CYCLOTOMIC POLYNOMIALS

1. Introduction

Let $\zeta = e^{2\pi i/n}$. Then $\zeta, \zeta^2, \ldots, \zeta^n$ are the n n^{th} roots of unity. They form the vertices of a regular n-gon in the complex plane. If $(a, n) > 1$ then ζ^a is a root of unity of order $n/(a, n) < n$, but if $(a, n) = 1$ then ζ is not a root of lower order, and in this case we call ζ^a a *primitive* n^{th} root of unity. We define the n^{th} cyclotomic polynomial $\Phi_n(x)$ to be the monic polynomial of degree $\phi(n)$ whose roots are the primitive n^{th} roots of unity:

$$\Phi_n(x) = \prod_{\substack{a=1\\(a,n)=1}}^{n} (x - \zeta^a). \tag{1}$$

Our first observation concerning cyclotomic polynomials is that

$$z^n - 1 = \prod_{d|n} \Phi_d(x). \tag{2}$$

To see this, it suffices to classify roots of unity ζ^a according to the value of (a, n). Thus we see that

$$\begin{aligned} z^n - 1 &= \prod_{a=1}^{n} (x - \zeta^a) \\ &= \prod_{d|n} \prod_{\substack{a=1\\(a,n)=n/d}}^{n} (x - \zeta^a). \end{aligned}$$

Write $a = bn/d$ where $(b, d) = 1$ and $1 \le b \le d$. Then the above is

$$\begin{aligned} &= \prod_{d|n} \prod_{\substack{b=1\\(b,d)=1}}^{d} (x - \zeta^{bn/d}) \\ &= \prod_{d|n} \Phi_d(x). \end{aligned}$$

Our next task is to show that $\Phi_n(x)$ has integral coefficients. To establish this, we induct on n. We note that $\Phi_1(x) = x - 1$ has integral coefficients. Suppose that $\Phi_d(x)$ has integral coefficients for all $d < n$. Put

$$G_n(x) = \prod_{\substack{d|n\\d<n}} \Phi_d(x).$$

Then by the inductive hypothesis, $G_d(x)$ has integral coefficients. Suppose that $F(x)$ and $G(x)$ are polynomials with integral coefficients. Then by the division algorithm there is a quotient polynomial $Q(x)$ and a remainder polynomial $R(x)$ such that $F(x) = G(x)Q(x) + R(x)$ and $\deg R < \deg G$. In general, the coefficients of $Q(x)$ and $R(x)$ are rational numbers, but if $G(x)$ is monic then the coefficients of $Q(x)$ and $R(x)$ are integers. We apply this with $F(x) = x^n - 1$, $G(x) = G_n(x)$. Then $R(x)$ is identically 0 and $Q(x) = \Phi_n(x)$.

The identity (2) can be inverted by the Möbius inversion formula to yield a formula for $\Phi_n(x)$ in terms of the polynomials $x^d - 1$:

$$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}. \tag{3}$$

Since

$$\frac{1}{1-x^d} = 1 + x^d + x^{2d} + x^{3d} + \cdots ,$$

it is evident that the right hand side of (3) is a power series with integral coefficients. This provides a second means of seeing that $\Phi_n(x)$ has integral coefficients.

The first few cyclotomic polynomials are as follows:

$$\begin{aligned}
\Phi_1(x) &= x - 1, \\
\Phi_2(x) &= x + 1, \\
\Phi_3(x) &= x^2 + x + 1, \\
\Phi_4(x) &= x^2 + 1, \\
\Phi_5(x) &= x^4 + x^3 + x^2 + x + 1, \\
\Phi_6(x) &= x^2 - x + 1, \\
\Phi_7(x) &= x^6 + x^5 + x^4 + x^3 + x^2 + x + 1, \\
\Phi_8(x) &= x^4 + 1, \\
\Phi_9(x) &= x^6 + x^3 + 1, \\
\Phi_{10}(x) &= x^4 - x^3 + x^2 - x + 1, \\
\Phi_{11}(x) &= x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1, \\
\Phi_{12}(x) &= x^4 - x^2 + 1, \\
\Phi_{13}(x) &= x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1, \\
\Phi_{14}(x) &= x^6 - x^5 + x^4 - x^3 + x^2 - x + 1, \\
\Phi_{15}(x) &= x^8 - x^7 + x^5 - x^4 + x^3 - x + 1, \\
\Phi_{16}(x) &= x^8 + 1.
\end{aligned}$$

It is noteworthy that the coefficients of the above polynomials take only the values ± 1 and 0. At one time this was conjectured to apply to all cyclotomic polynomials, but $\Phi_{105}(x)$ provides a counter-example, and we now know that there are cyclotomic polynomials with very large coefficients. This occurs particularly when n is highly composite.

2. Primitive roots modulo p

Euler used cyclotomic polynomials to prove the existence of primitive roots mod p. Gauss dismissed Euler's argument as incomplete, because Euler did not properly develop the material in the preceding section. To reconstruct how Euler might have reasoned, we take $n = p-1$ in (2) to see that

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

Since the left hand side has $p-1$ roots modulo p, each $\Phi_d(x)$ on the right hand side must have $\phi(d)$ roots (mod p), and moreover if d and e are distinct divisors of $p-1$, then the roots of $\Phi_d(x)$ (mod p) must be disjoint from the roots (mod p) of $\Phi_e(x)$.

Lemma 1. *If a has order h modulo p, then $\Phi_h(a) \equiv 0 \pmod p$.*

Proof. From (2) with $n = h$ and $x = a$, we see that the left hand side is a multiple of p, and hence $p|\Phi_d(a)$ for some $d|h$. From (2) again we see that $\Phi_d(x)$ divides $(x^d - 1)$ in $\mathbb{Z}[x]$, and hence $\Phi_d(a)|(a^d - 1)$. Hence $a^d \equiv 1 \pmod p$. By the minimality of h, it follows that $d = h$, so the proof is complete.

Lemma 2. *If $\Phi_d(a) \equiv 0 \pmod p$ and $d|(p-1)$, then a has order d.*

Proof. Let h denote the order of a modulo p. Since $\Phi_d(a)|(a^d-1)$, we have $a^d \equiv 1 \pmod p$, and hence $h|d$. From Lemma 1 we also know that $p|\Phi_h(a)$. That is, $\Phi_d(x)$ and $\Phi_h(x)$ have a common root a (mod p). This implies that $d = h$.

On combining these lemmas we see that if $h|(p-1)$, then the roots (mod p) of $\Phi_h(x)$ are precisely the residue classes of order h. Thus there are exactly $\phi(h)$ residue classes of order h. In particular, there are exactly $p-1$ residue classes of order $p-1$, which is to say primitive roots.

Lemma 2 is false if the hypothesis $d|(p-1)$ is omitted. To see this, note that $\Phi_p(1) \equiv 0 \pmod p$, but 1 does not have order p modulo p; it has order 1. Nevertheless, Lemma 2 can be extended, as follows.

Lemma 3. *If $\Phi_n(a) \equiv 0 \pmod p$, then a has order $n \pmod p$, or $p|n$.*

Proof. Let h denote the order of a modulo p. Since $a^n \equiv 1 \pmod p$, it follows that $h|n$. If $h = n$, then we are done. Suppose that $h < n$. Then $\Phi_h(x)$ and $\Phi_n(x)$ are distinct factors of $x^n - 1$. Moreover, $\Phi_h(x)$ has a factor $x - a$ modulo p, and so does $\Phi_n(x)$. Hence $F_n(x) = x^n - 1$ has a factor $(x-a)^2$ modulo p. Hence $F_n'(x)$ has a factor $x - a$ modulo p. But

$$nF_n(x) - xF_n'(x) = -n \tag{4}$$

is a polynomial identity. Substitute $x = a$. Since $p|F_n(a)$ and $p|F_n'(a)$, it follows that $p|n$.

One consequence of Lemma 3 is that if $n \nmid (p-1)$ and $p \nmid n$, then the congruence $\Phi_n(x) \equiv 0 \pmod p$ has no solution.

3. Primes $\equiv 1 \pmod{m}$

We prove that there are infinitely many prime numbers $p \equiv 1 \pmod{m}$. This is a special case of a theorem of Dirichlet, which asserts that if $(a, m) = 1$ then there exist infinitely many prime numbers $p \equiv a \pmod{m}$. Since the assertion is trivial for $m = 1$, we may suppose that $m \geq 2$. Suppose that $p_1, p_2, \ldots, p_r$ are primes that are $\equiv 1 \pmod{m}$. We show that there is at least one more such prime. Set $x = mp_1p_2 \cdots p_r$, and let p be a prime factor of $\Phi_m(x)$. Note that $x \geq 2$, so that each factor on the right hand side of (1) has absolute value > 1. Hence $|\Phi_m(x)| > 1$, which ensures that $\Phi_m(x)$ does indeed have at least one prime factor. By Lemma 3 it follows that $p|m$ or that x has order m modulo p. But $x \equiv 0 \pmod{m}$, which implies that $\Phi_m(x) \equiv \Phi_m(0) \equiv 1 \pmod{m}$. Hence $p \nmid m$, and consequently x has order m modulo p. But then m must divide $p-1$, which is to say that $p \equiv 1 \pmod{m}$.

To see how this works numerically, we note that

$$\begin{aligned} \Phi_8(101) &= 2 \cdot 89 \cdot 584609, & \Phi_{10}(101) &= 11 \cdot 9367291, \\ \Phi_8(102) &= 5857 \cdot 18481, & \Phi_{10}(102) &= 61 \cdot 251 \cdot 7001, \\ \Phi_8(103) &= 2 \cdot 56275441, & \Phi_{10}(103) &= 1171 \cdot 95191, \\ \Phi_8(104) &= 17 \cdot 1657 \cdot 4153, & \Phi_{10}(104) &= 5 \cdot 211 \cdot 109831. \end{aligned}$$

On the left we encounter 2 and primes $\equiv 1 \pmod{8}$, and on the right we have 5 and primes $\equiv 1 \pmod{10}$.

4. Irreducibility of cyclotomic polynomials

In this section we show that the cyclotomic polynomial $\Phi_n(x)$ is irreducible over the field $\mathbb{Q}$ of rational numbers.

Let p denote a given prime number. For any polynomial $F(x)$ with integral coefficients let $\overline{F}(x)$ be the polynomial whose coefficients are the residue classes (mod p) determined by the coefficients of $F(x)$. Thus the assertion $\overline{F} = \overline{G}$ means that there is a polynomial $H(x)$ with integral coefficients such that $F(x) = G(x) + pH(x)$.

Lemma 4. (Schönemann, 1846) *Let $A(x)$ be a monic polynomial with integral coefficients, say*

$$A(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 = \prod_{i=1}^{n}(x - \alpha_i).$$

Let p be a prime number, and put

$$C(x) = \prod_{i=1}^{n}(x - \alpha_i^p).$$

Then $\overline{C} = \overline{A}$.

Proof. Let $\sigma_k(\boldsymbol{\alpha})$ denote the k^{th} symmetric function of the α_i. When $\sigma_k(\boldsymbol{\alpha})^p$ is expanded by the multinomial theorem, all coefficients except the extreme ones are divisible by p. That is,

$$\frac{\sigma_k(\alpha_1, \alpha_2, \ldots, \alpha_n)^p - \sigma_k(\alpha_1^p, \alpha_2^p, \ldots, \alpha_n^p)}{p}$$

is a symmetric polynomial in the α_i with integral coefficients, and hence by the symmetric function theorem this quantity is a rational integer.

Lemma 5. *Put $F(x) = x^n - 1$. Then $\overline{F}$ is squarefree if and only if $p \nmid n$.*

Proof. By the identity (4) we see that if $p \nmid n$, then $(\overline{F}, \overline{F'}) = 1$, and hence that $\overline{F}$ is squarefree. On the other hand, if $p|n$, say $n = mp$, then $\overline{F} = \overline{x^m - 1}^p$, and hence $\overline{F}$ is not squarefree.

Let $\Phi_n(x)$ denote the n^{th} cyclotomic polynomial. Since $\Phi_n|F$, it follows from the above that if $p \nmid n$, then $\overline{\Phi_n}$ is squarefree.

Theorem. (Kronecker, 1854) *The polynomial $\Phi_n(x)$ is irreducible over the field $\mathbb{Q}$ of rational numbers.*

Proof. Suppose that A and B are monic polynomials with rational coefficients such that $\Phi_n = AB$, and suppose also that $\deg A > 0$. By Gauss's lemma we know that A and B have integral coefficients. Let $\mathcal{Z}$ denote the roots of A. Let C be the monic polynomial whose roots are the numbers ζ^p for $\zeta \in \mathcal{Z}$. Here p is an arbitrary prime not dividing n. Our first step is to show that $A = C$. Since the map $\zeta \mapsto \zeta^p$ merely permutes the roots of Φ_n, we know that $C \mid \Phi_n$. Let $G = (B, C)$. Then $\overline{G} \mid \overline{B}$ and $\overline{G} \mid \overline{C}$. But $\overline{A} = \overline{C}$ by Lemma 4, and hence $\overline{G}^2 \mid \overline{A}\,\overline{B} = \overline{\Phi_n}$. But $\overline{\Phi_n}$ is squarefree, by Lemma 5. Hence $\overline{G} = \overline{1}$, so $G = 1$, and consequently $C \mid A$. But C and A have the same degree, so in fact $A = C$.

Now let ζ be a root of A, and ζ' a root of Φ_n. Then there exists a positive integer a, $(a, n) = 1$, such that $\zeta' = \zeta^a$. We factor a, $a = p_1 p_2 \cdots p_k$. Since ζ is a root of A, it follows from the argument above that ζ^{p_1} is also a root of A. Then by a second application of the above argument, we see that $\zeta^{p_1 p_2}$ is also a root of A. Continuing in this manner, we deduce that ζ' is a root of A. Since this is valid for every root ζ' of Φ_n, we conclude that $A = \Phi_n$. Hence Φ_n is irreducible.

Gauss proved that Φ_p is irreducible. The first proof of Kronecker's theorem using Schönemann's theorem was given by Arndt in 1857. An alternative argument using Schönemann's theorem is found in the text of Nagell. Among the more elementary proofs, the one of Landau (1929) is remarkable for its brevity: only 8 lines. A detailed account of the various proofs has been given by K. Manteuffel, Wiss. Zeit. Tech. Hochschule Magdeburg **1** (1957), 69–75.