A Survey of Polynomial Results

(Number Theory Seminar)

Abdullah Al-Shaghay

Dalhousie University

Monday March 25, 2019

Overview

1. Cyclotomic Polynomials
2. Sums of Roots of Unity
3. Quadrinomials
4. Trinomials
5. Reciprocal Polynomials

Disclaimer

The following is meant to be a survey of results found in papers written by authors other than myself; none of the following are my own results. I am more than happy to point you in the direction of references upon request.

Overview

1. Cyclotomic Polynomials
2. Sums of Roots of Unity
3. Quadrinomials
4. Trinomials
5. Reciprocal Polynomials

Introduction

$$\Phi_n(x) = \prod_{\substack{1 \leq k \leq n \\ gcd(k,n)=1}} (x - e^{\frac{2\pi ik}{n}}).$$

Introduction

$$\Phi_n(x) = \prod_{\substack{1 \le k \le n \\ gcd(k,n)=1}} (x - e^{\frac{2\pi ik}{n}}).$$

$$\begin{aligned}
\Phi_1 &= x - 1 \\
\Phi_2 &= x + 1 \\
\Phi_3 &= x^2 + x + 1 \\
\Phi_4 &= x^2 + 1 \\
\Phi_5 &= x^4 + x^3 + x^2 + x + 1
\end{aligned}$$

Coefficients

- The case of the 105*th* cyclotomic polynomial is an interesting one; this is the first polynomial in the sequence to have coefficients outside of the set $\{-1, 0, 1\}$.

Coefficients

- The case of the 105*th* cyclotomic polynomial is an interesting one; this is the first polynomial in the sequence to have coefficients outside of the set $\{-1, 0, 1\}$.
- $\Phi_{105}(x) = x^{48} \pm \ldots - 2x^{41} + \ldots + 2x^{7} \pm \ldots + 1$

Coefficients

- The case of the 105*th* cyclotomic polynomial is an interesting one; this is the first polynomial in the sequence to have coefficients outside of the set $\{-1, 0, 1\}$.
- $\Phi_{105}(x) = x^{48} \pm \ldots - 2x^{41} + \ldots + 2x^7 \pm \ldots + 1$
- $105 = 3 \cdot 5 \cdot 7$ is the smallest positive integer that is the product of three distinct primes.

Coefficients

- The case of the 105*th* cyclotomic polynomial is an interesting one; this is the first polynomial in the sequence to have coefficients outside of the set $\{-1, 0, 1\}$.
- $\Phi_{105}(x) = x^{48} \pm \ldots - 2x^{41} + \ldots + 2x^{7} \pm \ldots + 1$
- $105 = 3 \cdot 5 \cdot 7$ is the smallest positive integer that is the product of three distinct primes.
- Bounding the magnitude has been a problem of interest to different researchers

Coefficients

- Migotti: If n has at most two distinct prime factors then $\Phi_n(x)$ has coefficients in the set $\{-1, 0, 1\}$

Coefficients

- Migotti: If n has at most two distinct prime factors then $\Phi_n(x)$ has coefficients in the set $\{-1, 0, 1\}$
- Not an if and only if statement: $\Phi_{231=3\cdot 7\cdot 11}(x)$ has coefficients in $\{-1, 0, 1\}$

Coefficients

- Migotti: If n has at most two distinct prime factors then $\Phi_n(x)$ has coefficients in the set $\{-1, 0, 1\}$
- Not an if and only if statement: $\Phi_{231=3\cdot7\cdot11}(x)$ has coefficients in $\{-1, 0, 1\}$
- Suzuki: Let $a(k, n)$ be the $k-th$ coefficient of the $n-th$ cyclotomic polynomial. Then $\{a(k, n) | n, k \in \mathbb{N}\} = \mathbb{Z}$

Coefficients

- Migotti: If n has at most two distinct prime factors then $\Phi_n(x)$ has coefficients in the set $\{-1, 0, 1\}$
- Not an if and only if statement: $\Phi_{231=3\cdot 7\cdot 11}(x)$ has coefficients in $\{-1, 0, 1\}$
- Suzuki: Let $a(k, n)$ be the $k-th$ coefficient of the $n-th$ cyclotomic polynomial. Then $\{a(k, n) | n, k \in \mathbb{N}\} = \mathbb{Z}$
- Ji, Li: $\{a(k, p^l n) | n, k \in \mathbb{N}\} = \mathbb{Z}$

Coefficients

- Migotti: If n has at most two distinct prime factors then $\Phi_n(x)$ has coefficients in the set $\{-1, 0, 1\}$
- Not an if and only if statement: $\Phi_{231=3\cdot7\cdot11}(x)$ has coefficients in $\{-1, 0, 1\}$
- Suzuki: Let $a(k, n)$ be the $k-th$ coefficient of the $n-th$ cyclotomic polynomial. Then $\{a(k, n) | n, k \in \mathbb{N}\} = \mathbb{Z}$
- Ji, Li: $\{a(k, p^l n) | n, k \in \mathbb{N}\} = \mathbb{Z}$
- Ji, Li, Moree: $\{a(k, mn) | n \geq 1, k \geq 0\} = \mathbb{Z}$

Moree

Moree has some interesting work studying what he calls reciprocal cyclotomic polynomials defined by,

$$\Psi_n = \frac{x^n - 1}{\Phi_n(x)}.$$

Moree has some interesting work studying what he calls reciprocal cyclotomic polynomials defined by,

$$\Psi_n = \frac{x^n - 1}{\Phi_n(x)}.$$

He has also done interesting work with co-authors on the evaluation of $\Phi_n(x)$ at $m - th$ roots of unity and self-reciprocal polynomials.

Falcone

Proposition

Let $m > n$ be two integers. If n does not divide m then two polynomial $a(x), b(x) \in \mathbb{Z}[x]$ exist, such that $1 = a(x)\Phi_m(x) + b(x)\Phi_n(x)$.

Falcone

Proposition

Let $m > n$ be two integers. If n does not divide m then two polynomial $a(x), b(x) \in \mathbb{Z}[x]$ exist, such that $1 = a(x)\Phi_m(x) + b(x)\Phi_n(x)$.

Proposition

Let $\Phi_m(x)$ and $\Phi_n(x)$ be two cyclotomic polynomials, and let n be a divisor of m. Then two polynomial $a(x), b(x) \in \mathbb{Z}[x]$ exist, such that $k = a(x)\Phi_m(x) + b(x)\Phi_n(x)$, where $k = 1$ if $\frac{m}{n}$ is not a prime power and $k = p$ if $\frac{m}{n} = p^t$.

Overview

1. Cyclotomic Polynomials
2. Sums of Roots of Unity
3. Quadrinomials
4. Trinomials
5. Reciprocal Polynomials

A problem that has been asked/investigated is the following: For a given natural number m, what are the possible integers n for which there exists $m-th$ roots of unity $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ such that $\alpha_1 + \ldots + \alpha_n = 0$.

$\mathbb{N} = \mathbb{N} \cup \{0\}$
$W(m) :=$ the set of weights n for which there exits a vanishing sum as above.

$\mathbb{N} = \mathbb{N} \cup \{0\}$
$W(m) :=$ the set of weights n for which there exits a vanishing sum as above.

Theorem (Lam,Leung)

For any integer $m = p_1^{a_1} \cdots p_r^{ar}$, $W(m)$ is exactly the set $\mathbb{N}p_1 + \ldots + \mathbb{N}p_r$.

$\mathbb{N} = \mathbb{N} \cup \{0\}$
$W(m) :=$ the set of weights n for which there exits a vanishing sum as above.

Theorem (Lam,Leung)

For any integer $m = p_1^{a_1} \cdots p_r^{ar}$, $W(m)$ is exactly the set $\mathbb{N}p_1 + \ldots + \mathbb{N}p_r$.

$\mathbb{N} = \mathbb{N} \cup \{0\}$
$W(m) :=$ the set of weights n for which there exits a vanishing sum as above.

Theorem (Lam,Leung)

For any integer $m = p_1^{a_1} \cdots p_r^{ar}$, $W(m)$ is exactly the set $\mathbb{N}p_1 + \ldots + \mathbb{N}p_r$.

Theorem (Sivek)

[Distinct Roots] With m written as above, $n \in W(m)$ if and only if m and $m - n$ are in $\mathbb{N}p_1 + \ldots + \mathbb{N}p_r$.

Overview

1 Cyclotomic Polynomials

2 Sums of Roots of Unity

3 Quadrinomials

4 Trinomials

5 Reciprocal Polynomials

Introduction

Motivated by the following result of Harrington,

Theorem

Let n, c, and d be positive integers with $n \geq 3, d \neq c, d \leq 2(c-1)$, and $(n, c) \neq (3, 3)$. If the trinomial $f(x) = x^n \pm x^{n-1} \pm d$ is reducible in $\mathbb{Z}[x]$, then $f(x) = (x \pm 1)g(x)$ for some irreducible $g(x) \in \mathbb{Z}[x]$.

I was interested in studying quadrinomials of the form:

$$x^{n+1} - x^n + cx^{n-a} - c.$$

Motivated by the following result of Harrington,

Theorem

Let n, c, and d be positive integers with $n \geq 3, d \neq c, d \leq 2(c-1)$, and $(n, c) \neq (3, 3)$. If the trinomial $f(x) = x^n \pm x^{n-1} \pm d$ is reducible in $\mathbb{Z}[x]$, then $f(x) = (x \pm 1)g(x)$ for some irreducible $g(x) \in \mathbb{Z}[x]$.

I was interested in studying quadrinomials of the form:

$$x^{n+1} - x^n + cx^{n-a} - c.$$

Along the way, I came across the following results on quadrinomials of different types:

Jankauskas

Let $P(x)$ be a polynomial with integer coefficients. $P(x)$ is called primitive if it cannot be written as $P(x) = P_1(x^l)$ for some positive integer $l > 1$ and $P_1(x) \in \mathbb{Z}[x]$.

Jankauskas

Let $P(x)$ be a polynomial with integer coefficients. $P(x)$ is called primitive if it cannot be written as $P(x) = P_1(x^l)$ for some positive integer $l > 1$ and $P_1(x) \in \mathbb{Z}[x]$.

Theorem

The only primitive polynomial irreducible polynomial $P \in \mathbb{Z}[x]$ of the form $P(x) = x^i + x^j + x^k + 4, i > j > k > 0$, such that the polynomial $P(x^l)$ for some positive integer l factors in $\mathbb{Z}[x]$, is the polynomial $P(x) = x^4 + x^3 + x^2 + 4$. More precisely, for $l = 2$, $P(x^2) = x^8 + x^6 + x^4 + 4 = (x^4 - x^3 + x^2 - 2x + 2)(x^4 + x^3 + x^2 + 2x + 2)$.

Bremner, Ulas

Proposition

Let $p \geq 5$ be a prime. Then the quadrinomial
$x^n + x^m + x^k + p, \quad n > m > k \geq 1$ *is irreducible over* $\mathbb{Q}$.

Bremner, Ulas

Proposition

Let $p \geq 5$ be a prime. Then the quadrinomial
$x^n + x^m + x^k + p, \quad n > m > k \geq 1$ *is irreducible over* $\mathbb{Q}$.

Proof.

Suppose, towards a contradiction, that $x^n + x^m + x^k + p = f_1(x)f_2(x)$ with $f_1, f_2 \in \mathbb{Z}[x]$ and $n > deg(f_1), deg(f_2) \geq 1$. Without loss of generality, the constant coefficient of f_1 is $\pm p$ and the constant coefficient of f_2 is ± 1. This implies that not all of the roots of f_2 can have absolute value greater than 1. Choose $z \in \mathbb{C}$ such that $|z| \leq 1$. Then
$p = |z^n + z^m + z^k| \leq |z|^m + |z|^n + |z|^k \leq 3.$ □

Ljunggren

Theorem

For any distinct positive integers n, m, *and* p, *and for any choice of* $\epsilon_j \in \{-1, 1\}$, *the polynomial* $x^n + \epsilon_1 x^m + \epsilon_2 x^p + \epsilon_3$, *with its cyclotomic factors removed is either the identity 1 or is irreducible over the integers.*

Overview

1. Cyclotomic Polynomials
2. Sums of Roots of Unity
3. Quadrinomials
4. Trinomials
5. Reciprocal Polynomials

Theorem (Perron)

The polynomial $f(x) = x^n + ax \pm 1$ *is irreducible for* $|a| \geq 3$. *For* $|a| = 2$, $f(x)$ *is either irreducible or has the factor* $(x \pm 1)$. *In the latter case, the second factor of* $f(x)$ *is irreducible.*

Theorem (Perron)

The polynomial $f(x) = x^n + ax \pm 1$ is irreducible for $|a| \geq 3$. For $|a| = 2$, $f(x)$ is either irreducible or has the factor $(x \pm 1)$. In the latter case, the second factor of $f(x)$ is irreducible.

Theorem (Nagell)

Let $g(x) = x^n + qx^p + r$ with $1 \leq p \leq n-1$. Then $g(x)$ is irreducible if

- $|q| > 1 + |r|^{n-1}$.
- *If $h|n, h > 1$, then $|r|$ is not an $h-th$ power. In particular, we must have $|r| > 1$.*

Selmer

Theorem

Let $f(x) = x^n + ax^m + b$ with $m < n$ be an irreducible trinomial satisfying the conditions

- $2^3 \nmid a, 2 \nmid b, n \neq 2m$, *or*
- $a \equiv 1, 2 \pmod 4, 2|b$.

Then $f(x^2)$ is also irreducible.

Overview

1 Cyclotomic Polynomials

2 Sums of Roots of Unity

3 Quadrinomials

4 Trinomials

5 Reciprocal Polynomials

Introduction

Given a polynomial $f(x) \in \mathbb{Q}[x]$,

$$f_{rev}(x) = x^{deg(f)} f(\frac{1}{x}).$$

Introduction

Given a polynomial $f(x) \in \mathbb{Q}[x]$,

$$f_{rev}(x) = x^{deg(f)} f(\frac{1}{x}).$$

$f(x)$ is a reciprocal polynomial if $f(x) = f_{rev}(x)$. Sometimes also called self-reciprocal or palindromic.

Introduction

Given a polynomial $f(x) \in \mathbb{Q}[x]$,

$$f_{rev}(x) = x^{deg(f)} f(\frac{1}{x}).$$

$f(x)$ is a reciprocal polynomial if $f(x) = f_{rev}(x)$. Sometimes also called self-reciprocal or palindromic.
Let $f(x) \in \mathbb{Q}[x]$ be of even degree and also be a reciprocal polynomial. Then there is a unique polynomial $p(x) = R(f(x))$ defined by the mapping

$$f(x) = x^{deg(p)} p(1 + \frac{1}{x}).$$

Cafure, Cesaratto

Theorem

Let $f(x)$ be a primitive polynomial in $\mathbb{Z}[x]$ and assume that the image polynomial $p(x) \in \mathbb{Q}[x]$ is irreducible.

Cafure, Cesaratto

Theorem

Let $f(x)$ be a primitive polynomial in $\mathbb{Z}[x]$ and assume that the image polynomial $p(x) \in \mathbb{Q}[x]$ is irreducible.

- *If $|f(-1)|$ or $|f(1)|$ are not perfect squares, then $f(x)$ is irreducible in $\mathbb{Q}[x]$.*

Cafure, Cesaratto

Theorem

Let $f(x)$ be a primitive polynomial in $\mathbb{Z}[x]$ and assume that the image polynomial $p(x) \in \mathbb{Q}[x]$ is irreducible.

- *If $|f(-1)|$ or $|f(1)|$ are not perfect squares, then $f(x)$ is irreducible in $\mathbb{Q}[x]$.*
- *If $f(1)$ and the middle coefficient of f have different signs, then f is irreducible in $\mathbb{Q}[x]$.*

Cafure, Cesaratto

Theorem

Let $f(x)$ be a primitive polynomial in $\mathbb{Z}[x]$ and assume that the image polynomial $p(x) \in \mathbb{Q}[x]$ is irreducible.

- *If $|f(-1)|$ or $|f(1)|$ are not perfect squares, then $f(x)$ is irreducible in $\mathbb{Q}[x]$.*
- *If $f(1)$ and the middle coefficient of f have different signs, then f is irreducible in $\mathbb{Q}[x]$.*
- *If the middle coefficient of f is 0 or ± 1, then f is irreducible in $\mathbb{Q}[x]$.*

Cafure, Cesaratto

Theorem

Let $f(x)$ be a primitive polynomial in $\mathbb{Z}[x]$ and assume that the image polynomial $p(x) \in \mathbb{Q}[x]$ is irreducible.

- *If $|f(-1)|$ or $|f(1)|$ are not perfect squares, then $f(x)$ is irreducible in $\mathbb{Q}[x]$.*
- *If $f(1)$ and the middle coefficient of f have different signs, then f is irreducible in $\mathbb{Q}[x]$.*
- *If the middle coefficient of f is 0 or ± 1, then f is irreducible in $\mathbb{Q}[x]$.*

Cafure, Cesaratto

Theorem

Let $f(x)$ be a primitive polynomial in $\mathbb{Z}[x]$ and assume that the image polynomial $p(x) \in \mathbb{Q}[x]$ is irreducible.

- *If $|f(-1)|$ or $|f(1)|$ are not perfect squares, then $f(x)$ is irreducible in $\mathbb{Q}[x]$.*
- *If $f(1)$ and the middle coefficient of f have different signs, then f is irreducible in $\mathbb{Q}[x]$.*
- *If the middle coefficient of f is 0 or ± 1, then f is irreducible in $\mathbb{Q}[x]$.*

Theorem

Almost all reciprocal polynomials with integer coefficients are irreducible over $\mathbb{Q}$.

The End

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.