On Binary Cyclotomic Polynomials

Jeremy West

June 6, 2016

1 Introduction

The mth cyclotomic polynomial is the lowest degree, unique polynomial divisor of $(x-1)$ with real coefficients. These take the forms

$$\Phi_m(x) = \Pi_{j=1}^{m}(x - e^{2i\pi(j/m)}),\ j\ and\ m\ relatively\ prime \tag{1}$$

$$\Phi_m(x) = \Sigma_{n=0}^{m-1} a_n x^n \tag{2}$$

$$\Phi_m(x) = \Pi_{d|n}(x^d - 1)^{\mu(n/d)}, \tag{3}$$

where $d|n$ means those n that do not divide d, and where $\mu(n)$ is the Möbius function. It is defined by

$$\mu(n) = \begin{cases} 0, & n\ has\ a\ repeated\ prime\ factor\ or\ is\ not\ an\ integer \\ 1, & n\ has\ an\ even\ number\ of\ prime\ factors \\ -1, & n\ has\ an\ odd\ number\ of\ prime\ factors \end{cases}$$

In this paper I shall reproduce several results about these coefficients. The first of these results will be the case of m = p, where all the a_n are 1. In the case of m = 2p, $\Phi_m(x) = \Phi_p(-x)$. Several other results shall be presented, culminating in the result

2 Notation

Throughout this paper the letters p and q shall be used exclusively to denote primes. $\Phi_m(x)$ shall be the mth cyclotomic polynomial. $\phi(m)$ shall be the degree of $\Phi_m(x)$. $\theta(m)$ shall be the number of non-zero coefficients of Φ_m, and θ_0 and θ_1 shall be, respectively, the number of positive and negative coefficients.

3 Lemmas

I shall prove a number of lemmas and other minor points to begin with, mostly taken from [3]. First, a proof that

$$\Phi_m(x) = \Pi_{d|n}(x^d - 1)^{\mu(n/d)}.$$

Consider $f(n) = \Pi_{d|n} g(d)$.

$$\begin{aligned} \Pi_{d|n} f(n/d)^{\mu(d)} &= \Pi_{d|n}(\Pi_{m|(n/d)} g(m))^{\mu(d)} \\ &= \Pi_{m|n}(\Pi_{d|(n/m)} g(m))^{\mu}(d) \\ &= \Pi_{m|n} g(m)^{\Sigma_{d|(n/m)} g(m)^{\mu(d)}} = g(n) \end{aligned}$$

Therefore $g(n) = \Pi_{d|n} f(n/d)^{\mu(d)}$. If we define

$$f(n) = x^n - 1 = \Pi_{d|n}\Phi_d(x),$$

then

$$\begin{aligned} g(n) = \Phi_n(x) &= \Pi_{d|n} f(n/d)^{\mu(d)} \\ = \Pi_{d|n}(x^{n/d} - 1)^{\mu(d)} &= \Pi_{d|n}(x^d - 1)^{\mu(n/d)}. \end{aligned}$$

Lemma 1 *if* $n = p_1^{a_1} p_2^{a_2} ... p_l^{a_l}$, $a_i > 0$, *and* $N = p_1 p_2 ... p_l$, *then* $\Phi_n(x) = \Phi_N(x^{n/N})$.

Proof.

$$\Phi_n(x) = \Pi_{d|n}(x^{n/d} - 1)^{\mu(d)} = \Pi_{d|\{n,N\}}(x^{n/d} - 1)^{\mu(d)}$$
$$= \Pi_{d|N}((x^{n/N})^{N/d} - 1)^{\mu(d)} = \Phi_N(x^{n/N}).$$

Lemma 2 *if* $n > 1$, *then* $x^{\phi(n)}\Phi_n(1/x) = \Phi_n(x)$.

Proof.

$$\Phi_n(1/x) = \Pi_{d|n}((1/x)^d - 1)^{\mu(n/d)}$$
$$= \Pi_{d|n}(1 - x^d)^{\mu(n/d)} \Pi_{d|n}(1/x^d)^{\mu(n/d)}$$

since $\Sigma_{d|n} d * \mu(n/d) = \phi(n)$, this is the desired result. One consequence of this is that the coefficients of Φ are symmetric, or $a_j = a_j(\phi(n) - j)$.

4 Case 1 (m = p)

Theorem 1 *Let* $m = p$ *be prime. Then* $\Phi_m(x) = \Sigma_{n=0}^{p-1} x^n$

Proof: First note that $x^p - 1 = (x-1)(x^{p-1} + x^{p-2} + ... + x + 1)$ (The elephant-teacup identity). $(x-1)$ is not a factor unique to $x^m - 1$ for $m \neq 1$. $x^{p-1} + x^{p-2} + ... + x + 1$ clearly has no zeros for $x \geq 0$; for $p = 2$, this problem is trivial; for $p > 2$, and therefore odd, it is simple to show that there are no zeros in $\{x < -1\}$: Each term of even power can be paired with it's neighboring term of lesser degree, and these pairings are positive in $\{x < -1\}$. In $\{-1 < x < 0\}$ the terms can be paired in the reverse order: $1 + x$, $x^2 + x^3$, and so on. All these terms will be positive. For $x = -1$, $x^{p-1} + x^{p-2} + ... + x + 1$ is simply 1. The polynomial $x^{p-1} + x^{p-2} + ... + x + 1$ therefore has no zeros on the real line, and is not factorable in real coefficients. Therefore, $\Phi_p(x) = x^{p-1} + x^{p-2} + ... + x + 1 = \Sigma_{n=0}^{p-1} x^n$

5 Case 2 (m = 2p, p ≠ 2)

Theorem 1 *Let* $m = 2p$. *Then* $\Phi_m(x) = \Sigma_{n=0}^{p-1}(-x)^n$

Proof: First note that $x^{2p} - 1 = (x^p - 1)(x^p + 1)$. The divisors of $(x^p - 1)$ are also divisors of lower cyclotomic polynomials, so we can refine our search to $(x^p + 1)$. This can be rewritten as $-((-x)^p - 1)$. Thus, it has been shown that for p an odd prime

$$\Phi_{2p}(x) = \Sigma_{n=0}^{p-1}(-x)^n = \Phi_p(-x) \tag{4}$$

6 Case 3 (m = pq)

Considering the results of case 1, note that

$$\Phi_{pq}(x) = (x^{pq} - 1)(x - 1)/((x^p - 1)(x^q - 1)) \tag{5}$$

and that $\Phi_{pq}(1) = 1$ (for this, factor out all the $(x - 1)$ terms). $\theta_0(pq) = 1 + \theta_1(pq)$, and

$$\theta(pq) = 2\theta_0(pq) - 1.$$

At this point, we assume that $q > p$, and define u by

$$(qu)(modulo\ p) = -1,\ (0 < u < p). \tag{6}$$

Carlitz gives a proof in [1] that $\theta_0(pq) = (p - u)(uq + 1)/p$. The formula holds for p, q relatively prime, but not necessarily prime themselves.

7 References

[1] Carlitz [1966] The Number of Terms in the Cyclotomic Polynomial $F_{pq}(x)$, American Mathematical Monthly Vol. 73, No. 9 (Nov., 1966), pp. 979-981
[2] Fouvry [2013] On Binary Cyclotomic Polynomials, Algebra and Number Theory Vol. 7, No. 5 (2013)
[3] Thangadurai [1999] On the Coefficients of Cyclotomic Polynomials, http://bprim.org/cyclotomicfieldbook/th.pdf