PRIMITIVE ROOTS THE CYCLOTOMIC WAY

Joseph B. Dence

1. Introduction. Every prime possesses a primitive root. So stated (in an equivalent way) J. H. Lambert in 1769; Legendre gave the first correct proof in 1785. Gauss, in 1801, published two proofs in his *Disquisitiones Arithmeticae* [3a]. This important theorem is standard material in any first course in number theory. A survey of 21 number theory texts, both old and recent, shows the following distribution of proofs:

(1) 13 texts prove the theorem with the aid of the following lemma on the Euler ϕ–function [1a–l,5a]:

$$\sum_{d|n} \phi(d) = n;$$

(2) 2 texts use the Möbius Inversion Formula, together with the lemma,

$$\sum_{d|n} \mu(d)(n/d) = \phi(n),$$

also drawn from material on multiplicative functions [1f,m];

(3) 4 texts use only elementary facts on the orders of integers, and possibly also Lagrange's Theorem on roots in a field [1n–q];

(4) 2 texts use only Lagrange's Theorem and the concept of the least (or minimal) universal exponent (first introduced by R. D. Carmichael) [1r,s];

(5) 1 text employs an algebraic proof that considers the generation of various subgroups of $\mathbb{Z}_p^x$ [1f];

(6) 1 text uses Lagrange's Theorem, together with a key result on orders of elements in finite Abelian groups [1t].

All of the above methods of proof have features of interest, and there are pros and cons of each. Gauss' own proofs belonged to methods (1) and (3).

In this expository paper we present an alternative approach to primitive roots that may appeal to some students. Although the theory is not new [6], it deserves to be better known. The approach makes contact with the topic of cyclotomic polynomials, which are both important [10] and interesting in their own right [2,7].

2. The Cyclotomic Polynomials. Let $n > 1$ be an integer; the nth cyclotomic polynomial, $\Phi_n(x)$, is defined as

$$\Phi_n(x) = \prod_{\zeta} (x - \zeta),$$

where ζ spans all of the primitive nth roots of unity. We define $\Phi_1(x) = x - 1$. The three basic properties of the $\Phi_n(x)$'s that we shall require are [4]:

Property 1. The algebraic degree of $\Phi_n(x)$ is $\phi(n)$;

Property 2. All of the coefficients in $\Phi_n(x)$ are integers;

Property 3. For all $n \geq 1$, $x^n - 1 = \prod_{d|n} \Phi_d(x)$.

For illustration, we show in Table 1 the first 16 cyclotomic polynomials. Despite what Table 1 suggests, there are cyclotomic polynomials that possess arbitrarily large coefficients [7,8].

n	$\Phi_n(x)$	n	$\Phi_n(x)$
1	$x - 1$	9	$x^6 + x^3 + 1$
2	$x + 1$	10	$x^4 - x^3 + x^2 - x + 1$
3	$x^2 + x + 1$	11	$x^{10} + x^9 + x^8 + \cdots + x + 1$
4	$x^2 + 1$	12	$x^4 - x^2 + 1$
5	$x^4 + x^3 + x^2 + x + 1$	13	$x^{12} + x^{11} + x^{10} + \cdots + x + 1$
6	$x^2 - x + 1$	14	$x^6 - x^5 + x^4 - x^3 + x^2 - x + 1$
7	$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$	15	$x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$
8	$x^4 + 1$	16	$x^8 + 1$

Table 1. The Polynomials $\Phi_n(x)$ for $n = 1$–16.

3. Zeros of the Cyclotomic Polynomials in Fields $\mathbb{Z}_\mathbf{p}$. In what follows, p is any prime and d (or d_i) is any divisor of $p - 1$.

Theorem 1. $\Phi_d(x) \equiv 0 \pmod p$ has $\phi(d)$ roots.

Proof. $x^d \equiv 1 \pmod p$ has d incongruent roots [5a,6]. Since, by Property 3, $x^d - 1 = \prod_{d_i|d} \Phi_d(x)$, then Property 1, together with Lagrange's Theorem, forces $\Phi_d(x)$, in particular, to have $\phi(d)$ zeros in $\mathbb{Z}_p$.

Theorem 2. $x_0 \in \mathbb{Z}_p^x$ is a root of $\Phi_d(x) \equiv 0 \pmod p$ if and only if the order of $x_0 \pmod p$ is d.

Proof. Let the divisors of $p-1$ be sequenced as follows: $1 = d_1 < d_2 < \cdots < d_n = p-1$. The theorem is trivially true for $d = d_1$; assume it is also true for the first k divisors of $p-1$ $(1 \leq k < n)$. We have

$$x^{d_{k+1}} - 1 = \prod_{d_i | d_{k+1}} \Phi_{d_i}(x),$$

and the d_{k+1} roots of all the congruences $\{\Phi_{d_i}(x) \equiv 0 \pmod p\}$ are distinct. Suppose the order of $x_0 \pmod p$ is d_{k+1}; then x_0 is a root of just one of the congruences $\Phi_{d_i}(x) \equiv 0 \pmod p$. In fact, it must be the congruence corresponding to $d_i = d_{k+1}$, since any of the smaller d_i's would imply a contradiction of the induction hypothesis.

On the other hand, if x_0 is one of the $\phi(d_{k+1})$ roots of $\Phi_{d_{k+1}}(x) \equiv 0 \pmod p$, then $x_0^{d_{k+1}} - 1 \equiv 0 \pmod p$ holds. The order of x_0 is thus d_{k+1}; for if the order were $h < d_{k+1}$, then $h|d_{k+1}$ would be true and x_0 would be a root of $\Phi_h(x) \equiv 0 \pmod p$, which again is a contradiction of the induction hypothesis. Thus, the theorem holds for $d = d_{k+1}$, and so is true for all divisors of $p-1$.

Corollary. Every prime p has $\phi(p-1)$ primitive roots.

Proof. By Theorem 1, $\Phi_{p-1}(x) \equiv 0 \pmod p$ has $\phi(p-1)$ roots, and by Theorem 2 these are all of order $p-1$.

In Table 2 we give an illustration of Theorem 2 for the case of $p = 19$.

d	Roots of $\Phi_d(x) \equiv 0 \pmod{19}$	Order (mod 19) of the Roots
1	1	1
2	18	2
3	7,11	3
6	8,12	6
9	4,5,6,9,16,17	9
18	2,3,10,13,14,15	18

Table 2. Orders of the Zeros in $\mathbb{Z}_p$ of the Cyclotomic Polynomial Factors Corresponding to $p-1=18$.

4. A Subsidiary Result. Let S_p denote the sum of the primitive roots of the prime p. Gauss proved a congruence theorem for S_p; his argument was combinatorial in nature [3b]. We can establish the same result by means of cyclotomic polynomials. If we write

$$\Phi_n(x) = \sum_{k=0}^{\phi(n)} c(n,k)x^k,$$

then in view of Theorem 1 the sum of the roots of $\Phi_n(x) \equiv 0 \pmod{p}$ is congruent to $-c(n,\phi(n)-1)$, $n|(p-1)$. Gauss' theorem is suggested by the very brief data given in Table 3.

n	$\Phi_n(x)$	$c(n,\phi(n)-1)$	$S_p \pmod{p}$
$4(=2^2)$	x^2+1	0	0
$12(=2^2\cdot 3)$	x^4-x^2+1	0	0
$18(=2\cdot 3^2)$	x^6-x^3+1	0	0
$6(=2\cdot 3)$	x^2-x+1	-1	-1
$10(=2\cdot 5)$	$x^4-x^3+x^2-x+1$	-1	-1
2	$x+1$	1	1
$30(=2\cdot 3\cdot 5)$	$x^8+x^7-x^5-x^4-x^3+x+1$	1	1

Table 3. Selected $\Phi_n(x)$ When n is Squarefree (lower half) or Not (upper half), and $n+1$ is a Prime p.

Theorem 3. If $n = \prod_{i=1}^{r} p_i^{\alpha_i}$, then $c(n, \phi(n) - 1) = 0$ if at least one $\alpha_i > 1$, and $c(n, \phi(n) - 1) = (-1)^{r-1}$ otherwise.

Proof. The theorem is trivially true for the first nonsquarefree integer ($n = 4$) and for all squarefree integers $n > 1$ for which $r = 1$ (i.e., primes). Assume it also holds for the first k nonsquarefree integers and the first k squarefree integers. Now, on the one hand, let $N = \prod_{i=1}^{s} p_i^{\alpha_i}$ be the $(k+1)$st nonsquarefree integer and define $m = \prod_{i=1}^{s} p_i$. We can write (using Property 3)

$$\Phi_n(x) = \frac{x^N - 1}{[\prod_d \Phi_d(x)] \prod_D \Phi_D(x)} = \frac{x^N - 1}{(x^m - 1)[\prod_D \Phi_D(x)]},$$

where the d's are squarefree divisors of N, $1 \leq d < N$, and the D's are nonsquarefree divisors of N, $1 < D < N$. The induction hypothesis gives us immediately that the term of next–to–highest degree is absent in the denominator, and so upon division the term of degree $\phi(N) - 1$ in $\Phi_N(x)$ is also absent. The first half of the theorem follows by mathematical induction.

On the other hand, if N is the $(k+1)$st squarefree integer, then there is no extended product over D's. There are $\binom{k+1}{m}$ factors $\Phi_d(x)$, $m = 0, 1, 2, \ldots k$, for which d is the product of m distinct primes. By the induction hypothesis the coefficient of the term of degree $\phi(d) - 1$ in each such $\Phi_d(x)$ is $(-1)^{m-1}$. Multiplication of all the $\Phi_d(x)$'s with a common m and summation over all m gives for the coefficient of the term of next–to–highest degree in $\prod_d \Phi_d(x)$ the value

$$\sum_{m=0}^{k} (-1)^{m-1} \binom{k+1}{m} = (-1)^{k+1}.$$

Hence, upon division, the coefficient of the term of next–to–highest degree in

$$\Phi_N(x) = \frac{x^N - 1}{\prod_d \Phi_d(x)}$$

is $(-1)^k = (-1)^{(k+1)-1}$. The second half of the theorem also holds by mathematical induction.

We note that Theorem 3 does not depend on $n+1$ being a prime. However, Gauss' Theorem now follows straight off if in Theorem 3 we do take $n = p-1 > 1$ there.

Corollary. (Gauss) For any odd prime

$$S_p \equiv \begin{cases} 0 \pmod{p} & \text{if } p-1 \text{ is not squarefree} \\ (-1)^r \pmod{p} & \text{if } p-1 = \prod_{i=1}^{r} p_i \end{cases}$$

It may be noted that the Corollary can be applied, with slight modification, to any of the sets of integers having a common order d, $d|(p-1)$ (see Table 2) [5b,9].

References

1. (a) G. E. Andrews, *Number Theory*, Dover Publications, New York, 1994, 97–98. (b) T. M. Apostol, *Introduction to Analytic Number Theory*, Springer–Verlag, New York, 1976, 206–208. (c) D. M. Burton, *Elementary Number Theory*, 3rd ed., McGraw–Hill, New York, 1997, 158–159. (d) H. Griffin, *Elementary Theory of Numbers*, McGraw–Hill, New York, 1954, 105–106. (e) E. Grosswald, *Topics from the Theory of Numbers*, 2nd ed., Birkhäuser, Boston, 1984, 54–55. (f) K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., Springer–Verlag, New York, 1990, 40–41. (g) N. Koblitz, *A Course in Number Theory and Cryptography*, Springer–Verlag, New York, 1987, 32–33. (h) W. J. LeVeque, *Elementary Theory of Numbers*, Addison–Wesley, Reading, 1962, 67–68. (i) T. Nagell, *Introduction to Number Theory*, John Wiley & Sons, New York, 1951, 107–108. (j) O. Ore, *Number Theory and its History*, McGraw–Hill, New York, 1948, 281–284. (k) K. H. Rosen, *Elementary Number Theory and its Applications*, 3rd ed., Addison–Wesley, Reading, 1993, 286–287. (l) C. Vanden Eynden, *Elementary Number Theory*, Random House, New York, 1987, 219–220. (m) H. E. Rose, *A Course in Number Theory*, 2nd ed., Oxford University Press, Oxford, 1994, 89–90. (n) L. E. Dickson, *Modern Elementary Theory of Numbers*, University of Chicago Press, Chicago, 1939, 26. (o) C. T. Long, *Elementary Introduction to Number Theory*, D. C. Heath, Boston, 1965, 94–95. (p) I. Niven, H. S. Zuckerman, and H. L. Montgomery, *An Introduction to the Theory of Numbers*, 5th ed., John Wiley & Sons, New York, 1991, 98–99. (q) I. M. Vinogradov, *Elements of Number Theory*, Dover Publications, New York, 1954, 106–107. (r) A. Adler and J. E. Coury, *The Theory of Numbers: A Text and Source Book of Problems*, Jones and Bartlett, Boston, 1995, 161. (s) R. Kumanduri and C. Romero, *Number Theory with Computer Applications*, Prentice–Hall, Upper Saddle River, NJ,

1998, 178. (t) J. B. Dence and T. P. Dence, *Elements of the Theory of Numbers*, Harcourt/Academic Press, San Diego, CA, 1999, 183–185.

2. (a) G. Bachman, "On the Coefficients of Cyclotomic Polynomials," *Memoirs of the American Mathematical Society*, Vol. 106, No. 510, American Mathematical Society, Providence, 1993. (b) P. Erdős and R. C. Vaughan, "Bounds for the rth Coefficients of Cyclotomic Polynomials," *Journal of the London Mathematical Society (2)*, 8 (1974), 393–400. (c) W. J. Guerrier, "The Factorization of the Cyclotomic Polynomials Mod p," *American Mathematical Monthly*, 75 (1968), 46. (d) H. Möller, "Über die Koeffizienten des n–ten Kreisteilungspolynoms," *Mathematische Zeitschrift*, 119 (1971), 33–40. (e) D. Zeitlin, "On Coefficient Identities for Cyclotomic Polynomials $F_{pq}(x)$," *American Mathematical Monthly*, 75 (1968), 976–980.

3. (a) C. F. Gauss, *Disquisitiones Arithmeticae* (trans. by A. A. Clarke), Yale University Press, New Haven, 1966, 33–36. (b) *ibid.*, 52–54.

4. L. J. Goldstein, *Abstract Algebra*, Prentice–Hall, Englewood Cliffs, NJ, 1973, 226–227. See also reference 1f, p. 194.

5. (a) G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 5th ed., Oxford University Press, Oxford, 1979, 85–86. (b) *ibid.*, 237–239. This treatment considers Ramanujan sums.

6. L. Kronecker, *Vorlesungen über Zahlentheorie*, Vol. 1, B. G. Teubner, Leipzig, 1901, 375–388 (reprinted by Springer–Verlag, Berlin, 1978).

7. E. Lehmer, "On the Magnitude of the Coefficients of the Cyclotomic Polynomial," *Bulletin of the American Mathematical Society*, 42 (1936), 389–392.

8. I. Schur (1931, unpublished), as cited in Lehmer [vide supra].

9. M. A. Stern, "Bemerkungen über hohere Arithmetik," *Journal für Mathematik*, 6 (1830), 147–153, as quoted in R. Moller, "Sums of Powers of Numbers Having a Given Exponent Modulo a Prime," *American Mathematical Monthly*, 59 (1952), 226–230.

10. See, for example, L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Springer–Verlag, New York, 1997, 12–13, where the author gives an accessible proof (via cyclotomic polynomials) that for any $n > 1$ there are infinitely many primes $p \equiv 1 \pmod{n}$, a special case of Dirichlet's theorem.

Joseph B. Dence
Department of Chemistry
University of Missouri – St. Louis
St. Louis, MO 63121