On the Middle Coefficient of a Cyclotomic Polynomial

Gregory P. Dresden

The cyclotomic polynomials Φ_n for $n = 1, 2, 3, \ldots$ (familiar to every student of algebra) are the minimal polynomials for the primitive nth roots of unity:

$$\Phi_n(x) = \prod_{(k,n)=1} \left(x - e^{2\pi i k/n}\right).$$

Clearly Φ_n has degree $\phi(n)$, where ϕ signifies Euler's totient function. These monic polynomials can be defined recursively as $\Phi_1(x) = x - 1$ and $\prod_{i|n} \Phi_i(x) = x^n - 1$ for $n > 1$. The first few are easily calculated to be $x - 1$, $x + 1$, $x^2 + x + 1$, $x^2 + 1, \ldots$. For these and other basic facts, see an algebra text such as [**5**].

While it might appear that the coefficients of the cyclotomic polynomials are always ± 1, the presence of $2x^7$ in $\Phi_{105}(x)$ shows that this is not invariably the case (and indeed is a good counterexample for those students who insist that the "law of small numbers" is universally valid; see [**4**] for further discussion). Naturally, much work has been done on the values of the coefficients of $\Phi_n(x)$. One amazing fact worthy of mention is that every integer appears as a coefficient in some cyclotomic polynomial (see [**1**], [**8**]).

In this article, we provide a short and elementary proof of the following result:

Theorem 1. *For $n \geq 3$ the middle coefficient of $\Phi_n(x)$ is either zero (when n is a power of 2) or an odd integer.*

A similar result can be found in [**6**], where Lam and Leung directly calculate the middle coefficient of $\Phi_{pq}(x)$ for distinct primes p and q and show it to be ± 1. This had been done earlier by Beiter [**2**] for the case of distinct odd primes. Both papers rely on the partition of $\phi(pq)/2$ into $rp + sq$. In contrast, our proof uses only some very basic facts about minimal polynomials. We also point out that for $n \neq pq$ the polynomial $\Phi_n(x)$ could indeed have a middle coefficient different from 1 or -1. The first such occurence is at $n = 385$ (giving a middle coefficient of -3), after which one sees 5 at $n = 4785$, followed by -7 at $n = 7735$, and 19 at $n = 11305$. All these values of n are square-free products of small odd primes, which is alluded to in [**8**].

Before proceeding with the proof of Theorem 1, we do a bit of preliminary work. The first lemma establishes a useful fact about $\Phi_n(x)$.

Lemma 1. *If $n \geq 3$ and n is odd, then $\Phi_n(-1) = 1$.*

Proof. For $n \geq 3$,

$$\prod_{i|n, i>1} \Phi_i(x) = \frac{x^n - 1}{x - 1},$$

so (since n is odd)

$$\prod_{i|n, i>1} \Phi_i(-1) = \frac{(-1)^n - 1}{(-1) - 1} = 1.$$

Also, $\Phi_3(-1) = 1$. By a simple induction argument we conclude that $\Phi_n(-1) = 1$ whenever n is at least three and odd. ■

Next we review some basic information. We use ζ_n to signify a primitive nth root of unity (that is, $\zeta_n = e^{2\pi ik/n}$ for some k relatively prime to n), and $f_n(x)$ to denote the minimal polynomial of $\zeta_n + \zeta_n^{-1}$ (recall that the *minimal polynomial* of an algebraic complex number α is the monic polynomial $p(x)$ in $\mathbb{Q}[x]$ of smallest degree such that $p(\alpha) = 0$). It is not hard to show using elementary methods (see [**7**]) that f_n has integer coefficients and that when $n \geq 3$ the degree of f_n is half that of $\Phi_n(x)$. In fact,

$$\Phi_n(x) = f_n(x + x^{-1}) \cdot x^{\phi(n)/2} \qquad (n \geq 3), \tag{1}$$

because (after simplifying the right-hand side) the polynomials on both sides of (1) are monic, are of degree $\phi(n)$, and have ζ_n as a root. The first few such polynomials f_n (for $n \geq 3$) are easy to derive from (1) and read as follows:

$$\begin{array}{lll} f_3(x) = x + 1, & f_5(x) = x^2 + x - 1, & f_7(x) = x^3 + x^2 - 2x - 1, \\ f_4(x) = x, & f_6(x) = x - 1, & f_8(x) = x^2 - 2. \end{array}$$

From this, we see that the constant term in f_n is not always ± 1 (equivalently, $\zeta_n + \zeta_n^{-1}$ is not necessarily an *algebraic unit*, meaning a unit in the ring of algebraic integers). However, by doing a careful comparison of the f_n with the Chebyshev polynomials, Carlitz and Thomas [**3**] showed that when $n \geq 3$ and n is not divisible by 4, the constant term in $f_n(x)$ is either 1 or -1. For the sake of completeness, we provide a nonelementary, but much shorter, proof of this fact.

Lemma 2. *If $n \geq 3$ and $n \not\equiv 0 (\mathrm{mod}\, 4)$, then $\zeta_n + \zeta_n^{-1}$ is an algebraic unit.*

Proof. Let $m = n$ for n odd and $m = n/2$ for n even. Note that m is itself odd and $m \geq 3$. Note as well that ${\zeta_n}^2$ is a primitive mth root of unity (and thus a root of $\Phi_m(x)$). Then ${\zeta_n}^2 + 1$ is a root of $\Phi_m(x - 1)$, which is a monic polynomial with constant term $\Phi_m(-1) = 1$ (by Lemma 1). It follows that ${\zeta_n}^2 + 1$ is an algebraic unit, as is ζ_n. Thus, $\zeta_n + \zeta_n^{-1} = ({\zeta_n}^2 + 1)/\zeta_n$ is likewise an algebraic unit. ■

We are now ready to bring everything together.

Proof of Theorem 1. If $n = 2^k$, then $\Phi_n(x) = x^{2^{k-1}} + 1$, a polynomial with zero as its middle coefficient. We proceed assuming that n is not a power of 2.

Note that if ζ is a primitive $4k$th root of unity, then ζ^2 is a primitive $2k$th root of unity. Since $\phi(4k) = 2\phi(2k)$, we know that $\Phi_{4k}(x) = \Phi_{2k}(x^2)$. Since the middle coefficient of $\Phi_{2k}(x^2)$ is the same as that of $\Phi_{2k}(x)$, we can further assume without loss of generality that 4 does not divide n.

Now letting $f_n(x)$ be the minimal polynomial of $\zeta_n + \zeta_n^{-1}$, we know from Lemma 2 that f_n has constant coefficient ± 1. Thus, we can write $f_n(x) = x^k + a_{k-1}x^{k-1} + \cdots + a_1 x \pm 1$ (for $k = \phi(n)/2$), and so from equation (1) we obtain

$$\Phi_n(x) = \left[(x + x^{-1})^k + a_{k-1}(x + x^{-1})^{k-1} + \cdots \pm 1\right] \cdot x^k. \tag{2}$$

The middle coefficient of $\Phi_n(x)$ is the coefficient of the x^k term in (2) (recall, $k = \phi(n)/2$). This number is simply the sum of the constant terms appearing in each expression $a_i(x + x^{-1})^i$ in (2), plus the final ± 1. The constant term in $a_i(x + x^{-1})^i$

is either zero (for i odd) or $a_i\binom{i}{i/2}$ (for i even). As a result, the middle coefficient of $\Phi_n(x)$ is

$$\sum_{i=2j} a_i \binom{i}{i/2} \pm 1 = \sum_j a_{2j}\binom{2j}{j} \pm 1. \tag{3}$$

By a familiar identity,

$$\binom{2j}{j} = \binom{2j-1}{j-1} + \binom{2j-1}{j} = 2\binom{2j-1}{j}.$$

Thus the middle coefficient of $\Phi_n(x)$ is odd when n is not a power of 2. ■

REFERENCES

1. S. D. Adhikari, S. A. Katre, and D. Thakur, eds., *Cyclotomic Fields and Related Topics*, Bhaskaracharya Pratishthana, Pune, 2000.
2. M. Beiter, The midterm coefficient of the cyclotomic polynomial $F_{pq}(x)$, this MONTHLY **71** (1964) 769–770.
3. L. Carlitz and J. M. Thomas, Rational tabulated values of trigonometric functions, this MONTHLY **69** (1962) 789–793.
4. R. K. Guy, The strong law of small numbers, this MONTHLY **95** (1988) 697–712.
5. T. W. Hungerford, *Algebra*, Springer-Verlag, New York, 1980.
6. T. Y. Lam and K. H. Leung, On the cyclotomic polynomial $\Phi_{pq}(X)$, this MONTHLY **103** (1996) 562–564.
7. D. H. Lehmer, A note on trigonometric algebraic numbers, this MONTHLY **40** (1933) 165–166.
8. J. Suzuki, On coefficients of cyclotomic polynomials, *Proc. Japan Acad. Ser. A Math. Sci.* **63** (1987) 279–280.

Department of Mathematics, Robinson Hall, Washington and Lee University, Lexington, VA 24450
dresdeng@wlu.edu