

Irreducibility of Generalized Stern Polynomials

Honours Research Project with Prof. Karl Dilcher

Mason Maxwell

Dalhousie University

1 April 2019

- 1 Motivation
- 2 Introduction
- 3 Cyclotomic Polynomials
- 4 Newman Polynomials, Borwein Polynomials, and Irreducibility
- 5 Previous Irreducibility Results for $a_{2,t}(n; z)$
- 6 My results

I will also prove:

Theorem

The real part of every non-trivial zero of the Riemann zeta function is $\frac{1}{2}$.

I will also prove:

Theorem

The real part of every non-trivial zero of the Riemann zeta function is $\frac{1}{2}$.

Proof.

April Fools!!



In 2007 the *Stern integer sequence* was extended by Klavžar, Milutinović, and Petr to the Stern polynomials $B_n(z)$, $n \in \mathbb{N}$.

In 2007 the *Stern integer sequence* was extended by Klavžar, Milutinović, and Petr to the Stern polynomials $B_n(z)$, $n \in \mathbb{N}$.

Conjecture (Ulas)

$B_p(z)$ is irreducible over \mathbb{Q} whenever p is prime.

In 2007 the *Stern integer sequence* was extended by Klavžar, Milutinović, and Petr to the Stern polynomials $B_n(z)$, $n \in \mathbb{N}$.

Conjecture (Ulas)

$B_p(z)$ is irreducible over \mathbb{Q} whenever p is prime.

- Verified computationally for the first 10^6 primes

In 2007 the *Stern integer sequence* was extended by Klavžar, Milutinović, and Petr to the Stern polynomials $B_n(z)$, $n \in \mathbb{N}$.

Conjecture (Ulas)

$B_p(z)$ is irreducible over \mathbb{Q} whenever p is prime.

- Verified computationally for the first 10^6 primes
- Various cases proved by Schinzel and by Dilcher, Kidwai, and Tomkins

In 2007 the *Stern integer sequence* was extended by Klavžar, Milutinović, and Petr to the Stern polynomials $B_n(z)$, $n \in \mathbb{N}$.

Conjecture (Ulas)

$B_p(z)$ is irreducible over \mathbb{Q} whenever p is prime.

- Verified computationally for the first 10^6 primes
- Various cases proved by Schinzel and by Dilcher, Kidwai, and Tomkins
- Here we study the analogous problem for the generalized Stern polynomials.

Definition (Stern sequence)

The Stern integer sequence, also known as Stern's diatomic series, is denoted $(a(n))_{n \geq 0}$ and defined by $a(0) = 0$, $a(1) = 1$, and for $n \geq 1$ by

$$a(2n) = a(n), \quad (1)$$

$$a(2n + 1) = a(n) + a(n + 1). \quad (2)$$

Definition (Stern sequence)

The Stern integer sequence, also known as Stern's diatomic series, is denoted $(a(n))_{n \geq 0}$ and defined by $a(0) = 0$, $a(1) = 1$, and for $n \geq 1$ by

$$a(2n) = a(n), \quad (3)$$

$$a(2n + 1) = a(n) + a(n + 1). \quad (4)$$

- Dates back as far as Eisenstein; introduced by M. A. Stern; studied by Lehmer, de Rham, Dijkstra, Calkin and Wilf, and others...

Definition (Stern sequence)

The Stern integer sequence, also known as Stern's diatomic series, is denoted $(a(n))_{n \geq 0}$ and defined by $a(0) = 0$, $a(1) = 1$, and for $n \geq 1$ by

$$a(2n) = a(n), \quad (5)$$

$$a(2n + 1) = a(n) + a(n + 1). \quad (6)$$

- Dates back as far as Eisenstein; introduced by M. A. Stern; studied by Lehmer, de Rham, Dijkstra, Calkin and Wilf, and others...

Related to

- Stern-Brocot tree
- Calkin-Wilf tree
- Counting the rationals; random Fibonacci sequences; Fibonacci representations

- Sequence begins as

$0, 1, 1, 2, 1, 3, 2, 3, 1, 4, 3, 5, 2, 5, 3, 4, 1, 5, 4, 7, 3, \dots$

- Sequence begins as
 $0, 1, 1, 2, 1, 3, 2, 3, 1, 4, 3, 5, 2, 5, 3, 4, 1, 5, 4, 7, 3, \dots$
- The sequence $(a(n)/a(n+1))_{n \in \mathbb{N}}$ of quotients of consecutive Stern numbers gives an enumeration without repetition of the positive reduced rational numbers.

- Sequence begins as
 $0, 1, 1, 2, 1, 3, 2, 3, 1, 4, 3, 5, 2, 5, 3, 4, 1, 5, 4, 7, 3, \dots$
- The sequence $(a(n)/a(n+1))_{n \in \mathbb{N}}$ of consecutive Stern numbers gives an enumeration without repetition of the positive reduced rational numbers.
- The number $a(n+1)$ gives the number of "hyperbinary expansions" of n , i.e., the number of ways of writing n as a sum of powers of 2 without repetition.

Extended in 2007 to two different polynomial analogues:

Extended in 2007 to two different polynomial analogues:

- one by Klavžar, Milutinović, and Petr

Extended in 2007 to two different polynomial analogues:

- one by Klavžar, Milutinović, and Petr
- and another independently by Karl Dilcher and Ken Stolarsky!!

Definition (Stern polynomials)

The Stern polynomials are denoted $B_n(z)$ and defined by $B_0(z) = 0$, $B_1(z) = 1$, and for $n \geq 1$,

$$B_{2n}(z) = zB_n(z), \quad (7)$$

$$B_{2n+1}(z) = B_n(z) + B_{n+1}(z). \quad (8)$$

Definition (Stern polynomials)

The Stern polynomials are denoted $B_n(z)$ and defined by $B_0(z) = 0$, $B_1(z) = 1$, and for $n \geq 1$,

$$B_{2n}(z) = zB_n(z), \quad (9)$$

$$B_{2n+1}(z) = B_n(z) + B_{n+1}(z). \quad (10)$$

We see immediately that

$$B_n(1) = a(n) \quad (n \geq 0), \quad (11)$$

and by induction that

$$B_n(2) = n \quad (n \geq 0). \quad (12)$$

Convention: From now on, *irreducible* means *irreducible over \mathbb{Q}* .

Convention: From now on, *irreducible* means *irreducible over \mathbb{Q}* .

Conjecture (Ulas)

$B_p(z)$ is *irreducible whenever p is prime*.

Convention: From now on, *irreducible* means *irreducible over \mathbb{Q}* .

Conjecture (Ulas)

$B_p(z)$ is *irreducible whenever p is prime*.

- Verified computationally for the first one-million primes

Convention: From now on, *irreducible* means *irreducible over \mathbb{Q}* .

Conjecture (Ulas)

$B_p(z)$ is irreducible whenever p is prime.

- Verified computationally for the first one-million primes

A. Schinzel proved

Theorem (Schinzel)

For all integers $n \geq 3$, $B_{2^n-3}(z)$ is irreducible.

- also proved for all primes $p < 2017$, without computation

Further cases proved by Karl Dilcher, Mohammad Kidwai, and Hayley Tomkins, including the following theorem:

Theorem (Dilcher, Kidwai, Thomkins)

Suppose that the prime p is of the form

$$p = 2^\nu \pm 2^\mu \pm 1$$

or

$$p = 2^\nu \pm 2^\mu \pm 3$$

where $\mu \geq 1$ and $\nu \geq \mu + 9$ are integers, and the instances of " \pm " are independent. Then $B_p(z)$ is irreducible.

Definition (Generalized Stern polynomials)

Let t be a fixed positive integer.

(1) The Type-1 generalized Stern polynomials $a_{1,t}(n; z)$ are polynomials in z defined by $a_{1,t}(0; z) = 0$, $a_{1,t}(1; z) = 1$, and for $n \geq 1$ by

$$a_{1,t}(2n; z) = za_{1,t}(n; z^t), \quad (13)$$

$$a_{1,t}(2n + 1; z) = a_{1,t}(n; z^t) + a_{1,t}(n + 1; z^t). \quad (14)$$

Definition (Generalized Stern polynomials)

Let t be a fixed positive integer.

(1) The Type-1 generalized Stern polynomials $a_{1,t}(n; z)$ are polynomials in z defined by $a_{1,t}(0; z) = 0$, $a_{1,t}(1; z) = 1$, and for $n \geq 1$ by

$$a_{1,t}(2n; z) = za_{1,t}(n; z^t), \quad (15)$$

$$a_{1,t}(2n + 1; z) = a_{1,t}(n; z^t) + a_{1,t}(n + 1; z^t). \quad (16)$$

(2) The Type-2 generalized Stern polynomials $a_{2,t}(n; z)$ are polynomials in z defined by $a_{2,t}(0; z) = 0$, $a_{2,t}(1; z) = 1$, and for $n \geq 1$ by

$$a_{2,t}(2n; z) = a_{2,t}(n; z^t), \quad (17)$$

$$a_{2,t}(2n + 1; z) = za_{2,t}(n; z^t) + a_{2,t}(n + 1; z^t). \quad (18)$$

n	$a_{1,t}(n; z)$	$a_{2,t}(n; z)$
1	1	1
2	z	1
3	$1 + z^t$	$1 + z$
4	z^{t+1}	1
5	$1 + z^t + z^{t^2}$	$1 + z + z^t$
6	$z + z^{t^2+1}$	$1 + z^t$
7	$1 + z^{t^2} + z^{t^2+t}$	$1 + z + z^{t+1}$
8	z^{t^2+t+1}	1
9	$1 + z^{t^2} + z^{t^2+t} + z^{t^3}$	$1 + z + z^t + z^{t^2}$
10	$z + z^{t^2+1} + z^{t^3+1}$	$1 + z^t + z^{t^2}$
11	$1 + z^t + z^{t^2} + z^{t^3} + z^{t^3+t}$	$1 + z + z^{t+1} + z^{t^2} + z^{t^2+1}$
12	$z^{t+1} + z^{t^2+t+1}$	$1 + z^{t^2}$
13	$1 + z^t + z^{t^3} + z^{t^3+t} + z^{t^3+t^2}$	$1 + z + z^t + z^{t^2+1} + z^{t^2+t}$
14	$z + z^{t^3+1} + z^{t^3+t^2+1}$	$1 + z^t + z^{t^2+1}$
15	$1 + z^{t^3} + z^{t^3+t^2} + z^{t^3+t^2+t}$	$1 + z + z^{t+1} + z^{t^2+t+1}$
16	$z^{t^3+t^2+t^1+1}$	1

By comparing (7)-(10) with (1) and (2) we see that for $z = 1$ both sequences reduce to the Stern integer sequence $a(n)$, i.e.,

$$a_{1,t}(n; 1) = a_{2,t}(n; 1) = a(n) \quad (t \geq 1, n \geq 0). \quad (19)$$

By comparing (7)-(10) with (1) and (2) we see that for $z = 1$ both sequences reduce to Stern's diatomic sequence $a(n)$, i.e.,

$$a_{1,t}(n; 1) = a_{2,t}(n; 1) = a(n) \quad (t \geq 1, n \geq 0). \quad (20)$$

- Table indicates that both sequences have a special structure
- For $t = 1$ the exponents in a given polynomial can coincide
- The following theorem describes the case $t \geq 2$

By comparing (7)-(10) with (1) and (2) we see that for $z = 1$ both sequences reduce to Stern's diatomic sequence $a(n)$, i.e.,

$$a_{1,t}(n; 1) = a_{2,t}(n; 1) = a(n) \quad (t \geq 1, n \geq 0). \quad (21)$$

- Table indicates that both sequences have a special structure
- For $t = 1$ the exponents in a given polynomial can coincide
- The following theorem describes the case $t \geq 2$

Theorem

For integers $t \geq 2$ and $n \geq 0$, the coefficients of $a_{1,t}(n; z)$ and $a_{2,t}(n; z)$ are either 0 or 1. Furthermore, all exponents of z are polynomials in t with only 0 or 1 as coefficients.

Remark

This theorem and (11) show that the number of terms of both polynomials is given by the Stern number $a(n)$.

Dilcher and Ericksen applied certain subsequences to

- tilings, colourings, and lattice paths
- continued fractions
- hyperbinary expansions

Dilcher and Ericksen applied certain subsequences to

- tilings, colourings, and lattice paths
- continued fractions
- hyperbinary expansions

Example

The hyperbinary expansions of $n = 10$ are

$$8 + 2, \quad 8 + 1 + 1, \quad 4 + 4 + 2, \quad 4 + 4 + 1 + 1, \quad 4 + 2 + 2 + 1 + 1,$$

and notice that $8 + 2$ is the unique binary expansion.

Observe that there are $5 = a(11) = a(10 + 1)$ such hyperbinary expansions.

Definition (Root of unity)

Let K be a field and n a positive integer. An element ζ is called an n th root of unity provided $\zeta^n = 1$, that is, if ζ is a root of $z^n - 1 \in K[z]$.

Definition (Root of unity)

Let K be a field and n a positive integer. An element ζ is called an n th root of unity provided $\zeta^n = 1$, that is, if ζ is a root of $z^n - 1 \in K[z]$.

Remark

- (1) If ζ_n is an n th root of unity, then $\zeta_n = e^{2\pi ik/n}$ for some $k \in \mathbb{N}$.
- (2) The n th roots of unity form a cyclic subgroup of the multiplicative group K^* of nonzero elements of K .

Definition (Primitive root of unity)

An n th root of unity ζ_n is primitive if it is not a k th root of unity for any $k < n$. In other words, ζ_n is a primitive n th root of unity if it has order n in the group of n th roots of unity.

Definition (Primitive root of unity)

An n th root of unity ζ_n is primitive if it is not a k th root of unity for some $k < n$. In other words, ζ_n is a primitive n th root of unity if it has order n in the group of n th roots of unity.

Theorem

The primitive n th roots of unity are the elements
 $\{\zeta_n^k \mid \zeta_n = e^{2\pi i/n}, \gcd(k, n) = 1\}$.

Definition (Cyclotomic polynomial)

For a positive integer n the n th cyclotomic polynomial $\Phi_n(z)$ is the unique irreducible polynomial in $\mathbb{Z}[z]$ given by

$$\Phi_n(z) = \prod_{\substack{1 \leq k < n, \\ \gcd(k,n)=1}} (z - \zeta_n^k) \quad (22)$$

where ζ_n is a primitive n th root of unity.

Cyclotomic Polynomials

Definition (Cyclotomic polynomial)

For a positive integer n the n th cyclotomic polynomial $\Phi_n(z)$ is the unique irreducible polynomial in $\mathbb{Z}[z]$ given by

$$\Phi_n(z) = \prod_{\substack{1 \leq k < n, \\ \gcd(k, n) = 1}} (z - \zeta_n^k) \quad (23)$$

where ζ_n is a primitive n th root of unity.

Remark

- (1) The roots of $\Phi_n(z)$ are precisely the primitive n th roots of unity.
- (2) $\Phi_n(z)$ divides $z^n - 1$ but doesn't divide $z^k - 1$ for any positive integer $k < n$.

Cyclotomic Polynomials

We have the following identities.

If p is prime, then

$$\Phi_p(z) = 1 + z + z^2 + \dots + z^{p-1} = \sum_{k=0}^{p-1} z^k, \quad (24)$$

and if $n = 2p$ where p is an odd prime, then

$$\Phi_{2p}(z) = 1 - z + z^2 - \dots + z^{p-1} = \sum_{k=0}^{p-1} (-z)^k. \quad (25)$$

Theorem (Eisenstein's Criterion)

Suppose that $f(x) = \sum_{k=0}^n a_k x^k \in \mathbb{Z}[x]$. If there exists a prime p for which $p \nmid a_n$, $p \mid a_k$ for all $k < n$, and $p^2 \nmid a_0$, then f is irreducible over \mathbb{Q} .

Theorem (Eisenstein's Criterion)

Suppose that $f(x) = \sum_{k=0}^n a_k x^k \in \mathbb{Z}[x]$. If there exists a prime p for which $p \nmid a_n$, $p \mid a_k$ for all $k < n$, and $p^2 \nmid a_0$, then f is irreducible over \mathbb{Q} .

Lemma

$\Phi_p(z)$ is irreducible if and only if $\Phi_p(z + 1)$ is.

Cyclotomic Polynomials

Theorem (Eisenstein's Criterion)

Suppose that $f(x) = \sum_{k=0}^n a_k x^k \in \mathbb{Z}[x]$. If there exists a prime p for which $p \nmid a_n$, $p \mid a_k$ for all $k < n$, and $p^2 \nmid a_0$, then f is irreducible over \mathbb{Q} .

Lemma

$\Phi_p(z)$ is irreducible if and only if $\Phi_p(z + 1)$ is.

Theorem

If p is prime, then the p th cyclotomic polynomial $\Phi_p(z)$ is irreducible.

Cyclotomic Polynomials

Proof.

Let p be prime. First notice that the binomial coefficient $\binom{p}{r}$ is divisible by p for all $0 \leq r \leq p - 1$. Indeed, let

$$N = \binom{p}{r} = \frac{p!}{r!(p-r)!}.$$

Then $p! = Nr!(p-r)!$. Clearly p divides $p!$ and hence p also divides $Nr!(p-r)!$. Since p is prime, it must divide N or $r!(p-r)!$. But $r, p-r < p$ so that $p \nmid r!, (p-r)!$. Thus p divides N . Now, we have

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

Every coefficient of $\Phi_p(z+1)$ except the coefficient of z^{p-1} is divisible by p by the above, and $p^2 \nmid p$. Hence by Eisenstein's Criterion $\Phi_p(z+1)$ is irreducible. Thus by the Lemma, $\Phi_p(z)$ is irreducible. □

Cyclotomic Polynomials

In fact, it is true that the n th cyclotomic polynomial is irreducible for all positive integers n .

Cyclotomic Polynomials

In fact, it is true that the n th cyclotomic polynomial is irreducible for all positive integers n .

Proof.

Exercise.

Cyclotomic Polynomials

In fact, it is true that the n th cyclotomic polynomial is irreducible for all positive integers n .

Proof.

Exercise. [There's a nice one in *A Classical Introduction to Modern Number Theory* by Ireland and Rosen.] □

Definition (Euler's totient function)

For a positive integer n , the number of positive integers less than n and relatively prime to n is given by Euler's totient function, $\varphi(n)$. That is, $\varphi(n) := \#\{k \in \mathbb{N} \mid k < n, \gcd(k, n) = 1\}$.

Definition (Euler's totient function)

For a positive integer n , the number of positive integers less than n and relatively prime to n is given by Euler's totient function, $\varphi(n)$. That is, $\varphi(n) := \#\{k \in \mathbb{N} \mid k < n, \gcd(k, n) = 1\}$.

Theorem

The degree of $\Phi_n(z)$ is $\varphi(n)$.

Cyclotomic Polynomials

Definition (Euler's totient function)

For a positive integer n , the number of positive integers less than n and relatively prime to n is given by Euler's totient function, $\varphi(n)$. That is, $\varphi(n) := \#\{k \in \mathbb{N} \mid k < n, \gcd(k, n) = 1\}$.

Theorem

The degree of $\Phi_n(z)$ is $\varphi(n)$.

Proof.

By definition,

$$\Phi_n(z) = \prod_{\substack{1 \leq k < n, \\ \gcd(k, n) = 1}} (z - \zeta_n^k),$$

which is a product of $\varphi(n)$ factors, each having as its leading term z with coefficient 1. □

Newman Polynomials, Borwein Polynomials, and Irreducibility

Definition (Borwein polynomial, Newman polynomial)

Let

$$P = \{z^n + a_{n-1}z^{n-1} + \cdots + a_1z + a_0 \mid a_i \in \{-1, 0, 1\}\}.$$

A polynomial $f \in P$ is called a Borwein polynomial if $f(0) \neq 0$ and called a Newman polynomial if every $a_i \in \{0, 1\}$.

Newman Polynomials, Borwein Polynomials, and Irreducibility

Definition (Borwein polynomial, Newman polynomial)

Let

$$P = \{z^n + a_{n-1}z^{n-1} + \cdots + a_1z + a_0 \mid a_i \in \{-1, 0, 1\}\}.$$

A polynomial $f \in P$ is called a *Borwein polynomial* if $f(0) \neq 0$ and called a *Newman polynomial* if every $a_i \in \{0, 1\}$.

- The length of a polynomial is the number of nonzero terms.

Newman Polynomials, Borwein Polynomials, and Irreducibility

Definition (Borwein polynomial, Newman polynomial)

Let

$$P = \{z^n + a_{n-1}z^{n-1} + \cdots + a_1z + a_0 \mid a_i \in \{-1, 0, 1\}\}.$$

A polynomial $f \in P$ is called a *Borwein polynomial* if $f(0) \neq 0$ and called a *Newman polynomial* if every $a_i \in \{0, 1\}$.

- The length of a polynomial is the number of nonzero terms.
- Notice that if $a_0 = 0$, then $f(z)$ is trivially reducible. So, we will sometimes restrict to the case $a_0 = 1$.

Newman Polynomials, Borwein Polynomials, and Irreducibility

Definition (Borwein polynomial, Newman polynomial)

Let

$$P = \{z^n + a_{n-1}z^{n-1} + \cdots + a_1z + a_0 \mid a_i \in \{-1, 0, 1\}\}.$$

A polynomial $f \in P$ is called a *Borwein polynomial* if $f(0) \neq 0$ and called a *Newman polynomial* if every $a_i \in \{0, 1\}$.

- The length of a polynomial is the number of nonzero terms.
- Notice that if $a_0 = 0$, then $f(z)$ is trivially reducible. So, we will sometimes restrict to the case $a_0 = 1$.
- $\mathbb{S} = \{z \in \mathbb{C} : |z| = 1\}$ will denote the unit circle in \mathbb{C} . Some but not all Newman polynomials have roots on \mathbb{S} , and some Newman polynomials are reducible over \mathbb{Q} while others are not.

Newman Polynomials, Borwein Polynomials, and Irreducibility

Remark

In light of these new definitions, we see that for $t \geq 2$ and $n \geq 0$ the polynomials $a_{1,t}(n; z)$ and $a_{2,t}(n; z)$ are Newman polynomials of length $a(n)$.

Newman Polynomials, Borwein Polynomials, and Irreducibility

Remark

In light of these new definitions, we see that for $t \geq 2$ and $n \geq 0$ the polynomials $a_{1,t}(n; z)$ and $a_{2,t}(n; z)$ are Newman polynomials of length $a(n)$.

Theorem (Lehmer)

Given an integer $k \geq 2$, the number of integers n in the interval $2^{k-1} \leq n \leq 2^k$ for which $a(n) = k$ is $\varphi(k)$. Furthermore, it is the same number in any subsequent interval between two consecutive powers of 2.

Newman Polynomials, Borwein Polynomials, and Irreducibility

Remark

In light of these new definitions, we see that for $t \geq 2$ and $n \geq 0$ the polynomials $a_{1,t}(n; z)$ and $a_{2,t}(n; z)$ are Newman polynomials of length $a(n)$.

Theorem (Lehmer)

Given an integer $k \geq 2$, the number of integers n in the interval $2^{k-1} \leq n \leq 2^k$ for which $a(n) = k$ is $\varphi(k)$. Furthermore, it is the same number in any subsequent interval between two consecutive powers of 2.

Corollary

The number of type-1 generalized Stern polynomials of length k in the interval $[2^{k-1}, 2^k]$ is $\varphi(k)$.

Newman Polynomials, Borwein Polynomials, and Irreducibility

Theorem (Ljunggren)

If a Newman polynomial of length 3 or 4 is reducible, then it has a cyclotomic factor (equivalently, it vanishes at some root of unity). That is, if

$$f(z) = z^n + z^m + z^r + 1, \quad n > m > r \geq 0$$

is reducible, then f has a cyclotomic factor.

Newman Polynomials, Borwein Polynomials, and Irreducibility

Theorem (Ljunggren)

If a Newman polynomial of length 3 or 4 is reducible, then it has a cyclotomic factor (equivalently, it vanishes at some root of unity). That is, if

$$f(z) = z^n + z^m + z^r + 1, \quad n > m > r \geq 0$$

is reducible, then f has a cyclotomic factor.

Conjecture (Mercer)

If a Newman polynomial of length 5 is reducible, then it has a cyclotomic factor. That is, if

$$f(z) = z^n + z^m + z^r + z^s + 1, \quad n > m > r > s > 0$$

is reducible, then f has a cyclotomic factor.

- Mercer checked his conjecture for all Newman polynomials up to degree 24.

Corollary

The number of type-1 generalized Stern polynomials which have a cyclotomic factor in the interval $[4, 8]$ is at most $\varphi(3) = 2$, in the interval $[8, 16]$ at most $\varphi(4) = 2$, and in the interval $[16, 32]$ at most $\varphi(5) = 4$.

Newman Polynomials, Borwein Polynomials, and Irreducibility

Theorem (Tverberg)

The trinomial

$$f(z) = z^n + z^m \pm 1 \quad (26)$$

is irreducible whenever no root of f lies on \mathbb{S} . If f has roots on \mathbb{S} , then f has a cyclotomic factor and a rational factor.

Theorem (Koley & Reddy)

Let $f(z)$ be a Newman polynomial of length 5 with a cyclotomic factor. Then f is divisible by either $\Phi_{5^\gamma}(z)$ or $\Phi_{2^\alpha 3^\beta}(z)$ for some $\alpha, \beta, \gamma \geq 1$.

Newman Polynomials, Borwein Polynomials, and Irreducibility

Theorem (Koley & Reddy)

Let $f(z)$ be a Newman polynomial of length 5 with a cyclotomic factor. Then f is divisible by either $\Phi_{5^\gamma}(z)$ or $\Phi_{2^\alpha 3^\beta}(z)$ for some $\alpha, \beta, \gamma \geq 1$.

Example

We have

$$a_{1,2}(5; z) = z^4 + z^2 + 1 = (z^2 + z + 1)(z^2 - z + 1) = \Phi_3(z)\Phi_6(z).$$

Newman Polynomials, Borwein Polynomials, and Irreducibility

Theorem (Koley & Reddy)

Let $f(z)$ be a Newman polynomial of length 5 with a cyclotomic factor. Then f is divisible by either $\Phi_{5^\gamma}(z)$ or $\Phi_{2^\alpha 3^\beta}(z)$ for some $\alpha, \beta, \gamma \geq 1$.

Example

$$a_{1,2}(5; z) = z^4 + z^2 + 1 = (z^2 + z + 1)(z^2 - z + 1) = \Phi_3(z)\Phi_6(z).$$

Example

$$\begin{aligned} a_{1,2}(17; z) &= z^{16} + z^{14} + z^{12} + z^8 + 1 \\ &= (z^4 + z^3 + z^2 + z + 1)(z^4 - z^3 + z^2 - z + 1)(z^8 - z^2 + 1) \\ &= \Phi_5(z)\Phi_{10}(z)(z^8 - z^2 + 1) \end{aligned}$$

Newman Polynomials, Borwein Polynomials, and Irreducibility

Theorem (Koley & Reddy)

Suppose that f is a Borwein polynomial and $\Phi_k(z) \mid f(z)$ for some $k \in \mathbb{N}$. Then $\Phi_{k_1}(z) \mid f(z)$ for some $k_1 \mid k$ such that every prime factor of k_1 is at most $\ell(f)$, where $\ell(f)$ denotes the length of f .

Newman Polynomials, Borwein Polynomials, and Irreducibility

Theorem (Koley & Reddy)

Suppose that f is a Borwein polynomial and $\Phi_k(z) \mid f(z)$ for some $k \in \mathbb{N}$. Then $\Phi_{k_1}(z) \mid f(z)$ for some $k_1 \mid k$ such that every prime factor of k_1 is at most $\ell(f)$, where $\ell(f)$ denotes the length of f .

Returning to the previous example, we see that indeed

Example

$$\begin{aligned} a_{1,2}(17; z) &= z^{16} + z^{14} + z^{12} + z^8 + 1 \\ &= (z^4 + z^3 + z^2 + z + 1)(z^4 - z^3 + z^2 - z + 1)(z^8 - z^2 + 1) \\ &= \Phi_5(z)\Phi_{10}(z)(z^8 - z^2 + 1) \end{aligned}$$

and $5 \mid 10$ and $5 = \ell(\Phi_5(z)), \ell(\Phi_{10}(z)) \leq \ell(a_{1,2}(17; z)) = 5$.

Theorem (Koley & Reddy)

Let $q \geq 5$ be a prime and f a primitive Newman polynomial of length q . Then $\Phi_{2q}(z) \nmid f(z)$ and $\Phi_{3q}(z) \nmid f(z)$.

Theorem (Koley & Reddy)

Let $q \geq 5$ be a prime and f a primitive Newman polynomial of length q . Then $\Phi_{2q}(z) \nmid f(z)$ and $\Phi_{3q}(z) \nmid f(z)$.

Example

We have

$$\begin{aligned} a_{1,4}(41; z) &= z^{1088} + z^{1044} + z^{1040} + z^{1024} + z^{276} \\ &\quad + z^{272} + z^{256} + z^{64} + z^{20} + z^{16} + 1 \\ &= \Phi_{40}(z) \cdot f(z) \end{aligned}$$

for a huge polynomial $f(z)$. Indeed, $\ell(a_{1,4}(41; z)) = a(41) = 11$ is a prime greater than 5, and neither $\Phi_{22}(z)$ nor $\Phi_{33}(z)$ divides $a_{1,4}(41; z)$.

Previous Irreducibility Results for $a_{2,t}(n; z)$

- The irreducibility and factors of the type-2 generalized Stern polynomials $a_{2,t}(n; z)$ have been studied by Dilcher and Ericksen.

Previous Irreducibility Results for $a_{2,t}(n; z)$

- The irreducibility and factors of the type-2 generalized Stern polynomials $a_{2,t}(n; z)$ have been studied by Dilcher and Ericksen.
- Here we state without proof their major results.

Previous Irreducibility Results for $a_{2,t}(n; z)$

- The irreducibility and factors of the type-2 generalized Stern polynomials $a_{2,t}(n; z)$ have been studied by Dilcher and Ericksen.
- Here we state without proof their major results.
- Throughout, they often employ the theorem of Lehmer mentioned earlier:

Theorem (Lehmer)

Given an integer $k \geq 2$, the number of integers n in the interval $2^{k-1} \leq n \leq 2^k$ for which $a(n) = k$ is $\varphi(k)$. Furthermore, it is the same number in any subsequent interval between two consecutive powers of 2.

Previous Irreducibility Results for $a_{2,t}(n; z)$

Since for $t \geq 2$ the $a_{2,t}(n; z)$ are all Newman polynomials, by earlier results this means we can write down all binomials, trinomials, quadrinomials, and pentanomials among the $a_{2,t}(n; z)$ for $t \geq 2$, of which there are $\varphi(2) + \cdots + \varphi(5) = 9$ different classes.

Theorem

For $k \geq 1$ the binomial $a_{2,t}(3 \cdot 2^k; z)$ is irreducible if and only if $t \geq 1$ is a power of 2.

Previous Irreducibility Results for $a_{2,t}(n; z)$

Theorem

Let $k \geq 0$ and $t \geq 2$ be integers.

(a) If $t \equiv 0, 1 \pmod{3}$, then $a_{2,t}(5 \cdot 2^k; z)$ is irreducible.

(b) If $t \equiv 2 \pmod{3}$, then we have $z^2 + z + 1 \mid a_{2,t}(5 \cdot 2^k; z)$. That is, $a_{2,t}(5 \cdot 2^k; z)$ is reducible except for $a_{2,2}(5; z) = z^2 + z + 1$.

Previous Irreducibility Results for $a_{2,t}(n; z)$

Theorem

Let $k \geq 0$ and $t \geq 2$ be integers.

(a) If $t \equiv 0, 1 \pmod{3}$, then $a_{2,t}(5 \cdot 2^k; z)$ is irreducible.

(b) If $t \equiv 2 \pmod{3}$, then we have $z^2 + z + 1 \mid a_{2,t}(5 \cdot 2^k; z)$. That is, $a_{2,t}(5 \cdot 2^k; z)$ is reducible except for $a_{2,2}(5; z) = z^2 + z + 1$.

Theorem

Let $k \geq 0$ and $t \geq 2$ be integers.

(a) If $t \equiv 0, 2 \pmod{3}$, then $a_{2,t}(7 \cdot 2^k; z)$ is irreducible.

(b) If $t \equiv 1 \pmod{3}$, then $a_{2,t}(7 \cdot 2^k; z)$ is reducible.

Previous Irreducibility Results for $a_{2,t}(n; z)$

Theorem

Let $k \geq 0$ and $t \geq 2$ be integers.

(a) If $t \equiv 0, 1 \pmod{3}$, then $a_{2,t}(5 \cdot 2^k; z)$ is irreducible.

(b) If $t \equiv 2 \pmod{3}$, then we have $z^2 + z + 1 \mid a_{2,t}(5 \cdot 2^k; z)$. That is, $a_{2,t}(5 \cdot 2^k; z)$ is reducible except for $a_{2,2}(5; z) = z^2 + z + 1$.

Theorem

Let $k \geq 0$ and $t \geq 2$ be integers.

(a) If $t \equiv 0, 2 \pmod{3}$, then $a_{2,t}(7 \cdot 2^k; z)$ is irreducible.

(b) If $t \equiv 1 \pmod{3}$, then $a_{2,t}(7 \cdot 2^k; z)$ is reducible.

Theorem

For all integers $k \geq 0$ and $t \geq 2$, the quadrinomial $a_{2,t}(9 \cdot 2^k; z)$ is irreducible.

Previous Irreducibility Results for $a_{2,t}(n; z)$

Theorem

Let $k \geq 0$ and $t \geq 2$ be integers.

(a) If t is even, then $a_{2,t}(15 \cdot 2^k; z)$ is irreducible.

(b) If t is odd, then $a_{2,t}(15 \cdot 2^k; z)$ is divisible by $1 + z^{t^k}$.

Previous Irreducibility Results for $a_{2,t}(n; z)$

Theorem

Let $k \geq 0$ and $t \geq 2$ be integers.

(a) If t is even, then $a_{2,t}(15 \cdot 2^k; z)$ is irreducible.

(b) If t is odd, then $a_{2,t}(15 \cdot 2^k; z)$ is divisible by $1 + z^{t^k}$.

Theorem

Let $t \geq 2$ be an integer.

(a) If $t \equiv 2, 3 \pmod{5}$, then $\Phi_5(z) \mid a_{2,t}(17; z)$.

(b) If $t \equiv 1 \pmod{5}$, then $\Phi_5(z) \mid a_{2,t}(31; z)$.

Previous Irreducibility Results for $a_{2,t}(n; z)$

Theorem

Let $t \geq 2$ be an integer, and let $p \geq 3$ be a prime which has t as a primitive root. Then

$$(1 + z + z^2 + \cdots + z^{p-1}) \mid a_{2,t}(2^{p-1} + 1; z).$$

In particular, $a_{2,t}(2^{p-1}; z)$ is reducible in this case, with the exception of $a_{2,t}(5; z) = 1 + z + z^2$.

Previous Irreducibility Results for $a_{2,t}(n; z)$

Theorem

Let $t \geq 2$ be an integer, and let $p \geq 3$ be a prime which has t as a primitive root. Then

$$(1 + z + z^2 + \cdots + z^{p-1}) \mid a_{2,t}(2^{p-1} + 1; z).$$

In particular, $a_{2,t}(2^{p-1}; z)$ is reducible in this case, with the exception of $a_{2,t}(5; z) = 1 + z + z^2$.

Corollary

If $t \equiv 3, 5 \pmod{7}$, then $\Phi_7(z) \mid a_{2,t}(65; z)$.

Previous Irreducibility Results for $a_{2,t}(n; z)$

Theorem

Let $t \geq 2$ be an integer, and let $p \geq 3$ be a prime which has t as a primitive root. Then

$$(1 + z + z^2 + \cdots + z^{p-1}) \mid a_{2,t}(2^{p-1} + 1; z).$$

In particular, $a_{2,t}(2^{p-1}; z)$ is reducible in this case, with the exception of $a_{2,t}(5; z) = 1 + z + z^2$.

Corollary

If $t \equiv 3, 5 \pmod{7}$, then $\Phi_7(z) \mid a_{2,t}(65; z)$.

Previous Irreducibility Results for $a_{2,t}(n; z)$

Theorem

Let $p \geq 3$ be a prime and $t \geq 2$ be an integer satisfying $t \equiv 1 \pmod{p}$. Then

$$1 + z + z^2 + \cdots + z^{p-1} = \Phi_p(z) \mid a_{2,t}(2^p - 1; z).$$

In particular, $a_{2,t}(2^p - 1; z)$ is reducible in this case.

Corollary

Due to Ljunggren, we have that every reducible type-1 generalized Stern polynomial of length 3 or 4 has a cyclotomic factor.

Corollary

Due to Ljunggren, we have that every reducible type-1 generalized Stern polynomial of length 3 or 4 has a cyclotomic factor.

If Mercer's conjecture is true, then we can say more:

Corollary

Given Mercer's conjecture, every reducible type-1 generalized Stern polynomial of length 5 has a cyclotomic factor.

- Using Maple, determined analogous conjecture to that of Ulas for the generalized Stern polynomials is false

- Using Maple, determined analogous conjecture to that of Ulas for the generalized Stern polynomials is false
- I.e., there are primes p for which $a_{1,t}(p; z)$ and $a_{2,t}(p; z)$ are not irreducible over \mathbb{Q}

- Using Maple, determined analogous conjecture to that of Ulas for the generalized Stern polynomials is false
- I.e., there are primes p for which $a_{1,t}(p; z)$ and $a_{2,t}(p; z)$ are not irreducible over \mathbb{Q}

Example

We have

$$a_{1,2}(5; z) = z^4 + z^2 + 1 = (z^2 + z + 1)(z^2 - z + 1) = \Phi_3(z)\Phi_6(z).$$

My results

- Using Maple, determined analogous conjecture to that of Ulas for the generalized Stern polynomials is false
- I.e., there are primes p for which $a_{1,t}(p; z)$ and $a_{2,t}(p; z)$ are not irreducible over \mathbb{Q}

Example

We have

$$a_{1,2}(5; z) = z^4 + z^2 + 1 = (z^2 + z + 1)(z^2 - z + 1) = \Phi_3(z)\Phi_6(z).$$

Example

We have

$$a_{2,1}(7; z) = 2z^2 + z = z(2z + 1).$$

Observation: when p is prime and $a_{1,t}(p; z)$ is not irreducible, the polynomial always has cyclotomic factors.

Observation: when p is prime and $a_{1,t}(p; z)$ is not irreducible, the polynomial always has cyclotomic factors.

Example

We have

$$\begin{aligned}a_{1,2}(17; z) &= z^{16} + z^{14} + z^{12} + z^8 + 1 \\ &= (z^4 + z^3 + z^2 + z + 1)(z^4 - z^3 + z^2 - z + 1)(z^8 - z^2 + 1) \\ &= \Phi_5(z)\Phi_{10}(z)(z^8 - z^2 + 1)\end{aligned}$$

My results

Observation: when p is prime and $a_{1,t}(p; z)$ is not irreducible, the polynomial always has cyclotomic factors.

Example

We have

$$\begin{aligned}a_{1,2}(17; z) &= z^{16} + z^{14} + z^{12} + z^8 + 1 \\ &= (z^4 + z^3 + z^2 + z + 1)(z^4 - z^3 + z^2 - z + 1)(z^8 - z^2 + 1) \\ &= \Phi_5(z)\Phi_{10}(z)(z^8 - z^2 + 1)\end{aligned}$$

Example

We have

$$\begin{aligned}a_{1,4}(7; z) &= z^{20} + z^{16} + 1 \\ &= (z^2 + z + 1)(z^2 - z + 1)(z^4 - z^2 + 1)(z^{12} - z^4 + 1) \\ &= \Phi_3(z)\Phi_6(z)\Phi_{12}(z)(z^{12} - z^4 + 1).\end{aligned}$$

Conjecture

Let p be a prime. If $a_{1,t}(p; z)$ is not irreducible and $t = p_1^{e_1} \cdots p_r^{e_r}$ is the prime factorization of t , then

$$a_{1,t}(p; z) = \Phi_{j_1}(z) \cdots \Phi_{j_{r+2}}(z) f_1(z) \cdots f_m(z), \quad (27)$$

for at least two cyclotomic polynomials $\Phi_{j_1}, \dots, \Phi_{j_{r+2}}$ with $\gcd(j_1, \dots, j_{r+2}) = j_1$ and polynomials f_1, \dots, f_m .

Furthermore:

Conjecture

If $a_{1,t}(p; z)$ factors completely into a product of cyclotomic polynomials

$$a_{1,t}(p; z) = \Phi_{j_1}(z) \cdots \Phi_{j_{r+2}}(z), \quad j_1 < j_2 < \cdots < j_{r+2}, \quad (28)$$

then

(1) If $t = p_1^{e_1}$ is a prime power and $\gcd(j_1, t) = 1$, then

$$j_k = j_1 p_1^{k-1} \quad (1 \leq k-1 \leq e_1)$$

(2) If $\gcd(j_1, t) = p_i$ for some $1 \leq i \leq r$, then p_i is not a factor of any of the j_k ;

Conjecture (Cont'd)

(3) If $t = p_1 \cdots p_r$ is squarefree, then

$$j_2 = p_1 j_1,$$

$$j_3 = p_2 j_1,$$

$$\vdots$$

$$j_r = p_{r-1} j_1,$$

$$j_{r+1} = p_r j_1,$$

$$j_{r+2} = p_1 \cdots p_r j_1.$$

(4) If $t = p_1^{e_1} \cdots p_r^{e_r}$, $r > 1$, is a product of distinct prime powers and $\gcd(t, j_1) = 1$, then ???

- If a prime-indexed type-1 generalized Stern polynomial is not irreducible, then it has at least two cyclotomic polynomial factors whose indices are not relatively prime

- If a prime-indexed type-1 generalized Stern polynomial is not irreducible, then it has at least two cyclotomic polynomial factors whose indices are not relatively prime
- Furthermore, if $a_{1,t}(p, z)$ equals the product of cyclotomic polynomials, then the indices of the cyclotomic factors follow a multiplication rule with the prime factorization of the parameter t

- If a prime-indexed type-1 generalized Stern polynomial is not irreducible, then it has at least two cyclotomic polynomial factors whose indices are not relatively prime
- Furthermore, if $a_{1,t}(p, z)$ equals the product of cyclotomic polynomials, then the indices of the cyclotomic factors follow a multiplication rule with the prime factorization of the parameter t

Corollary

The number of type-1 generalized Stern polynomials which have a cyclotomic factor is equal to the number of reducible type-1 generalized Stern polynomials.

t	n	$a_{1,t}(n; z)$	$\{j : \Phi_j \mid a_{1,t}(n; z)\}$	Case
2	5	$z^4 + z^2 + 1$	3, 6	1
	17	$z^{16} + z^{14} + z^{12} + z^8 + 1$	5, 10	1
3	3	$z^3 + 1$	2, 6	1
	73	z^{756} + too big for this margin	5, 15	1
4	7	$z^{20} + z^{16} + 1$	3, 6, 12	3
	41	$z^{1088} + z^{1044} + z^{1040} + z^{1024} + z^{276} + z^{272} + z^{256} + z^{64} + z^{20} + z^{16} + 1$	40 (up to 10,000)	3
5	3	$z^5 + 1$	2, 10	1
	5	$z^{25} + z^5 + 1$	5, 15	1
6	3	$z^6 + 1$	4, 12	2
	31	$z^{1554} + z^{1548} + z^{1512} + z^{1296} + 1$	5, 10, 15, 30	3
7	3	$z^7 + 1$	2, 14	1
	7	$z^{56} + z^{49} + 1$	3, 21	1
	17	$z^{2401} + z^{399} + z^{392} + z^{343} + 1$	5, 35	1
8	5	$z^{64} + z^8 + 1$	3, 6, 12, 24	1
9	3	$z^9 + 1$	2, 6, 18	1

t	n	$a_{1,t}(n; z)$	$\{j : \Phi_j \mid a_{1,t}(n; z)\}$	Case
10	3	$z^{10} + 1$	4, 20	2
	7	$z^{110} + z^{100} + 1$	3, 6, 15, 30	3
11	3	$z^{11} + 1$	2, 22	1
	5	$z^{121} + z^{11} + 1$	3, 33	1
12	3	$z^{12} + 1$	8, 24	2
13	3	$z^{13} + 1$	2, 26	1
	7	$z^{182} + z^{169} + 1$	3, 39	1
14	3	$z^{14} + 1$	4, 28	2
	5	$z^{196} + z^{14} + 1$	3, 6, 21, 42	3
15	3	$z^{15} + 1$	2, 6, 10, 30	3?
16	7	$z^{272} + z^{256} + 1$	3, 6, 12, 24, 48	1
17	3	$z^{17} + 1$	2, 34	1
	5	$z^{289} + z^{17} + 1$	3, 51	1
18	3	$z^{18} + 1$	4, 12, 36	2

Table: Classification of $a_{1,t}(n; z)$ by cyclotomic factors

- Notice that the first instance of Case 4 doesn't occur until $t = 2^23^2 = 36$.

- Notice that the first instance of Case 4 doesn't occur until $t = 2^2 3^3 = 36$.
- Since the "size" of these polynomials grows very quickly, it becomes computationally expensive to factor them for large n and t .

- Notice that the first instance of Case 4 doesn't occur until $t = 2^23^3 = 36$.
- Since the "size" of these polynomials grows very quickly, it becomes computationally expensive to factor them for large n and t .
- Use cluster for this

n	$a_{1,t}(n; z)$
17	$z^{t^4} + z^{t^3+t^2+t} + z^{t^3+t^2} + z^{t^3} + 1$
18	$z^{t^4+1} + z^{t^3+t^2+1} + z^{t^3+1} + z$
19	$z^{t^4+1} + z^{t^4} + z^{t^3+t^2} + z^{t^3+1} + z^{t^3} + z^t + 1$
20	$z^{t^4+t+1} + z^{t^3+t+1} + z^{t+1}$
21	$z^{t^4+t^2} + z^{t^4+t} + z^{t^4} + z^{t^3+t} + z^{t^3} + z^{t^2} + z^t + 1$
22	$z^{t^4+t^2+1} + z^{t^4+1} + z^{t^3+1} + z^{t^2+1} + z$
23	$z^{t^4+t^2+t} + z^{t^4+t^2} + z^{t^4} + z^{t^3} + z^{t^2+t} + z^{t^2} + 1$
24	$z^{t^4+t^2+t+1} + z^{t^2+t+1}$
25	$z^{t^4+t^3} + z^{t^4+t^2+t} + z^{t^4+t^2} + z^{t^4} + z^{t^2+t} + z^{t^2} + 1$
26	$z^{t^4+t^3+1} + z^{t^4+t^2+1} + z^{t^4+1} + z^{t^2+1} + z$
27	$z^{t^4+t^3+t} + z^{t^4+t^3} + z^{t^4+t^2} + z^{t^4+t} + z^{t^4} + z^{t^2} + z^t + 1$
28	$z^{t^4+t^3+t+1} + z^{t^4+t^3+t} + z^{t^4+t^3} + z^{t^4+t} + z^{t^4} + z^t + 1$
29	$z^{t^4+t^3+t^2} + z^{t^4+t^3+t} + z^{t^4+t^3} + z^{t^4+t} + z^{t^4} + z^t + 1$
30	$z^{t^4+t^3+t^2+1} + z^{t^4+t^3+1} + z^{t^4+1} + z$
31	$z^{t^4+t^3+t^2+t} + z^{t^4+t^3+t^2} + z^{t^4+t^3} + z^{t^4} + 1$
32	$z^{t^4+t^3+t^2+t+1}$

Proposition

For $t > 0$ and $m \geq 1$,

$$a_{1,t}(2^m; z) = z^{t^{m-1} + t^{m-2} + \dots + t + 1} \quad (29)$$

is trivially reducible.

Proposition

For $t > 0$ and $m \geq 1$,







$$a_{1,t}(2^m; z) = z^{t^{m-1} + t^{m-2} + \dots + t + 1} \quad (30)$$

is trivially reducible.

Proof.

First note that $a(n) = 1$ if and only if $n = 2^m$, $m \geq 0$. Furthermore, $a_{1,t}(2^m; z)$ is a positive power of z for every $m \geq 1$. □

References

-  K. Dilcher, M. Kidwai and H. Thomkins, *Zeros and irreducibility of Stern polynomials*, Publ. Math. Debrecen. 90 (2017), no. 3-4, 407-433.
-  K. Dilcher and L. Ericksen, *Generalized Stern polynomials and hyperbinary representations*, Bull. Pol. Acad. Sci. Math. 65 (2017), no.1, 11-28
-  K. Dilcher and L. Ericksen, *Factors and irreducibility of generalized Stern polynomials*, Integers 15 (2015), Paper no. A50, 17 pp.
-  I. Mercer, *Newman polynomials, Reducibility, and Roots on the Unit Circle*, Integers 12 (2012), 503-519.
-  B. Koley and A. S. Reddy, *Cyclotomic factors of Borwein polynomials*, Bull. Aus. Math. Soc. (2019) (To appear)
-  H. Tverberg, *On the irreducibility of the trinomials*, Math. Scand. 8 (1960), 121-126.

Thanks!

- Thanks!
- Questions, comments, suggestions?