Zeros and irreducibility of some classes of special polynomials

Karl Dilcher

Dalhousie Number Theory Seminar
January 21, 2019

Part I: Chebyshev-like polynomials

Pafnutiy L'vovich Chebyshev
1821 – 1894

Joint work with

Kenneth B. Stolarsky
University of Illinois, Urbana-Champaign

1. Introduction

The Chebyshev polynomials $T_n(x)$ are among the most important and interesting classical orthogonal polynomials.

1. Introduction

The Chebyshev polynomials $T_n(x)$ are among the most important and interesting classical orthogonal polynomials.

Numerous applications, e.g., in Approximation Theory.

1. Introduction

The Chebyshev polynomials $T_n(x)$ are among the most important and interesting classical orthogonal polynomials.

Numerous applications, e.g., in Approximation Theory.

They can be defined by $T_0(x) = 1$, $T_1(x) = x$, and

$$T_{n+1}(x) = 2xT_n(x) - T_{n-1}(x) \qquad (n \geq 1).$$

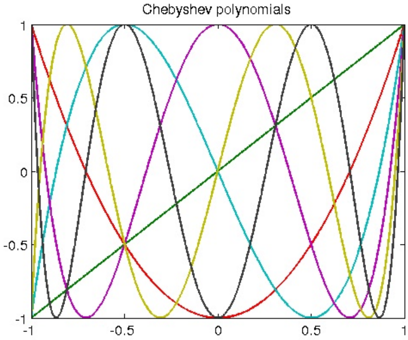
1. Introduction

The Chebyshev polynomials $T_n(x)$ are among the most important and interesting classical orthogonal polynomials.

Numerous applications, e.g., in Approximation Theory.

They can be defined by $T_0(x) = 1$, $T_1(x) = x$, and

$$T_{n+1}(x) = 2xT_n(x) - T_{n-1}(x) \qquad (n \geq 1).$$



Here is the definition again:

$T_0(x) = 1$, $T_1(x) = x$, and

$$T_{n+1}(x) = 2xT_n(x) - T_{n-1}(x) \qquad (n \geq 1).$$

Here is the definition again:

$T_0(x) = 1,\ T_1(x) = x$, and

$$T_{n+1}(x) = 2xT_n(x) - T_{n-1}(x) \qquad (n \geq 1).$$

We compute:

$T_2(x) = 2x^2 - 1,\ T_3(x) = 4x^3 - 3x,\ T_4(x) = 8x^4 - 8x^2 + 1, \ldots$

Here is the definition again:

$T_0(x) = 1,\ T_1(x) = x$, and

$$T_{n+1}(x) = 2xT_n(x) - T_{n-1}(x) \qquad (n \geq 1).$$

We compute:

$T_2(x) = 2x^2 - 1,\ T_3(x) = 4x^3 - 3x,\ T_4(x) = 8x^4 - 8x^2 + 1, \ldots$

Now consider a slight variant:

$V_0(x) = 1,\ V_1(x) = x$, and

Here is the definition again:

$T_0(x) = 1,\ T_1(x) = x$, and

$$T_{n+1}(x) = 2xT_n(x) - T_{n-1}(x) \qquad (n \geq 1).$$

We compute:

$T_2(x) = 2x^2 - 1,\ T_3(x) = 4x^3 - 3x,\ T_4(x) = 8x^4 - 8x^2 + 1, \ldots$

Now consider a slight variant:

$V_0(x) = 1,\ V_1(x) = x$, and

$$V_{n+1}(x) = 2xV_n(x) - V_{n-1}(x) - x^{n+1} \qquad (n \geq 1).$$

Here is the definition again:

$T_0(x) = 1,\ T_1(x) = x$, and

$$T_{n+1}(x) = 2xT_n(x) - T_{n-1}(x) \qquad (n \geq 1).$$

We compute:

$T_2(x) = 2x^2 - 1,\ T_3(x) = 4x^3 - 3x,\ T_4(x) = 8x^4 - 8x^2 + 1, \dots$

Now consider a slight variant:

$V_0(x) = 1,\ V_1(x) = x$, and

$$V_{n+1}(x) = 2xV_n(x) - V_{n-1}(x) - x^{n+1} \qquad (n \geq 1).$$

Do we get anything sensible?

Let’s look at a table:

Let’s look at a table:

n	$V_n(x)$
1	x
2	$x^2 - 1$
3	$x^3 - 3x$
4	$x^4 - 7x^2 + 1$
5	$x^5 - 15x^3 + 5x$
6	$x^6 - 31x^4 + 17x^2 - 1$
7	$x^7 - 63x^5 + 49x^3 - 7x$
8	$x^8 - 127x^6 + 129x^4 - 31x^2 + 1$
9	$x^9 - 255x^7 + 321x^5 - 111x^3 + 9x$
10	$x^{10} - 511x^8 + 769x^6 - 351x^4 + 49x^2 - 1$
11	$x^{11} - 1023x^9 + 1793x^7 - 1023x^5 + 209x^3 - 11x$
12	$x^{12} - 2047x^{10} + 4097x^8 - 2815x^6 + 769x^4 - 71x^2 + 1$

$V_0(x) = 1$, $V_1(x) = x$, and

$$V_{n+1}(x) = 2xV_n(x) - V_{n-1}(x) - x^{n+1} \qquad (n \geq 1).$$

$V_0(x) = 1$, $V_1(x) = x$, and

$$V_{n+1}(x) = 2xV_n(x) - V_{n-1}(x) - x^{n+1} \qquad (n \geq 1).$$

Some properties:

$$V_n(x) = \frac{x^{n+2} - T_n(x)}{x^2 - 1}; \tag{1}$$

$V_0(x) = 1$, $V_1(x) = x$, and

$$V_{n+1}(x) = 2xV_n(x) - V_{n-1}(x) - x^{n+1} \qquad (n \geq 1).$$

Some properties:

$$V_n(x) = \frac{x^{n+2} - T_n(x)}{x^2 - 1}; \tag{1}$$

$$V_n(x) = x^n - \sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2k} (x^2 - 1)^{k-1} x^{n-2k}. \tag{2}$$

$V_0(x) = 1$, $V_1(x) = x$, and

$$V_{n+1}(x) = 2xV_n(x) - V_{n-1}(x) - x^{n+1} \qquad (n \geq 1).$$

Some properties:

$$V_n(x) = \frac{x^{n+2} - T_n(x)}{x^2 - 1}; \tag{1}$$

$$V_n(x) = x^n - \sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2k} (x^2 - 1)^{k-1} x^{n-2k}. \tag{2}$$

Compare with

$$T_n(x) = x^n + \sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2k} (x^2 - 1)^{k} x^{n-2k},$$

from which (2) is derived, by way of (1).

Some special values:

$$V_n(1) = 1 - \binom{n}{2}, \qquad V_n(-1) = (-1)^n \left(1 - \binom{n}{2}\right).$$

Some special values:

$$V_n(1) = 1 - \binom{n}{2}, \qquad V_n(-1) = (-1)^n \left(1 - \binom{n}{2}\right).$$

Generating function:

$$\frac{1 - 2tx}{(1 - tx)(1 - 2tx + t^2)} = \sum_{n=0}^{\infty} V_n(x) t^n. \tag{3}$$

Some special values:

$$V_n(1) = 1 - \binom{n}{2}, \qquad V_n(-1) = (-1)^n \left(1 - \binom{n}{2}\right).$$

Generating function:

$$\frac{1-2tx}{(1-tx)(1-2tx+t^2)} = \sum_{n=0}^{\infty} V_n(x)t^n. \tag{3}$$

Compare with

$$\frac{1-tx}{1-2tx+t^2} = \sum_{n=0}^{\infty} T_n(x)t^n,$$

from which (3) is derived.

2. Irreducibility and Zeros

2. Irreducibility and Zeros

The Chebyshev polynomial $T_n(x)$

2. Irreducibility and Zeros

The Chebyshev polynomial $T_n(x)$

- has a well-known factorization over $\mathbb{Q}$ in terms of cyclotomic polynomials

2. Irreducibility and Zeros

The Chebyshev polynomial $T_n(x)$

- has a well-known factorization over $\mathbb{Q}$ in terms of cyclotomic polynomials
- is irreducible over $\mathbb{Q}$ iff $n = 2^k$, $k = 0, 1, 2, \ldots$.

2. Irreducibility and Zeros

The Chebyshev polynomial $T_n(x)$

- has a well-known factorization over $\mathbb{Q}$ in terms of cyclotomic polynomials
- is irreducible over $\mathbb{Q}$ iff $n = 2^k$, $k = 0, 1, 2, \ldots$.

How about the $V_n(x)$?

2. Irreducibility and Zeros

The Chebyshev polynomial $T_n(x)$
- has a well-known factorization over $\mathbb{Q}$ in terms of cyclotomic polynomials
- is irreducible over $\mathbb{Q}$ iff $n = 2^k$, $k = 0, 1, 2, \ldots$.

How about the $V_n(x)$?

Easy to see:

$$V_2(x) = (x-1)(x+1), \qquad V_4(x) = (x^2-3x+1)(x^2+3x+1)$$

2. Irreducibility and Zeros

The Chebyshev polynomial $T_n(x)$

- has a well-known factorization over $\mathbb{Q}$ in terms of cyclotomic polynomials
- is irreducible over $\mathbb{Q}$ iff $n = 2^k$, $k = 0, 1, 2, \ldots$.

How about the $V_n(x)$?

Easy to see:

$$V_2(x) = (x-1)(x+1), \qquad V_4(x) = (x^2-3x+1)(x^2+3x+1)$$

However, all other $V_{2k}(x)$ and $\frac{1}{x}V_{2k+1}(x)$ appear to be irreducible.

The Chebyshev polynomial $T_n(x)$

- has a well-known factorization over $\mathbb{Q}$ in terms of cyclotomic polynomials
- is irreducible over $\mathbb{Q}$ iff $n = 2^k$, $k = 0, 1, 2, \ldots$.

How about the $V_n(x)$?

Easy to see:

$$V_2(x) = (x-1)(x+1), \qquad V_4(x) = (x^2-3x+1)(x^2+3x+1)$$

However, all other $V_{2k}(x)$ and $\frac{1}{x}V_{2k+1}(x)$ appear to be irreducible.

We can prove a partial result:

Proposition

The following are irreducible over $\mathbb{Q}$:

(a) $V_{2^k-2}(x)$ *for all* $k \geq 3$*;*

Proposition

The following are irreducible over $\mathbb{Q}$:

(a) $V_{2^k-2}(x)$ *for all* $k \geq 3$*;*

(b) $\frac{1}{x}V_p(x)$ *for all odd primes* p*.*

Proposition

The following are irreducible over $\mathbb{Q}$*:*

(a) $V_{2^k-2}(x)$ *for all* $k \geq 3$*;*

(b) $\frac{1}{x}V_p(x)$ *for all odd primes* p*.*

Sketch of Proof: Using the explicit expansion

$$V_n(x) = x^n - \sum_{r=0}^{\lfloor\frac{n}{2}\rfloor-1}(-1)^r\left(\sum_{k=r+1}^{\lfloor\frac{n}{2}\rfloor}\binom{n}{2k}\binom{k-1}{r}\right)x^{n-2-2r},$$

it can be shown that the polynomials in (a) and (b) are 2-Eisenstein.

Proposition

The following are irreducible over $\mathbb{Q}$:

(a) $V_{2^k-2}(x)$ *for all* $k \geq 3$*;*

(b) $\frac{1}{x}V_p(x)$ *for all odd primes* p*.*

Sketch of Proof: Using the explicit expansion

$$V_n(x) = x^n - \sum_{r=0}^{\lfloor\frac{n}{2}\rfloor-1}(-1)^r\left(\sum_{k=r+1}^{\lfloor\frac{n}{2}\rfloor}\binom{n}{2k}\binom{k-1}{r}\right)x^{n-2-2r},$$

it can be shown that the polynomials in (a) and (b) are 2-Eisenstein.

(No other $V_{2k}(x)$ or $\frac{1}{x}V_{2k+1}(x)$ is Eisenstein).

Recall: All zeros of $T_n(x)$ lie in the interval $(-1, 1)$.

Recall: All zeros of $T_n(x)$ lie in the interval $(-1, 1)$.

The zeros of $V_n(x)$ are also all real. However:

Recall: All zeros of $T_n(x)$ lie in the interval $(-1, 1)$.

The zeros of $V_n(x)$ are also all real. However:

n	r_n	n	r_n
1	0	11	31.956928
2	1	12	45.221645
3	1.7320508	13	63.974591
4	2.6180339	14	90.490325
5	3.8286956	15	127.98534
6	5.5174860	16	181.00828
7	7.8875983	17	255.99169
8	11.223990	18	362.03245
9	15.929112	19	511.99536
10	22.571929	20	724.07389

Table 2: The largest zeros r_n of $V_n(x)$, $2 \leq n \leq 20$.

Recall: All zeros of $T_n(x)$ lie in the interval $(-1,1)$.

The zeros of $V_n(x)$ are also all real. However:

n	r_n	$2^{(n-1)/2}$	n	r_n	$2^{(n-1)/2}$
1	0	1	11	31.956928	32
2	1	1.4142135	12	45.221645	45.254833
3	1.7320508	2	13	63.974591	64
4	2.6180339	2.8284271	14	90.490325	90.509667
5	3.8286956	4	15	127.98534	128
6	5.5174860	5.6568542	16	181.00828	181.01933
7	7.8875983	8	17	255.99169	256
8	11.223990	11.313708	18	362.03245	362.03867
9	15.929112	16	19	511.99536	512
10	22.571929	22.627416	20	724.07389	724.07734

Table 2: The largest zeros r_n of $V_n(x)$, $2 \le n \le 20$.

Proposition

Let $n \geq 2$, and $\pm r_n$ be the largest zeros in absolute value of $V_n(x)$. Then

(a) *$n-2$ zeros of $V_n(x)$ lie in the interval $(-1, 1)$;*

Proposition

Let $n \geq 2$, and $\pm r_n$ be the largest zeros in absolute value of $V_n(x)$. Then

(a) *$n-2$ zeros of $V_n(x)$ lie in the interval $(-1, 1)$;*

(b) $(\sqrt{2})^{n-1} - \frac{n}{(\sqrt{2})^{n-1}} < r_n < (\sqrt{2})^{n-1}$.

Proposition

Let $n \geq 2$, and $\pm r_n$ be the largest zeros in absolute value of $V_n(x)$. Then

(a) *$n-2$ zeros of $V_n(x)$ lie in the interval $(-1,1)$;*

(b) $(\sqrt{2})^{n-1} - \frac{n}{(\sqrt{2})^{n-1}} < r_n < (\sqrt{2})^{n-1}$.

Idea of proof: For (a), use $(x^2-1)\,V_n(x) = x^{n+2} - T_n(x)$.

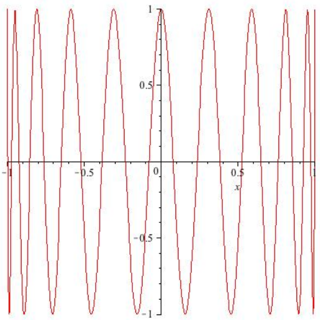
Proposition

Let $n \geq 2$, and $\pm r_n$ be the largest zeros in absolute value of $V_n(x)$. Then

(a) *$n - 2$ zeros of $V_n(x)$ lie in the interval $(-1, 1)$;*

(b) $(\sqrt{2})^{n-1} - \frac{n}{(\sqrt{2})^{n-1}} < r_n < (\sqrt{2})^{n-1}$.

Idea of proof: For (a), use $(x^2 - 1)\,V_n(x) = x^{n+2} - T_n(x)$.
Consider graph of $y = T_n(x)$; count intersections with $y = x^{n+2}$.



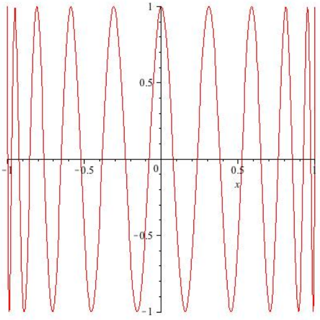
Proposition

Let $n \geq 2$, and $\pm r_n$ be the largest zeros in absolute value of $V_n(x)$. Then

(a) *$n-2$ zeros of $V_n(x)$ lie in the interval $(-1, 1)$;*

(b) $(\sqrt{2})^{n-1} - \frac{n}{(\sqrt{2})^{n-1}} < r_n < (\sqrt{2})^{n-1}$.

Idea of proof: For (a), use $(x^2-1)V_n(x) = x^{n+2} - T_n(x)$.
Consider graph of $y = T_n(x)$; count intersections with $y = x^{n+2}$.



(b): Evaluate $V_n(x)$ at the two boundary points of the interval.

$T_{20}(x)$

3. A Related Polynomial

3. A Related Polynomial

The Chebyshev polynomials $T_n(x)$ satisfy the (2×2 Hankel determinant) identity

$$T_{n+1}(x)^2 - T_n(x)T_{n+2}(x) = 1 - x^2 \qquad (n \geq 0).$$

3. A Related Polynomial

The Chebyshev polynomials $T_n(x)$ satisfy the (2×2 Hankel determinant) identity

$$T_{n+1}(x)^2 - T_n(x)T_{n+2}(x) = 1 - x^2 \qquad (n \geq 0).$$

How about the analogue for $\{V_n(x)\}$?

3. A Related Polynomial

The Chebyshev polynomials $T_n(x)$ satisfy the (2×2 Hankel determinant) identity

$$T_{n+1}(x)^2 - T_n(x)T_{n+2}(x) = 1 - x^2 \qquad (n \geq 0).$$

How about the analogue for $\{V_n(x)\}$?

Define

$$W_n(x) := V_{n+1}(x)^2 - V_n(x)V_{n+2}(x) \qquad (n \geq 0).$$

3. A Related Polynomial

The Chebyshev polynomials $T_n(x)$ satisfy the (2×2 Hankel determinant) identity

$$T_{n+1}(x)^2 - T_n(x)T_{n+2}(x) = 1 - x^2 \qquad (n \geq 0).$$

How about the analogue for $\{V_n(x)\}$?

Define

$$W_n(x) := V_{n+1}(x)^2 - V_n(x)V_{n+2}(x) \qquad (n \geq 0).$$

We'll see: These polynomials have some interesting properties.

n	$W_n(x)$
0	1
1	x^2+1
2	$2x^4+x^2+1$
3	$4x^6+x^4+x^2+1$
4	$8x^8+x^4+x^2+1$
5	$16x^{10}-4x^8+x^6+x^4+x^2+1$
6	$32x^{12}-16x^{10}+2x^8+x^6+x^4+x^2+1$
7	$64x^{14}-48x^{12}+8x^{10}+x^8+x^6+x^4+x^2+1$
8	$128x^{16}-128x^{14}+32x^{12}+x^8+x^6+x^4+x^2+1$
9	$256x^{18}-320x^{16}+112x^{14}-8x^{12}+x^{10}+x^8+x^6$ $+x^4+x^2+1$
10	$512x^{20}-768x^{18}+352x^{16}-48x^{14}+2x^{12}+x^{10}$ $+x^8+x^6+x^4+x^2+1$

Some properties:

$$W_n(x) = \frac{1 - x^{n+2}T_n(x)}{1 - x^2}.$$

Some properties:

$$W_n(x) = \frac{1 - x^{n+2}T_n(x)}{1 - x^2}.$$

Compare:

$$V_n(x) = \frac{T_n(x) - x^{n+2}}{1 - x^2}.$$

Some properties:

$$W_n(x) = \frac{1 - x^{n+2}\,T_n(x)}{1 - x^2}.$$

Compare:

$$V_n(x) = \frac{T_n(x) - x^{n+2}}{1 - x^2}.$$

Recurrence: $W_0(x) = 1$, $W_1(x) = x^2 + 1$, and for $n \geq 1$,

$$W_{n+1}(x) = x^2\,(2\,W_n(x) - W_{n-1}(x)) + 1.$$

Some properties:

$$W_n(x) = \frac{1 - x^{n+2} T_n(x)}{1 - x^2}.$$

Compare:

$$V_n(x) = \frac{T_n(x) - x^{n+2}}{1 - x^2}.$$

Recurrence: $W_0(x) = 1$, $W_1(x) = x^2 + 1$, and for $n \geq 1$,

$$W_{n+1}(x) = x^2 \left(2 W_n(x) - W_{n-1}(x)\right) + 1.$$

Generating function:

$$\frac{1 - tx^2 + t^2 x^2}{(1-t)(1 - 2tx^2 + t^2 x^2)} = \sum_{n=0}^{\infty} W_n(x) t^n.$$

Let's look at the table again:

Let's look at the table again:

n	$W_n(x)$
0	1
1	$x^2 + 1$
2	$2x^4 + x^2 + 1$
3	$4x^6 + x^4 + x^2 + 1$
4	$8x^8 + x^4 + x^2 + 1$
5	$16x^{10} - 4x^8 + x^6 + x^4 + x^2 + 1$
6	$32x^{12} - 16x^{10} + 2x^8 + x^6 + x^4 + x^2 + 1$
7	$64x^{14} - 48x^{12} + 8x^{10} + x^8 + x^6 + x^4 + x^2 + 1$
8	$128x^{16} - 128x^{14} + 32x^{12} + x^8 + x^6 + x^4 + x^2 + 1$
9	$256x^{18} - 320x^{16} + 112x^{14} - 8x^{12} + x^{10} + x^8 + x^6$ $+x^4 + x^2 + 1$
10	$512x^{20} - 768x^{18} + 352x^{16} - 48x^{14} + 2x^{12} + x^{10}$ $+x^8 + x^6 + x^4 + x^2 + 1$

Let's look at the table again:

n	$W_n(x)$
0	1
1	$x^2 + 1$
2	$2x^4 + x^2 + 1$
3	$4x^6 + x^4 + x^2 + 1$
4	$8x^8 + x^4 + x^2 + 1$
5	$16x^{10} - 4x^8 + x^6 + x^4 + x^2 + 1$
6	$32x^{12} - 16x^{10} + 2x^8 + x^6 + x^4 + x^2 + 1$
7	$64x^{14} - 48x^{12} + 8x^{10} + x^8 + x^6 + x^4 + x^2 + 1$
8	$128x^{16} - 128x^{14} + 32x^{12} + x^8 + x^6 + x^4 + x^2 + 1$
9	$256x^{18} - 320x^{16} + 112x^{14} - 8x^{12} + x^{10} + x^8 + x^6$ $+x^4 + x^2 + 1$
10	$512x^{20} - 768x^{18} + 352x^{16} - 48x^{14} + 2x^{12} + x^{10}$ $+x^8 + x^6 + x^4 + x^2 + 1$

Do we get anything sensible if we cut the $W_n(x)$ into two halves?

Define the lower and upper parts, respectively, of $W_n(x)$ by

$$W_n^{\ell}(x) := \sum_{j=0}^{\lfloor\frac{n+1}{2}\rfloor} x^{2j},$$

$$W_n^{u}(x) := \frac{1}{x^{n+2}}\left(W_n(x) - W_n^{\ell}(x)\right).$$

Define the lower and upper parts, respectively, of $W_n(x)$ by

$$W_n^{\ell}(x) := \sum_{j=0}^{\lfloor \frac{n+1}{2} \rfloor} x^{2j},$$

$$W_n^{u}(x) := \frac{1}{x^{n+2}} \left(W_n(x) - W_n^{\ell}(x) \right).$$

Easy to establish generating functions for both, and with these we get

$$W_n^u(x) = 2 \sum_{k=0}^{\lfloor \frac{n-2}{2} \rfloor} U_{n-2-2k}(x)$$

where the $U_n(x)$ are the Chebyshev polynomials of the second kind, which can be defined by the generating function

$$\frac{1}{1 - 2tx + t^2} = \sum_{n=0}^{\infty} U_n(x) t^n.$$

Using known identities:

$$W_{2k}^{u}(x) = \frac{1 - T_{2k}(x)}{1 - x^2} = 2U_{k-1}(x)^2,$$
$$W_{2k+1}^{u}(x) = \frac{x - T_{2k+1}(x)}{1 - x^2} = 2U_{k-1}(x)U_k(x).$$

Using known identities:

$$W_{2k}^{u}(x) = \frac{1 - T_{2k}(x)}{1 - x^2} = 2U_{k-1}(x)^2,$$
$$W_{2k+1}^{u}(x) = \frac{x - T_{2k+1}(x)}{1 - x^2} = 2U_{k-1}(x)U_k(x).$$

This, together with the definition of the $W_n^{\ell}(z)$, gives

Proposition

For all $n \geq 1$, the zeros

(a) *of $W_n^{\ell}(z)$ lie on the unit circle;*

(b) *of $W_n^{u}(z)$ lie in the open interval $(-1, 1)$.*

Using known identities:

$$W_{2k}^u(x) = \frac{1 - T_{2k}(x)}{1 - x^2} = 2U_{k-1}(x)^2,$$
$$W_{2k+1}^u(x) = \frac{x - T_{2k+1}(x)}{1 - x^2} = 2U_{k-1}(x)U_k(x).$$

This, together with the definition of the $W_n^\ell(z)$, gives

Proposition

For all $n \geq 1$, the zeros

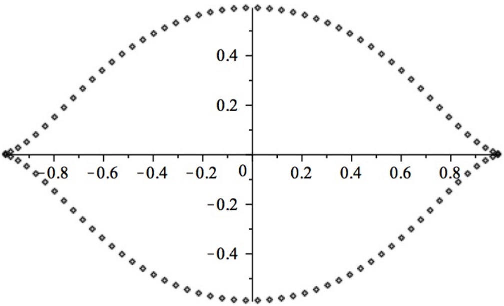
(a) *of $W_n^\ell(z)$ lie on the unit circle;*

(b) *of $W_n^u(z)$ lie in the open interval $(-1, 1)$.*

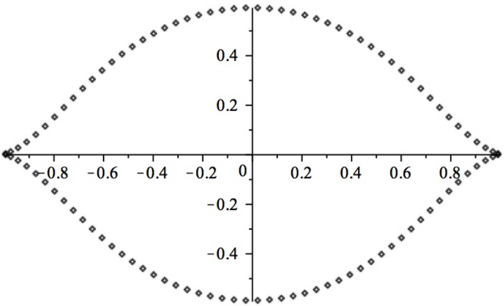
What can we say about the zeros of $W_n(z)$ as a whole?

Plot of the zeros of $W_{50}(z)$ (degree 100):

Plot of the zeros of $W_{50}(z)$ (degree 100):



Plot of the zeros of $W_{50}(z)$ (degree 100):



Do they lie on (or near) an identifiable curve?

Proposition

The zeros of $W_n(z)$, as $n \to \infty$, lie arbitrarily close to the curve

$$3r^8 - 8r^6\cos(2\theta) + 6r^4 - 1 = 0, \qquad z = re^{i\theta},\ 0 \le \theta \le 2\pi. \quad (4)$$

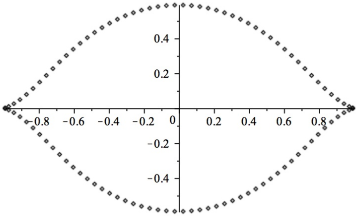
Furthermore, they all lie outside the closed region defined by this curve.

Proposition

The zeros of $W_n(z)$, as $n \to \infty$, lie arbitrarily close to the curve

$$3r^8 - 8r^6\cos(2\theta) + 6r^4 - 1 = 0, \qquad z = re^{i\theta},\ 0 \le \theta \le 2\pi. \quad (4)$$

Furthermore, they all lie outside the closed region defined by this curve.



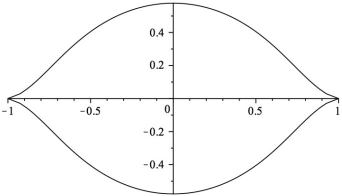
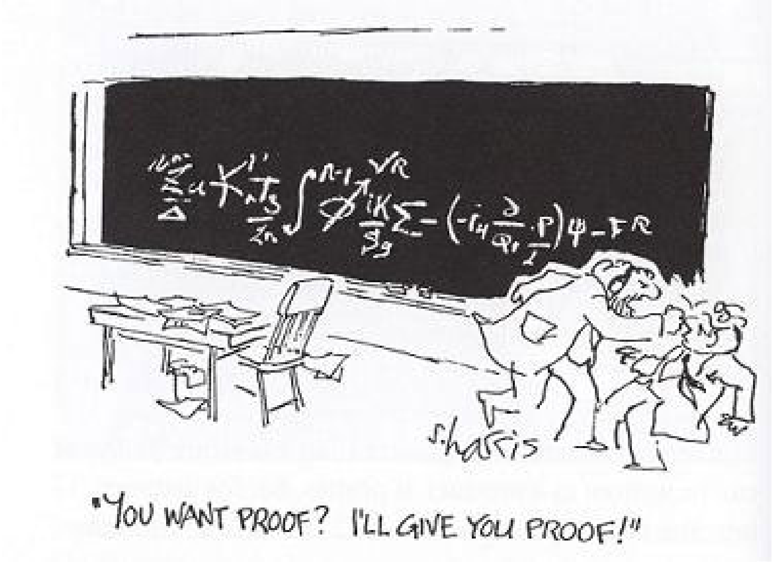


Figure: The zeros of $W_{50}(z)$ and the curve (4).

Proof:

Proof:



Ingredients in the proof:

Ingredients in the proof:

- The identity

$$W_n(x) = \frac{1 - x^{n+2}T_n(x)}{1 - x^2}.$$

Ingredients in the proof:

- The identity

$$W_n(x) = \frac{1 - x^{n+2}T_n(x)}{1 - x^2}.$$

- The Binet-type expression

$$T_n(x) = \frac{1}{2}\left((x - \sqrt{x^2 - 1})^n + (x + \sqrt{x^2 - 1})^n\right).$$

Ingredients in the proof:

- The identity
$$W_n(x) = \frac{1 - x^{n+2}T_n(x)}{1 - x^2}.$$
- The Binet-type expression
$$T_n(x) = \frac{1}{2}\left((x - \sqrt{x^2-1})^n + (x + \sqrt{x^2-1})^n\right).$$
- Concentrate on the larger of the two summands.

Ingredients in the proof:

- The identity

$$W_n(x) = \frac{1 - x^{n+2} T_n(x)}{1 - x^2}.$$

- The Binet-type expression

$$T_n(x) = \frac{1}{2}\left((x - \sqrt{x^2 - 1})^n + (x + \sqrt{x^2 - 1})^n\right).$$

- Concentrate on the larger of the two summands.
- A chain of tricky estimates.

An older result of a similar flavour:

Let $Lp(x)$, $Up(x)$ be the lower and upper sections of an even-degree polynomial $p(x)$.

An older result of a similar flavour:

Let $Lp(x)$, $Up(x)$ be the lower and upper sections of an even-degree polynomial $p(x)$.

Proposition (D. & Stolarsky, 1992)

There is a sequence of polynomials $\{Q_n(x)\}$ such that

(a) *the zeros of $Q_n(x)$ lie on the oval $|x(x-1)| = 1/2$;*

An older result of a similar flavour:

Let $Lp(x)$, $Up(x)$ be the lower and upper sections of an even-degree polynomial $p(x)$.

Proposition (D. & Stolarsky, 1992)

There is a sequence of polynomials $\{Q_n(x)\}$ *such that*

(a) *the zeros of* $Q_n(x)$ *lie on the oval* $|x(x-1)| = 1/2$*;*

(b) *the zeros of* $LQ_n(x)$ *lie on the circle of radius* $1/\sqrt{2}$ *centered at the origin;*

An older result of a similar flavour:

Let $Lp(x)$, $Up(x)$ be the lower and upper sections of an even-degree polynomial $p(x)$.

Proposition (D. & Stolarsky, 1992)

There is a sequence of polynomials $\{Q_n(x)\}$ such that

(a) *the zeros of $Q_n(x)$ lie on the oval $|x(x-1)| = 1/2$;*

(b) *the zeros of $LQ_n(x)$ lie on the circle of radius $1/\sqrt{2}$ centered at the origin;*

(c) *the zeros of $UQ_n(x)$ lie on the circle of radius $1/\sqrt{2}$ centered at $x = 1$.*

Remarks: (i) The centers of the circles in (b), (c) are the foci of the oval (an oval of Cassini) in (a).

An older result of a similar flavour:

Let $Lp(x)$, $Up(x)$ be the lower and upper sections of an even-degree polynomial $p(x)$.

Proposition (D. & Stolarsky, 1992)

There is a sequence of polynomials $\{Q_n(x)\}$ *such that*

(a) *the zeros of* $Q_n(x)$ *lie on the oval* $|x(x-1)| = 1/2$;

(b) *the zeros of* $LQ_n(x)$ *lie on the circle of radius* $1/\sqrt{2}$ *centered at the origin;*

(c) *the zeros of* $UQ_n(x)$ *lie on the circle of radius* $1/\sqrt{2}$ *centered at* $x = 1$.

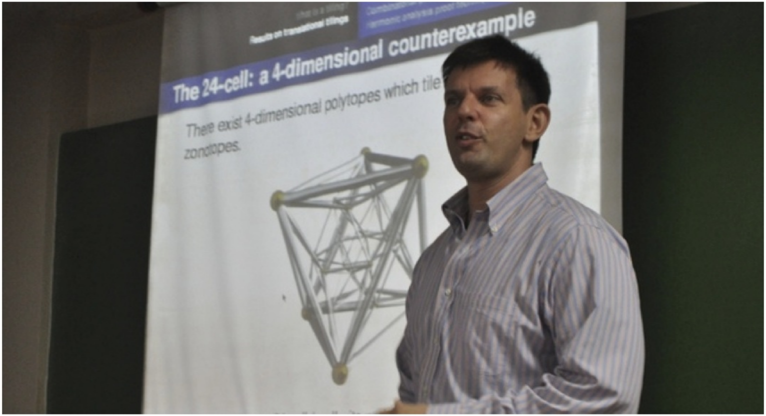
Remarks: (i) The centers of the circles in (b), (c) are the foci of the oval (an oval of Cassini) in (a).

(ii) The polynomials can be given explicitly and are also related to Chebyshev polynomials.

Part II:

Zeros and irreducibility of gcd-polynomials

Joint work with



Sinai Robins

University of São Paulo, Brazil

1. Introduction

Some classes of polynomials with special number theoretic sequences as coefficients:

1. Introduction

Some classes of polynomials with special number theoretic sequences as coefficients:

1. Fekete polynomials:

$$f_p(z) := \sum_{j=0}^{p-1} \left(\frac{j}{p}\right) z^j \qquad (p \text{ prime}),$$

where $(\frac{a}{p})$ is the Legendre symbol.

1. Introduction

Some classes of polynomials with special number theoretic sequences as coefficients:

1. Fekete polynomials:

$$f_p(z) := \sum_{j=0}^{p-1} \left(\frac{j}{p}\right) z^j \qquad (p \text{ prime}),$$

where $(\frac{a}{p})$ is the Legendre symbol.

Conrey, Granville, Poonen, and Soundararajan (2000) showed:

For each p, at least half of the zeros of $f_p(z)$ lie on the unit circle.

1. Introduction

Some classes of polynomials with special number theoretic sequences as coefficients:

1. Fekete polynomials:

$$f_p(z) := \sum_{j=0}^{p-1} \left(\frac{j}{p}\right) z^j \qquad (p \text{ prime}),$$

where $(\frac{a}{p})$ is the Legendre symbol.

Conrey, Granville, Poonen, and Soundararajan (2000) showed:

For each p, at least half of the zeros of $f_p(z)$ lie on the unit circle.

Deep connections with the distribution of primes.

2. Ramanujan polynomials:

$$R_{2k+1}(z) := \sum_{j=0}^{k+1} \left(\frac{B_{2j} B_{2k+2-2j}}{(2j)!(2k+2-2j)!} \right) z^{2j},$$

where B_n is the nth Bernoulli number.

2. Ramanujan polynomials:

$$R_{2k+1}(z) := \sum_{j=0}^{k+1} \left(\frac{B_{2j} B_{2k+2-2j}}{(2j)!(2k+2-2j)!} \right) z^{2j},$$

where B_n is the nth Bernoulli number.

Murty, Smyth, and Wang (2011) showed:

With the exception of four real zeros, all others zeros lie on the unit circle and have uniform angular distribution.

2. Ramanujan polynomials:

$$R_{2k+1}(z) := \sum_{j=0}^{k+1} \left(\frac{B_{2j} B_{2k+2-2j}}{(2j)!(2k+2-2j)!} \right) z^{2j},$$

where B_n is the nth Bernoulli number.

Murty, Smyth, and Wang (2011) showed:

With the exception of four real zeros, all others zeros lie on the unit circle and have uniform angular distribution.

Applications to the theory of the Riemann zeta function.

2. Ramanujan polynomials:

$$R_{2k+1}(z) := \sum_{j=0}^{k+1} \left(\frac{B_{2j} B_{2k+2-2j}}{(2j)!(2k+2-2j)!} \right) z^{2j},$$

where B_n is the nth Bernoulli number.

Murty, Smyth, and Wang (2011) showed:

With the exception of four real zeros, all others zeros lie on the unit circle and have uniform angular distribution.

Applications to the theory of the Riemann zeta function.

Later extended by other authors to similar polynomials (Lalín & Smyth, 2013; Berndt & Straub, 2017).

3. Dedekind polynomials:

$$p_k(z) := \sum_{j=0}^{k-1} s(j,k) z^j,$$

where $s(d,c)$ is the *Dedekind sum*

3. Dedekind polynomials:

$$p_k(z) := \sum_{j=0}^{k-1} s(j,k) z^j,$$

where $s(d,c)$ is the *Dedekind sum* defined by

$$s(d,c) = \sum_{j=1}^{c} \left(\left(\frac{j}{c}\right)\right) \left(\left(\frac{dj}{c}\right)\right),$$

with $((x))$ denoting the “sawtooth function"

$$((x)) = \begin{cases} 0, & \text{if } x \in \mathbb{Z}, \\ x - [x] - \frac{1}{2}, & \text{otherwise.} \end{cases}$$

3. Dedekind polynomials:

$$p_k(z) := \sum_{j=0}^{k-1} s(j,k) z^j,$$

where $s(d,c)$ is the *Dedekind sum* defined by

$$s(d,c) = \sum_{j=1}^{c} \left(\left(\frac{j}{c}\right)\right)\left(\left(\frac{dj}{c}\right)\right),$$

with $((x))$ denoting the “sawtooth function"

$$((x)) = \begin{cases} 0, & \text{if } x \in \mathbb{Z}, \\ x - [x] - \frac{1}{2}, & \text{otherwise.} \end{cases}$$

Observation:
For each k, most of the zeros of $p_k(z)$ lies on the unit circle.

3. Dedekind polynomials:

$$p_k(z) := \sum_{j=0}^{k-1} s(j,k) z^j,$$

where $s(d,c)$ is the *Dedekind sum* defined by

$$s(d,c) = \sum_{j=1}^{c} \left(\left(\frac{j}{c}\right)\right)\left(\left(\frac{dj}{c}\right)\right),$$

with $((x))$ denoting the “sawtooth function"

$$((x)) = \begin{cases} 0, & \text{if } x \in \mathbb{Z}, \\ x - [x] - \frac{1}{2}, & \text{otherwise.} \end{cases}$$

Observation:
For each k, most of the zeros of $p_k(z)$ lies on the unit circle.

In an effort to prove this, we were led to studying the following class of polynomials.

2. GCD Polynomials

What can we say about the polynomials

$$\sum_{j=0}^{n} \gcd(n,j) z^j ?$$

2. GCD Polynomials

What can we say about the polynomials

$$\sum_{j=0}^{n} \gcd(n,j) z^j?$$

It turns out: A more general class has basically the same properties.

2. GCD Polynomials

What can we say about the polynomials

$$\sum_{j=0}^{n} \gcd(n,j) z^j ?$$

It turns out: A more general class has basically the same properties. For $k \geq 0$ and $n \geq 1$, let

$$g_n^{(k)}(z) := \sum_{j=0}^{n} \gcd(n,j)^k z^j .$$

2. GCD Polynomials

What can we say about the polynomials

$$\sum_{j=0}^{n} \gcd(n,j) z^j ?$$

It turns out: A more general class has basically the same properties. For $k \geq 0$ and $n \geq 1$, let

$$g_n^{(k)}(z) := \sum_{j=0}^{n} \gcd(n,j)^k z^j.$$

For $k = 0$, obviously

$$g_n^{(0)}(z) = \frac{z^{n+1} - 1}{z - 1},$$

so all the zeros are roots of unity and thus lie on the unit circle.

2. GCD Polynomials

What can we say about the polynomials

$$\sum_{j=0}^{n} \gcd(n,j) z^j?$$

It turns out: A more general class has basically the same properties. For $k \geq 0$ and $n \geq 1$, let

$$g_n^{(k)}(z) := \sum_{j=0}^{n} \gcd(n,j)^k z^j.$$

For $k = 0$, obviously

$$g_n^{(0)}(z) = \frac{z^{n+1} - 1}{z - 1},$$

so all the zeros are roots of unity and thus lie on the unit circle.

For $n = p - 1$ (p a prime), these are cyclotomic polynomials; hence irreducible.

From now on: Disregard the case $k = 0$.

From now on: Disregard the case $k = 0$.

However, we will see:
$g_n^{(k)}(z)$ for $k \geq 1$ have properties similar to the case $k = 0$.

From now on: Disregard the case $k = 0$.

However, we will see:
$g_n^{(k)}(z)$ for $k \geq 1$ have properties similar to the case $k = 0$.

Theorem

For all $k \geq 1$ and all $n \geq 1$, all the zeros of $g_n^{(k)}(z)$ lie on the unit circle and have uniform angular distribution.

From now on: Disregard the case $k = 0$.

However, we will see:
$g_n^{(k)}(z)$ for $k \geq 1$ have properties similar to the case $k = 0$.

Theorem

For all $k \geq 1$ and all $n \geq 1$, all the zeros of $g_n^{(k)}(z)$ lie on the unit circle and have uniform angular distribution.

Idea of proof: Consider

$$g_n^{(k)}(e^{2\pi i x})$$

and show it has n *real* zeros for $0 < x < 1$.

3. Zeros; proof of the Theorem

Since $\gcd(j,n)=\gcd(n-j,n)$ for $0\le j\le n$, the $g_n^{(k)}(z)$ are *self-inversive* (or *reciprocal*):

$$g_n^{(k)}(z)=z^n g_n^{(k)}(\tfrac{1}{z}).$$

3. Zeros; proof of the Theorem

Since $\gcd(j,n)=\gcd(n-j,n)$ for $0\le j\le n$, the $g_n^{(k)}(z)$ are *self-inversive* (or *reciprocal*):

$$g_n^{(k)}(z)=z^n g_n^{(k)}(\tfrac{1}{z}).$$

Set $z=e^{2\pi ix}$ for a real variable x. Then

$$e^{-\pi inx}g_n^{(k)}(e^{2\pi ix})=e^{\pi inx}g_n^{(k)}(e^{-2\pi ix}).$$

3. Zeros; proof of the Theorem

Since $\gcd(j,n) = \gcd(n-j,n)$ for $0 \le j \le n$, the $g_n^{(k)}(z)$ are *self-inversive* (or *reciprocal*):

$$g_n^{(k)}(z) = z^n g_n^{(k)}(\tfrac{1}{z}).$$

Set $z = e^{2\pi ix}$ for a real variable x. Then

$$e^{-\pi inx} g_n^{(k)}(e^{2\pi ix}) = e^{\pi inx} g_n^{(k)}(e^{-2\pi ix}).$$

If we define

$$h_n^{(k)}(x) := e^{-\pi inx} g_n^{(k)}(e^{2\pi ix}),$$

then $\overline{h_n^{(k)}(x)} = h_n^{(k)}(x)$ for $x \in \mathbb{R}$.

3. Zeros; proof of the Theorem

Since $\gcd(j,n) = \gcd(n-j,n)$ for $0 \le j \le n$, the $g_n^{(k)}(z)$ are *self-inversive* (or *reciprocal*):

$$g_n^{(k)}(z) = z^n g_n^{(k)}(\tfrac{1}{z}).$$

Set $z = e^{2\pi ix}$ for a real variable x. Then

$$e^{-\pi inx} g_n^{(k)}(e^{2\pi ix}) = e^{\pi inx} g_n^{(k)}(e^{-2\pi ix}).$$

If we define

$$h_n^{(k)}(x) := e^{-\pi inx} g_n^{(k)}(e^{2\pi ix}),$$

then $\overline{h_n^{(k)}(x)} = h_n^{(k)}(x)$ for $x \in \mathbb{R}$.

Hence $h_n^{(k)}(x)$ is real-valued.

$$h_n^{(k)}(x) := e^{-\pi i n x} g_n^{(k)}(e^{2\pi i x}).$$

$$h_n^{(k)}(x) := e^{-\pi i n x} g_n^{(k)}(e^{2\pi i x}).$$

For $m = 0, 1, \ldots, n$, consider

$$h_n^{(k)}(\tfrac{m}{n}) = e^{-\pi i m} g_n^{(k)}(e^{2\pi i m/n}) = (-1)^m \sum_{j=0}^{n} \gcd(j, n)^k e^{2\pi i j m/n}.$$

$$h_n^{(k)}(x) := e^{-\pi i n x} g_n^{(k)}(e^{2\pi i x}).$$

For $m = 0, 1, \ldots, n$, consider

$$h_n^{(k)}(\tfrac{m}{n}) = e^{-\pi i m} g_n^{(k)}(e^{2\pi i m/n}) = (-1)^m \sum_{j=0}^{n} \gcd(j,n)^k e^{2\pi i j m/n}.$$

Last sum is, essentially, discrete Fourier transform of $gcd(j,n)^k$.

$$h_n^{(k)}(x) := e^{-\pi i n x} g_n^{(k)}(e^{2\pi i x}).$$

For $m = 0, 1, \ldots, n$, consider

$$h_n^{(k)}(\tfrac{m}{n}) = e^{-\pi i m} g_n^{(k)}(e^{2\pi i m/n}) = (-1)^m \sum_{j=0}^{n} \mathrm{gcd}(j, n)^k e^{2\pi i j m/n}.$$

Last sum is, essentially, discrete Fourier transform of $gcd(j, n)^k$. Denote it here by

$$S^{(k)}(m, n) := \sum_{j=1}^{n} \mathrm{gcd}(j, n)^k e^{2\pi i j m/n}.$$

$$h_n^{(k)}(x) := e^{-\pi inx} g_n^{(k)}(e^{2\pi ix}).$$

For $m = 0, 1, \ldots, n$, consider

$$h_n^{(k)}(\tfrac{m}{n}) = e^{-\pi im} g_n^{(k)}(e^{2\pi im/n}) = (-1)^m \sum_{j=0}^{n} \gcd(j,n)^k e^{2\pi ijm/n}.$$

Last sum is, essentially, discrete Fourier transform of $gcd(j,n)^k$. Denote it here by

$$S^{(k)}(m,n) := \sum_{j=1}^{n} \gcd(j,n)^k e^{2\pi ijm/n}.$$

So we have

$$h_n^{(k)}(\tfrac{m}{n}) = (-1)^m \left(S^{(k)}(m,n) + n^k \right).$$

$$h_n^{(k)}\left(\tfrac{m}{n}\right) = (-1)^m \left(S^{(k)}(m,n) + n^k \right).$$

$$h_n^{(k)}(\tfrac{m}{n}) = (-1)^m \left(S^{(k)}(m,n) + n^k\right).$$

Thus, if we can show

$$S^{(k)}(m,n) > 0, \tag{5}$$

then for fixed k and n, $h_n^{(k)}(\frac{m}{n})$ is alternating positive and negative.

$$h_n^{(k)}(\tfrac{m}{n}) = (-1)^m \left(S^{(k)}(m,n) + n^k\right).$$

Thus, if we can show

$$S^{(k)}(m,n) > 0, \tag{5}$$

then for fixed k and n, $h_n^{(k)}(\frac{m}{n})$ is alternating positive and negative.

This means that $h_n^{(k)}(x)$ has n real zeros between the $n+1$ points $0, 1/n, 2/n, \ldots, 1$.

$$h_n^{(k)}(\tfrac{m}{n}) = (-1)^m \left(S^{(k)}(m,n) + n^k \right).$$

Thus, if we can show

$$S^{(k)}(m,n) > 0, \tag{5}$$

then for fixed k and n, $h_n^{(k)}(\frac{m}{n})$ is alternating positive and negative.

This means that $h_n^{(k)}(x)$ has n real zeros between the $n+1$ points $0, 1/n, 2/n, \ldots, 1$.

This in turn implies that $g_n^{(k)}(z)$

- has all its n zeros on the unit circle, and

$$h_n^{(k)}(\tfrac{m}{n}) = (-1)^m \left(S^{(k)}(m,n) + n^k\right).$$

Thus, if we can show

$$S^{(k)}(m,n) > 0, \tag{5}$$

then for fixed k and n, $h_n^{(k)}(\frac{m}{n})$ is alternating positive and negative.

This means that $h_n^{(k)}(x)$ has n real zeros between the $n+1$ points $0, 1/n, 2/n, \ldots, 1$.

This in turn implies that $g_n^{(k)}(z)$

- has all its n zeros on the unit circle, and
- one each in adjacent sectors of angle $2\pi/n$.

$$h_n^{(k)}(\tfrac{m}{n}) = (-1)^m \left(S^{(k)}(m,n) + n^k\right).$$

Thus, if we can show

$$S^{(k)}(m,n) > 0, \tag{5}$$

then for fixed k and n, $h_n^{(k)}(\frac{m}{n})$ is alternating positive and negative.

This means that $h_n^{(k)}(x)$ has n real zeros between the $n+1$ points $0, 1/n, 2/n, \ldots, 1$.

This in turn implies that $g_n^{(k)}(z)$

- has all its n zeros on the unit circle, and
- one each in adjacent sectors of angle $2\pi/n$.

This proves Theorem 1, provided we can prove (5).

$$h_n^{(k)}(\tfrac{m}{n}) = (-1)^m \left(S^{(k)}(m,n) + n^k\right).$$

Thus, if we can show

$$S^{(k)}(m,n) > 0, \tag{5}$$

then for fixed k and n, $h_n^{(k)}(\frac{m}{n})$ is alternating positive and negative.

This means that $h_n^{(k)}(x)$ has n real zeros between the $n+1$ points $0, 1/n, 2/n, \dots, 1$.

This in turn implies that $g_n^{(k)}(z)$

- has all its n zeros on the unit circle, and
- one each in adjacent sectors of angle $2\pi/n$.

This proves Theorem 1, provided we can prove (5).

$$h_n^{(k)}(\tfrac{m}{n}) = (-1)^m \left(S^{(k)}(m,n) + n^k\right).$$

$$h_n^{(k)}(\tfrac{m}{n}) = (-1)^m \left(S^{(k)}(m,n) + n^k \right).$$

DFTs have recently been studied for

- arithmetic, especially multiplicative, functions in general;

$$h_n^{(k)}(\tfrac{m}{n}) = (-1)^m \left(S^{(k)}(m,n) + n^k\right).$$

DFTs have recently been studied for

- arithmetic, especially multiplicative, functions in general;
- the gcd and its powers as special cases.

$$h_n^{(k)}(\tfrac{m}{n}) = (-1)^m \left(S^{(k)}(m,n) + n^k \right).$$

DFTs have recently been studied for

- arithmetic, especially multiplicative, functions in general;
- the gcd and its powers as special cases.

For instance:

Theorem (L. Tóth, 2011)

For all $m \in \mathbb{Z}$ and $n \in \mathbb{N}$,

$$S^{(1)}(m,n) = \sum_{d \mid \gcd(m,n)} d\varphi(\tfrac{n}{d}).$$

$$h_n^{(k)}(\tfrac{m}{n}) = (-1)^m \left(S^{(k)}(m,n) + n^k \right).$$

DFTs have recently been studied for

- arithmetic, especially multiplicative, functions in general;
- the gcd and its powers as special cases.

For instance:

Theorem (L. Tóth, 2011)

For all $m \in \mathbb{Z}$ and $n \in \mathbb{N}$,

$$S^{(1)}(m,n) = \sum_{d \mid \gcd(m,n)} d\varphi(\tfrac{n}{d}).$$

This proves our theorem for $k = 1$.

$$h_n^{(k)}(\tfrac{m}{n}) = (-1)^m \left(S^{(k)}(m,n) + n^k\right).$$

DFTs have recently been studied for

- arithmetic, especially multiplicative, functions in general;
- the gcd and its powers as special cases.

For instance:

Theorem (L. Tóth, 2011)

For all $m \in \mathbb{Z}$ and $n \in \mathbb{N}$,

$$S^{(1)}(m,n) = \sum_{d \mid \gcd(m,n)} d\varphi(\tfrac{n}{d}).$$

This proves our theorem for $k = 1$.

Can this be extended to general $k \geq 1$?

4. Jordan's totient function

We need a generalization of Euler's φ-function.

Definition

Jordan's totient function is defined by

$$J_k(n) = n^k \prod_{p|n} \left(1 - \frac{1}{p^k}\right),$$

4. Jordan's totient function

We need a generalization of Euler's φ-function.

Definition

Jordan's totient function is defined by

$$J_k(n) = n^k \prod_{p|n} \left(1 - \frac{1}{p^k}\right),$$

or equivalently as the number of different sets of k (equal or distinct) positive integers $\leq n$ whose gcd is relatively prime to n.

4. Jordan's totient function

We need a generalization of Euler's φ-function.

Definition

Jordan's totient function is defined by

$$J_k(n) = n^k \prod_{p|n} \left(1 - \frac{1}{p^k}\right),$$

or equivalently as the number of different sets of k (equal or distinct) positive integers $\leq n$ whose gcd is relatively prime to n.

This equivalence was first established by Camille Jordan in 1870.

4. Jordan's totient function

We need a generalization of Euler's φ-function.

Definition

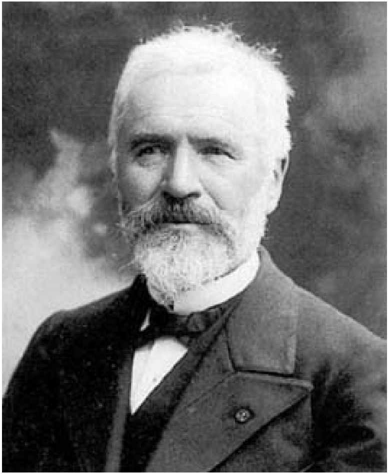
Jordan's totient function is defined by

$$J_k(n) = n^k \prod_{p|n} \left(1 - \frac{1}{p^k}\right),$$

or equivalently as the number of different sets of k (equal or distinct) positive integers $\leq n$ whose gcd is relatively prime to n.

This equivalence was first established by Camille Jordan in 1870.

Clearly, $J_1(n) = \varphi(n)$.



Camille Jordan
(1838–1922)

Other properties are similar to those of Euler's φ-function; e.g.,

$$m^k = \sum_{d|m} J_k(d).$$

Other properties are similar to those of Euler's φ-function; e.g.,

$$m^k = \sum_{d|m} J_k(d).$$

W. Schramm (2008) showed;

$$S^{(k)}(1, n) = J_k(n) \qquad (n \geq 1).$$

Other properties are similar to those of Euler's φ-function; e.g.,

$$m^k = \sum_{d|m} J_k(d).$$

W. Schramm (2008) showed;

$$S^{(k)}(1,n) = J_k(n) \qquad (n \geq 1).$$

This can be extended:

Proposition

For all $k, n \in \mathbb{N}$ *and all* $m \in \mathbb{Z}$ *we have*

$$S^{(k)}(m,n) = \sum_{d \mid \gcd(m,n)} d J_k\left(\tfrac{n}{d}\right).$$

In particular, $S^{(k)}(m,n)$ *is always a positive integer.*

Proposition

For all $k, n \in \mathbb{N}$ and all $m \in \mathbb{Z}$ we have

$$S^{(k)}(m,n) = \sum_{d \mid \gcd(m,n)} d J_k\left(\tfrac{n}{d}\right).$$

In particular, $S^{(k)}(m,n)$ is always a positive integer.

Since the summands on the right are positive, this proves the Theorem.

Proposition

For all $k, n \in \mathbb{N}$ and all $m \in \mathbb{Z}$ we have

$$S^{(k)}(m,n) = \sum_{d \mid \gcd(m,n)} dJ_k(\tfrac{n}{d}).$$

In particular, $S^{(k)}(m,n)$ is always a positive integer.

Since the summands on the right are positive, this proves the Theorem.

Compare with Tóth's result:

$$S^{(1)}(m,n) = \sum_{d \mid \gcd(m,n)} d\varphi(\tfrac{n}{d}).$$

Proof of Proposition. Using

$$\gcd(j,n)^k = \sum_{d \mid \gcd(j,n)} J_k(d),$$

we have

$$\begin{aligned}
S^{(k)}(m,n) &= \sum_{j=1}^{n} \sum_{\ell \mid \gcd(n,j)} J_k(\ell) e^{2\pi ijm/n} \\
&= \sum_{\ell \mid n} J_k(\ell) \sum_{j=1}^{n/\ell} e^{2\pi ijm/(n/\ell)}.
\end{aligned}$$

Proof of Proposition. Using

$$\gcd(j,n)^k = \sum_{d \mid \gcd(j,n)} J_k(d),$$

we have

$$\begin{aligned} S^{(k)}(m,n) &= \sum_{j=1}^{n} \sum_{\ell \mid \gcd(n,j)} J_k(\ell) e^{2\pi i j m/n} \\ &= \sum_{\ell \mid n} J_k(\ell) \sum_{j=1}^{n/\ell} e^{2\pi i j m/(n/\ell)}. \end{aligned}$$

Inner sum in the last term is

- n/ℓ if n/ℓ divides m;
- 0 otherwise.

Proof of Proposition. Using

$$\gcd(j,n)^k = \sum_{d\mid \gcd(j,n)} J_k(d),$$

we have

$$\begin{aligned} S^{(k)}(m,n) &= \sum_{j=1}^{n} \sum_{\ell\mid \gcd(n,j)} J_k(\ell) e^{2\pi i jm/n} \\ &= \sum_{\ell\mid n} J_k(\ell) \sum_{j=1}^{n/\ell} e^{2\pi i jm/(n/\ell)}. \end{aligned}$$

Inner sum in the last term is

- n/ℓ if n/ℓ divides m;
- 0 otherwise.

Hence, setting $d = n/\ell$, we get the desired identity.

An interesting consequence: Recall

$$S^{(k)}(m,n) := \sum_{j=1}^{n} \gcd(j,n)^k e^{2\pi ijm/n}$$

An interesting consequence: Recall

$$S^{(k)}(m,n) := \sum_{j=1}^{n} \gcd(j,n)^k e^{2\pi ijm/n}$$

and

$$S^{(k)}(m,n) = \sum_{d\,|\,\gcd(m,n)} dJ_k(\tfrac{n}{d}).$$

An interesting consequence: Recall

$$S^{(k)}(m,n) := \sum_{j=1}^{n} \gcd(j,n)^k e^{2\pi i j m/n}$$

and

$$S^{(k)}(m,n) = \sum_{d \mid \gcd(m,n)} d J_k(\tfrac{n}{d}).$$

Set $m = n$; then

Corollary

For all $k, n \in \mathbb{N}$ we have

$$\sum_{d \mid n} d J_k(\tfrac{n}{d}) = \sum_{j=1}^{n} \gcd(j,n)^k.$$

An interesting consequence: Recall

$$S^{(k)}(m,n) := \sum_{j=1}^{n} \gcd(j,n)^k e^{2\pi ijm/n}$$

and

$$S^{(k)}(m,n) = \sum_{d \mid \gcd(m,n)} dJ_k(\tfrac{n}{d}).$$

Set $m = n$; then

Corollary

For all $k, n \in \mathbb{N}$ we have

$$\sum_{d \mid n} dJ_k(\tfrac{n}{d}) = \sum_{j=1}^{n} \gcd(j,n)^k.$$

This was published by K. Alladi (1975) when he was 19 years old, and with a different goal in mind.

5. Irreducibility

Recall:

$$g_n^{(k)}(z) := \sum_{j=0}^{n} \gcd(n,j)^k z^j.$$

5. Irreducibility

Recall:

$$g_n^{(k)}(z) := \sum_{j=0}^{n} \gcd(n,j)^k z^j.$$

Observation: When n is odd then by symmetry,

$$g_n^{(k)}(-1) = 0,$$

so $z+1$ is always a factor of $g_n^{(k)}(z)$ in that case.

5. Irreducibility

Recall:

$$g_n^{(k)}(z) := \sum_{j=0}^{n} \gcd(n,j)^k z^j.$$

Observation: When n is odd then by symmetry,

$$g_n^{(k)}(-1) = 0,$$

so $z+1$ is always a factor of $g_n^{(k)}(z)$ in that case.

However, it appears that this is the *only* factor. In fact:

5. Irreducibility

Recall:

$$g_n^{(k)}(z) := \sum_{j=0}^{n} \gcd(n,j)^k z^j.$$

Observation: When n is odd then by symmetry,

$$g_n^{(k)}(-1) = 0,$$

so $z+1$ is always a factor of $g_n^{(k)}(z)$ in that case.

However, it appears that this is the *only* factor. In fact:

Theorem

For $\alpha, k \in \mathbb{N}$ and odd primes p,

$$g_{2^\alpha}^{(k)}(z) \quad \textit{and} \quad \frac{g_{p^\alpha}^{(k)}(z)}{z+1}$$

are irreducible over $\mathbb{Q}$.

Proof. (Sketch).

Part 1: We begin with the smallest cases:

$$g_2^{(k)}(z) = 2^k + z + 2^k z^2, \qquad \frac{1}{z+1} g_3^{(k)}(z) = 3^k + (1-3^k)z + 3^k z^2.$$

Proof. (Sketch).

Part 1: We begin with the smallest cases:

$$g_2^{(k)}(z) = 2^k + z + 2^k z^2, \qquad \frac{1}{z+1} g_3^{(k)}(z) = 3^k + (1-3^k)z + 3^k z^2.$$

The only self-reciprocal reducible quadratics are $z^2 \pm 2z + 1$ and their integer multiples.

Proof. (Sketch).

Part 1: We begin with the smallest cases:

$$g_2^{(k)}(z) = 2^k + z + 2^k z^2, \qquad \frac{1}{z+1} g_3^{(k)}(z) = 3^k + (1 - 3^k) z + 3^k z^2.$$

The only self-reciprocal reducible quadratics are $z^2 \pm 2z + 1$ and their integer multiples.
But none of the polynomials above are of this form.
This proves the Theorem for $p = 2$, $p = 3$ and $\alpha = 1$.

Proof. (Sketch).

Part 1: We begin with the smallest cases:

$$g_2^{(k)}(z) = 2^k + z + 2^k z^2, \qquad \frac{1}{z+1} g_3^{(k)}(z) = 3^k + (1-3^k)z + 3^k z^2.$$

The only self-reciprocal reducible quadratics are $z^2 \pm 2z + 1$ and their integer multiples.
But none of the polynomials above are of this form.
This proves the Theorem for $p = 2$, $p = 3$ and $\alpha = 1$.

For the remaining cases, let $p \geq 2$ be any prime, and $\alpha, k \in \mathbb{N}$. Set

$$\overline{g}_n^{(k)}(z) = \begin{cases} g_n^{(k)}(z) & \text{when } n \text{ is even,} \\ \frac{1}{z+1} g_n^{(k)}(z) & \text{when } n \text{ is odd.} \end{cases}$$

Part 2: Assume that $\overline{g}_n^{(k)}(z)$ is reducible for $n \geq 4$.

Part 2: Assume that $\overline{g}_n^{(k)}(z)$ is reducible for $n \geq 4$.

Then it's a product of $r \geq 2$ irreducible polynomials with integer coefficients.

Part 2: Assume that $\overline{g}_n^{(k)}(z)$ is reducible for $n \geq 4$.

Then it's a product of $r \geq 2$ irreducible polynomials with integer coefficients.

These are themselves self-inversive and thus have even degrees since all their zeros are conjugate pairs of complex numbers with modulus 1.

Part 2: Assume that $\overline{g}_n^{(k)}(z)$ is reducible for $n \geq 4$.

Then it's a product of $r \geq 2$ irreducible polynomials with integer coefficients.

These are themselves self-inversive and thus have even degrees since all their zeros are conjugate pairs of complex numbers with modulus 1.

So we can write, for any $n \geq 4$,

$$\begin{aligned}\overline{g}_n^{(k)}(z) &= (a_1 + b_1 z + \dots)(a_2 + b_2 z + \dots)\dots(a_r + b_r z + \dots)\\ &= a_1 a_2 \dots a_r + a_1 a_2 \dots a_r \left(\sum_{j=1}^{r} \frac{b_j}{a_j}\right) z + \dots\end{aligned}$$

On the other hand, it is clear from the definition that

$$\overline{g}_{p^\alpha}^{(k)}(z) = \begin{cases} p^{\alpha k} + (1 - p^{\alpha k})z + \dots & \text{when } p \geq 3, \\ p^{\alpha k} + z + \dots & \text{when } p = 2. \end{cases}$$

On the other hand, it is clear from the definition that

$$\overline{g}_{p^\alpha}^{(k)}(z) = \begin{cases} p^{\alpha k} + (1 - p^{\alpha k})z + \dots & \text{when } p \geq 3, \\ p^{\alpha k} + z + \dots & \text{when } p = 2. \end{cases}$$

Equating coefficients, we therefore have

$$a_1 a_2 \dots a_r = p^{\alpha k}, \tag{6}$$

$$\begin{aligned} b_1 a_2 \dots a_r + a_1 b_2 \dots a_r + \dots \\ + a_1 a_2 \dots b_r = 1 - [p \geq 3] p^{\alpha k}, \end{aligned} \tag{7}$$

On the other hand, it is clear from the definition that

$$\overline{g}_{p^\alpha}^{(k)}(z) = \begin{cases} p^{\alpha k} + (1 - p^{\alpha k})z + \dots & \text{when } p \geq 3, \\ p^{\alpha k} + z + \dots & \text{when } p = 2. \end{cases}$$

Equating coefficients, we therefore have

$$a_1 a_2 \dots a_r = p^{\alpha k}, \tag{6}$$

$$b_1 a_2 \dots a_r + a_1 b_2 \dots a_r + \dots + a_1 a_2 \dots b_r = 1 - [p \geq 3] p^{\alpha k}, \tag{7}$$

- By (6): the a_j can only be powers of p;

On the other hand, it is clear from the definition that

$$\overline{g}_{p^\alpha}^{(k)}(z) = \begin{cases} p^{\alpha k} + (1 - p^{\alpha k})z + \dots & \text{when } p \geq 3, \\ p^{\alpha k} + z + \dots & \text{when } p = 2. \end{cases}$$

Equating coefficients, we therefore have

$$a_1 a_2 \dots a_r = p^{\alpha k}, \tag{6}$$

$$\begin{aligned} b_1 a_2 \dots a_r + a_1 b_2 \dots a_r + \dots \\ + a_1 a_2 \dots b_r = 1 - [p \geq 3] p^{\alpha k}, \end{aligned} \tag{7}$$

- By (6): the a_j can only be powers of p;
- by (7): at least one of them has to be 1

(otherwise p would divide LHS of (7) — contradiction.)

This means: at least one of the r irreducible factors (which are self-inversive) is monic, with all its zeros on the unit circle.

This means: at least one of the r irreducible factors (which are self-inversive) is monic, with all its zeros on the unit circle.

We now use a classical theorem of Kronecker (1857):

This means: at least one of the r irreducible factors (which are self-inversive) is monic, with all its zeros on the unit circle.

We now use a classical theorem of Kronecker (1857):

Leopold Kronecker 1823 – 1891

These polynomials have to be cyclotomic, i.e., of the form

$$\Phi_n(z) = \prod_{\substack{j=1 \\ (j,n)=1}}^{n} \left(z - e^{2\pi ij/n}\right).$$

These polynomials have to be cyclotomic, i.e., of the form

$$\Phi_n(z) = \prod_{\substack{j=1 \\ (j,n)=1}}^{n} \left(z - e^{2\pi ij/n} \right).$$

Our proof is complete if we can show that this cannot happen.

These polynomials have to be cyclotomic, i.e., of the form

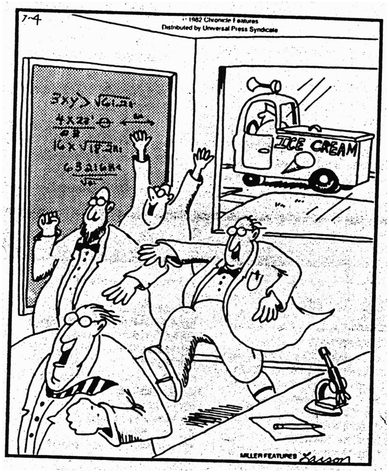
$$\Phi_n(z) = \prod_{\substack{j=1 \\ (j,n)=1}}^{n} \left(z - e^{2\pi ij/n}\right).$$

Our proof is complete if we can show that this cannot happen.

Proof requires a detailed analysis using resultants of polynomials.

We skip this.

Thank you



7-4
© 1982 Chronicle Features
Distributed by Universal Press Syndicate
ICE CREAM
MILLER FEATURES
Larson

Part 3: Given

$$f(z) = a_m z^m + \cdots + a_1 z + a_0,$$
$$g(z) = b_n z^n + \cdots + b_1 z + b_0,$$

Part 3: Given

$$f(z) = a_m z^m + \cdots + a_1 z + a_0,$$
$$g(z) = b_n z^n + \cdots + b_1 z + b_0,$$

the *resultant* of f and g is usually defined by the Sylvester determinant,

Part 3: Given

$$f(z) = a_m z^m + \cdots + a_1 z + a_0,$$
$$g(z) = b_n z^n + \cdots + b_1 z + b_0,$$

the *resultant* of f and g is usually defined by the Sylvester determinant,
i.e., the determinant of a certain $(m+n) \times (m+n)$ matrix which has the coefficients of f and g as entries.

Part 3: Given

$$f(z) = a_m z^m + \cdots + a_1 z + a_0,$$
$$g(z) = b_n z^n + \cdots + b_1 z + b_0,$$

the *resultant* of f and g is usually defined by the Sylvester determinant,
i.e., the determinant of a certain $(m+n) \times (m+n)$ matrix which has the coefficients of f and g as entries.

In particular, this means:

- the resultant of two integer polynomials is a rational integer;

Part 3: Given

$$f(z) = a_m z^m + \cdots + a_1 z + a_0,$$
$$g(z) = b_n z^n + \cdots + b_1 z + b_0,$$

the *resultant* of f and g is usually defined by the Sylvester determinant,
i.e., the determinant of a certain $(m+n) \times (m+n)$ matrix which has the coefficients of f and g as entries.

In particular, this means:
- the resultant of two integer polynomials is a rational integer;
- reducing the coefficients of f and g modulo some integer will carry through to their resultant.

Part 3: Given

$$f(z) = a_m z^m + \cdots + a_1 z + a_0,$$
$$g(z) = b_n z^n + \cdots + b_1 z + b_0,$$

the *resultant* of f and g is usually defined by the Sylvester determinant,
i.e., the determinant of a certain $(m+n) \times (m+n)$ matrix which has the coefficients of f and g as entries.

In particular, this means:
- the resultant of two integer polynomials is a rational integer;
- reducing the coefficients of f and g modulo some integer will carry through to their resultant.

We denote the resultant of f and g by

$$\mathrm{Res}(f, g)$$

if there is no ambiguity as to the variable z.

Suppose that the zeros of f and g are $\alpha_1, \ldots, \alpha_m$ and $\beta_1, \ldots, \beta_n$, respectively. Then the most important property is

$$\mathrm{Res}(f, g) = a_m^n b_n^m \prod_{i=1}^{m} \prod_{j=1}^{n} (\alpha_i - \beta_j),$$

an alternative definition.

Suppose that the zeros of f and g are $\alpha_1, \dots, \alpha_m$ and $\beta_1, \dots, \beta_n$, respectively. Then the most important property is

$$\mathrm{Res}(f, g) = a_m^n b_n^m \prod_{i=1}^{m} \prod_{j=1}^{n} (\alpha_i - \beta_j),$$

an alternative definition. Some consequences:

$$\mathrm{Res}(f, g) = a_m^n \prod_{i=1}^{m} g(\alpha_i),$$

$$\mathrm{Res}(f, g) = (-1)^{nm} \mathrm{Res}(g, f),$$

$$\mathrm{Res}(f, g_1 g_2) = \mathrm{Res}(f, g_1) \mathrm{Res}(f, g_2).$$

Suppose that the zeros of f and g are $\alpha_1, \ldots, \alpha_m$ and $\beta_1, \ldots, \beta_n$, respectively. Then the most important property is

$$\mathrm{Res}(f, g) = a_m^n b_n^m \prod_{i=1}^{m} \prod_{j=1}^{n} (\alpha_i - \beta_j),$$

an alternative definition. Some consequences:

$$\mathrm{Res}(f, g) = a_m^n \prod_{i=1}^{m} g(\alpha_i),$$

$$\mathrm{Res}(f, g) = (-1)^{nm} \mathrm{Res}(g, f),$$

$$\mathrm{Res}(f, g_1 g_2) = \mathrm{Res}(f, g_1) \mathrm{Res}(f, g_2).$$

The first identity shows that $\mathrm{Res}(f, g) = 0$
iff f and g have a factor in common.

Important for us:

Lemma (Apostol (1970))

For $m > n > 1$ we have

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

Important for us:

Lemma (Apostol (1970))

For $m > n > 1$ we have

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

With this we will prove

Lemma

Let p be any prime and α, k be positive integers. Then

$$\mathrm{Res}(g_{p^\alpha}^{(k)}(z), \Phi_n(z)) \neq 0$$

for any $n \geq 3$.

Important for us:

Lemma (Apostol (1970))

For $m > n > 1$ we have

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

With this we will prove

Lemma

Let p be any prime and α, k be positive integers. Then

$$\operatorname{Res}(g_{p^\alpha}^{(k)}(z), \Phi_n(z)) \neq 0$$

for any $n \geq 3$.

Hence no cyclotomic polynomial of degree ≥ 2 can divide any $g_{p^\alpha}^{(k)}(z)$.

Important for us:

Lemma (Apostol (1970))

For $m > n > 1$ we have

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

With this we will prove

Lemma

Let p be any prime and α, k be positive integers. Then

$$\mathrm{Res}(g_{p^\alpha}^{(k)}(z), \Phi_n(z)) \neq 0$$

for any $n \geq 3$.

Hence no cyclotomic polynomial of degree ≥ 2 can divide any $g_{p^\alpha}^{(k)}(z)$. This completes the proof of the Theorem.

Part 4: Proof of the Lemma.

Case 1: p is odd. We'll prove the Lemma by showing:
Resultant cannot be simultaneously 0 (mod 2) and 0 (mod p).

Part 4: Proof of the Lemma.

Case 1: p is odd. We'll prove the Lemma by showing:
Resultant cannot be simultaneously 0 (mod 2) and 0 (mod p).

(a) The gcd's are all odd, and therefore

$$g_{p^\alpha}^{(k)}(z) \equiv 1 + z + \cdots + z^{p^\alpha} = \prod_{\substack{d \mid p^\alpha+1 \\ d \neq 1}} \Phi_d(z) \pmod{2},$$

Part 4: Proof of the Lemma.

Case 1: p is odd. We'll prove the Lemma by showing:
Resultant cannot be simultaneously 0 (mod 2) and 0 (mod p).

(a) The gcd's are all odd, and therefore

$$g_{p^\alpha}^{(k)}(z) \equiv 1 + z + \cdots + z^{p^\alpha} = \prod_{\substack{d \mid p^\alpha+1 \\ d \neq 1}} \Phi_d(z) \pmod{2},$$

so by multiplicativity of resultants,

$$\mathrm{Res}(g_{p^\alpha}^{(k)}(z), \Phi_n(z)) \equiv \prod_{\substack{d \mid p^\alpha+1 \\ d \neq 1}} \mathrm{Res}(\Phi_d(z), \Phi_n(z)) \pmod{2}.$$

Part 4: Proof of the Lemma.

Case 1: p is odd. We'll prove the Lemma by showing: Resultant cannot be simultaneously 0 (mod 2) and 0 (mod p).

(a) The gcd's are all odd, and therefore

$$g_{p^\alpha}^{(k)}(z) \equiv 1 + z + \cdots + z^{p^\alpha} = \prod_{\substack{d \mid p^\alpha+1 \\ d\neq 1}} \Phi_d(z) \pmod{2},$$

so by multiplicativity of resultants,

$$\mathrm{Res}(g_{p^\alpha}^{(k)}(z), \Phi_n(z)) \equiv \prod_{\substack{d \mid p^\alpha+1 \\ d\neq 1}} \mathrm{Res}(\Phi_d(z), \Phi_n(z)) \pmod{2}.$$

By Apostol's result and commutativity (up to sign) of resultants:

$$\mathrm{Res}(g_{p^\alpha}^{(k)}(z), \Phi_n(z)) \equiv 1 \pmod{2}$$

Part 4: Proof of the Lemma.

Case 1: p is odd. We'll prove the Lemma by showing: Resultant cannot be simultaneously 0 (mod 2) and 0 (mod p).

(a) The gcd's are all odd, and therefore

$$g_{p^\alpha}^{(k)}(z) \equiv 1 + z + \cdots + z^{p^\alpha} = \prod_{\substack{d \mid p^\alpha+1 \\ d \neq 1}} \Phi_d(z) \pmod 2,$$

so by multiplicativity of resultants,

$$\mathrm{Res}(g_{p^\alpha}^{(k)}(z), \Phi_n(z)) \equiv \prod_{\substack{d \mid p^\alpha+1 \\ d \neq 1}} \mathrm{Res}(\Phi_d(z), \Phi_n(z)) \pmod 2.$$

By Apostol's result and commutativity (up to sign) of resultants:

$$\mathrm{Res}(g_{p^\alpha}^{(k)}(z), \Phi_n(z)) \equiv 1 \pmod 2$$

unless $n = 2^j d$ for some nonzero j and $d > 1$ where $d \mid p^\alpha + 1$ (j may be positive or negative).

(b) On the other hand,

$$
\begin{aligned}
g_{p^\alpha}^{(k)}(z) &\equiv (z+\cdots+z^{p-1})+(z^{p+1}+\cdots+z^{2p-1})\\
&\quad+\cdots+(z^{p\alpha-p+1}+\cdots+z^{p\alpha-1}) \pmod p\\
&= z\left(1+z+\cdots+z^{p-2}\right)\left(1+z^p+\cdots+z^{(p^{\alpha-1}-1)p}\right)\\
&= z\cdot\frac{z^{p-1}-1}{z-1}\cdot\frac{z^{p^\alpha}-1}{z^p-1}\\
&= z\prod_{\substack{d\mid p-1\\ d\neq 1}}\Phi_d(z)\prod_{j=2}^{\alpha}\Phi_{p^j}(z).
\end{aligned}
$$

By properties of resultants,

$$\mathrm{Res}(z, \Phi_n(z)) = 1 \quad \text{for} \quad n \geq 3,$$

and so

$$\mathrm{Res}(g_{p^\alpha}^{(k)}(z), \Phi_n(z)) \equiv \pm \prod_{\substack{d|p-1 \\ d\neq 1}} \mathrm{Res}(\Phi_d(z), \Phi_n(z)) \times \prod_{j=2}^{\alpha} \mathrm{Res}(\Phi_{p^j}(z), \Phi_n(z)) \pmod{p}.$$

By properties of resultants,

$$\mathrm{Res}(z, \Phi_n(z)) = 1 \quad \text{for} \quad n \geq 3,$$

and so

$$\mathrm{Res}(g_{p^\alpha}^{(k)}(z), \Phi_n(z)) \equiv \pm \prod_{\substack{d|p-1 \\ d\neq 1}} \mathrm{Res}(\Phi_d(z), \Phi_n(z)) \\ \times \prod_{j=2}^{\alpha} \mathrm{Res}(\Phi_{p^j}(z), \Phi_n(z)) \pmod{p}.$$

By Apostol's result:

$$\mathrm{Res}(g_{p^\alpha}^{(k)}(z), \Phi_n(z)) \equiv \pm 1 \pmod{p}$$

By properties of resultants,

$$\mathrm{Res}(z, \Phi_n(z)) = 1 \quad \text{for} \quad n \geq 3,$$

and so

$$\mathrm{Res}(g_{p^\alpha}^{(k)}(z), \Phi_n(z)) \equiv \pm \prod_{\substack{d|p-1 \\ d\neq 1}} \mathrm{Res}(\Phi_d(z), \Phi_n(z)) \times \prod_{j=2}^{\alpha} \mathrm{Res}(\Phi_{p^j}(z), \Phi_n(z)) \pmod{p}.$$

By Apostol's result:

$$\mathrm{Res}(g_{p^\alpha}^{(k)}(z), \Phi_n(z)) \equiv \pm 1 \pmod{p}$$

unless $n = p^\ell d$ for some $\ell \geq 1$ and $d \geq 1$ with $d \mid p - 1$.

Combining the conditions:

The above congruences (mod 2) and (mod p) fail simultaneously only if

$$2^j d_1 = p^\ell d_2, \quad \text{where} \quad d_1 \mid p^\alpha + 1, \quad d_2 \mid p - 1.$$

Combining the conditions:

The above congruences (mod 2) and (mod p) fail simultaneously only if

$$2^j d_1 = p^\ell d_2, \quad \text{where} \quad d_1 \mid p^\alpha + 1, \quad d_2 \mid p - 1.$$

Impossible for an odd prime p since $\ell \geq 1$ and $p \nmid d_1$.

Combining the conditions:

The above congruences (mod 2) and (mod p) fail simultaneously only if

$$2^j d_1 = p^\ell d_2, \quad \text{where} \quad d_1 \mid p^\alpha + 1, \quad d_2 \mid p - 1.$$

Impossible for an odd prime p since $\ell \geq 1$ and $p \nmid d_1$.

Hence at least one of the congruences holds, which means that the resultant is nonzero.

Combining the conditions:

The above congruences (mod 2) and (mod p) fail simultaneously only if

$$2^j d_1 = p^\ell d_2, \quad \text{where} \quad d_1 \mid p^\alpha + 1, \quad d_2 \mid p - 1.$$

Impossible for an odd prime p since $\ell \geq 1$ and $p \nmid d_1$.

Hence at least one of the congruences holds, which means that the resultant is nonzero.

Case 2: $p = 2$ — Similar.

Combining the conditions:

The above congruences (mod 2) and (mod p) fail simultaneously only if

$$2^j d_1 = p^\ell d_2, \quad \text{where} \quad d_1 \mid p^\alpha + 1, \quad d_2 \mid p - 1.$$

Impossible for an odd prime p since $\ell \geq 1$ and $p \nmid d_1$.

Hence at least one of the congruences holds, which means that the resultant is nonzero.

Case 2: $p = 2$ — Similar.

This completes the proof of the resultant lemma, and thus of the irreducibility theorem.

6. Further Remarks

1. Irreducibility proof fails when n has ≥ 2 prime divisors.

6. Further Remarks

1. Irreducibility proof fails when n has ≥ 2 prime divisors.

Still, we propose

Conjecture

For any integers $n \geq 2$ and $k \geq 1$, the polynomial $g_n^{(k)}(z)$ is irreducible, apart from the obvious factor $z+1$ when n is odd.

6. Further Remarks

1. Irreducibility proof fails when n has ≥ 2 prime divisors.

Still, we propose

Conjecture

For any integers $n \geq 2$ and $k \geq 1$, the polynomial $g_n^{(k)}(z)$ is irreducible, apart from the obvious factor $z+1$ when n is odd.

Verified by computation for all $n \leq 1000$ and $1 \leq k \leq 10$.

6. Further Remarks

1. Irreducibility proof fails when n has ≥ 2 prime divisors.

Still, we propose

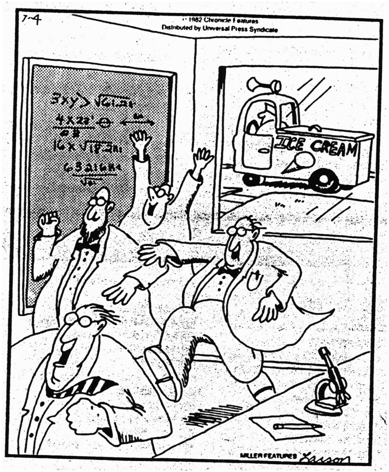
Conjecture

For any integers $n \geq 2$ and $k \geq 1$, the polynomial $g_n^{(k)}(z)$ is irreducible, apart from the obvious factor $z + 1$ when n is odd.

Verified by computation for all $n \leq 1000$ and $1 \leq k \leq 10$.

2. Our results give a large supply of algebraic numbers on the unit circle that are not roots of unity.

Thank you



7-4
© 1982 Chronicle Features
Distributed by Universal Press Syndicate
ICE CREAM
MILLER FEATURES
Larson