Irreducibility of Classical Polynomials and their Generalizations

Irreducibility of Classical Polynomials and their Generalizations

by Michael Filaseta

Irreducibility of Classical Polynomials and their Generalizations

by Michael Filaseta

University of South Carolina

Irreducibility of Classical Polynomials and their Generalizations

by Michael Filaseta

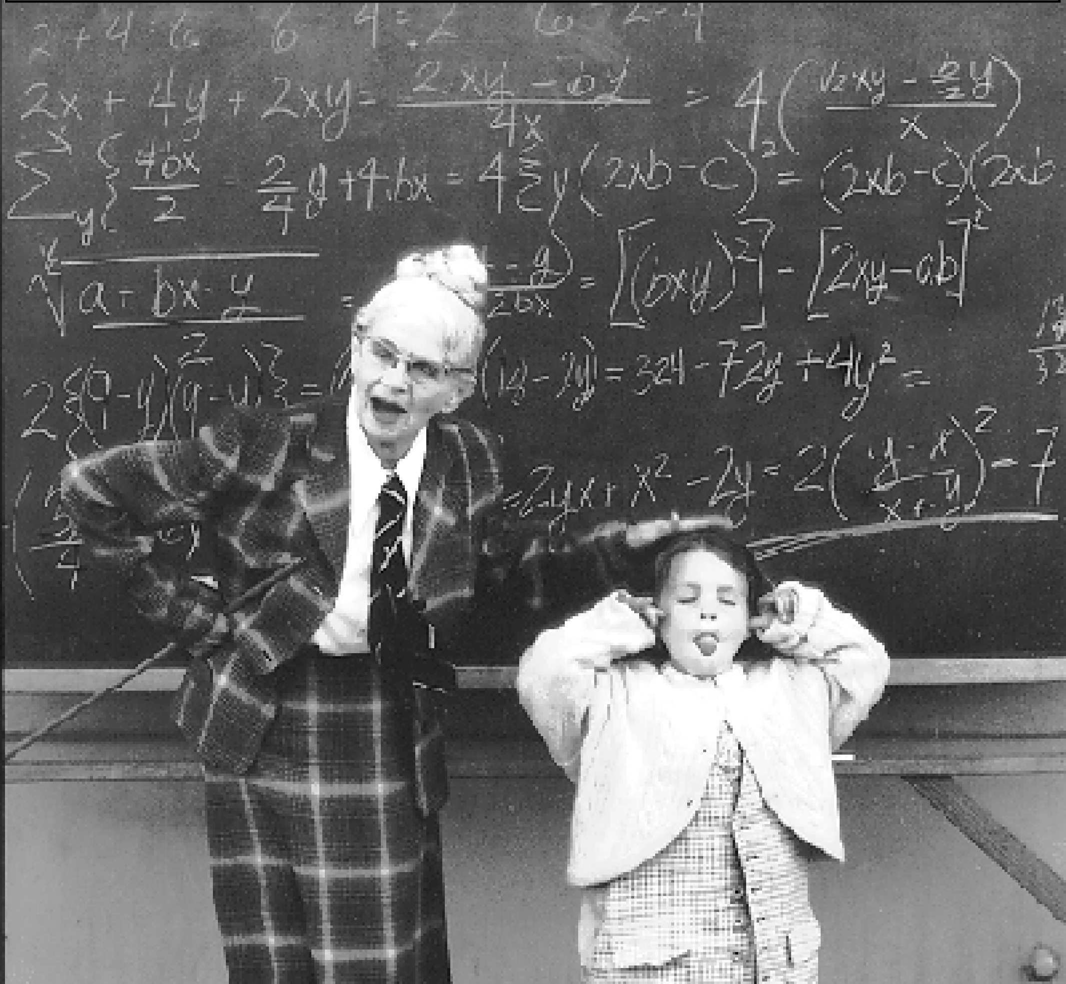
University of South Carolina

This talk is dedicated to John Brillhart and his influence on my mathematics.

En route to a conference, we stop at the San Diego Zoo.

At a conference in Assilomar.

John at a young age refusing to learn his mathematics.



Irreducibility:

A polynomial $f(x) \in \mathbb{Q}[x]$ is *irreducible* provided

Irreducibility:

A polynomial $f(x) \in \mathbb{Q}[x]$ is *irreducible* provided

- $f(x)$ has degree at least 1,

Irreducibility:

A polynomial $f(x) \in \mathbb{Q}[x]$ is *irreducible* provided

- $f(x)$ has degree at least 1,
- $f(x)$ does not factor as a product of two polynomials in $\mathbb{Q}[x]$ each of degree ≥ 1.

Examples:

Examples:

$x^2 + 1$ is irreducible

Examples:

$x^2 + 1$ is irreducible

$2x^2 + 2$ is irreducible

Examples:

$x^2 + 1$ is irreducible

$2x^2 + 2$ is irreducible

$x^4 + x^2 + 1 = (x^2 + x + 1)(x^2 - x + 1)$ is reducible

Examples:

$x^2 + 1$ is irreducible

$2x^2 + 2$ is irreducible

$x^4 + x^2 + 1 = (x^2 + x + 1)(x^2 - x + 1)$ is reducible

$\frac{x^4}{4} + 1 = \left(\frac{x^2}{2} + x + 1\right)\left(\frac{x^2}{2} - x + 1\right)$ is reducible

Examples:

$x^2 + 1$ is irreducible

$2x^2 + 2$ is irreducible

$x^4+x^2+1 = (x^2+x+1)(x^2-x+1)$ is reducible

$\frac{x^4}{4}+1 = \left(\frac{x^2}{2}+x+1\right)\left(\frac{x^2}{2}-x+1\right)$ is reducible

$\frac{x^4}{2}+1$ is irreducible

Joint Work with Brillhart and Odlyzko:

Joint Work with Brillhart and Odlyzko:

85711 is prime

Joint Work with Brillhart and Odlyzko:

$\mathbf{85711}$ is prime

$$\Longrightarrow \ \mathbf{8}\boldsymbol{x}^{\mathbf{4}} + \mathbf{5}\boldsymbol{x}^{\mathbf{3}} + \mathbf{7}\boldsymbol{x}^{\mathbf{2}} + \boldsymbol{x} + \mathbf{1} \text{ is irreducible}$$

Joint Work with Brillhart and Odlyzko:

$\mathbf{85711}$ is prime

$$\Longrightarrow \underbrace{\mathbf{8}x^{\mathbf{4}} + \mathbf{5}x^{\mathbf{3}} + \mathbf{7}x^{\mathbf{2}} + x + \mathbf{1}}_{f(x)} \text{ is irreducible}$$

Joint Work with Brillhart and Odlyzko:

$\mathbf{85711}$ is prime

$$\Longrightarrow \underbrace{\mathbf{8}x^{\mathbf{4}} + \mathbf{5}x^{\mathbf{3}} + \mathbf{7}x^{\mathbf{2}} + x + \mathbf{1}}_{f(x)} \text{ is irreducible}$$

Result (due to A. Cohn): If $f(x)$ has digits as coefficients and $f(10)$ is prime, then $f(x)$ is irreducible.

Joint Work with Brillhart and Odlyzko:

$\mathbf{85711}$ is prime

$$\Longrightarrow \underbrace{\mathbf{8}x^{\mathbf{4}} + \mathbf{5}x^{\mathbf{3}} + \mathbf{7}x^{\mathbf{2}} + x + \mathbf{1}}_{f(x)} \text{ is irreducible}$$

Result (due to A. Cohn): If $f(x)$ has digits as coefficients and $f(\mathbf{10})$ is prime, then $f(x)$ is irreducible.

Theorem: The analogous result holds in any base $b \geq \mathbf{2}$.

Theorem: Let $f(x) = \sum_{j=0}^{n} a_j x^j$ with $0 \le a_j < 10$ and $f(10)$ prime. Then $f(x)$ is irreducible.

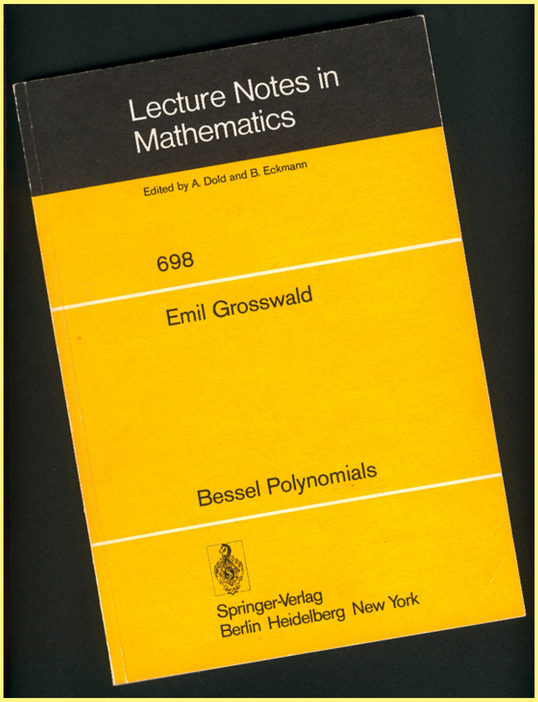
Theorem: Let $f(x) = \sum_{j=0}^{n} a_j x^j$ with $0 \le a_j < 10^{30}$ and $f(10)$ prime. Then $f(x)$ is irreducible.

Theorem: Let $f(x) = \sum_{j=0}^{n} a_j x^j$ with $0 \le a_j < 10^{30}$ and $f(10)$ prime. Then $f(x)$ is irreducible.

Comment: There exist polynomials $f(x) \in \mathbb{Z}[x]$ with non-negative coefficients with $f(10)$ prime and with $f(x)$ reducible.

Letter from Emil Grosswald (dated 04/28/85): Noted that he had seen the above result and asked me to consider the conjecture that the Bessel polynomials are irreducible.

Letter from Emil Grosswald (dated 04/28/85): Noted that he had seen the above result and asked me to consider the conjecture that the Bessel polynomials are irreducible.



Letter from Emil Grosswald (dated 04/28/85): Noted that he had seen the above result and asked me to consider the conjecture that the Bessel polynomials are irreducible.

Remark: In joint work with Ognian Trifonov this conjecture has now been resolved in the affirmative (to appear).

Some Goals of the Talk:

Some Goals of the Talk:

- Give a general discussion of the irreducibility of some classical polynomials

Some Goals of the Talk:

- Give a general discussion of the irreducibility of some classical polynomials
- Show connections to

Some Goals of the Talk:

- Give a general discussion of the irreducibility of some classical polynomials
- Show connections to
  - problems in the distribution of primes

Some Goals of the Talk:

- Give a general discussion of the irreducibility of some classical polynomials
- Show connections to
  - problems in the distribution of primes
  - diophantine and transcendence results

Some Goals of the Talk:

- Give a general discussion of the irreducibility of some classical polynomials
- Show connections to
  - problems in the distribution of primes
  - diophantine and transcendence results
  - Galois theory

Some Goals of the Talk:

- Give a general discussion of the irreducibility of some classical polynomials
- Show connections to
  - problems in the distribution of primes
  - diophantine and transcendence results
  - Galois theory
  - applications to wavelets and dynamical systems

Some Goals of the Talk:

- Give a general discussion of the irreducibility of some classical polynomials
- Show connections to
  - problems in the distribution of primes
  - diophantine and transcendence results
  - Galois theory
  - applications to wavelets and dynamical systems
  - Calvin and Hobbes

Some Polynomials to be Discussed:

Some Polynomials to be Discussed:

- Laguerre Polynomials

Some Polynomials to be Discussed:

- Laguerre Polynomials
- Hermite Polynomials

Some Polynomials to be Discussed:

- Laguerre Polynomials
- Hermite Polynomials
- Bessel Polynomials

Some Polynomials to be Discussed:

- Laguerre Polynomials
- Hermite Polynomials
- Bessel Polynomials

Some Polynomials NOT to be Discussed:

Some Polynomials to be Discussed:

- Laguerre Polynomials
- Hermite Polynomials
- Bessel Polynomials

Some Polynomials NOT to be Discussed:

- Cyclotomic Polynomials (too well-known)

Some Polynomials to be Discussed:

- Laguerre Polynomials
- Hermite Polynomials
- Bessel Polynomials

Some Polynomials NOT to be Discussed:

- Cyclotomic Polynomials (too well-known)
- Chebyshev Polynomials (too easy)

Some Polynomials to be Discussed:

- Laguerre Polynomials
- Hermite Polynomials
- Bessel Polynomials

Some Polynomials NOT to be Discussed:

- Cyclotomic Polynomials (too well-known)
- Chebyshev Polynomials (too easy)
- Bernoulli Polynomials (except for a special case)

Some Polynomials to be Discussed:

- Laguerre Polynomials
- Hermite Polynomials
- Bessel Polynomials

Some Polynomials NOT to be Discussed:

- Cyclotomic Polynomials (too well-known)
- Chebyshev Polynomials (too easy)
- Bernoulli Polynomials (except for a special case)
- Legendre Polynomials (too hard)

The Laguerre Polynomials:

The Laguerre Polynomials:

$$L_n(x) = \frac{e^x}{n!}\frac{d^n(x^n e^{-x})}{dx^n} = \sum_{j=0}^{n} \frac{(-1)^j}{j!}\binom{n}{j}x^j$$

The Laguerre Polynomials:

$$L_n(x) = \frac{e^x}{n!}\frac{d^n(x^n e^{-x})}{dx^n} = \sum_{j=0}^{n} \frac{(-1)^j}{j!}\binom{n}{j}x^j$$

Theorem 1 (I. Schur, 1929): Let n be a positive integer, and let $a_0, a_1, \cdots, a_n$ denote arbitrary integers with $|a_0| = |a_n| = 1$. Then

$$a_n\frac{x^n}{n!} + a_{n-1}\frac{x^{n-1}}{(n-1)!} + \cdots + a_1 x + a_0$$

is irreducible.

Theorem (1996): Let $a_0, a_1, \ldots, a_n$ denote arbitrary integers with $|a_0| = 1$, and let

$$f(x) = \sum_{j=0}^{n} a_j x^j / j!.$$

If $0 < |a_n| < n$, then $f(x)$ is irreducible

Theorem (1996): Let $a_0, a_1, \ldots, a_n$ denote arbitrary integers with $|a_0| = 1$, and let

$$f(x) = \sum_{j=0}^{n} a_j x^j / j!.$$

If $0 < |a_n| < n$, then $f(x)$ is irreducible unless

$$(a_n, n) \in \{(\pm 5, 6), (\pm 7, 10)\}$$

Theorem (1996): Let $a_0, a_1, \ldots, a_n$ denote arbitrary integers with $|a_0| = 1$, and let

$$f(x) = \sum_{j=0}^{n} a_j x^j / j!.$$

If $0 < |a_n| < n$, then $f(x)$ is irreducible unless

$$(a_n, n) \in \{(\pm 5, 6), (\pm 7, 10)\}$$

in which cases either $f(x)$ is irreducible or $f(x)$ is the product of two irreducible polynomials of equal degree.

Theorem (1996): Let $a_0, a_1, \ldots, a_n$ denote arbitrary integers with $|a_0| = 1$, and let

$$f(x) = \sum_{j=0}^{n} a_j x^j / j!.$$

If $0 < |a_n| < n$, then $f(x)$ is irreducible unless

$$(a_n, n) \in \{(\pm 5, 6), (\pm 7, 10)\}$$

in which cases either $f(x)$ is irreducible or $f(x)$ is the product of two irreducible polynomials of equal degree. If $|a_n| = n$, then for some choice of $a_1, \ldots, a_{n-1} \in \mathbb{Z}$ and $a_0 = \pm 1$, we have that $f(x)$ is divisible by $x \pm 1$.

The Generalized Laguerre Polynomials:

The Generalized Laguerre Polynomials:

$$
\begin{aligned}
L_n^{(\alpha)}(x) &= \frac{e^x x^{-\alpha}}{n!} \frac{d^n\left(x^{n+\alpha}e^{-x}\right)}{dx^n} \\
&= \sum_{j=0}^{n} \frac{(n+\alpha)\cdots(j+1+\alpha)(-x)^j}{(n-j)!j!}
\end{aligned}
$$

The Generalized Laguerre Polynomials:

$$L_n^{(\alpha)}(x) = \frac{e^x x^{-\alpha}}{n!}\frac{d^n(x^{n+\alpha}e^{-x})}{dx^n}$$
$$= \sum_{j=0}^{n} \frac{(n+\alpha)\cdots(j+1+\alpha)(-x)^j}{(n-j)!j!}$$

$L_n^{(0)}(x) = L_n(x)$ (the Laguerre Polynomials)

$$\boldsymbol{L_n^{(1)}(x) = (n+1)\sum_{j=0}^{n}\binom{n}{j}\frac{(-x)^j}{(j+1)!}}$$

$$L_n^{(1)}(x) = (n+1)\sum_{j=0}^{n}\binom{n}{j}\frac{(-x)^j}{(j+1)!}$$

Theorem 2 (I. Schur): Let n be a positive integer, and let $a_0, a_1, \cdots, a_n$ denote arbitrary integers with $|a_0| = |a_n| = 1$. Then

$$a_n\frac{x^n}{(n+1)!} + a_{n-1}\frac{x^{n-1}}{n!} + \cdots + a_1\frac{x}{2} + a_0$$

is irreducible (over the rationals) unless $n = 2^r - 1 > 1$ (when $x \pm 2$ can be a factor) or $n = 8$ (when a quadratic factor is possible).

Theorem (joint with M. Allen): For n an integer ≥ 1, define

$$f(x) = \sum_{j=0}^{n} a_j \frac{x^j}{(j+1)!}$$

where the a_j's are arbitrary integers with $|a_0| = 1$. Write

$$n + 1 = k' 2^u \quad \text{with } k' \text{ odd}$$

and

$$(n+1)n = k'' 2^v 3^w \quad \text{with } \gcd(k'', 6) = 1.$$

If

$$0 < |a_n| < \min\{k', k''\},$$

then $f(x)$ is irreducible.

$$L_n^{(\alpha)}(x) = \sum_{j=0}^{n} \frac{(n+\alpha)\cdots(j+1+\alpha)(-x)^j}{(n-j)!j!}$$

$$L_n^{(\alpha)}(x) = \sum_{j=0}^{n} \frac{(n+\alpha)\cdots(j+1+\alpha)(-x)^j}{(n-j)!j!}$$

$$\begin{aligned}
L_2^{(2)}(x) &= \frac{1}{2}(x-2)(x-6) \\
L_2^{(23)}(x) &= \frac{1}{2}(x-20)(x-30) \\
L_4^{(23)}(x) &= \frac{1}{24}(x-30)(x^3-78x^2+1872x-14040) \\
L_4^{(12/5)}(x) &= \frac{1}{15000}(25x^2-420x+1224)(25x^2-220x+264) \\
L_5^{(39/5)}(x) &= \frac{-1}{375000}(5x-84)\big(625x^4-29500x^3 \\
&\qquad +448400x^2-2662080x+5233536\big)
\end{aligned}$$

$$L_n^{(\alpha)}(x) = \sum_{j=0}^{n} \frac{(n+\alpha)\cdots(j+1+\alpha)(-x)^j}{(n-j)!j!}$$

$$L_2^{(2)}(x) = \frac{1}{2}(x-2)(x-6)$$

$$L_2^{(23)}(x) = \frac{1}{2}(x-20)(x-30)$$

$$L_4^{(23)}(x) = \frac{1}{24}(x-30)(x^3-78x^2+1872x-14040)$$

$$L_4^{(12/5)}(x) = \frac{1}{15000}(25x^2-420x+1224)(25x^2-220x+264)$$

$$L_5^{(39/5)}(x) = \frac{-1}{375000}(5x-84)\big(625x^4-29500x^3 + 448400x^2-2662080x+5233536\big)$$

Theorem (joint with T.-Y. Lam): Let α be a rational number which is not a negative integer. Then for all but finitely many positive integers n, the polynomial $L_n^{(\alpha)}(x)$ is irreducible over the rationals.

$$L_n^{(\alpha)}(x) = \sum_{j=0}^{n} \frac{(n+\alpha)\cdots(j+1+\alpha)(-x)^j}{(n-j)!j!}$$

$$L_n^{(\alpha)}(x) = \sum_{j=0}^{n} \frac{(n+\alpha)\cdots(j+1+\alpha)(-x)^j}{(n-j)!j!}$$

A Special Case: $\alpha = n$

Background:

Background:

- D. Hilbert (1892) used his now classical Hilbert's Irreducibility Theorem to show that for each integer $n \geq 1$, there is a polynomial $f(x) \in \mathbb{Z}[x]$ such that the Galois group associated with $f(x)$ is the symmetric group S_n.

Background:

- D. Hilbert (1892) used his now classical Hilbert's Irreducibility Theorem to show that for each integer $n \geq 1$, there is a polynomial $f(x) \in \mathbb{Z}[x]$ such that the Galois group associated with $f(x)$ is the symmetric group S_n. He also showed the analogous result in the case of the alternating group A_n.

Background:

- D. Hilbert (1892) used his now classical Hilbert's Irreducibility Theorem to show that for each integer $n \geq 1$, there is a polynomial $f(x) \in \mathbb{Z}[x]$ such that the Galois group associated with $f(x)$ is the symmetric group S_n. He also showed the analogous result in the case of the alternating group A_n.
- Hilbert's work and work of E. Noether (1918) began what has come to be known as Inverse Galois Theory.

Background:

- D. Hilbert (1892) used his now classical Hilbert's Irreducibility Theorem to show that for each integer $n \geq 1$, there is a polynomial $f(x) \in \mathbb{Z}[x]$ such that the Galois group associated with $f(x)$ is the symmetric group S_n. He also showed the analogous result in the case of the alternating group A_n.
- Hilbert's work and work of E. Noether (1918) began what has come to be known as Inverse Galois Theory.
- Van der Waerden showed that for "almost all" polynomials $f(x) \in \mathbb{Z}[x]$, the Galois group associated with $f(x)$ is the symmetric group S_n.

- Schur showed $L_n^{(0)}(x)$ has Galois group S_n.

- Schur showed $L_n^{(0)}(x)$ has Galois group S_n.
- Schur showed $L_n^{(1)}(x)$ has Galois group A_n (the alternating group) if n is odd.

- Schur showed $L_n^{(0)}(x)$ has Galois group S_n.
- Schur showed $L_n^{(1)}(x)$ has Galois group A_n (the alternating group) if n is odd.
- Schur showed $\displaystyle\sum_{j=0}^{n} \frac{x^j}{j!}$ has Galois group A_n if $4|n$.

- Schur showed $L_n^{(0)}(x)$ has Galois group S_n.
- Schur showed $L_n^{(1)}(x)$ has Galois group A_n (the alternating group) if n is odd.
- Schur showed $\displaystyle\sum_{j=0}^{n} \frac{x^j}{j!}$ has Galois group A_n if $4|n$.
- Schur did not find an explicit sequence of polynomials having Galois group A_n with $n \equiv 2 \pmod 4$.

Theorem (R. Gow, 1989): If $n > 2$ is even and $L_n^{(n)}(x)$ is irreducible, then the Galois group of $L_n^{(n)}(x)$ is A_n.

Theorem (R. Gow, 1989): If $n > 2$ is even and $L_n^{(n)}(x)$ is irreducible, then the Galois group of $L_n^{(n)}(x)$ is A_n.

Comment: Gow also showed that $L_n^{(n)}(x)$ is irreducible if

- $n = 2p^k$ where $k \in \mathbb{Z}^+$ and $p > 3$ is prime
- $n = 4p^k$ where $k \in \mathbb{Z}^+$ and $p > 7$ is prime

Theorem (R. Gow, 1989): If $n > 2$ is even and $L_n^{(n)}(x)$ is irreducible, then the Galois group of $L_n^{(n)}(x)$ is A_n.

Comment: Gow also showed that $L_n^{(n)}(x)$ is irreducible if

- $n = 2p^k$ where $k \in \mathbb{Z}^+$ and $p > 3$ is prime
- $n = 4p^k$ where $k \in \mathbb{Z}^+$ and $p > 7$ is prime

Conjecture: If $n > 2$, then $L_n^{(n)}(x)$ is irreducible.

Theorem (joint work with R. Williams): For almost all positive integers n the polynomial $L_n^{(n)}(x)$ is irreducible (and, hence, has Galois group A_n for almost all $n \equiv 2 \pmod 4$). More precisely, the number of $n \le t$ such that $L_n^{(n)}(x)$ is reducible is

$$\ll \exp\left(\frac{9\log(2t)}{\log\log(2t)}\right).$$

Furthermore, for all but finitely many n, $L_n^{(n)}(x)$ is either irreducible or $L_n^{(n)}(x)$ is the product of a linear polynomial times an irreducible polynomial of degree $n-1$.

Theorem (joint work with R. Williams): For all but

$$O\big(\exp(9\log(2t)/\log\log(2t))\big)$$

positive integers $n \le t$, the polynomial

$$f(x) = \sum_{j=0}^{n} a_j \binom{2n}{n-j} \frac{x^j}{j!}$$

is irreducible over the rationals for every choice of integers $a_0, a_1, \dots, a_n$ with $|a_0| = |a_n| = 1$.

Theorem (joint work with R. Williams): For all but

$$O\big(\exp(9\log(2t)/\log\log(2t))\big)$$

positive integers $n \le t$, the polynomial

$$f(x) = \sum_{j=0}^{n} a_j \binom{2n}{n-j} \frac{x^j}{j!}$$

is irreducible over the rationals for every choice of integers $a_0, a_1, \ldots, a_n$ with $|a_0| = |a_n| = 1$.

Comment: The number of $n \le t$ for which $f(x)$ is reducible for some choice of a_j as above is

$$\gg \log t.$$

Is the irreducibility of $L_n^{(n)}(x)$ doable for all $n > 2$?

Is the irreducibility of $L_n^{(n)}(x)$ doable for all $n > 2$?

The proof for almost all n is not effective. If n is large enough, $L_n^{(n)}(x)$ cannot have a *quadratic factor* but what's "large enough"?

Is the irreducibility of $L_n^{(n)}(x)$ doable for all $n > 2$?

The proof for almost all n is not effective. If n is large enough, $L_n^{(n)}(x)$ cannot have a *quadratic factor* but what's "large enough"?

However, in joint work with O. Trifonov (and input from R. Tijdeman, F. Beukers, and M. Bennett), the argument can now be made effective. What's needed is:

Is the irreducibility of $L_n^{(n)}(x)$ doable for all $n > 2$?

The proof for almost all n is not effective. If n is large enough, $L_n^{(n)}(x)$ cannot have a *quadratic factor* but what's "large enough"?

However, in joint work with O. Trifonov (and input from R. Tijdeman, F. Beukers, and M. Bennett), the argument can now be made effective. What's needed is:

> *There exist explicit numbers α and $\beta > 0$ such that, for $n \geq \alpha$,*
>
> $$n(n+1) = 2^k 3^\ell m \implies m > n^\beta.$$

Application of the Same Method:

Application of the Same Method:

The Ramanujan-Nagell equation

$$x^2 + 7 = 2^n$$

has as its only solutions $(\pm x, n)$ in

$$\{(1,3),(3,4),(5,5),(11,7),(181,15)\}.$$

Application of the Same Method:

The Ramanujan-Nagell equation

$$x^2 + 7 = 2^n$$

has as its only solutions $(\pm x, n)$ in

$$\{(1,3),(3,4),(5,5),(11,7),(181,15)\}.$$

Moreover, there exist explicit numbers α and $\beta > 0$ such that, for $x \geq \alpha$,

$$x^2 + 7 = 2^n m \implies m \geq x^\beta.$$

The Hermite Polynomials:

The Hermite Polynomials:

$$H_n(x) = (-1)^n e^{x^2/2} \frac{d^n \left(e^{-x^2/2}\right)}{dx^n}$$
$$= \sum_{j=0}^{[n/2]} (-1)^n \binom{n}{2j} u_{2j}\, x^{m-2j}$$

where

$$u_{2j} = (2j-1)(2j-3)\cdots 3 \cdot 1$$

The Hermite Polynomials:

$$H_{2n}(x) = (-1)^n u_{2n} \sum_{j=0}^{n} (-1)^j \binom{n}{j} \frac{x^{2j}}{u_{2j}}$$

$$H_{2n+1}(x) = (-1)^n u_{2n+2} x \sum_{j=0}^{n} (-1)^j \binom{n}{j} \frac{x^{2j}}{u_{2j+2}}$$

$$H_{2n}(x) = (-1)^n u_{2n} \sum_{j=0}^{n} (-1)^j \binom{n}{j} \frac{x^{2j}}{u_{2j}}$$

$$H_{2n+1}(x) = (-1)^n u_{2n+2} x \sum_{j=0}^{n} (-1)^j \binom{n}{j} \frac{x^{2j}}{u_{2j+2}}$$

Theorem 3 (I. Schur, 1929): For $n > 1$ and arbitrary integers a_j with $|a_0| = |a_n| = 1$, the polynomial

$$f(x) = \sum_{j=0}^{n} a_j x^{2j} / u_{2j}$$

is irreducible.

$$H_{2n}(x) = (-1)^n u_{2n} \sum_{j=0}^{n} (-1)^j \binom{n}{j} \frac{x^{2j}}{u_{2j}}$$

$$H_{2n+1}(x) = (-1)^n u_{2n+2} x \sum_{j=0}^{n} (-1)^j \binom{n}{j} \frac{x^{2j}}{u_{2j+2}}$$

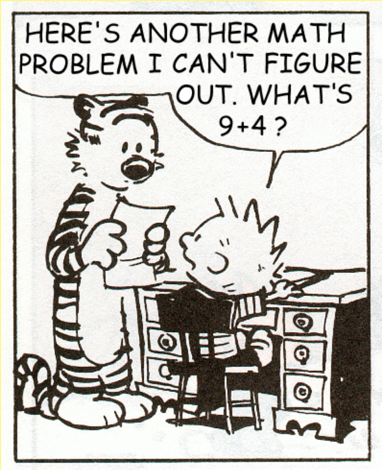
Theorem 4 (I. Schur, 1929): For $n \geq 1$ and arbitrary integers a_j with $|a_0| = |a_n| = 1$, the polynomial

$$f(x) = \sum_{j=0}^{n} a_j x^{2j} / u_{2j+2}$$

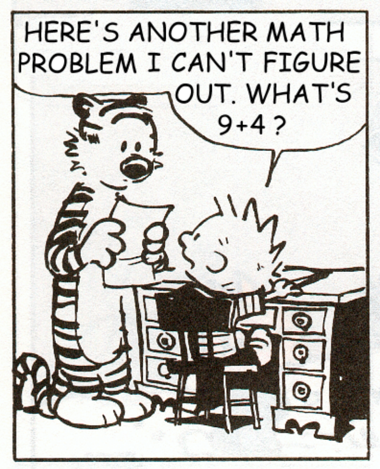
is irreducible unless $2n$ is of the form $3^u - 1$ with $u > 1$.

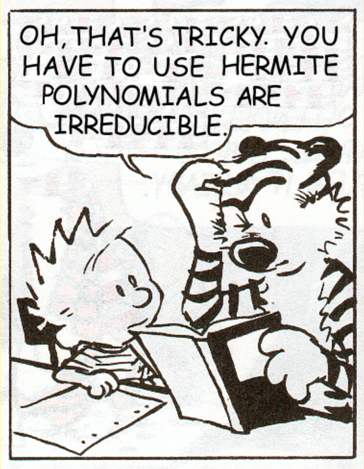
Applications:

Applications:



Applications:





Email from Mark Kon:

Given a function $f(x)$, its wavelet transform consists of the family of functions $g(2^j x) * f(x)$, where g is the gaussian function, and j is an integer. The question was: if we know the zeroes of the second derivatives of this family of functions (over all j), can we recover f? ... The problem reduces to showing that none of these polynomials [certain Hermite polynomials] has zeroes (aside from the trivial one at the origin) which coincides with a zero of another one. So the bottom line is that the conjecture that f is uniquely recoverable follows from the non-overlapping of the zeroes of the Hermite polynomials.

Email from Mark Kon:

Given a function $f(x)$, its wavelet transform consists of the family of functions $g(2^j x) * f(x)$, where g is the gaussian function, and j is an integer. The question was: if we know the zeroes of the second derivatives of this family of functions (over all j), can we recover f? ... The problem reduces to showing that none of these polynomials [certain Hermite polynomials] has zeroes (aside from the trivial one at the origin) which coincides with a zero of another one. So the bottom line is that the conjecture that f is uniquely recoverable follows from the non-overlapping of the zeroes of the Hermite polynomials.

A Similar Type Application of Irreducibility:

A Similar Type Application of Irreducibility:

E. Gutkin dealt with a billards question in Dynamical Systems. J. Lagarias posed a related conjecture at the West Coast Number Theory Conference in 1991:

A Similar Type Application of Irreducibility:

E. Gutkin dealt with a billards question in Dynamical Systems. J. Lagarias posed a related conjecture at the West Coast Number Theory Conference in 1991:

Let $n \geq 4$ and

$$p(x) = (n-1)\big(x^{n+1} - 1\big) - (n+1)\big(x^n - x\big).$$

Then $p(x)$ is $(x-1)^3$ times an irreducible polynomial if n is even and $(x-1)^3(x+1)$ times an irreducible polynomial if n is odd.

A Similar Type Application of Irreducibility:

E. Gutkin dealt with a billards question in Dynamical Systems. J. Lagarias posed a related conjecture at the West Coast Number Theory Conference in 1991:

Let $n \geq 4$ *and*

$$p(x) = (n-1)\big(x^{n+1} - 1\big) - (n+1)\big(x^n - x\big).$$

Then $p(x)$ *is* $(x - 1)^3$ *times an irreducible polynomial if* n *is even and* $(x-1)^3(x+1)$ *times an irreducible polynomial if* n *is odd.*

Joint Work With A. Borisov, T.-Y. Lam, O. Trifonov:

True for all but $O(t^{4/5+\varepsilon})$ *values of* $n \leq t$.

Theorem 3 (I. Schur, 1929): For $n > 1$ and arbitrary integers a_j with $|a_0| = |a_n| = 1$, the polynomial

$$f(x) = \sum_{j=0}^{n} a_j x^{2j} / u_{2j}$$

is irreducible.

Theorem 3 (I. Schur, 1929): For $n > 1$ and arbitrary integers a_j with $|a_0| = |a_n| = 1$, the polynomial

$$f(x) = \sum_{j=0}^{n} a_j x^{2j} / u_{2j}$$

is irreducible.

Theorem (joint with M. Allen): For $n > 1$ and arbitrary integers a_j with $|a_0| = 1$ and

$$0 < |a_n| < 2n - 1,$$

the polynomial $f(x)$ above is irreducible for all but finitely many pairs (a_n, n).

Theorem 4 (I. Schur, 1929): For $n \geq 1$ and arbitrary integers a_j with $|a_0| = |a_n| = 1$, the polynomial

$$f(x) = \sum_{j=0}^{n} a_j x^{2j} / u_{2j+2}$$

is irreducible unless $2n$ is of the form $3^u - 1$ with $u > 1$.

Theorem (joint with M. Allen): For n an integer ≥ 1, define

$$f(x) = \sum_{j=0}^{n} a_j \frac{x^{2j}}{u_{2j+2}}$$

where the a_j's are arbitrary integers with $|a_0| = 1$. Write

$$2n+1 = k' 3^u \quad \text{with} \quad 3 \nmid k'$$

and

$$(2n+1)(2n-1) = k'' 3^v 5^w \quad \text{with} \quad (k'', 15) = 1.$$

If

$$0 < |a_n| < \min\{k', k''\},$$

then $f(x)$ is irreducible for all but finitely many pairs (a_n, n).

The Bessel Polynomials:

The Bessel Polynomials:

$$y_n(x) = \sum_{j=0}^{n} \frac{(n+j)!}{2^j (n-j)! j!} x^j$$

The Bessel Polynomials:

$$y_n(x) = \sum_{j=0}^{n} \frac{(n+j)!}{2^j (n-j)! j!} x^j$$

Brief History:

The Bessel Polynomials:

$$y_n(x) = \sum_{j=0}^{n} \frac{(n+j)!}{2^j (n-j)! j!} x^j$$

Brief History:

- E. Grosswald studied the irreducibility of the Bessel polynomials in 1951 and conjectured their irreducibility. He obtained a variety of special cases of irreducibility.

The Bessel Polynomials:

$$y_n(x) = \sum_{j=0}^{n} \frac{(n+j)!}{2^j (n-j)! j!} x^j$$

Brief History:

- E. Grosswald studied the irreducibility of the Bessel polynomials in 1951 and conjectured their irreducibility. He obtained a variety of special cases of irreducibility.
- In 1995, M.F. showed that all but finitely many Bessel polynomials are irreducible.

The Bessel Polynomials:

$$y_n(x) = \sum_{j=0}^{n} \frac{(n+j)!}{2^j (n-j)! j!} x^j$$

Brief History:

- E. Grosswald studied the irreducibility of the Bessel polynomials in 1951 and conjectured their irreducibility. He obtained a variety of special cases of irreducibility.
- In 1995, M.F. showed that all but finitely many Bessel polynomials are irreducible.
- O. Trifonov and M.F. have now shown that all Bessel polynomials are irreducible.

The Bessel Polynomials:

$$y_n(x) = \sum_{j=0}^{n} \frac{(n+j)!}{2^j (n-j)! j!} x^j$$

The Bessel Polynomials:

$$y_n(x) = \sum_{j=0}^{n} \frac{(n+j)!}{2^j (n-j)! j!} x^j$$

Theorem (joint with O. Trifonov): If $a_0, a_1, \dots, a_n$ are arbitrary integers with $|a_0| = |a_n| = 1$, then

$$\sum_{j=0}^{n} a_j \frac{(n+j)!}{2^j (n-j)! j!} x^j$$

is irreducible.

Main Ingredients of the Proofs:

Main Ingredients of the Proofs:

- Newton polygons are used to show that if certain conditions on divisibility by primes holds, then $f(x)$ is irreducible.

Main Ingredients of the Proofs:

- Newton polygons are used to show that if certain conditions on divisibility by primes holds, then $f(x)$ is irreducible.
- Analysis to show that the conditions hold; usually this involves cases to eliminate possible factors depending on the size of their degrees.

Main Ingredients of the Proofs:

- Newton polygons are used to show that if certain conditions on divisibility by primes holds, then $f(x)$ is irreducible.
- Analysis to show that the conditions hold; usually this involves cases to eliminate possible factors depending on the size of their degrees.
  - small gaps between primes for large degrees

Main Ingredients of the Proofs:

- Newton polygons are used to show that if certain conditions on divisibility by primes holds, then $f(x)$ is irreducible.
- Analysis to show that the conditions hold; usually this involves cases to eliminate possible factors depending on the size of their degrees.
  - small gaps between primes for large degrees
  - results about products of consecutive integers having some large prime factors for intermediate degrees

Main Ingredients of the Proofs:

- Newton polygons are used to show that if certain conditions on divisibility by primes holds, then $f(x)$ is irreducible.
- Analysis to show that the conditions hold; usually this involves cases to eliminate possible factors depending on the size of their degrees.
  - small gaps between primes for large degrees
  - results about products of consecutive integers having some large prime factors for intermediate degrees
  - Diophantine equations for small degrees

- Newton polygons are used to show that if certain conditions on divisibility by primes holds, then $f(x)$ is irreducible.

- Newton polygons are used to show that if certain conditions on divisibility by primes holds, then $f(x)$ is irreducible.

A result of M.G. Dumas (in 1906) eliminates possible degrees for the factors of a polynomial using information about the divisibility of the coefficients by a given prime p (forming Newton polygons with respect to p).

- Newton polygons are used to show that if certain conditions on divisibility by primes holds, then $f(x)$ is irreducible.

> "Two such factorization schemes with a common, non-trivial factorization, will be called *compatible*. Otherwise, we call them incompatible. It is clear that if one can exhibit two incompatible factorization schemes, one thereby will have proved the irreducibility of the polynomial considered."
>
> Emil Grosswald
> Bessel Polynomials
> Lecture Notes Series

- Newton polygons are used to show that if certain conditions on divisibility by primes holds, then $f(x)$ is irreducible.

  Idea: To consider factorization schemes using many primes and show that they are incompatible. For a polynomial of degree n and a $k \in [1, n/2]$, find a prime p such that the Newton polygon with respect to p does not allow for a factor of $f(x)$ to have degree k.

- Analysis to show that the conditions hold; usually this involves cases to eliminate possible factors depending on the size of their degrees.

- Analysis to show that the conditions hold; usually this involves cases to eliminate possible factors depending on the size of their degrees.

Example: For $3 \le k \le n/2$, show

$$\prod_{\substack{p^r || n(n-1)\cdots(n-k+1) \\ p \ge k+1}} p^r > n.$$

- Analysis to show that the conditions hold; usually this involves cases to eliminate possible factors depending on the size of their degrees.

Example: For $3 \le k \le n/2$, show

$$\prod_{\substack{p^r || n(n-1)\cdots(n-k+1) \\ p \ge k+1}} p^r > n.$$

For n large and k large (say $> n^{2/3}$), use that there are two primes in the interval $[n-k+1, n]$.

- Analysis to show that the conditions hold; usually this involves cases to eliminate possible factors depending on the size of their degrees.

Example: For $3 \le k \le n/2$, show

$$\prod_{\substack{p^r || n(n-1)\cdots(n-k+1) \\ p \ge k+1}} p^r > n.$$

Now consider k small.

- Analysis to show that the conditions hold; usually this involves cases to eliminate possible factors depending on the size of their degrees.

$$\boldsymbol{k = 3 :} \qquad \prod_{\substack{p^r || n(n-1)(n-2) \\ p \geq 4}} p^r > n$$

- Analysis to show that the conditions hold; usually this involves cases to eliminate possible factors depending on the size of their degrees.

$$k = 3: \quad \prod_{\substack{p^r \| n(n-1)(n-2) \\ p \geq 4}} p^r > n$$

Problem n: 6

- Analysis to show that the conditions hold; usually this involves cases to eliminate possible factors depending on the size of their degrees.

$$\boldsymbol{k = 3:} \quad \prod_{\substack{p^r \| n(n-1)(n-2) \\ p \geq 4}} p^r > n$$

Problem n: 6, 8

- Analysis to show that the conditions hold; usually this involves cases to eliminate possible factors depending on the size of their degrees.

$$\boldsymbol{k = 3:} \quad \prod_{\substack{p^r \| n(n-1)(n-2) \\ p \geq 4}} p^r > n$$

Problem n: 6, 8, 9

- Analysis to show that the conditions hold; usually this involves cases to eliminate possible factors depending on the size of their degrees.

$$\boldsymbol{k = 3:} \quad \prod_{\substack{p^r \| n(n-1)(n-2) \\ p \geq 4}} p^r > n$$

Problem n**: 6, 8, 9, 10**

- Analysis to show that the conditions hold; usually this involves cases to eliminate possible factors depending on the size of their degrees.

$$\boldsymbol{k = 3:} \quad \prod_{\substack{p^r \| n(n-1)(n-2) \\ p \geq 4}} p^r > n$$

Problem n**:** $\mathbf{6, 8, 9, 10, 18}$

- Analysis to show that the conditions hold; usually this involves cases to eliminate possible factors depending on the size of their degrees.

$$\boldsymbol{k = 3:} \quad \prod_{\substack{p^r \| n(n-1)(n-2) \\ p \geq 4}} p^r > n$$

Problem $\boldsymbol{n}$**:** $\mathbf{6}$, $\mathbf{8}$, $\mathbf{9}$, $\mathbf{10}$, $\mathbf{18}$, and that's it!!

- Analysis to show that the conditions hold; usually this involves cases to eliminate possible factors depending on the size of their degrees.

$$k = 4 : \prod_{\substack{p^r \| n(n-1)(n-2)(n-3) \\ p \geq 5}} p^r > n$$

- Analysis to show that the conditions hold; usually this involves cases to eliminate possible factors depending on the size of their degrees.

$$k = 4: \prod_{\substack{p^r \| n(n-1)(n-2)(n-3) \\ p \geq 5}} p^r > n$$

Problem n: 9

- Analysis to show that the conditions hold; usually this involves cases to eliminate possible factors depending on the size of their degrees.

$$k = 4: \prod_{\substack{p^r \| n(n-1)(n-2)(n-3) \\ p \geq 5}} p^r > n$$

Problem n: $\mathbf{9}$, and that's it.

- Analysis to show that the conditions hold; usually this involves cases to eliminate possible factors depending on the size of their degrees.

$$\boldsymbol{k = 5 :} \quad \prod_{\substack{p^r \| n(n-1)(n-2)(n-3)(n-4) \\ p \geq 6}} p^r > n$$

- Analysis to show that the conditions hold; usually this involves cases to eliminate possible factors depending on the size of their degrees.

$$k = 5 : \prod_{\substack{p^r || n(n-1)(n-2)(n-3)(n-4) \\ p \geq 6}} p^r > n$$

Problem n**:** $\mathbf{10}$

- Analysis to show that the conditions hold; usually this involves cases to eliminate possible factors depending on the size of their degrees.

$$\boldsymbol{k = 5 :} \qquad \prod_{\substack{p^r || n(n-1)(n-2)(n-3)(n-4) \\ p \geq 6}} p^r > n$$

Problem n: 10, 12

- Analysis to show that the conditions hold; usually this involves cases to eliminate possible factors depending on the size of their degrees.

$$\boldsymbol{k = 5:} \qquad \prod_{\substack{p^r \| n(n-1)(n-2)(n-3)(n-4) \\ p \geq 6}} p^r > n$$

Problem n: $\mathbf{10}$, $\mathbf{12}$, and that's it.

- Analysis to show that the conditions hold; usually this involves cases to eliminate possible factors depending on the size of their degrees.

Lemma. For $3 \le k \le n/2$,

$$\prod_{\substack{p^r || n(n-1)\cdots(n-k+1) \\ p \ge k+1}} p^r > n$$

unless one of the following holds:

$$\begin{array}{lll} k = 3 & \text{and} & n = 6, 8, 9, 10, \text{ or } 18 \\ k = 4 & \text{and} & n = 9 \\ k = 5 & \text{and} & n = 10 \text{ or } 12. \end{array}$$

The Generalized Bernoulli Polynomials:

The Generalized Bernoulli Polynomials:

$$\left(\frac{t}{e^t - 1}\right)^{\alpha} e^{xt} = \sum_{n=0}^{\infty} B_n^{(\alpha)}(x) \frac{t^n}{n!}$$

The Generalized Bernoulli Polynomials:

$$\left(\frac{t}{e^t - 1}\right)^{\alpha} e^{xt} = \sum_{n=0}^{\infty} B_n^{(\alpha)}(x) \frac{t^n}{n!}$$

Classical Case:

The Generalized Bernoulli Polynomials:

$$\left(\frac{t}{e^t - 1}\right)^\alpha e^{xt} = \sum_{n=0}^{\infty} B_n^{(\alpha)}(x)\frac{t^n}{n!}$$

Classical Case: $\alpha = 1$

The Generalized Bernoulli Polynomials:

$$\left(\frac{t}{e^t - 1}\right)^{\alpha} e^{xt} = \sum_{n=0}^{\infty} B_n^{(\alpha)}(x)\frac{t^n}{n!}$$

Classical Case: $\alpha = 1$

J. Brillhart's Observation (1969):

$$\begin{aligned} 6B_{11}(x) = {} & x(x-1)(2x-1)(x^2-x-1) \\ & \times (3x^6-9x^5+2x^4+11x^3+3x^2-10x-5) \end{aligned}$$

The Generalized Bernoulli Polynomials:

$$\left(\frac{t}{e^t - 1}\right)^{\alpha} e^{xt} = \sum_{n=0}^{\infty} B_n^{(\alpha)}(x) \frac{t^n}{n!}$$

A Special Case:

The Generalized Bernoulli Polynomials:

$$\left(\frac{t}{e^t - 1}\right)^{\alpha} e^{xt} = \sum_{n=0}^{\infty} B_n^{(\alpha)}(x) \frac{t^n}{n!}$$

A Special Case: $\alpha = n$

The Generalized Bernoulli Polynomials:

$$\left(\frac{t}{e^t - 1}\right)^{\alpha} e^{xt} = \sum_{n=0}^{\infty} B_n^{(\alpha)}(x) \frac{t^n}{n!}$$

A Special Case: $\alpha = n$

Theorem (joint with A. Adelberg): A positive proportion of the polynomials $B_n^{(n)}(x)$ are Eisenstein (and, hence, irreducible).

The Generalized Bernoulli Polynomials:

$$\left(\frac{t}{e^t-1}\right)^{\alpha} e^{xt} = \sum_{n=0}^{\infty} B_n^{(\alpha)}(x)\frac{t^n}{n!}$$

A Special Case: $\alpha = n$

Theorem (joint with A. Adelberg): A positive proportion of the polynomials $B_n^{(n)}(x)$ are Eisenstein (and, hence, irreducible). More precisely, if the number of $n \le t$ for which $B_n^{(n)}(x)$ is Eisenstein is $\mathcal{B}(t)$, then

$$\mathcal{B}(t) > t/5 \qquad \text{for } t \text{ sufficiently large.}$$

Time for Questions