Cyclotomic Polynomials

Melissa De La Cruz

Historical Timeline

The history of the discovery of cyclotompic polynomials is:

1706 Abraham de Moivre had early ideas of prime number solutions with radical expressions and being able to reduce the roots of unity

1771 Leonhard Euler studied cases $C_n(x) = 0, n < 10$

1771 Alexandre-Théophile Vandermonde studied $C_{11}(x) = 0$

1772 Joseph-Louis Lagrange

1796 Carl Friedrich Gauss studied $C_{17}(x) = 0$ and concluded that cyclotomic polynomials are irreducible

1824/29 Niels Henrik Abel showed that $C_n(x) = 0$ can always be solved in radicals

1845 Leopold Kronecker has the Kronecker-Weber theorem that aids in cyclotomic fields and abelian extensions

1850 Ferdinand Gotthold Max Eisenstein discovered that cyclotomic polynomials can be proven irreducible by Eisenstien's criterion, which was easier than the original way by Gauss.

1883 Ana Migott

1871 Léon-François-Antoine Aurifeuille made an algerbraic factorization specific to cyclotomic polynomials (with special restrictions) called aurifeuillean factorization. Édouard Lucas also added to this idea and discovered a general form for the factorization.

1872 Paul Bachmann

1936 Leonard Carlitz

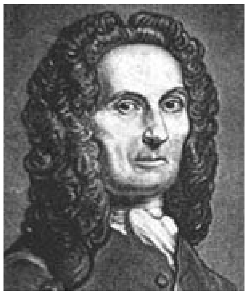
1936 Emma Lehmer

What are Cyclotomic Polynomials (and Applications)

They are polynomials that have complex roots, which are located in the complex plane. These roots are also primitive roots of unity. They are significant to multiple theories such as algebraic number theory, Galois theory, and basic number theory. In algebric number theory, these polynomials give explicit minimal polynomials (with leading coefficients of 1) for roots of unity. In Galois theory, these polynomials provide example of abelian field extenions. In this specific theory, cyclotomic polynomilas may be sovled in terms of radicals, thus allowing the roots of unity to be expressed using intergers and opening up the possiblity of using the operations of addition, subtraction, multiplication, and division. In basic number theory, they contribute to Dirichlet's Theorem for Primes that states, for every integer n, there are infinitely many primes congrugent to 1 mod n. These polynomials also provide in helping answer the question of which regular polygons are constructible with a ruler and compass.

Importance of Cyclotomic Polynomials

There are general forms on how to solve linear and quadratic equations as well as solving cubic and quartic equations. Though there is nor general form on how to solve quintic equations, cyclotomic polynomials give us an opportunity to be able to give us the example of simplest form of a solution of a closed, quintic equation with radicals. Also, the growth of of cyclotomic polynomials is great. It first started with de Moivre's interest in dividing the unit circle into n equal parts with solutions containing trigonometric terms or complex functions. Second, Vandermonde wrote solutions for small values of degree n and Gauss came in solving solutions for all values of n. Gauss also applied cyclotomic polynomials to the contruction of regualr polygons. Then in Galois theory, cyclotomic polynomials are solved by radicals for an integer n.



Intoduction to Cyclotomic Polynomials

Minimal polynomial for an algebraic number: polynomials wirh rational coefficients, minimal degree that has the algebraic number as a root and leading coefficient of 1.

Ex) the minimal polynomial of $\sqrt{2}$ is $p(x) = x^2 - 2$

Euler's formula: $e^{ix} = \cos(x) + i\sin(x) \qquad e^{i\pi} = -1$

$$(e^{\frac{2\pi i}{n}})^n = e^{\frac{2\pi in}{n}} = e^{2\pi i} = \cos(2\pi) + i\sin(2\pi) = 1$$

In $e^{\frac{2\pi ik}{n}}$: $k = 0, 1, ...1, n-1$: the number of verticies of a regular n-gon in a complex plane ex) n=4 is a square

Roots of Unity:

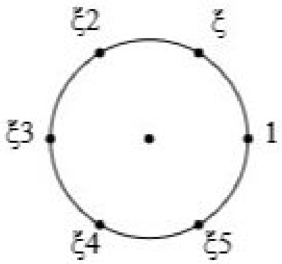
Let $\zeta = e^{\frac{2\pi i1}{n}}$:

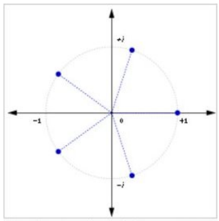
$e^{\frac{2\pi i1}{n}}$ is the the nth root of unity, an element $\omega \in \mathbb{C} : \omega n = 1$

Let n be a positive integer:

The cyclic group of nth roots of unity is $\mu n = \{1, \zeta, \zeta 2, ..., \zeta n - 1\}$ where $\zeta = e^{\frac{2\pi i}{n}} \in \mathbb{C}$, containing the operation of multiplication of complex numbers. In the complex plane, the elements of μn all lie on the unit circle.

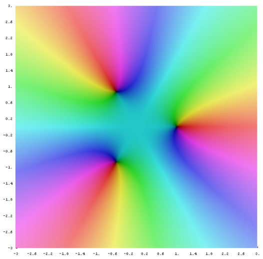
Cyclotomy means dividing the circle. The first circle shows the 6th roots of unity while, the second shows the 5th.

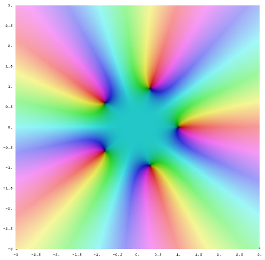




The 5th roots of unity in the complex plane

These next pictures show the roots of unity projected on the complex plane (shown with a polychromatic background). The first picture is a plot of $z^3 - 1$ and the second is a plot of $z^5 - 1$. The zeros of the functions are represented with the black area.





Primitive Roots of Unity:

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 now ζ^a is a primitive n^{th} root of unity. We then use $\Phi_n(x)$ to define the cyclotomic polynomial to be the monic polynomial of degree $\phi(n)$ that whose roots are the primitive n^{th} roots of unity:

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

To show that cyclotomic polynomials are $z^n - 1 = \prod_{d|n} \Phi_d(x)$ According to the value of (a,n), we can classify that the roots of unity ζ^a

$$z^n - 1 = \prod_{a=1}^{n} (x - \zeta^a)$$

$$\prod_{d|n} \prod_{a=1_{(a,n)=n/d}}^{n} (x - \zeta^a)$$

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

$$= \prod_{d|n} \prod_{b=1_{(b,d)=1}}^{d} (x - \zeta^{bn/d})$$

$$= \prod_{d|n} \Phi_d(x)$$

Hence:

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

Examples of Cyclotomic Polynomials

For prime p, the factorization of $x^p - 1$ into cyclotomic polynomials is,

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + ... + x^2 + x + 1$$

For $n = 2p$ with odd prime p,

$$\Phi_{2p}(x) = \frac{x^{2p} - 1}{\Phi_1(x)\Phi_2(x)\Phi_p(x)} = \frac{x^{2p} - 1}{\Phi_2(x)(x^p - 1)} = \frac{x^p + 1}{x + 1}$$

$$= x^{p-1} - x^{p-2} + x^{p-3} - ... + x^2 - x + 1$$

For $n = p^2$ with p prime,

$$\Phi_{p^2}(x) = \frac{x^{p^2} - 1}{\Phi_1(x)\Phi_p(x)} = \frac{x^{p^2} - 1}{x^p - 1} = x^{p(p-1)} + x^{p(p-2)} + ... + x^p + 1$$

Generally, one observes that for $n = p^b$ a prime power,

$$\Phi_{p^b}(x) = \Phi_p(x^{p^{b-1}}) = x^{p^{b-1}(p-1)} + x^{p^{b-1}(p-2)} + ... + x^{2p^{b-1}} + 1$$

For $n = 2m$ where m is odd and greater than 1, it stands that,

$$\Phi_{2m}(x) = \Phi_m(-x)$$

For $n = pq$ and p, q are distinct primes, it will be more complex,

$$\Phi_{15}(x) = \frac{x^{15} - 1}{\Phi_1(x)\Phi_3(x)\Phi_5(x)} = \frac{x^{15} - 1}{\Phi_3(x)(x^5 - 1)} = \frac{x^{10} + x^5 + 1}{x^2 + x + 1}$$

then by divding we have,

$$= x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$$

Examples of Written Out Cyclotomic Polynomials:

$\Phi_1(x) = x - 1$

$\Phi_2(x) = x + 1$

$\Phi_3(x) = x^2 + x + 1$

$\Phi_4(x) = x^2 + 1$

$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$

$\Phi_6(x) = x^2 - x + 1$

$\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$

$\Phi_8(x) = x^4 + 1$

$\Phi_9(x) = x^6 + x^3 + 1$

$\Phi_{10}(x) = x^4 - x^3 + x^2 = x + 1$

$\Phi_{11}(x) = x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$

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

$\Phi_{13}(x) = x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$

$\Phi_{14}(x) = x^6 - x^5 + x^4 - x^3 + x^2 - x + 1$

$\Phi_{15}(x) = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$

$\Phi_{16}(x) = x^8 + 1$

$\Phi_{17}(x) = x^{16} + x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$

$\Phi_{18}(x) = x^6 - x^3 + 1$

$\Phi_{19}(x) = x^{18} + x^{17} + x^{16} + x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$

$\Phi_{20}(x) = x^8 - x^6 + x^4 - x^2 + 1$

$\Phi_{22}(x) = x^{10} - x^9 + x^8 - x^7 + x^6 - x^5 + x^4 - x^3 + x^2 - x + 1$

$\Phi_{23}(x) = x^{22} + x^{21} + x^{20} + x^{19} + x^{18} + x^{17} + x^{16} + x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$

$\Phi_{26}(x) = x^{12} - x^{11} + x^{10} - x^9 + x^8 - x^7 + x^6 - x^5 + x^4 - x^3 + x^2 - x + 1$

$\Phi_{30}(x) = x^8 + x^7 - x^5 - x^4 - x^3 + x + 1$

Coefficients of $C_n(x)$:

The coefficients of cyclotomic polynomials ($C_{pq}(x)$) for distinct primes have coefficients of +1, -1, or 0. $C_{105}(x)$ is the first cyclotomic polynomial to have a different coefficient of -2 for x^7 and x^{41}. This is because 105 is the first prime number starting from zero to be composed of three distinct odd prime factors (3, 5, 7). The smallest value of n for which $C_n(x)$ has one or more coefficients are other than +1, -1, or 0 are 105, 385, 1365, 1785, 2805, 3135, and 6545.

Degree of $C_n(x)$:

$C_n(x)$ are irreducible polynomials over $\mathbb{Z}$ with degree $\varphi(n)$, where φ is Euler's totient function. The degree of $C_n(x)$ is also the number of the nth primitive roots if unity/

The Möbius Function

Note that when cyclotomic polynomials are mentioned, the Möbius inversion formula is also connected to show a valid inverse

$$\varphi(n) = \sum_{d|n} \mu(d) \frac{n}{d}$$

Eisenstein's Irreducibility Criterion

Eisenstein's irreducibility criterion is a condition used to assure that cyclotomic polynomials are irreducible

$$f(x) = x^n + c_{n-1}x^{n-1} + ... + c_1 x + c_0$$

$$p / c_n ..., c_1, c_0$$

$$p^2 \nmid c_0$$

Proof by contradiction: If these polynomials were reducible

$$f(x) = g(x)h(x)$$

Keep in mind that both funtions have integer coefficients. Now we reduce it by mod p,

$$x^n = \bar{g}(x)\bar{h}(x)$$

$$\bar{g}(x) = x^a \qquad \bar{h} = x^n - a$$

$$g(x) = x^a + d_{a-1}x^{a-1} + ... + d_1 x + d_0$$

$$h(x) = x^{n-a} + b_{n-a-1}x^{n-a-1} + ... + b_1 x + b_0$$

Note that because we reduced f(x) by mod p to get x^n,

$$d_{a-1}, .., d_1, d_0$$

is divisible by p as well as

$$b_{n-a-1}, ..., b_1, b_0$$

$$g(x)h(x) = +... + b_0 d_0$$

$$p^2 / b_0 d_0$$

which cannot be, therefore a contradiction!

References

1. http://functions.wolfram.com/PDF/Cyclotomic.pdf
2. http://www.wolframalpha.com/input/?i=eisenstein
3. http://www.ms.unimelb.edu.au/ ram/Notes/CyclotomicContent.html
4. http://www.math.umn.edu/ garrett/m/algebra/notes/08.pdf
5. http://www-personal.umich.edu/ hlm/nzm/cycpoly.pdf
6. https://brilliant.org/wiki/cyclotomic-polynomials/applications
7. https://en.wikipedia.org/wiki/Root_of_unity
8. http://archives.math.utk.edu/ICTCM/VOL25/C040/paper.pdf