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:

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 .

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

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

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

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

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

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

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

• Laguerre Polynomials

- Laguerre Polynomials
- Hermite Polynomials

- Laguerre Polynomials
- Hermite Polynomials
- Bessel Polynomials

- Laguerre Polynomials
- Hermite Polynomials
- Bessel Polynomials

- Laguerre Polynomials
- Hermite Polynomials
- Bessel Polynomials

Some Polynomials NOT to be Discussed:

• Cyclotomic Polynomials (too well-known)

- Laguerre Polynomials
- Hermite Polynomials
- Bessel Polynomials

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

- Laguerre Polynomials
- Hermite Polynomials
- Bessel Polynomials

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

- Laguerre Polynomials
- Hermite Polynomials
- Bessel Polynomials

- 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:

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

The Laguerre Polynomials:

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

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

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

is irreducible.

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

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

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

If $0 < |a_n| < n$, then f(x) is irreducible unless $(a_n, n) \in \{(\pm 5, 6), (\pm 7, 10)\}$

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

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

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

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

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

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

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

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:

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

The Generalized Laguerre Polynomials:

$$L_n^{(lpha)}(x) = rac{e^x x^{-lpha} d^n ig(x^{n+lpha} e^{-x} ig)}{n!} \ = \sum_{j=0}^n rac{(n+lpha) \cdots (j+1+lpha) (-x)^j}{(n-j)! j!}$$

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

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

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

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

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

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 n

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

where the a_j 's are arbitrary integers with $|a_0| = 1$. Write $n+1 = k' 2^u$ with k' odd

and

$$(n+1)n = k'' 2^v 3^w$$
 with $gcd(k'', 6) = 1$.
If

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

then f(x) is irreducible.

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

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

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

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

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

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.

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

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

A Special Case: $\alpha = n$

• 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 .

• 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 .

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

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

• Schur showed $\sum_{j=0}^{n} \frac{x^{j}}{j!}$ has Galois group A_{n} if 4|n.

- 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 $L_n^{(1)}(x)$ has Galois group A_n (the alternating group) if n is odd.
- Schur showed $\sum_{j=0}^{n} \frac{x^{j}}{j!}$ has Galois group A_{n} if 4|n.
- Schur did not find a 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

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

- $ullet n=2p^k$ where $k\in\mathbb{Z}^+$ and p>3 is prime
- $ullet n=4p^k$ 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 $n \equiv 2$ (mod 4)). More precisely, the number of $n \leq t$ such that $L_n^{(n)}(x)$ is reducible is

$$\ll \exp{igg(rac{9\log(2t)}{\log\log(2t)}igg)}.$$

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

positive integers $n \leq t$, the polynomial

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

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

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

 $Oig(\exp(9\log(2t)/\log\log(2t))ig)$

positive integers $n \leq t$, the polynomial

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

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 $n \leq t$ for which f(x) is reducible for some choice of a_i 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 our next speaker), 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 our next speaker), the argument can now be made effective. What's needed is:

There exist explicit numbers α and $\beta > 0$ such that, for $n \ge \alpha$,

 $n(n+1)=2^k3^\ell m\implies m>n^eta.$

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 $x \ge \alpha$,

 $x^2+7=2^nm\implies m\ge x^{eta}.$

The Hermite Polynomials:

The Hermite Polynomials:

$$egin{aligned} H_n(x) &= (-1)^n e^{x^2/2} rac{d^n ig(e^{-x^2/2} ig)}{dx^n} \ &= \sum_{j=0}^{[n/2]} (-1)^n ig({n \ 2j} ig) u_{2j} x^{m-2j} \end{aligned}$$

where

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

The Hermite Polynomials:

$$egin{aligned} H_{2n}(x) &= (-1)^n u_{2n} \sum_{j=0}^n (-1)^j \binom{n}{j} rac{x^{2j}}{u_{2j}} \ H_{2n+1}(x) &= (-1)^n u_{2n+2} x \sum_{j=0}^n (-1)^j \binom{n}{j} rac{x^{2j}}{u_{2j+2}} \end{aligned}$$

$$egin{aligned} H_{2n}(x) &= (-1)^n u_{2n} \sum_{j=0}^n (-1)^j \binom{n}{j} rac{x^{2j}}{u_{2j}} \ H_{2n+1}(x) &= (-1)^n u_{2n+2} x \sum_{j=0}^n (-1)^j \binom{n}{j} rac{x^{2j}}{u_{2j+2}} \end{aligned}$$

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.

$$egin{aligned} H_{2n}(x) &= (-1)^n u_{2n} \sum_{j=0}^n (-1)^j \binom{n}{j} rac{x^{2j}}{u_{2j}} \ H_{2n+1}(x) &= (-1)^n u_{2n+2} x \sum_{j=0}^n (-1)^j \binom{n}{j} rac{x^{2j}}{u_{2j+2}} \end{aligned}$$

Theorem 4 (I. Schur, 1929): For $n \ge 1$ 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.

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.

E. Gutkin (speaking in the Dynamical Systems session this evening) dealt with a certain billards question.

E. Gutkin (speaking in the Dynamical Systems session this evening) dealt with a certain billards question. J. Lagarias posed a related conjecture at the West Coast Number Theory Conference in 1991:

E. Gutkin (speaking in the Dynamical Systems session this evening) dealt with a certain billards question. J. Lagarias posed a related conjecture at the West Coast Number Theory Conference in 1991:

Let $n \geq 4$ *and*

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

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 (speaking in the Dynamical Systems session this evening) dealt with a certain billards question. J. Lagarias posed a related conjecture at the West Coast Number Theory Conference in 1991:

Let $n \geq 4$ *and*

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

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 $n \ge 1$ 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 $n \qquad 2i$

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

where the a_j 's are arbitrary integers with $|a_0| = 1$. Write $2n + 1 = k' 3^u$ with $3 \nmid k'$

and

$$(2n+1)(2n-1) = k''3^v5^w$$
 with $(k'', 15) = 1$.
If

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

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

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

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

Brief History:

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

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.

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

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.

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

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.

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

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

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

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

is irreducible.

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

- 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

- 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

- 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
 - Thue type 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
$$1 \le k \le n/2$$
, show
 $\prod_{\substack{p^r \parallel (2n-1)(2n-3)\cdots(2n-2k+1)\\p>2k+1}} p^r > 2n-1.$

$$\left(rac{t}{e^t-1}
ight)^lpha e^{xt} = \sum_{n=0}^\infty B_n^{(lpha)}(x)rac{t^n}{n!}$$

$$\left(rac{t}{e^t-1}
ight)^lpha e^{xt} = \sum_{n=0}^\infty B_n^{(lpha)}(x)rac{t^n}{n!}$$

A Special Case:

$$\left(rac{t}{e^t-1}
ight)^lpha e^{xt} = \sum_{n=0}^\infty B_n^{(lpha)}(x)rac{t^n}{n!}$$

A Special Case: $\alpha = n$

$$\left(rac{t}{e^t-1}
ight)^lpha e^{xt} = \sum_{n=0}^\infty B_n^{(lpha)}(x)rac{t^n}{n!}$$

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).

$$\left(rac{t}{e^t-1}
ight)^lpha e^{xt} = \sum_{n=0}^\infty B_n^{(lpha)}(x)rac{t^n}{n!}$$

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 $n \leq t$ for which $B_n^{(n)}(x)$ is Eisenstein is $\mathcal{B}(t)$, then

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