i.e. $q < 2^{31}$ or $q < 2^{63}$ relying upon the engineering) with the end goal that a total u+v can fit in a machine word before we lessen it modulo q.

$$u = U_1.2^{21} + U_{0,} \qquad v = V_1.2^{21} + V_0,$$

5. THE CHINESE REMAINDER ALGORITHM'

In a considerable lot of our algorithms for registering $\Phi_n(z)$, we don't figure $\Phi_n(z)$ itself but instead pictures of $\Phi_n(z)$ modulo primes p_1, p_2, and so forward. The Chinese remainder algorithm enables us to recover $\Phi_n(z)$, if we have adequately numerous pictures.

Theorem 1.15 (The Chinese remainder theorem): Let q1, . . . $q_M \in Z$ be pairwise coprime integers, and let ui $\in Z_{qi}$ for $1 \le i \le M$. Then there exists a unique integer $U \in Z$ such that, $-\frac{Q}{2} \le U \le \frac{Q}{2}$, where Q = q1 · q2 . . . q_M, and

$$U \equiv u_1 \pmod{q}_i \quad \text{for } 1 \le i \le M.$$

We omit the proof of the Chinese remainder theorem. A proof can be found, for instance.

Given u_i and q_i for $1 \le i \le M$, the Chinese remainder algorithm allows us to find U satisfying the congruence's (1.41). For $1 \le k \le n$, let $U_k \in Z$ be the integer satisfying $U_k \equiv u_i \bmod q_i$ for $1 \le i \le k$ and $-\frac{Q_k}{2} \le U \le \frac{Q_k}{2}$, where Qk = q1 · · · qk. UM and QM are exactly U and Q of Theorem 1.15, respectively. One can obtain Q_{k+1} from Qk,

$$U_{k+1} = U_k + Q_k.\left(Q_k^{-1}.u_{k+1} - U_k \bmod u_i\right) \bmod Q_{k+1} :$$

where "modK" here means in the symmetric range $\left[-\frac{k}{2}, \frac{k}{2},\right)$.

6. CONCLUSION

A characteristic generalization of the work on heights of cyclotomic polynomials is to consider the maximal height over all divisors of x^n-1. First analyzed this issue, demonstrating that the maximal height is at most exp $\{n^{(\log 3+o(1))/\log\log n}\}$this imbalance is "best conceivable," as in it can be turned around for infinitely numerous values of n. In 2009, unequivocal recipe to the maximal height over all divisors of x^n -1 when $n = p^2q$, where p < q are primes. In a similar paper, he got upper and lower bounds for the maximal height when n = pqr, where p < q < r are primes.

REFERENCES

[1]. G. Tenenbaum, Sur un probl`eme de crible et ses applications, Ann. Sci. Ecole Norm. ´ Sup. (4) 19 (1986), 1 – 30.

[2]. R. Thangadurai, On the coefficients of cyclotomic polynomials, Cyclotomic Fields and Related Topics, Pune, 1999, Bhaskaracharya Pratishthana, Pune (2000), 311 – 322.

[3]. R. C. Vaughan, Bounds for the coefficients of cyclotomic polynomials, Michigan Math. J. 21 (1974), 289 – 295.

[4]. S. Li and C. Pomerance, On generalizing Artin's conjecture on primitive roots to composite moduli, J. Reine Angew. Math. 556 (2003), 205 – 224.

[5]. F. Luca and P. Pollack, An arithmetic function arising from Carmichael's conjecture, J. Th´eorie des Nombres de Bordeaux (to appear).

[6]. M. Beiter, Magnitude of the coefficients of the cyclotomic polynomial Fpqr(x). II, Duke Math. J. 38 (1971), 591 – 594.

[7]. D. M. Bloom, On the coefficients of the cyclotomic polynomials, Amer. Math. Monthly 75 (1968), 372 – 377.

[8]. W. Stein et al. SAGE Mathematical Software Version 4.2.6, 2011.

[9]. J. Suzuki. On the coefficients of cyclotomic polynomials. Proc. Japan Acad. Soc., A63:279– 280, 1987.

[10]. K. Ireland and M. Rosen. A classical introduction to modern number theory, volume 84 of Graduate Texts in Mathematics. Springer-Verlag, New York, second edition, 1990.