Some Classes of Generalized Cyclotomic Polynomials

Number Theory Seminar

Abdullah Al-Shaghay

Dalhousie University

Wednesday November 20, 2019

Overview

1. Cyclotomic Subgroup-Polynomials
2. Certain Classes of Quadrinomials
3. Binomial Congruences and Honda-Type Congruences

Overview

For a fixed positive integer n we set $w = e^{\frac{2\pi i}{n}}$. Then we can write the n-th cyclotomic polynomial as the following product:

$$\Phi_n(x) = \prod_{k \in (\mathbb{Z}/n\mathbb{Z})^\times} (x - w^k).$$

For a fixed positive integer n we set $w = e^{\frac{2\pi i}{n}}$. Then we can write the n-th cyclotomic polynomial as the following product:

$$\Phi_n(x) = \prod_{k \in (\mathbb{Z}/n\mathbb{Z})^\times} (x - w^k).$$

Definition (Galois Subgroup-Polynomial)

Let H be a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$ and $(\mathbb{Z}/n\mathbb{Z})^\times/H = \{h_1H, h_2H, \ldots, h_lH\}$ be its corresponding quotient group. For each k, let

$$a_k = \sum_{h \in H} w^{h_k h}, \quad k = 1, \ldots, l. \tag{1}$$

The monic polynomial having $a_1, \ldots, a_l$ as its roots denoted by $J_{n,H}(x)$ will be called the Galois Subgroup-Polynomial. That is,

$$J_{n,H}(x) = (x - a_1)(x - a_2)\cdots(x - a_l).$$

Example

If we take $n = 7$, then $G = (\mathbb{Z}/7\mathbb{Z})^\times = \{1, 2, 3, 4, 5, 6\}$ and $w = e^{\frac{2\pi i}{7}}$. G has the subgroups

$$H_1 = \{1\}, H_2 = \{1, 6\}, H_3 = \{1, 2, 4\}, H_4 = \{1, 2, 3, 4, 5, 6\}.$$

$$\begin{aligned}
J_{7,H_1}(x) &= (x - w)(x - w^2)(x - w^3)(x - w^4)(x - w^5)(x - w^6) \\
&= x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = \Phi_7(x). \\
J_{7,H_2}(x) &= (x - (w + w^6))(x - (w^2 + w^5))(x - (w^3 + w^4)) \\
&= x^3 + x^2 - 2x - 1. \\
J_{7,H_3}(x) &= (x - (w + w^2 + w^4))(x - (w^3 + w^5 + w^6)) \\
&= x^2 + x + 2. \\
J_{7,H_4}(x) &= (x - (w + w^2 + w^3 + w^4 + w^5 + w^6)) = x + 1.
\end{aligned}$$

The authors who introduced these polynomials in their paper, presented the following two main results:

The authors who introduced these polynomials in their paper, presented the following two main results:

Theorem

For any subgroup H of $(\mathbb{Z}/n\mathbb{Z})^\times$, $J_{n,H}(x) \in \mathbb{Z}[x]$.

The authors who introduced these polynomials in their paper, presented the following two main results:

Theorem

For any subgroup H of $(\mathbb{Z}/n\mathbb{Z})^{\times}$, $J_{n,H}(x) \in \mathbb{Z}[x]$.

Theorem

Let n be a square-free integer. Then $J_{n,H}(x)$ is irreducible over $\mathbb{Q}$ for any subgroup H of $(\mathbb{Z}/n\mathbb{Z})^{\times}$.

Lemma

Let p be an odd prime. Then the leading and next-to-leading coefficients of $J_{p,H}(x)$ are all 1.

Lemma

Let p be an odd prime. Then the leading and next-to-leading coefficients of $J_{p,H}(x)$ are all 1.

Lemma

Let $J_{p,H}(x) = x^m + x^{m-1} + b_{m-2}x^{m-2} + \ldots + b_0$. Then

$$b_{m-2} = \begin{cases} \frac{p-1}{2} - \frac{|H|}{2}, & \text{if } |H| \text{ is even,} \\ \frac{|H|+1}{2}, & \text{if } |H| \text{ is odd.} \end{cases}$$

Theorem

For any prime $p > 2$, we have

$$\begin{aligned} J_{p,\{1,-1\}}(x) &= \prod_{k=1}^{\frac{p-1}{2}} \left(x - 2\cos\left(\frac{2\pi k}{p}\right)\right) \\ &= U_{\frac{p-1}{2}}\left(\frac{x}{2}\right) + U_{\frac{p-1}{2}-1}\left(\frac{x}{2}\right) \\ &= \frac{(-1)^{\frac{p-1}{2}}}{\sqrt{\frac{1}{2}-\frac{x}{4}}} T_p\left(\sqrt{\frac{1}{2}-\frac{x}{4}}\right), \end{aligned}$$

where $T_n(x)$ denotes the n-th Chebyshev polynomial of the first kind and $U_n(x)$ denotes the n-th Chebyshev polynomial of the second kind.

Conjecture

Let $p \equiv 1 \pmod 3$ *and* $|H| = 3$, *and write* $J_{p,H}(x) = x^m + x^{m-1} + b_{m-2}x^{m-2} + \ldots + b_0$. *Then*

$$b_{m-3} = 2\left(\frac{p-1}{3}\right) - 4 = \frac{2p-14}{3}.$$

Conjecture

Let $p \equiv 1 \pmod 3$ *and* $|H| = 3$*, and write* $J_{p,H}(x) = x^m + x^{m-1} + b_{m-2}x^{m-2} + \ldots + b_0$*. Then*

$$b_{m-3} = 2\left(\frac{p-1}{3}\right) - 4 = \frac{2p-14}{3}.$$

Lemma

Let $p \equiv 1 \pmod 4$ *and* $|H| = 4$*. Then the constant coefficient of* $J_{p,H}(x)$ *is always equal to* 1*.*

Theorem

The sets of irreducible polynomials $\{J_{p^k,H}(x) : H \leq (\mathbb{Z}/p^k\mathbb{Z})^\times\}$ *and* $\{J_{2p^k,H}(x) : H \leq (\mathbb{Z}/2p^k\mathbb{Z})^\times\}$ *are identical up to the signs of the coefficients of the individual polynomials.*

Theorem

The sets of irreducible polynomials $\{J_{p^k,H}(x) : H \leq (\mathbb{Z}/p^k\mathbb{Z})^\times\}$ *and* $\{J_{2p^k,H}(x) : H \leq (\mathbb{Z}/2p^k\mathbb{Z})^\times\}$ *are identical up to the signs of the coefficients of the individual polynomials.*

n	H	$J_{n,H}(x)$
7	$\{1\}$	$x^6+x^5+x^4+x^3+x^2+x+1$
7	$\{1,6\}$	x^3+x^2-2x-1
7	$\{1,9,11\}$	x^2-x+2
7	$\{1,3,5,9,11,13\}$	$x-1$
14	$\{1\}$	$x^6-x^5+x^4-x^3+x^2-x+1$
14	$\{1,13\}$	x^3-x^2-2x+1
14	$\{1,2,4\}$	x^2+x+2
14	$\{1,2,3,4,5,6\}$	$x+1$

Theorem

For an odd prime p we have

$$J_{p,H_2}(x) = x^2 + x + \frac{1 - (-1)^{\frac{p-1}{2}} p}{4}.$$

Theorem

For an odd prime p we have

$$J_{p,H_2}(x) = x^2 + x + \frac{1 - (-1)^{\frac{p-1}{2}} p}{4}.$$

Theorem

Let $p \equiv 1 \pmod 3$ *be a prime, and the integer c be such that* $4p = c^2 + 27b^2$ *and* $c \equiv 1 \pmod 3$. *Then*

$$J_{p,H_3}(x) = x^3 + x^2 - \frac{p-1}{3}x - \frac{1}{27}(p(c+3) - 1).$$

Theorem

Let $p \equiv 1 \pmod 8$ *be a prime, and the integer* s *be such that* $p = s^2 + 4t^2$ *and* $s \equiv 1 \pmod 4$*. Then*

$$J_{p,H_4}(x) = x^4 + x^3 - \frac{3(p-1)}{8}x^2 + \frac{1}{16}\Big((2s-3)p+1\Big)x + \frac{1}{256}\Big(p^2 - (4s^2-8s+6)p + 1\Big).$$

Let $p \equiv 5 \pmod 8$ *be a prime, and the integer* s *be such that* $p = s^2 + 4t^2$ *and* $s \equiv 1 \pmod 4$*. Then*

$$J_{p,H_4}(x) = x^4 + x^3 + \frac{1}{8}(p+3)x^2 + \frac{1}{16}\Big((2s+1)p+1\Big)x + \frac{1}{256}\Big(9p^2 - (4s^2-8s-2)p + 1\Big).$$

Theorem

The constant coefficient b_0 of the Cyclotomic Subgroup-Polynomial $J_{n,H}(x)$ is given by the integral formula

$$b_0 = |a_1| \cdot |a_2| \cdots |a_N| \frac{(2i)^N}{\pi} \int_0^{\pi} \prod_{k=1}^{N} \sin\left(t - \tfrac{\alpha_k}{N}\right) e^{i\left(Nt + \frac{\alpha}{2}\right)} dt,$$

where N is the degree of $J_{n,H}(x)$, and $\alpha = \alpha_1 + \alpha_2 + \ldots + \alpha_N$ with $\arg(a_k) = \alpha_k$, and $a_1, \ldots, a_N$ given by (1).

Theorem (Apostol)

For $0 < m < n$ *integers, we have*

$$\rho(\Phi_m, \Phi_n) = \begin{cases} p^{\varphi(m)} & \text{if } n/m \text{ is a power of a prime } p, \\ 1 & \text{otherwise.} \end{cases}$$

Theorem (Apostol)

For $0 < m < n$ integers, we have

$$\rho(\Phi_m, \Phi_n) = \begin{cases} p^{\varphi(m)} & \textit{if } n/m \textit{ is a power of a prime } p, \\ 1 & \textit{otherwise.} \end{cases}$$

Theorem

For $0 < m < n$ integers, we have

$$\rho(J_{m,\{-1,1\}}, J_{n,\{-1,1\}}) = \begin{cases} \pm p^{\frac{\varphi(m)}{2}} & \textit{if } n/m \textit{ is a power of a prime } p, \\ \pm 1 & \textit{otherwise,} \end{cases}$$

where the signs can be specified in some cases.

Theorem

If p is an odd prime, then the polynomials $J_{p,H}(x)$ become p-Eisenstein polynomials for all proper subgroups $H \leq (\mathbb{Z}/p\mathbb{Z})^\times$ when x is replaced by $\frac{x-1}{\deg(J_{p,H}(x))}$ and the polynomial is multiplied by the constant n^n.

Theorem

If p is an odd prime, then the polynomials $J_{p,H}(x)$ become p-Eisenstein polynomials for all proper subgroups $H \leq (\mathbb{Z}/p\mathbb{Z})^\times$ when x is replaced by $\frac{x-1}{\deg(J_{p,H}(x))}$ and the polynomial is multiplied by the constant n^n.

Theorem

If $n = p^m$, then for each subgroup $H \leq (\mathbb{Z}/p\mathbb{Z})^\times$ and corresponding subgroup $H' \leq (\mathbb{Z}/p^m\mathbb{Z})^\times$ such that $|H'| = |H|$, we have

$$J_{p^m,H'}(x) \equiv J_{p,H}(x^{p^{m-1}}) \pmod{p}.$$

Overview

For $n = p$ an odd prime we can write the n-th cyclotomic polynomial as

$$\Phi_p(x) = \sum_{k=0}^{p-1} x^k = 1 + x + x^2 + \cdots + x^{p-1}.$$

For $n = p$ an odd prime we can write the n-th cyclotomic polynomial as

$$\Phi_p(x) = \sum_{k=0}^{p-1} x^k = 1 + x + x^2 + \cdots + x^{p-1}.$$

Theorem (Harrington)

Let n and c be positive integers with $c \geq 2$. Then the polynomials

$$f(x) = x^n + \sum_{j=0}^{n-1} cx^j, \qquad g(x) = x^n + \sum_{j=0}^{n-1} (-1)^{n-j} cx^j,$$

$$h(x) = x^n - \sum_{j=0}^{n-1} cx^j, \qquad k(x) = x^n - \sum_{j=0}^{n-1} (-1)^{n-j} cx^j,$$

are irreducible in $\mathbb{Z}[x]$ with the exceptions of $f(x) = x^2 + 4x + 4 = (x+2)^2$ and $g(x) = x^2 - 4x + 4 = (x-2)^2$.

Theorem

Let n, c and a be positive integers with $c \geq 2$ and $a < n$. Then the polynomials

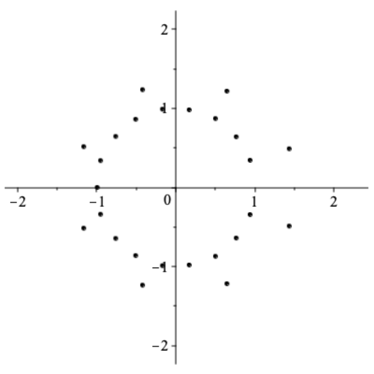
$$f_n^{a,c}(x) = x^n + \sum_{j=0}^{n-a-1} cx^j, \qquad g_n^{a,c}(x) = x^n + \sum_{j=0}^{n-a-1} (-1)^{n-j} cx^j,$$

$$h_n^{a,c}(x) = x^n - \sum_{j=0}^{n-a-1} cx^j, \qquad k_n^{a,c}(x) = x^n - \sum_{j=0}^{n-a-1} (-1)^{n-j} cx^j,$$

are irreducible in $\mathbb{Z}[x]$ with the exception of the cases $x^n - s^n$ and $x^n + s^n$.

Example

Consider $f_{25}^{7,12}(x) = x^{25} + 12 \cdot \sum_{n=0}^{17} x^n$. The following diagram is an illustration of the roots of $f_{25}^{7,12}(x)$ in the plane:



Varying one parameter while keeping the other two parameters fixed affects the roots in the following manner:

- Fixing the parameters a and c while increasing n fills more roots on the the “unit circle”.
- Fixing the parameters n and c while increasing a fills more roots on the outer “circle”.
- Fixing the parameters n and a while increasing c increases the diameter of the outer “circle”.

Varying one parameter while keeping the other two parameters fixed affects the roots in the following manner:

- Fixing the parameters a and c while increasing n fills more roots on the the "unit circle".
- Fixing the parameters n and c while increasing a fills more roots on the outer "circle".
- Fixing the parameters n and a while increasing c increases the diameter of the outer "circle".

Theorem

For $f_n^{a,c}(x), g_n^{a,c}(x), h_n^{a,c}(x)$, and $k_n^{a,c}(x)$, we have

$$D(f_n^{a,c}(x)) \equiv D(g_n^{a,c}(x)) \equiv D(h_n^{a,c}(x)) \equiv D(k_n^{a,c}(x)) \equiv 0 \pmod{c^{n-1}},$$

for all $n \geq 2$ and all values of a and c.

Overview

Definition

$$u^{\epsilon}_{a,b}(n) := \sum_{k=0}^{n} (-1)^{\epsilon k} \binom{n}{k}^{a} \binom{2n}{k}^{b}.$$

Definition

$$u^{\epsilon}_{a,b}(n) := \sum_{k=0}^{n} (-1)^{\epsilon k} \binom{n}{k}^{a} \binom{2n}{k}^{b}.$$

Theorem (Chamberland and Dilcher)

For all primes $p \geq 5$ and integers $m \geq 1$ we have

$$u(mp) \equiv u(m) \pmod{p^3},$$

where $u(n) := u^{1}_{1,1}(n)$.

Definition

$$u^{\epsilon}_{a,b}(n) := \sum_{k=0}^{n} (-1)^{\epsilon k} \binom{n}{k}^{a} \binom{2n}{k}^{b}.$$

Theorem (Chamberland and Dilcher)

For all primes $p \geq 5$ and integers $m \geq 1$ we have

$$u(mp) \equiv u(m) \pmod{p^3},$$

where $u(n) := u^{1}_{1,1}(n)$.

Theorem

For any prime $p \geq 5$ and nonnegative integers m, s we have

$$u(mp^{s+1}) \equiv u(mp^{s}) \pmod{p^{s+3}}.$$

The Legendre polynomials have the explicit formula

$$P_n(1+2t) = \sum_{k=0}^{n} \binom{n}{k} \binom{n+k}{k} t^k. \tag{2}$$

The Legendre polynomials have the explicit formula

$$P_n(1+2t) = \sum_{k=0}^{n} \binom{n}{k} \binom{n+k}{k} t^k. \tag{2}$$

Theorem

With the prime $p \geq 5$ fixed we have

$$P_{np-1}(1+2t) \equiv P_{n-1}(1+2t^p) \pmod{np}, \tag{3}$$

$$P_{np}(1+2t) \equiv P_n(1+2t^p) \pmod{np}, \tag{4}$$

where $n = 1, 2, p, 2p, p^2, 2p^2, \ldots$.

The Chebyshev polynomials of the first kind have the explicit formula

$$T_n(x) = \frac{n}{2} \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} (-1)^k \frac{(n-k-1)!}{k!(n-2k)!} (2x)^{n-2k}.$$

The Chebyshev polynomials of the first kind have the explicit formula

$$T_n(x) = \frac{n}{2} \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} (-1)^k \frac{(n-k-1)!}{k!(n-2k)!} (2x)^{n-2k}.$$

Theorem

For any prime p, we have

$$T_{np}(x) \equiv T_n(x^p) \pmod{np},$$

where $n = 2^i p^j$, $i, j \geq 0$.

Thank you very much for your time and patience ! Please feel free to ask any questions and I will do my best to answer them.