

Factoring $x^n - 1$ over the integers and cyclotomic polynomials

We wish to completely factor $x^n - 1$ over Z . To this end, we first note that

$$x^n - 1 = \prod_{k=1}^n (x - \xi^k),$$

where $\xi = \cos(\frac{2\pi}{n}) + i \sin(\frac{2\pi}{n})$ is a primitive complex n th root of unity. Recall that the set $C = \{\xi, \xi^2, \dots, \xi^n = 1\}$ of all the complex roots of unity form the vertices of a regular n -gon and constitute a cyclic group of order n isomorphic to Z_n . For each divisor d of n let $C_d = \{\eta \in C : \text{order of } \eta \text{ is } d\}$. We can now partition C as the disjoint union of the sets C_d . This follows because if $d|n$, then $\eta = \xi^{\frac{n}{d}}$ has order d and belongs to C_d . The other elements of C_d are η^k such that k is relatively prime to d . These elements all generate a cyclic subgroup of order d in C .

For example, let $n = 12$. Then $\xi = \cos(\frac{2\pi}{12}) + i \sin(\frac{2\pi}{12}) = \frac{\sqrt{3}}{2} + i\frac{1}{2}$, is a unit vector making an angle of 30° with the x -axis. The divisors of 12 are 1,2,3,4,6, and 12. In this case:

$$\begin{aligned} C &= \{\xi, \xi^2, \xi^3, \xi^4, \xi^5, \xi^6, \xi^7, \xi^8, \xi^9, \xi^{10}, \xi^{11}, \xi^{12} = 1\} \\ C_1 &= \{\xi^{12} = 1\} \\ C_2 &= \{\xi^6 = -1\} \\ C_3 &= \{\xi^4 = -\frac{1}{2} + i\frac{\sqrt{3}}{2}, \xi^8 = -\frac{1}{2} - i\frac{\sqrt{3}}{2}\} \\ C_4 &= \{\xi^3 = i, \xi^9 = -i\} \\ C_6 &= \{\xi^2 = \frac{1}{2} + i\frac{\sqrt{3}}{2}, \xi^{10} = -\frac{1}{2} - i\frac{\sqrt{3}}{2}\} \\ C_{12} &= \{\xi = \frac{\sqrt{3}}{2} + i\frac{1}{2}, \xi^5 = -\frac{\sqrt{3}}{2} + i\frac{1}{2}, \xi^7 = -\frac{\sqrt{3}}{2} - i\frac{1}{2}, \xi^{11} = \frac{\sqrt{3}}{2} - i\frac{1}{2}\} \end{aligned}$$

Now for each divisor d of n define the *cyclotomic polynomial*

$$\phi_d(x) = \prod_{z \in C_d} (x - z)$$

By definition of $\phi_d(x)$ and the fact that C is partitioned by the sets C_d ,

$$x^n - 1 = \prod_{d|n} \phi_d(x)$$

For example,

$$x^{12} - 1 = \phi_1(x)\phi_2(x)\phi_3(x)\phi_4(x)\phi_6(x)\phi_{12}(x).$$

Let's calculate some of these cyclotomic polynomials. Clearly, $\phi_1(x) = x - 1$ and $\phi_2(x) = x + 1$. What is $\phi_3(x)$? Since $x^3 - 1 = (x + 1)(x^2 + x + 1) = \phi_1(x)\phi_3(x)$, it follows that $\phi_3(x) = x^2 + x + 1$. Now $x^4 - 1 = (x - 1)(x + 1)(x^2 + 1) = \phi_1(x)\phi_2(x)\phi_4(x)$ implies that $\phi_4(x) = x^2 + 1$. In this manner, we can recursively compute $\phi_n(x)$ from previously computed cyclotomic polynomials. It is left as an easy exercise to show that $\phi_6(x) = x^2 - x + 1$ and $\phi_{12}(x) = x^4 - x^2 + 1$. Thus

$$x^{12} - 1 = (x - 1)(x + 1)(x^2 + x + 1)(x^2 + 1)(x^2 - x + 1)(x^4 - x^2 + 1)$$

Note that although each cyclotomic polynomial $\phi_n(x)$ is by definition a product of linear factors with complex coefficients, it has integer coefficients. The fact that $\phi_n(x) \in Z[x]$ for all n can be shown by an induction argument. If $n = 1$ the $\phi_1(x) = x - 1 \in Z[x]$. Assume that $\phi_k(x) \in Z[x]$ for all $k < n$. Since

$$x^n - 1 = \phi_n(x) \prod_{d|n \text{ and } d < n} \phi_d(x)$$

we have

$$\phi_n(x) = \frac{x^n - 1}{\prod_{d|n \text{ and } d < n} \phi_d(x)}.$$

By induction hypothesis each $\phi_d(x) \in Z[x]$. Thus $\phi_n(x) \in Z[x]$.