# Different Uses of Diophantine Analysis in the Theory of Irreducibility

Michael Filaseta
University of South Carolina

**Simple Puzzle: What two numbers can be written as a sum with summands from**

$$\{2, 3, 3\}$$

**and also as a sum with summands from**

$$\{1, 3, 4\}$$

**and also as a sum with summands from**

$$\{2, 2, 2, 2\}\,?$$

**Answers:** $\mathbf{8,\ 0}$

# Needed Background: Newton Polygons

## Required Elements:

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

$p$, a prime

## Terminology:

Newton polygon of $f(x)$ (with respect to $p$)

# How to Construct the Newton polygon of $f(x)$

Write $f(x) = \sum_{j=0}^{n} p^{k_j} b_j x^j$ where $p \nmid b_j$ and $b_n b_0 \neq 0$.

Make a grid with width $n = \deg f$ & height $\max\{k_j\}$.

Plot the points $(n - j, k_j)$.

The lower convex hull of these points is the Newton polygon of $f(x)$ with respect to $p$.

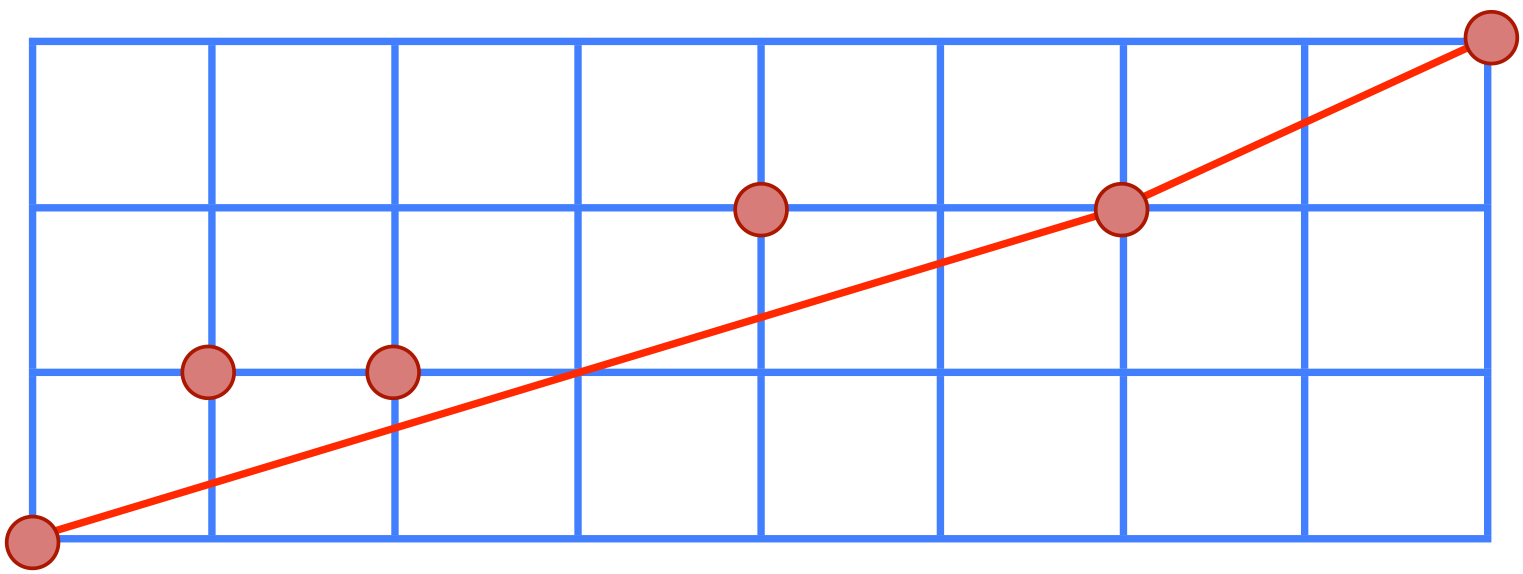
# Now to Try an Example

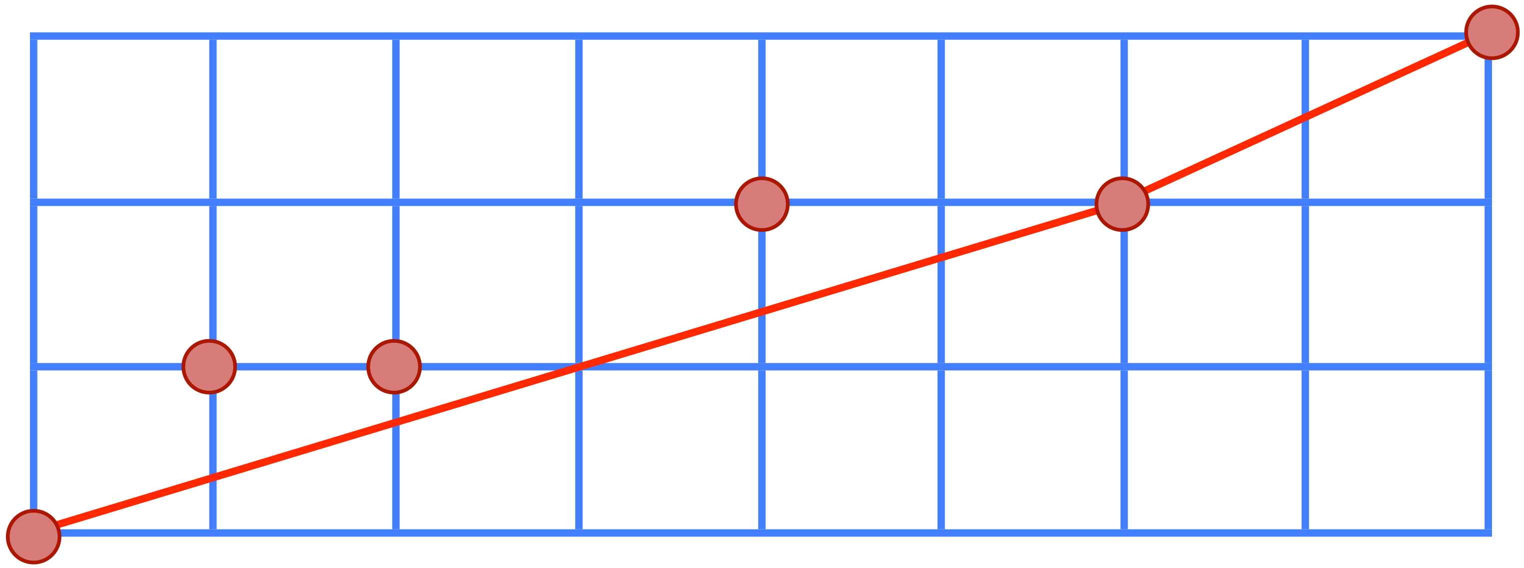
$$f(x) = 42x^8 + 20x^7 + 15x^6 + 150x^4 + 2700x^2 + 81000$$

$$p = 5$$

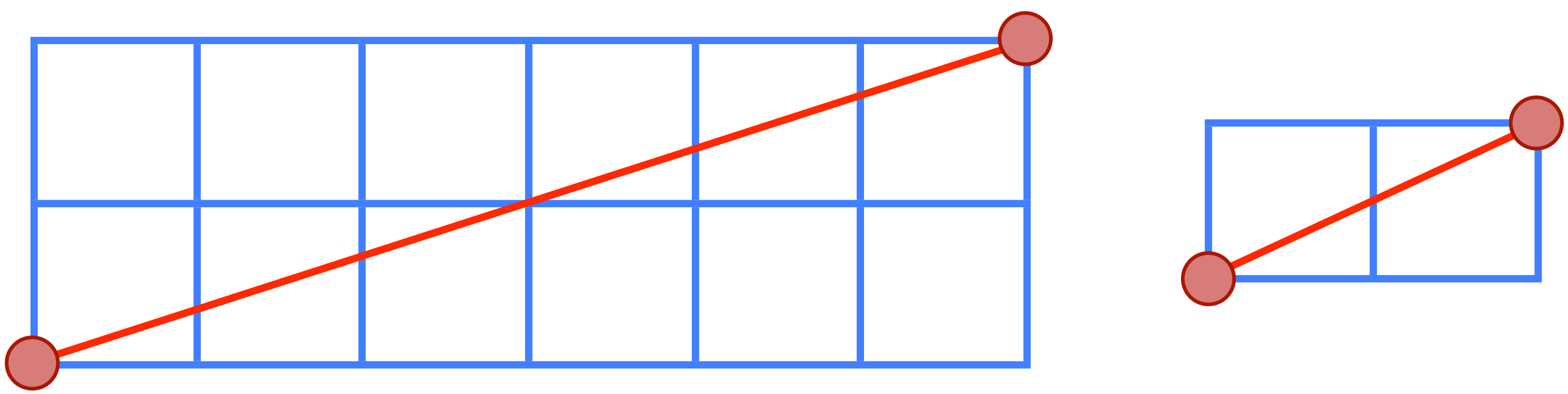
$$5^0 \cdot 42x^8 + 5^1 \cdot 4x^7 + 5^1 \cdot 3x^6 + 5^2 \cdot 6x^4 + 5^2 \cdot 108x^2 + 5^3 \cdot 648$$

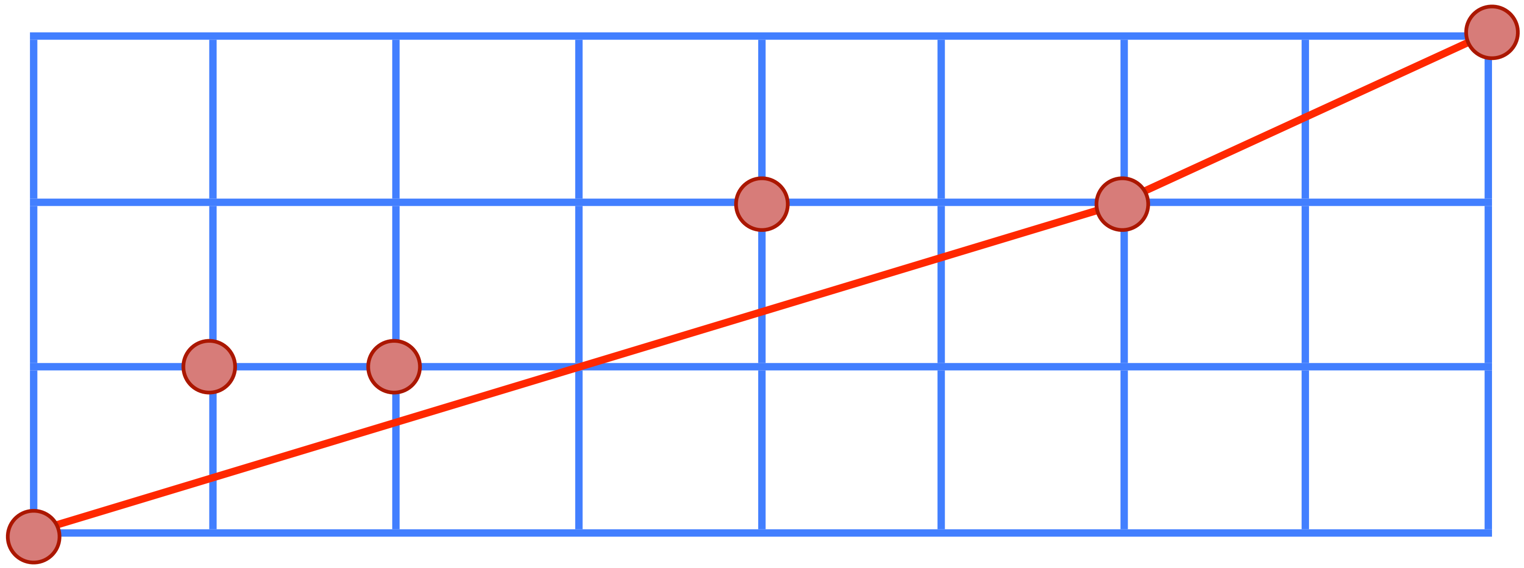
## The Newton polygon of $f(x)$ with respect to 5



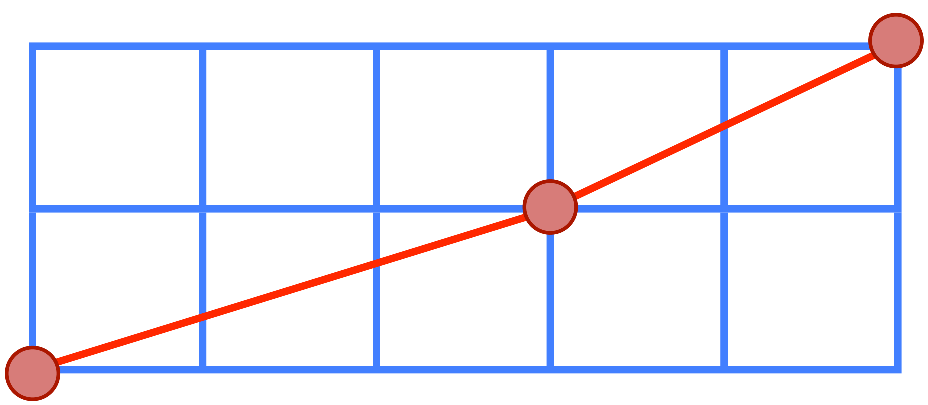


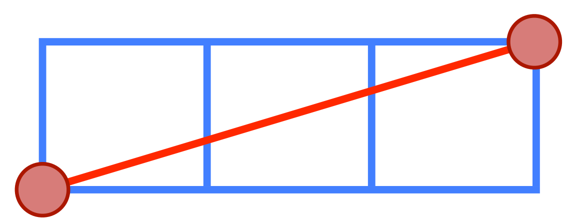
**Dumas' Theorem: The Newton polygon of $g(x)h(x)$ can be formed by translating the edges of the Newton polygons of $g(x)$ and $h(x)$.**

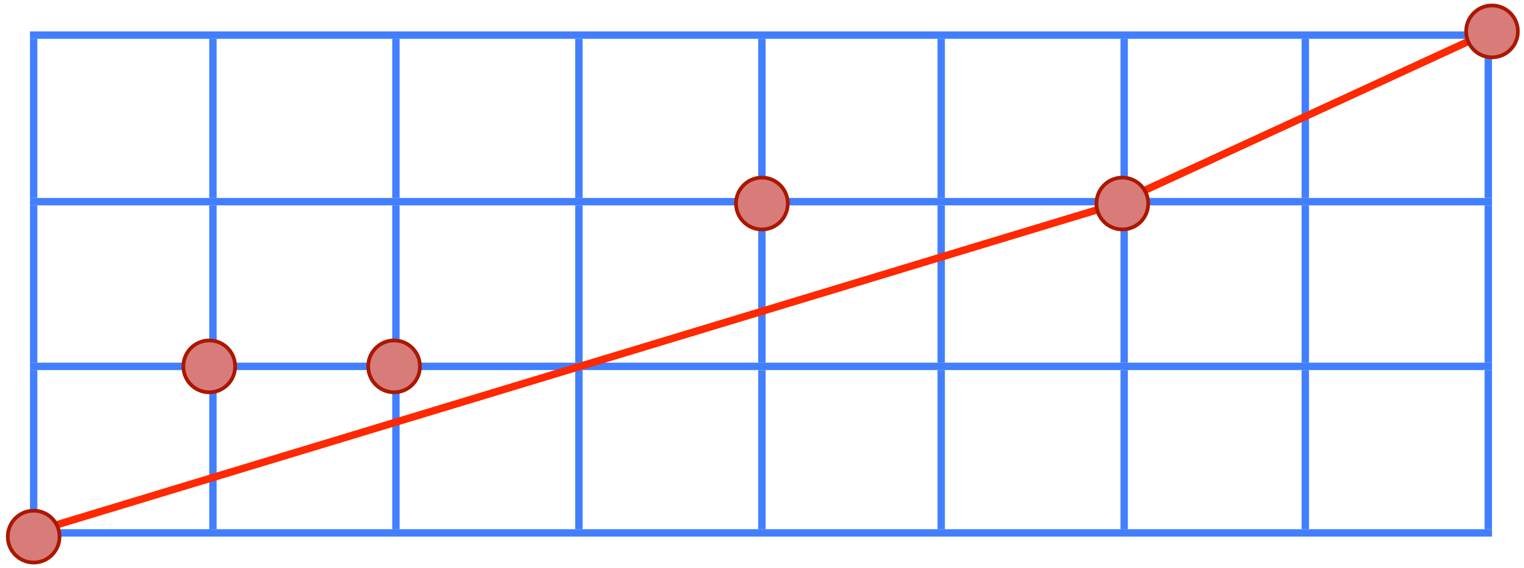




**Dumas' Theorem: The Newton polygon of $g(x)h(x)$ can be formed by translating the edges of the Newton polygons of $g(x)$ and $h(x)$.**



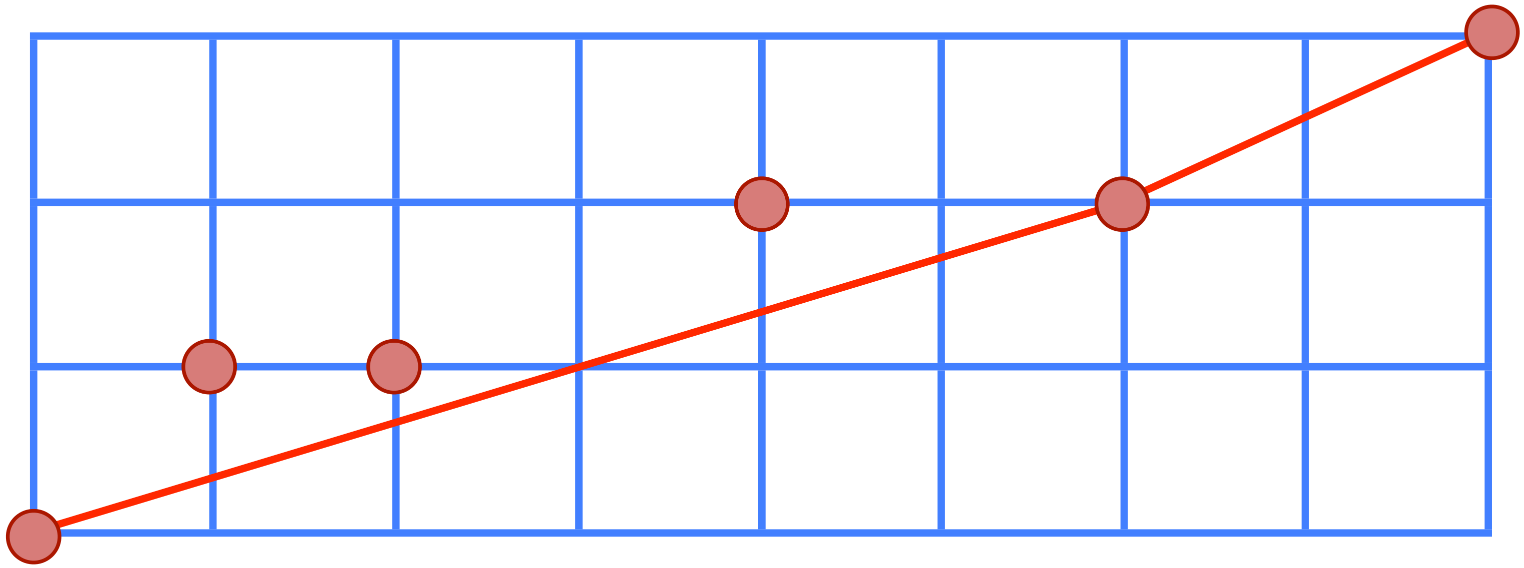




**Dumas' Theorem: The Newton polygon of $g(x)h(x)$ can be formed by translating the edges of the Newton polygons of $g(x)$ and $h(x)$.**

**Recall: The above is the Newton polygon of $f(x)$ with respect to 5.**

**What can we say about quadratic factors of $f(x)$?**



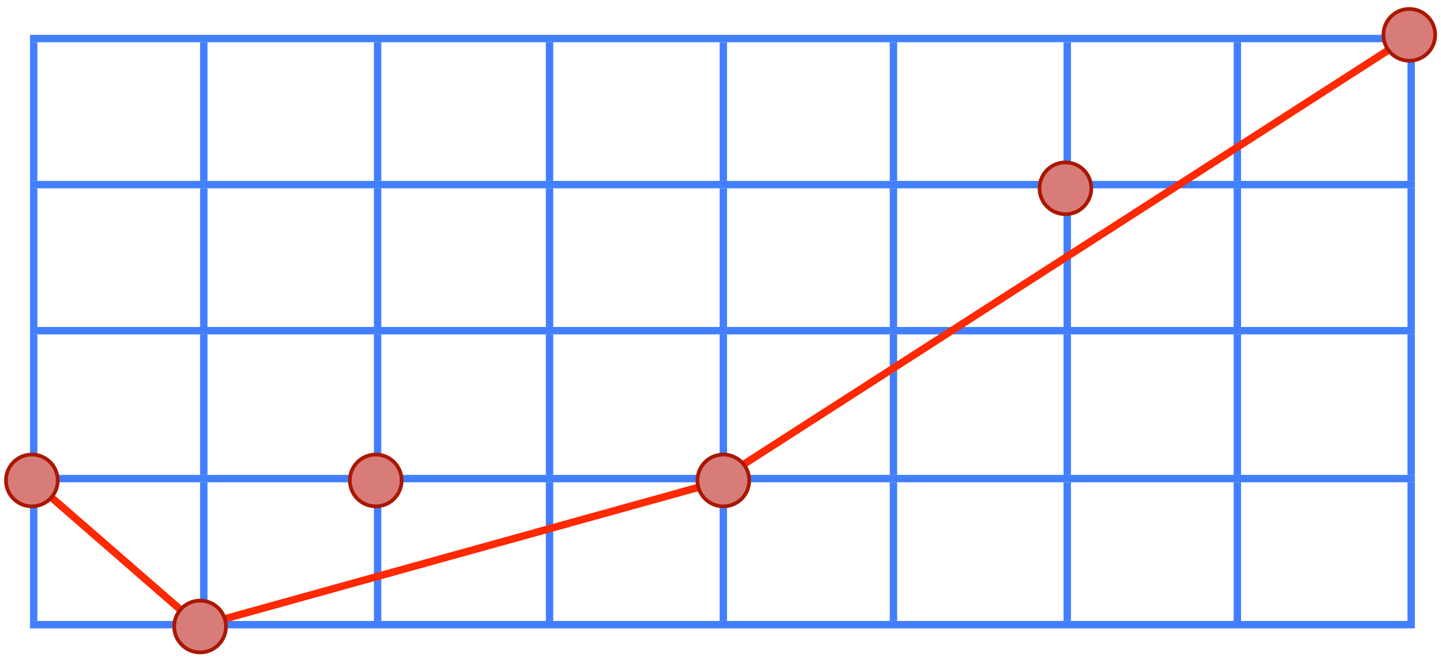
**Dumas' Theorem: The Newton polygon of $g(x)h(x)$ can be formed by translating the edges of the Newton polygons of $g(x)$ and $h(x)$.**

**Note: The degree of a factor of $f(x)$ must be the sum of horizontal distances between consecutive lattice points on any Newton polygon of $f(x)$.**

$$f(x) = 42x^8 + 20x^7 + 15x^6 + 150x^4 + 2700x^2 + 81000$$

$$p = 3$$

**The Newton polygon of $f(x)$ with respect to 3**

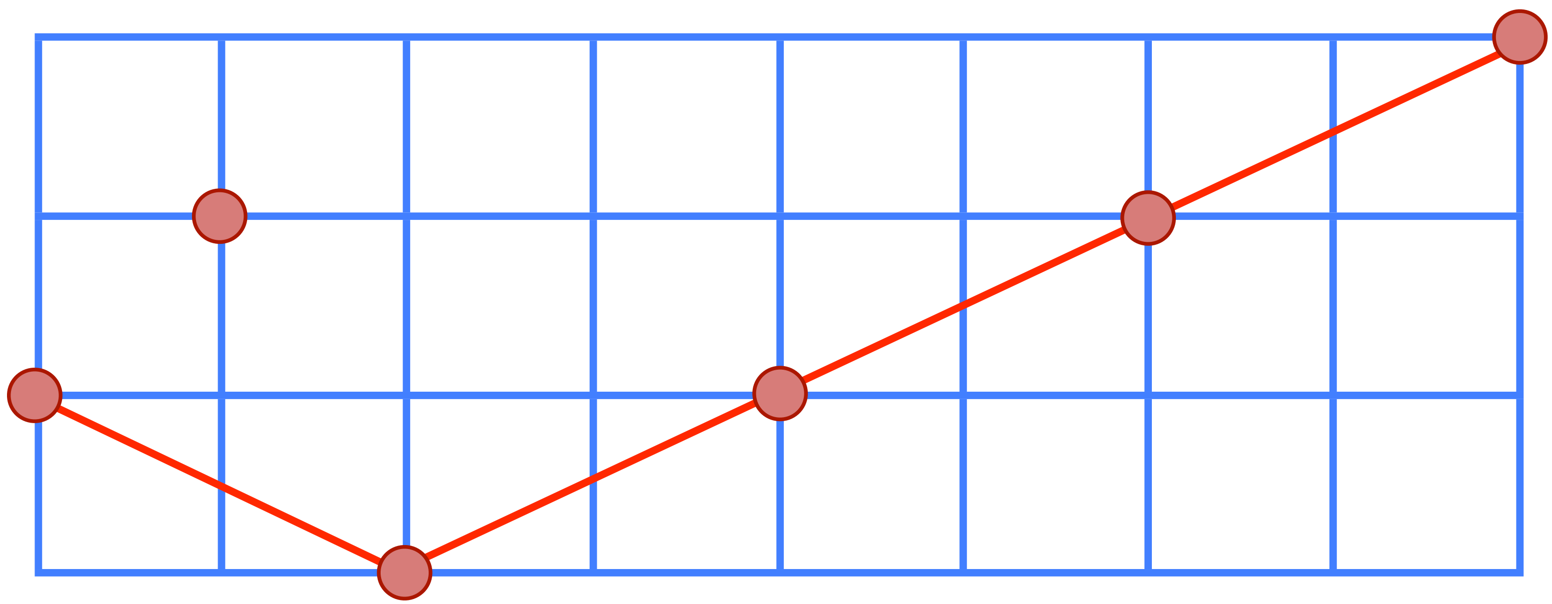


**What can we say about quadratic factors of $f(x)$?**

$$f(x) = 42x^8 + 20x^7 + 15x^6 + 150x^4 + 2700x^2 + 81000$$

$$p = 2$$

**The Newton polygon of $f(x)$ with respect to 2**



**What are the possible degrees of factors of $f(x)$?**

**Simple Puzzle: What two numbers can be written as a sum with summands from**

$$\{2, 3, 3\}$$

**and also as a sum with summands from**

$$\{1, 3, 4\}$$

**and also as a sum with summands from**

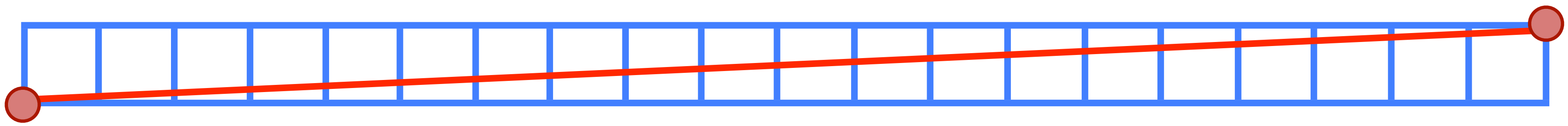
$$\{2, 2, 2, 2\}\,?$$

$$f(x) = 42x^8 + 20x^7 + 15x^6 + 150x^4 + 2700x^2 + 81000$$

**is irreducible**

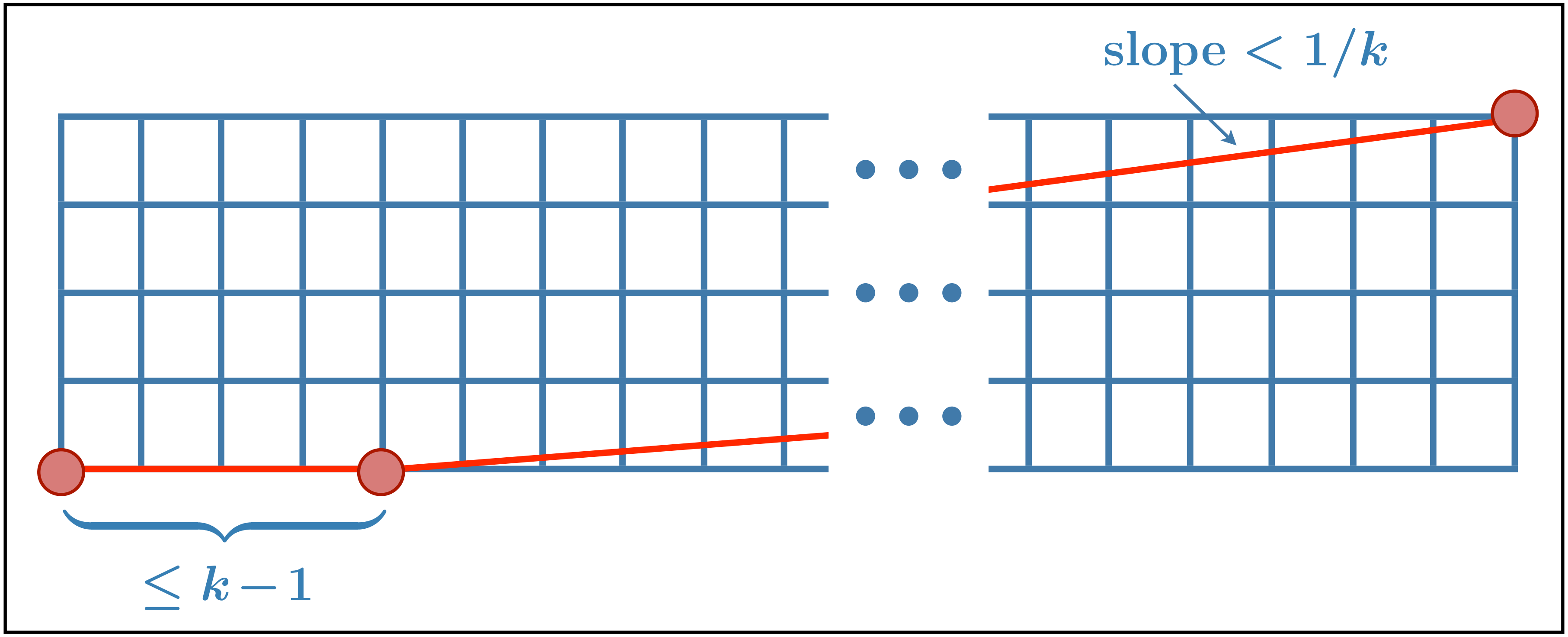
**Eisenstein's Criterion:** If $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$ and there is a prime $p$ such that $p \nmid a_n$, $p | a_j$ for $j < n$, and $p^2 \nmid a_0$, then $f$ is irreducible over $\mathbb{Q}[x]$.

**Eisenstein's Criterion Restated:** If $f \in \mathbb{Z}[x]$ and the Newton polygon of $f$ with respect to $p$ looks something like

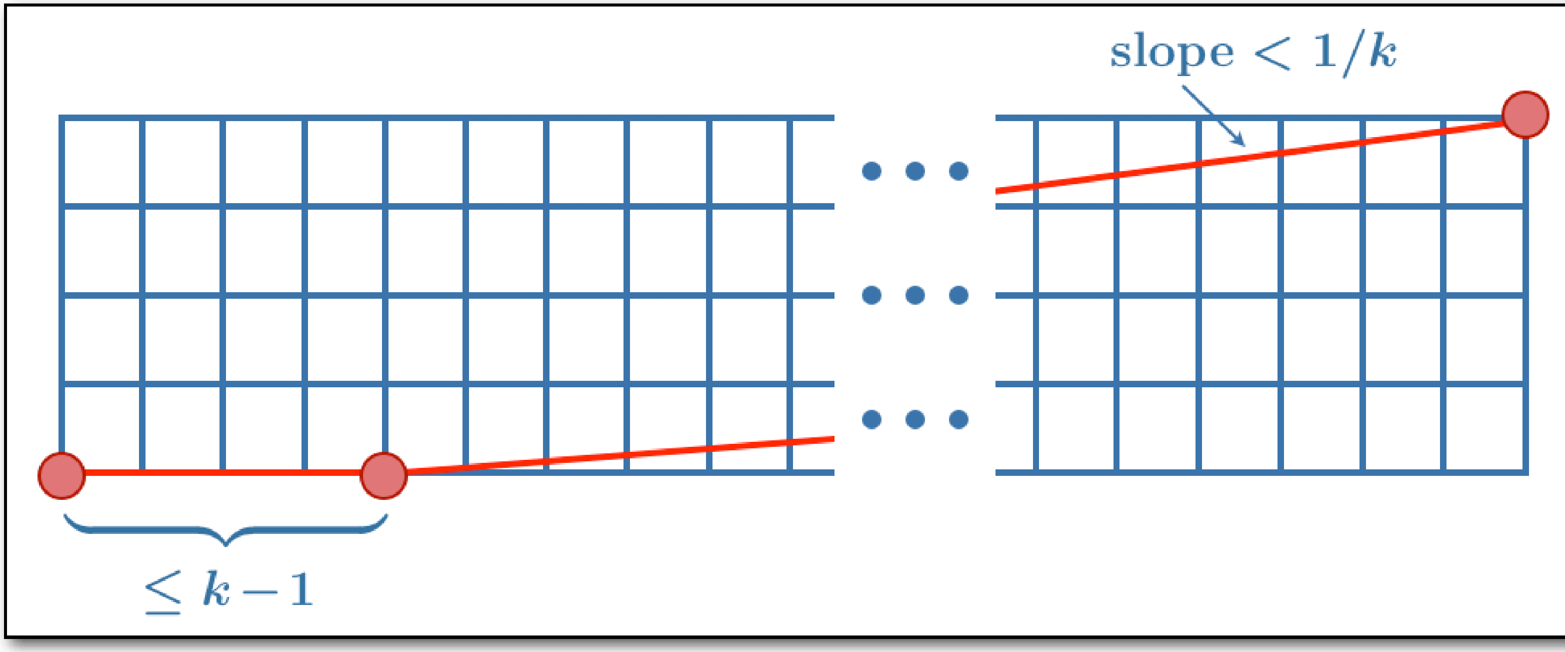


then $f$ is irreducible over $\mathbb{Q}$.

**Example:** **Let $f(x) \in \mathbb{Z}[x]$ and $k$ be a positive integer. Suppose for some prime $p$ the Newton polygon of $f(x)$ with respect to $p$ looks like:**




**Then $f(x)$ cannot have a factor of degree $k$.**




**If $(a, b)$ and $(c, d)$, with $a < c$, are two lattice points on an edge with positive slope, then**

$$\frac{1}{c-a} \leq \frac{d-b}{c-a} < \frac{1}{k} \quad \Longrightarrow \quad c-a > k.$$

**Thus, $f(x)$ cannot have a factor of degree $k$ as the horizontal distances between lattice points can't sum to $k$.**

**Theorem (I. Schur):** *Let $a_n, a_{n-1}, \ldots, a_0$ denote arbitrary integers with $|a_n| = |a_0| = 1$. Then*

$$a_n \frac{x^n}{n!} + a_{n-1} \frac{x^{n-1}}{(n-1)!} + \cdots + a_2 \frac{x^2}{2!} + a_1 x + a_0$$

*is irreducible over $\mathbb{Q}$.*

**Notes:**

**Schur (1929) used prime ideals in number fields but with a "hint" of Newton polygons.**

**Coleman (1987): Used Newton polygons for $a_j = 1$.**

**Both obtained information about the Galois groups.**

$$f(x) = \pm\frac{x^n}{n!} + a_{n-1}\frac{x^{n-1}}{(n-1)!} + \cdots + a_2\frac{x^2}{2!} + a_1 x \pm 1$$

Assume $n! \cdot f(x)$ has a factor of degree $k \in [1, n/2]$.

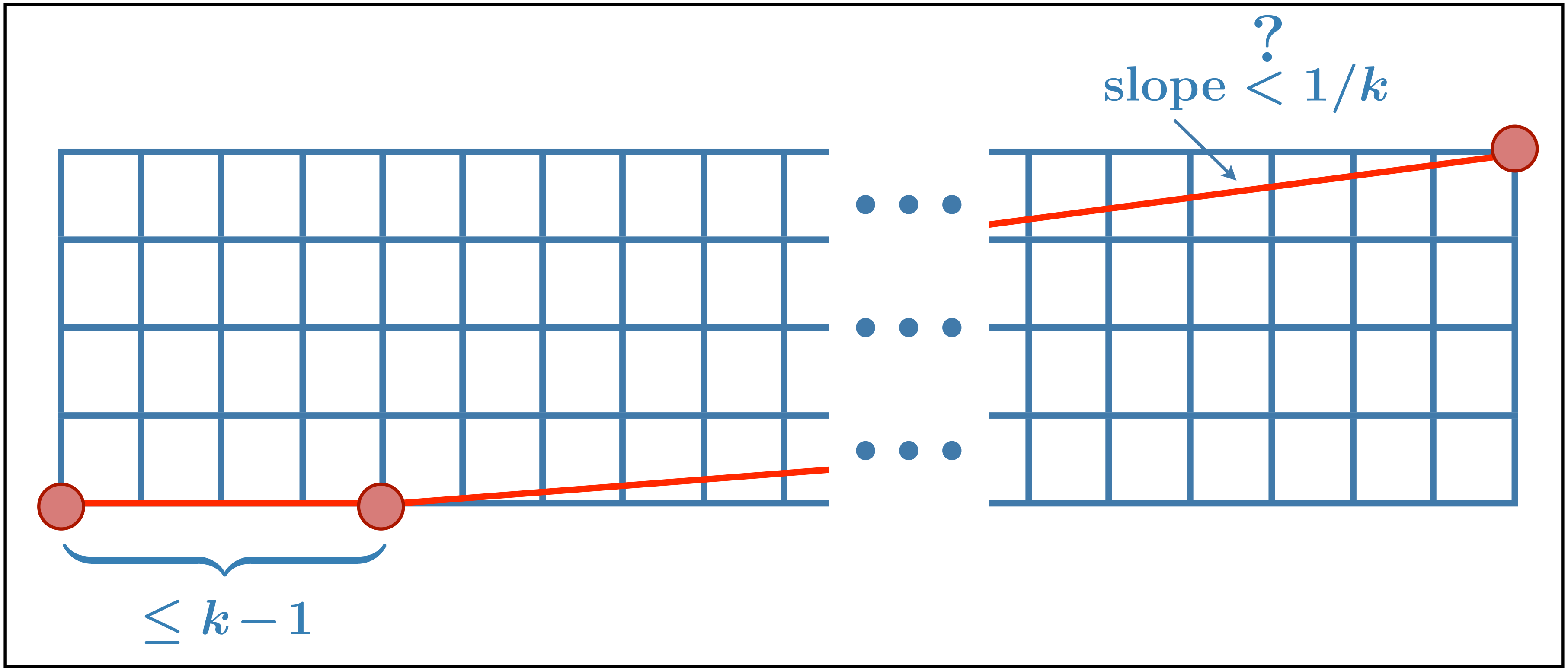
The coefficient of $x^{n-j}$ is $a_{n-j}n(n-1)\cdots(n-j+1)$.

Sylvester (1892) showed that the product of $k$ consecutive integers $> k$ has a prime factor $> k$.

Hence, there is a prime $p \geq k+1$ dividing

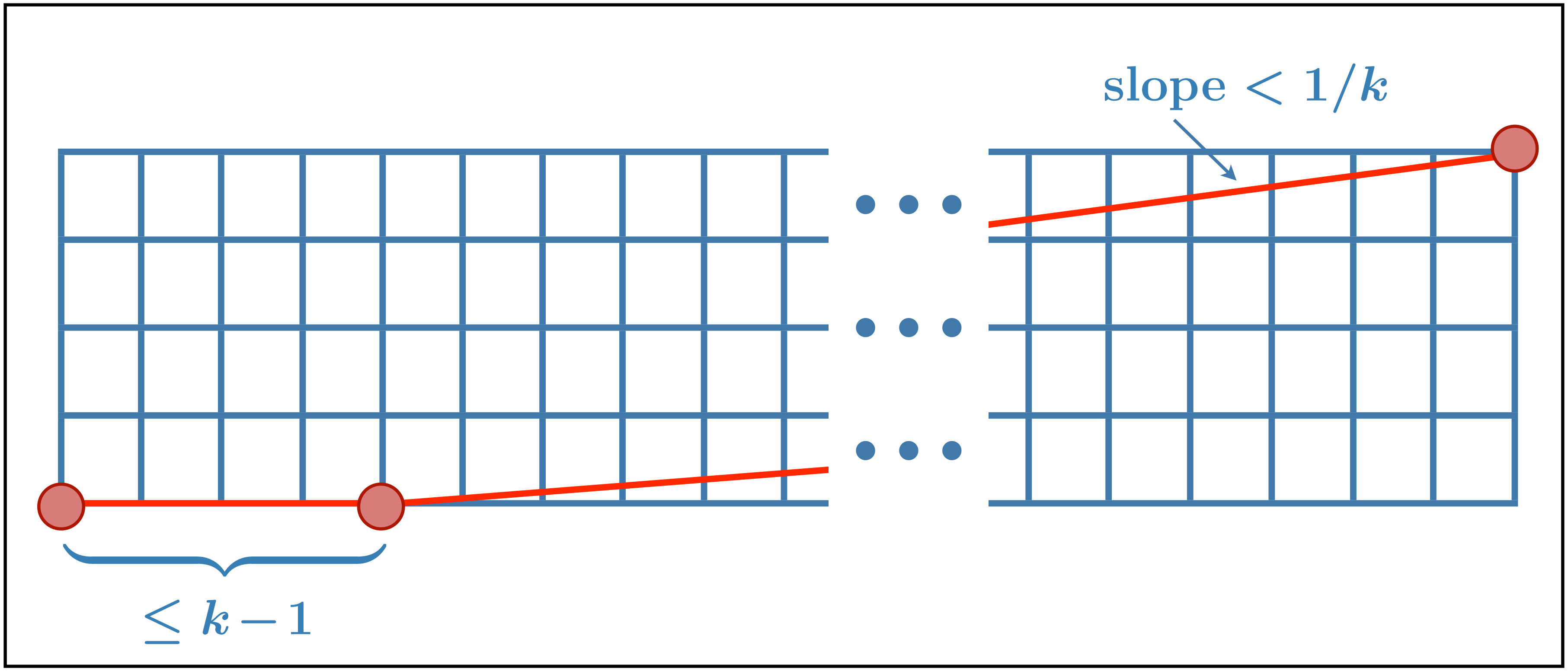
$$n(n-1)(n-2)\cdots(n-k+1).$$

Note: $p | a_{n-j}n(n-1)\cdots(n-j+1)$ for each $j \geq k$.




$$\text{slope} = \max\left\{\frac{\nu_p(n!) - \nu_p(a_j n!/j!)}{j}\right\} \leq \max\left\{\frac{\nu_p(j!)}{j}\right\}$$

$$= \max\left\{\frac{1}{j}\sum_{u=1}^{\infty}\left[\frac{j}{p^u}\right]\right\} < \frac{1}{p-1} \leq \frac{1}{k} \quad \blacksquare$$




**Two Important Properties of the Prime $p$:**

- $p | n(n-1)\cdots(n-k+1)$ (so left part is $\leq k-1$)
- $p$ is large (so that the right slope is $< 1/k$)

**Theorem (F., 1996):** *Let $a_n, a_{n-1}, \ldots, a_0$ denote arbitrary integers with $|a_0| = 1$ and $0 < |a_n| < n$. Then*

$$a_n \frac{x^n}{n!} + a_{n-1} \frac{x^{n-1}}{(n-1)!} + \cdots + a_2 \frac{x^2}{2!} + a_1 x + a_0$$

*is irreducible over the rationals unless*

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

**Comment: The result is "best" possible.**

**Lemma:** Let $k$ be an integer $\in [2, n/2]$. Then

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

unless one of the following holds:

$$\begin{aligned}
n &= 12 &\quad \text{and} &\quad k = 5\\
n &= 10 &\quad \text{and} &\quad k = 5\\
n &= 9 &\quad \text{and} &\quad k = 4\\
n &= 18 &\quad \text{and} &\quad k = 3\\
n &= 10 &\quad \text{and} &\quad k = 3\\
n &= 9 &\quad \text{and} &\quad k = 3\\
n &= 8 &\quad \text{and} &\quad k = 3\\
n &= 6 &\quad \text{and} &\quad k = 3\\
n &= 2^\ell + 1 &\quad \text{and} &\quad k = 2\\
n &= 2^\ell &\quad \text{and} &\quad k = 2,
\end{aligned}$$

where $\ell$ represents an arbitrary positive integer.

**Theorem (M. Allen & F., 2004):** *Let $a_n, a_{n-1}, \dots,$ $a_0$ denote arbitrary integers with $a_0 = \pm 1$ and $0 < |a_n| < 2n - 1$. Then*

$$\sum_{j=0}^{n} a_j \frac{x^{2j}}{\prod_{1 \le u \le j} (2u - 1)}$$

*is irreducible over the rationals.*

**Lemma:** Let $k$ be an odd integer in $[3, n]$. Then

$$\prod_{\substack{p^r \| (2n-1)(2n-3)\cdots(2n-k) \\ p \ge k+2}} p^r > 2n - 1$$

unless one of the following conditions hold:

$k = 3$ and either $2n - 1$ or $2n - 3$ is a power of 3

$k = 5$ and $n \in \{5, 14, 15\}$

$k = 7$ and $n = 14$

**Lemma (D. H. Lehmer, 1964):** Let $P(m)$ denote the largest prime factor of $m$. If $m$ is an odd positive integer $> 243$, then

$$P(m(m+2)) \ge 11 \quad \text{and} \quad P(m(m+4)) \ge 11.$$

$$f(x) = \sum_{j=0}^{n} \frac{(n+j)!}{2^j (n-j)! j!} x^j \qquad \text{(Bessel polynomials)}$$

**Lemma:** *Let $n$ be a positive integer. Suppose that $p$ is a prime and that $k$ and $r$ are positive integers for which:*

*(i)* $p^r \| n(n-1)\cdots(n-k+1)$

*(ii)* $p \geq 2k+1$

*(iii)* $\dfrac{\log(2n)}{p^r \log p} + \dfrac{1}{p-1} \leq \dfrac{1}{k}$

*Then $f(x)$ cannot have a factor of degree $k$.*

**Lemma:** *Let $n$ be a positive integer. Suppose that $p$ is a prime and that $k$ and $r$ are positive integers for which:*

*(i)* $p^r \| n(n-1)\cdots(n-k+1)$

*(ii)* $p \geq 2k+1$

*(iii)* $$\frac{\log(2n)}{p^r \log p} + \frac{1}{p-1} \leq \frac{1}{k}$$

*Then $f(x)$ cannot have a factor of degree $k$.*

**Idea:** Use similar lemmas and consider different ranges of $k \in [1, n/2]$. The larger $p$ is the better. So take advantage of information concerning large prime factors of $n(n-1)\cdots(n-k+1)$.

**Theorem (O. Trifonov & F., 2002):** *Let $n$ denote a positive integer, and let $a_0, a_1, \dots, a_n$ be 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 over the rationals.*

## The Generalized Laguerre Polynomials

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

$$L_n^{(-n-1)}(x) = (-1)^n\left(\frac{x^n}{n!}+\frac{x^{n-1}}{(n-1)!}+\cdots+\frac{x^2}{2!}+x+1\right)$$

$$\left(\frac{x}{2}\right)^n L_n^{(-2n-1)}\left(\frac{2}{x}\right) = \frac{(-1)^n}{n!}\cdot\sum_{j=0}^{n}\frac{(n+j)!}{2^j(n-j)!j!}x^j$$

(pointed out to me by F. Hajir)

**Brief History:** D. Hilbert (1892) showed, using what is now Hilbert's Irreducibility Theorem, that for $n$ a positive integer, there are polynomials in $Q[x]$ with Galois group over $\mathbb{Q}$ the symmetric group $S_n$ and polynomials in $Q[x]$ with Galois group over $\mathbb{Q}$ the alternating group $A_n$. His proof was not constructive. B. L. van der Waerden (1934) showed that almost all polynomials in $\mathbb{Z}[x]$ have Galois group $S_n$. In the late 1920's and early 1930's, I. Schur showed that

$$n \equiv 1 \pmod{2} \Longrightarrow L_n^{(1)}(x) \text{ has Galois group } A_n$$

$$n \equiv 0 \pmod{4} \Longrightarrow L_n^{(-n-1)}(x) \text{ has Galois group } A_n$$

R. Gow (1989) showed if $n \equiv 2 \pmod{4}$ and $L_n^{(n)}(x)$ is irreducible, then $L_n^{(n)}(x)$ has Galois group $A_n$.

**Theorem (T. Kidd, O. Trifonov, F.):** *For every integer $n > 2$ with $n \equiv 2 \pmod 4$, the polynomial $L_n^{(n)}(x)$ is irreducible over $\mathbb{Q}$.*

**Comment:** In addition to lemmas similar to those needed for the previous irreducibility results, the following was important, in particular, to establish that $L_n^{(n)}(x)$ does not have a small degree factor.

**Lemma (M. Bennett, O. Trifonov, F.):** Let $m$ be a positive integer not in the set $\{1, 2, 3, 8\}$. Then $m(m+1)$ has a divisor that is relatively prime to 6 and greater than $m^{0.27}$.

**Theorem (T. Kidd, O. Trifonov, F.):** *For every integer $n > 2$ with $n \equiv 2 \pmod 4$, the polynomial $L_n^{(n)}(x)$ is irreducible over $\mathbb{Q}$.*

**Comment:** In addition to lemmas similar to those needed for the previous irreducibility results, the following was important, in particular, to establish that $L_n^{(n)}(x)$ does not have a small degree factor.

**Lemma (M. Bennett, O. Trifonov, F.):** Let $m$ be a positive integer not in the set $\{1, 2, 3, 8\}$. Then

$$\prod_{\substack{p^r \| m(m+1) \\ p \ge 5}} p^r \ge m^{0.27}.$$

## A Similar (but Seemingly Hard) Diophantine Problem

"More" could be said about the irreducibility of

$$\sum_{j=0}^{n} a_j \frac{x^{2j}}{\prod_{1 \le u \le j} (2u+1)}$$

with an effective version of the

**Lemma:** For $n$ a sufficiently large integer,

$$\prod_{\substack{p^r \| (2n+1)(2n-1)(2n-3) \\ p \ge 11}} p^r > 2n+1.$$