

# A Walk through Irreducible Polynomials over $\mathbb{Q}$

Sudesh K. Khanduja

Sudesh Kaur Khanduja  
INSA Honorary Scientist, IISER, Mohali (INDIA)  
and

Emeritus Professor, Dept. of Mathematics, Panjab University, Chandigarh  
Email : [skhanduja@iisermohali.ac.in](mailto:skhanduja@iisermohali.ac.in), [sudeshkaur@yahoo.com](mailto:sudeshkaur@yahoo.com)



# Dedicated to Professor Sudhir Ghorpade on his 60th Birthday



Prof. Sudhir Ghorpade

# Irreducible polynomials

## Definition

The degree of a non-zero polynomial  $a_0 + a_1x + \dots + a_nx^n$  in a variable  $x$  is defined to be  $n$  when  $a_n \neq 0$ . The degree of the zero polynomial is defined to be  $-\infty$ .

The degree of a non-zero polynomial  $\sum_{i,j} a_{ij}x^i y^j$  in two variables  $x, y$  is defined to be  $\max\{i + j \mid a_{ij} \neq 0\}$ . A constant polynomial is either a zero polynomial or has degree 0.

## Definition

A polynomial of degree  $n \geq 1$  in one or more variables with coefficients in a field  $\mathbb{F}$  is said to be irreducible over  $\mathbb{F}$  if it cannot be written as a product of two polynomials over  $\mathbb{F}$  of degree less than  $n$ .

- Every polynomial of degree one is irreducible.
- $x^2 + 1$  is irreducible over  $\mathbb{R}$  but reducible over  $\mathbb{C}$ .
- $x^2 + x + 1$  is reducible over the field of three elements.

# Uses of polynomials

- Irreducible polynomials are building blocks for all polynomials.
- Polynomials are used to define finite fields.
- Roller coaster designers can use polynomials to describe the curves of the rides.
- Engineers use polynomials to graph the curves of bridges.
- In hospitals, polynomials are used to keep records of patients' progress.
- Polynomials of several variables are useful for studying Quantum Information Theory.

## The Fundamental Theorem of Algebra (Gauss, 1797)

*An irreducible polynomial over  $\mathbb{R}$  has degree one or two.*



Gauss (1777 - 1855)

## Eisenstein Irreducibility Criterion (1850)

Let  $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$  be a polynomial with coefficients in the ring  $\mathbb{Z}$  of integers. Suppose that there exists a prime number  $p$  such that

- $a_n$  is not divisible by  $p$ ,
- $a_i$  is divisible by  $p$  for  $0 \leq i \leq n-1$ ,
- $a_0$  is not divisible by  $p^2$ .

Then  $f(x)$  is irreducible over the field  $\mathbb{Q}$  of rational numbers.



Eisenstein (1823 - 1852)

A polynomial which satisfies the above three conditions is called an **Eisenstein polynomial** with respect to prime  $p$ .

## Example

For a prime number  $p$ , consider the  $p^{\text{th}}$  cyclotomic polynomial

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1 = \frac{x^p - 1}{x - 1}.$$

$$\Phi_p(x+1) = \frac{(x+1)^p - 1}{x} = x^{p-1} + \binom{p}{1}x^{p-2} + \cdots + \binom{p}{p-1}$$

is irreducible over  $\mathbb{Q}$  by Eisenstein Irreducibility Criterion.

## Question

When is some translate  $f(x+c)$  of a given polynomial  $f(x) \in \mathbb{Z}[x]$  an Eisenstein polynomial with respect to a prime  $p$ ?

## Classical Dumas Irreducibility Criterion (1906)

Let  $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$  be a polynomial with coefficients in  $\mathbb{Z}$ . Suppose there exists a prime  $p$  whose highest power  $p^{r_i}$  dividing  $a_i$  (where  $r_i = \infty$  if  $a_i = 0$ ),  $0 \leq i \leq n$ , satisfy

- $r_n = 0$ ,
- $r_i/(n-i) \geq r_0/n$  for  $1 \leq i \leq n-1$  and
- $\gcd(r_0, n) = 1$ .

Then  $f(x)$  is irreducible over  $\mathbb{Q}$ .



Gustave Dumas (1872- 1955)

- Note that Eisenstein Irreducibility criterion is a special case of the above criterion with  $r_0 = 1$ .

### Example

$x^3 + 3x^2 + 9x + 9$  is irreducible over  $\mathbb{Q}$ .



## Classical Dumas Irreducibility Criterion (1906)

Let  $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$  be a polynomial with coefficients in  $\mathbb{Z}$ . Suppose there exists a prime  $p$  whose highest power  $p^{r_i}$  dividing  $a_i$  (where  $r_i = \infty$  if  $a_i = 0$ ),  $0 \leq i \leq n$ , satisfy

- $r_n = 0$ ,
- $r_i/(n-i) \geq r_0/n$  for  $1 \leq i \leq n-1$  and
- $\gcd(r_0, n) = 1$ .

Then  $f(x)$  is irreducible over  $\mathbb{Q}$ .



Gustave Dumas (1872- 1955)

- Note that Eisenstein Irreducibility criterion is a special case of the above criterion with  $r_0 = 1$ .

### Example

$x^3 + 3x^2 + 9x + 9$  is irreducible over  $\mathbb{Q}$ .

## Notation

Let  $p$  be a prime number. For any non-zero integer  $c$ ,  $v_p(c)$  will denote the highest power of  $p$  dividing  $c$ . Set  $v_p(0) = \infty$ . The map  $v_p$  satisfies the following properties for all  $a, b \in \mathbb{Z}$ :

$$(i) \quad v_p(ab) = v_p(a) + v_p(b),$$

$$(ii) \quad v_p(a+b) \geq \min\{v_p(a), v_p(b)\}.$$

$v_p$  is called the  $p$ -adic valuation of integers.

## Classical Dumas Irreducibility Criterion

Let  $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$  be a polynomial with coefficients in  $\mathbb{Z}$ . Suppose there exists a prime number  $p$  such that

- $v_p(a_n) = 0$ ,
- $v_p(a_i)/(n-i) \geq v_p(a_0)/n$  for  $1 \leq i \leq n-1$
- $v_p(a_0)$  is coprime to  $n$ , then  $f(x)$  is irreducible over  $\mathbb{Q}$ .

A polynomial which satisfies the above three conditions is called an Eisenstein-Dumas polynomial with respect to prime  $p$ .

In 1923, Classical Dumas Irreducibility Criterion was extended to polynomials over more general fields namely, fields with discrete valuations by Kürschák. Indeed it was the Hungarian Mathematician JOSEPH KÜRSCHÁK who gave the formal definition of the notion of valuation of a field in 1912.

## Classical Dumas Irreducibility Criterion

Let  $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$  be a polynomial with coefficients in  $\mathbb{Z}$ . Suppose there exists a prime number  $p$  such that

- $v_p(a_n) = 0$ ,
- $v_p(a_i)/(n-i) \geq v_p(a_0)/n$  for  $1 \leq i \leq n-1$
- $v_p(a_0)$  is coprime to  $n$ , then  $f(x)$  is irreducible over  $\mathbb{Q}$ .

A polynomial which satisfies the above three conditions is called an **Eisenstein-Dumas polynomial** with respect to prime  $p$ .

In 1923, Classical Dumas Irreducibility Criterion was extended to polynomials over more general fields namely, fields with discrete valuations by Kürschák. Indeed it was the Hungarian Mathematician **JOSEPH KÜRSCHÁK** who gave the formal definition of the notion of valuation of a field in 1912.

## Definition

A real valuation  $v$  of a field  $K$  is a mapping  $v : K \rightarrow \mathbb{R} \cup \{\infty\}$  satisfying

- (i)  $v(a) = \infty \iff a = 0$ ,
- (ii)  $v(ab) = v(a) + v(b)$ ,
- (iii)  $v(a+b) \geq \min\{v(a), v(b)\}$ .

The pair  $(K, v)$  is called a **valued field**. The set  $R_v = \{a \in K \mid v(a) \geq 0\}$  is a subring of  $K$  called the **valuation ring** of  $v$ ; it has unique maximal ideal  $m_v$  given by

$$m_v = \{a \in K \mid v(a) > 0\}.$$

$R_v/m_v$  is called the **residue field** of  $v$  and  $v(K^\times)$  the **value group** of  $v$ . A valuation  $v$  of  $K$  is said to be **discrete** if the group  $v(K^\times)$  is isomorphic to  $\mathbb{Z}$ .

# When is a translate an Eisenstein-Dumas polynomial?

## Theorem (-, A. Bishnoi, 2010)

Let  $g(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$  be a polynomial with coefficients in  $\mathbb{Z}$ . Let  $p$  be a prime number coprime with  $na_n$ . If there exists an integer  $c$  such that  $g(x+c)$  is an Eisenstein-Dumas polynomial with respect to  $p$ , then so is  $n^n g(x - \frac{a_{n-1}}{n})$ .



Anuj Bishnoi

## Classical Schönemann Irreducibility Criterion (1846)

Let  $\phi(x)$  belonging to  $\mathbb{Z}[x]$  be a monic polynomial which is irreducible modulo a given prime  $p$ . Let  $f(x)$  belonging to  $\mathbb{Z}[x]$  be of the form  $f(x) = \phi(x)^n + pM(x)$  where  $M(x) \in \mathbb{Z}[x]$  has degree less than  $n \deg \phi(x)$ . If  $\phi(x)$  is coprime to  $M(x)$  modulo  $p$ , then  $f(x)$  is irreducible in  $\mathbb{Q}[x]$ .

Eisenstein Irreducibility Criterion is easily seen to be a particular case of Schönemann Criterion by setting  $\phi(x) = x$ .

## Classical Schönemann Irreducibility Criterion (1846)

Let  $\phi(x)$  belonging to  $\mathbb{Z}[x]$  be a monic polynomial which is irreducible modulo a given prime  $p$ . Let  $f(x)$  belonging to  $\mathbb{Z}[x]$  be of the form  $f(x) = \phi(x)^n + pM(x)$  where  $M(x) \in \mathbb{Z}[x]$  has degree less than  $n \deg \phi(x)$ . If  $\phi(x)$  is coprime to  $M(x)$  modulo  $p$ , then  $f(x)$  is irreducible in  $\mathbb{Q}[x]$ .

Eisenstein Irreducibility Criterion is easily seen to be a particular case of Schönemann Criterion by setting  $\phi(x) = x$ .



# Restatement of Schönemann Criterion

Let  $R$  be an integral domain and  $\phi(x) \in R[x]$  be a monic polynomial. Then on dividing by successive powers of  $\phi(x)$ , every polynomial  $f(x) \in R[x]$  can be uniquely written as a finite sum  $\sum_{i \geq 0} f_i(x)\phi(x)^i$  with  $\deg f_i(x) < \deg \phi(x)$  called the  $\phi(x)$ -expansion of  $f(x)$ .

## Schönemann Irreducibility Criterion

Let  $\phi(x)$  belonging to  $\mathbb{Z}[x]$  be a monic polynomial which is irreducible modulo a given prime  $p$ . Let  $f(x)$  belonging to  $\mathbb{Z}[x]$  be a monic polynomial having  $\phi(x)$ -expansion  $\sum_{i=0}^n f_i(x)\phi(x)^i$  with  $f_n(x) = 1$ . If  $p$  divides the content of  $f_i(x)$  for  $0 \leq i < n$  and  $p^2$  does not divide the content of  $f_0(x)$ , then  $f(x)$  is irreducible over  $\mathbb{Q}$ .

## Example

The polynomial  $(x^2 + 1)^3 + 3(b_1x + b_2)(x^2 + 1)^2 + 3(c_1x + c_2)(x^2 + 1) + 3(d_1x + d_2)$  is irreducible over  $\mathbb{Q}$  for all integers  $b_1, b_2, c_1, c_2, d_1, d_2$ , with 3 not dividing at least one of  $d_1, d_2$  in view of Schönemann Irreducibility Criterion.

# Generalised Schönemann Irreducibility Criterion

For a prime  $p$ , we shall denote by  $v_p^x$  the **Gaussian valuation** extending  $v_p$  defined on the polynomial ring  $\mathbb{Z}[x]$  by

$$v_p^x\left(\sum_i c_i x^i\right) = \min_i \{v_p(c_i)\}, \quad c_i \in \mathbb{Z}.$$

Note that for  $g(x) \in \mathbb{Z}[x]$ ,  $v_p^x(g(x)) = v_p(\text{content}(g(x)))$ .

## Generalised Schönemann Irreducibility Criterion (Ore 1928, Brown 2008)

Let  $\phi(x)$  belonging to  $\mathbb{Z}[x]$  be a monic polynomial which is irreducible modulo a fixed prime  $p$ . If the  $\phi$ -expansion of a polynomial  $f(x)$  belonging to  $\mathbb{Z}[x]$  given by

$$\sum_{i=0}^n f_i(x)\phi(x)^i \text{ satisfies}$$

- (i)  $f_0(x) \neq 0$ ,  $f_n(x)$  is a constant polynomial not divisible by  $p$ ,
- (ii)  $\frac{v_p^x(f_i(x))}{n-i} \geq \frac{v_p^x(f_0(x))}{n} > 0$  for  $0 \leq i \leq n-1$ ,
- (iii)  $v_p^x(f_0(x))$  and  $n$  are coprime,

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

# Newton polygon with respect to a prime $p$

Let  $p$  be a prime number and  $v_p$  denote the  $p$ -adic valuation.

- Let  $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$  with  $a_0 a_n \neq 0$ .
- Let  $P_i$  stand for the point in the plane having the coordinates  $(i, v_p(a_{n-i}))$  when  $a_{n-i} \neq 0$ ,  $0 \leq i \leq n$ .
- Let  $\mu_{ij}$  denote the slope of the line joining  $P_i$  and  $P_j$  if  $a_{n-i} a_{n-j} \neq 0$ .
- Let  $i_1$  be the largest index not exceeding  $n$  such that

$$\mu_{0i_1} = \min\{\mu_{0j} \mid 0 < j \leq n, a_{n-j} \neq 0\}.$$

If  $i_1 < n$ , let  $i_2$  be the largest index  $i_1 < i_2 \leq n$  such that

$$\mu_{i_1 i_2} = \min\{\mu_{i_1 j} \mid i_1 < j \leq n, a_{n-j} \neq 0\}.$$

and so on.

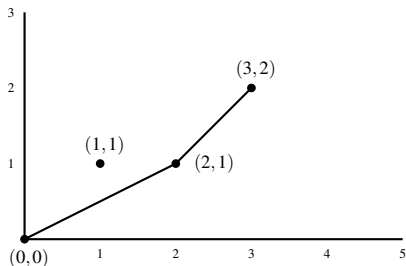
- The **Newton polygon of  $f(x)$  with respect to  $p$**  is the polygonal path having segments  $P_0P_{i_1}, P_{i_1}P_{i_2}, \dots, P_{i_{k-1}}P_{i_k}$  with  $i_k = n$ .
- These segments are called the edges of the Newton polygon of  $f(x)$  with respect to  $p$  and their slopes from left to right form a strictly increasing sequence.
- Newton polygon of  $f(x)$  with respect to  $p$  is the polygonal path formed by the lower edges along the convex hull of points of the set  $S$  defined by

$$S = \{(i, v_p(a_{n-i})) \mid 0 \leq i \leq n, a_{n-i} \neq 0\}.$$

# Example

Let  $p = 3$ . Consider the polynomial  $f(x) = x^3 + 3x^2 + 12x + 9$ .

$$\begin{array}{cccc} f(x) = x^3 & + & 3x^2 & + 12x & + 9 \\ & & \downarrow & \downarrow & \downarrow & \downarrow \\ S = \{(0,0), & (1,1), & (2,1), & (3,2)\} \end{array}$$



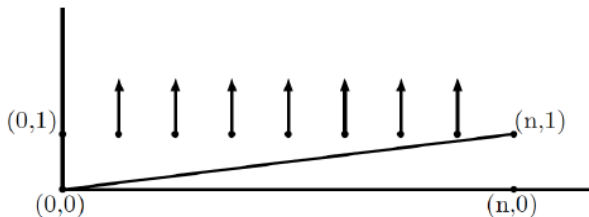
Newton Polygon of  $f(x) = x^3 + 3x^2 + 12x + 9$  w.r.t. 3

# Newton polygon w.r.t. to $p$ of an Eisenstein polynomial

Let

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$$

be an Eisenstein polynomial w.r.t. to  $p$ .



## Restatement of Eisenstein Irreducibility Criterion:

- Let  $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ .
- Assume that the Newton polygon w.r.t. to  $p$  of  $f(x)$  for some prime  $p$  has only one edge with vertices  $\{(0,0), (n,1)\}$ .
- Then  $f(x)$  is irreducible over  $\mathbb{Q}$ .

# Ore's Generalisation of Dumas Irreducibility Criterion

## Restatement of Classical Dumas Irreducibility Criterion

- Let  $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0 \in \mathbb{Z}[x]$ .
- Assume that the  $p$ -Newton polygon of  $f(x)$  for some prime  $p$  has only one edge joining the points  $\{(0,0), (n, v_p(a_0))\}$ .
- If  $v_p(a_0)$  is coprime to  $n$ , then  $f(x)$  is irreducible over  $\mathbb{Q}$ .

## Ore's Generalisation of Dumas Irreducibility Criterion (1928)

Let  $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0 \in \mathbb{Z}[x]$  be such that the  $p$ -Newton polygon of  $f(x)$  for some prime  $p$  has only one edge joining the points  $(0,0), (n, v_p(a_0))$ . If  $e$  is the smallest positive integer such that  $e \frac{v_p(a_0)}{n}$  is in  $\mathbb{Z}$ , then each factor of  $f(x)$  over  $\mathbb{Q}$  has degree divisible by  $e$ .

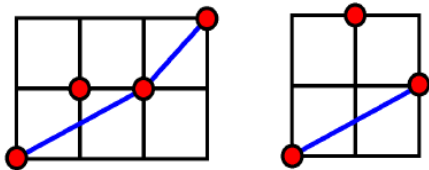
# Dumas' result on the Newton polygon of product of polynomials w.r.t. $p$

## Theorem (Dumas, 1906)

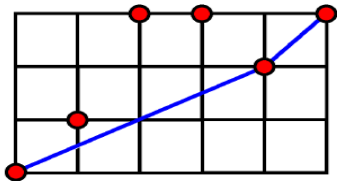
Let  $g(x), h(x) \in \mathbb{Z}[x]$  with  $g(0)h(0) \neq 0$ , and let  $p$  be a prime. Let  $p^t \geq 1$  be the highest power of  $p$  dividing the leading coefficient of  $g(x)h(x)$ . Then the Newton polygon of  $g(x)h(x)$  w.r.t.  $p$  can be formed by constructing a polygonal path beginning at  $(0, t)$  and using translates of the edges in the Newton polygons of  $g(x)$  and  $h(x)$  w.r.t.  $p$  in the increasing order of slopes.



Let  $p = 3$ .



Newton polygons of  $g(x) = x^3 + 3x^2 + 12x + 9$  and  $h(x) = 2x^2 + 9x + 3$  w.r.t. 3



Newton polygon of  $g(x)h(x) = 2x^5 + 15x^4 + 54x^3 + 135x^2 + 117x + 27$  w.r.t. 3

## $\phi$ -Newton polygon with respect to a prime $p$

Let  $p$  be a prime number and  $\phi(x) \in \mathbb{Z}[x]$  be a monic polynomial which is irreducible modulo  $p$ .

- Let  $f(x)$  belonging to  $\mathbb{Z}[x]$  be a polynomial having  $\phi(x)$ -expansion  $\sum_{i=0}^n f_i(x)\phi(x)^i$  with  $f_0(x)f_n(x) \neq 0$ .
- $\phi$ -Newton polygon of  $f(x)$  with respect to  $p$  is the polygonal path formed by the lower edges along the convex hull of points of the set  $S$  defined by

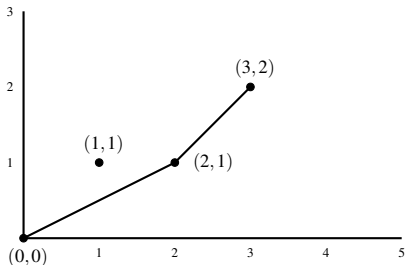
$$S = \{(i, v_p^x(f_{n-i}(x))) \mid 0 \leq i \leq n, f_{n-i}(x) \neq 0\}.$$

- The slopes of these edges from left to right form a strictly increasing sequence.
- The  $\phi$ -Newton polygon minus the horizontal part (if any) is called its **principal part**.

# Example of $\phi$ -Newton Polygon

Let  $p = 5$ ,  $\phi(x) = x^2 + 2$  and  $f(x) = \phi(x)^3 + (5x + 20)\phi(x)^2 + (25x - 5)\phi(x) + 75$ .

$$f(x) = \phi(x)^3 + (5x + 20)\phi(x)^2 + (25x - 5)\phi(x) + 75$$
$$S = \left\{ \begin{array}{cccc} & \downarrow & \downarrow & \downarrow & \downarrow \\ (0,0), & (1,1), & (2,1), & (3,2) \end{array} \right\}$$



$(x^2 + 2)$ -Newton Polygon of  $f(x)$  w.r.t. 5

# Generalised Schönemann Irreducibility Criterion restated

- Let  $\phi(x)$  belonging to  $\mathbb{Z}[x]$  be a monic polynomial which is irreducible modulo a fixed prime  $p$ . Let  $f(x) \in \mathbb{Z}[x]$  be a polynomial having  $\phi$ -expansion given by  $\sum_{i=0}^n f_i(x)\phi(x)^i$  with  $f_0(x) \neq 0$ ,  $f_n(x)$  a constant polynomial not divisible by  $p$ .
- Assume that the  $\phi$ -Newton polygon of  $f(x)$  for some prime  $p$  has only one edge joining the points  $(0,0)$  with  $(n, v_p^x(f_0(x)))$ .
- If  $v_p^x(f_0(x))$  is coprime to  $n$ , then  $f(x)$  is irreducible over  $\mathbb{Q}$ .

# A well-known result of I. Schur

In what follows, a polynomial  $f(x) \in \mathbb{Q}[x]$  will be called irreducible, if it is irreducible over  $\mathbb{Q}$ .

## Theorem 1 (I. Schur, 1930)

*The polynomial*

$$1 + x + \frac{x^2}{2!} + \cdots + \frac{x^n}{n!}$$

*is irreducible for each  $n \geq 1$ .*

- Indeed Schur proved that for arbitrary integers  $a_0, a_1, \dots, a_n$  with  $|a_0| = |a_n| = 1$ , the polynomial

$$a_0 + a_1x + a_2\frac{x^2}{2!} + \cdots + a_n\frac{x^n}{n!}$$

is irreducible for each  $n \geq 1$ .



10.01.1875 - 10.01.1941

## Theorem 2 (-, Jindal, 2023)

Let  $n \geq 2$  be an integer. Let  $\phi(x)$  belonging to  $\mathbb{Z}[x]$  be a monic polynomial which is irreducible modulo all primes dividing  $n$ . Let  $a_0(x), a_1(x), \dots, a_{n-1}(x)$  belonging to  $\mathbb{Z}[x]$  be polynomials each having degree less than  $\deg \phi$  and  $a_n$  be an integer.

Assume that  $a_n$  and the content of the polynomial  $\prod_{i=0}^{n-1} a_i(x)$  are coprime with  $n$ .

Then the polynomial

$$\sum_{i=0}^{n-1} a_i(x) \frac{\phi(x)^i}{i!} + a_n \frac{\phi(x)^n}{n!}$$

is irreducible over  $\mathbb{Q}$ .

### Example 1

Let  $\phi(x) \in \mathbb{Z}[x]$  be a monic polynomial which is irreducible modulo the primes 2, 3. We may take  $\phi(x) = x^3 - x^2 + 1$  or  $x^4 - x - 1$ . Let  $a_0(x), a_1(x), \dots, a_5(x)$  in  $\mathbb{Z}[x]$  be polynomials with degree less than  $\deg \phi$  and each having content coprime with 6. Then  $F(x)$  is irreducible over  $\mathbb{Q}$  where

$$F(x) = \phi(x)^6 + \sum_{i=0}^5 \frac{6!}{i!} a_i(x) \phi(x)^i.$$

### Theorem 3 (-, Jindal, 2023)

Let  $n \geq 2$  be an integer. Let  $\phi(x)$  belonging to  $\mathbb{Z}[x]$  be a monic polynomial which is irreducible modulo all primes less than or equal to  $n$ . Let  $a_0(x), a_1(x), \dots, a_{n-1}(x)$  belonging to  $\mathbb{Z}[x]$  be polynomials each having degree less than  $\deg \phi(x)$  and  $a_n$  be an integer. Assume that  $a_n$  and the content of  $a_0(x)$  are coprime with  $n!$ . Then the polynomial

$$\sum_{i=0}^{n-1} a_i(x) \frac{\phi(x)^i}{i!} + a_n \frac{\phi(x)^n}{n!}$$

is irreducible over  $\mathbb{Q}$ .

### Example 2

Let  $\phi(x) \in \mathbb{Z}[x]$  be a monic polynomial which is irreducible modulo the primes 2, 3 and 5. We may take  $\phi(x) = x^4 + ax + a$  where 30 divides  $a + 1$ . Let  $a_i(x) \in \mathbb{Z}[x]$  be polynomials each having degree less than 4 for  $0 \leq i \leq 5$  and  $a_6$  be an integer. If the content of  $a_6 a_0(x)$  is coprime with 30, then  $F(x)$  is irreducible over  $\mathbb{Q}$  where

$$F(x) = a_6 \phi(x)^6 + \sum_{i=0}^5 \frac{6!}{i!} a_i(x) \phi(x)^i.$$



- In Theorem 3, the assumptions “ $a_n$  and the content of  $a_0(x)$  are coprime with  $n!$ ” cannot be dispensed with. Consider  $\phi(x) = x^2 + x + 1$  which is irreducible modulo 2. The polynomial

$$F(x) = \frac{\phi(x)^2}{2!} + \phi(x) - 4 = \frac{1}{2}(\phi(x) + 4)(\phi(x) - 2)$$

is reducible over  $\mathbb{Q}$ . So is the polynomial

$$G(x) = 12 \frac{\phi(x)^2}{2!} - \phi(x) - 1 = (3\phi(x) + 1)(2\phi(x) - 1).$$

- Theorems 2, 3 do not hold if  $a_n$  is replaced by a (monic) polynomial over  $\mathbb{Z}$  having degree less than  $\deg \phi(x)$ . With  $\phi(x) = x^2 + x + 1$ , the polynomial

$$(x+1) \frac{\phi(x)^2}{2!} + (x+2)\phi(x) + (4x+3)$$

has  $-1$  as a root.

- The analogues of Theorems 2 and 3 do not hold for  $n = 1$  because if  $\phi(x)$  is a monic polynomial of degree  $m \geq 2$ , then the polynomial  $\phi(x) - (\phi(x) - x^m)$  is reducible.

# A key result for the proof

## Theorem 4 (-, Jindal, 2023)

Let  $n, k$  and  $\ell$  be integers with  $0 \leq \ell < k \leq \frac{n}{2}$  and  $p$  be a prime. Let  $\phi(x) \in \mathbb{Z}[x]$  be a monic polynomial which is irreducible modulo  $p$ . Let  $f(x)$  belonging to  $\mathbb{Z}[x]$  be a monic polynomial not divisible by  $\phi(x)$  having  $\phi$ -expansion  $\sum_{i=0}^n f_i(x)\phi(x)^i$  with  $f_n(x) \neq 0$ . Assume that  $v_p^x(f_i(x)) > 0$  for  $0 \leq i \leq n - \ell - 1$  and the right-most edge of the  $\phi$ -Newton polygon of  $f(x)$  with respect to  $p$  has slope less than  $\frac{1}{k}$ . Let  $a_0(x), a_1(x), \dots, a_n(x)$  be polynomials over  $\mathbb{Z}$  satisfying the following conditions.

- (i)  $\deg a_i(x) < \deg \phi(x) - \deg f_i(x)$  for  $0 \leq i \leq n$ ,
- (ii)  $v_p^x(a_0(x)) = 0$ , i.e., the content of  $a_0(x)$  is not divisible by  $p$ ,
- (iii) the leading coefficient of  $a_n(x)$  is not divisible by  $p$ .

Then the polynomial  $\sum_{i=0}^n a_i(x)f_i(x)\phi(x)^i$  does not have a factor in  $\mathbb{Z}[x]$  with degree lying in the interval  $[(\ell + 1) \deg \phi, (k + 1) \deg \phi)$ .

# Bessel polynomials

- The **Bessel polynomial** of degree  $n$  is defined by

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

- These polynomials may also be defined using Bessel functions. **Bessel functions** were first defined by the mathematician Daniel Bernoulli (1700-1782) and they were generalized by **Friedrich Bessel** around 1817.
- In 1951, Grosswald conjectured that  $y_n(x)$  is irreducible for each  $n \geq 1$ .
- Note that  $x^n y_n\left(\frac{2}{x}\right) = \sum_{j=0}^n \frac{(2n-j)!}{(n-j)!j!} x^j$  is a monic polynomial with integral coefficients.

## Theorem 5 (M. Filaseta and O. Trifonov, 2002)

Let  $n$  be a positive integer and let  $a_0, a_1, \dots, a_n$  be arbitrary integers with  $|a_0| = |a_n| = 1$ . Then the polynomial  $z_n(x)$  is irreducible over  $\mathbb{Q}$  where

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

# Bessel polynomials

- The **Bessel polynomial** of degree  $n$  is defined by

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

- These polynomials may also be defined using Bessel functions. **Bessel functions** were first defined by the mathematician Daniel Bernoulli (1700-1782) and they were generalized by **Friedrich Bessel** around 1817.
- In 1951, Grosswald conjectured that  $y_n(x)$  is irreducible for each  $n \geq 1$ .
- Note that  $x^n y_n\left(\frac{2}{x}\right) = \sum_{j=0}^n \frac{(2n-j)!}{(n-j)!j!} x^j$  is a monic polynomial with integral coefficients.

## Theorem 5 (M. Filaseta and O. Trifonov, 2002)

Let  $n$  be a positive integer and let  $a_0, a_1, \dots, a_n$  be arbitrary integers with  $|a_0| = |a_n| = 1$ . Then the polynomial  $z_n(x)$  is irreducible over  $\mathbb{Q}$  where

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



**Michael Filaseta**



**Ognian Trifonov**

# Generalized Laguerre Polynomials

## Definition

Let  $\alpha$  and  $n$  be integers with  $n \geq 1$ . The **Generalized Laguerre Polynomial** of degree  $n$  with parameter  $\alpha$  is denoted by  $L_n^{(\alpha)}(x)$ . It is defined by

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

These polynomials are named after the famous mathematician **Edmond Nicolas Laguerre** (1834-1886) and are the solutions of the Laguerre's differential equation

$$xy'' + (\alpha + 1 - x)y' + ny = 0, \quad y = y(x).$$

One can also define the Generalised Laguerre polynomials recursively, defining the first two polynomials as  $L_0^{(\alpha)}(x) = 1$ ,  $L_1^{(\alpha)}(x) = x - 1 - \alpha$  and then using the following recurrence relation for  $k \geq 1$ ,

$$L_{k+1}^{(\alpha)}(x) = \frac{(x - 2k - 1 - \alpha)L_k^{(\alpha)}(x) - (k + \alpha)L_{k-1}^{(\alpha)}(x)}{k + 1}.$$

# Special types of Laguerre polynomials

- For  $\alpha = -n - 1$ ,  $L_n^{(-n-1)}(x)$  also has a familiar form given by

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

So  $L_n^{(-n-1)}(x)$  is the  $n^{\text{th}}$  Taylor polynomial of the exponential function.

- For  $\alpha = 0$ ,  $L_n^{(0)}(x)$  has a simple form given by

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

$L_n^{(0)}(x)$  is called the classical Laguerre polynomial of degree  $n$ .

- Generalized Laguerre polynomials are related to Bessel polynomials. Indeed

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

# Special types of Laguerre polynomials

- For  $\alpha = -n - 1$ ,  $L_n^{(-n-1)}(x)$  also has a familiar form given by

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

So  $L_n^{(-n-1)}(x)$  is the  $n^{\text{th}}$  Taylor polynomial of the exponential function.

- For  $\alpha = 0$ ,  $L_n^{(0)}(x)$  has a simple form given by

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

$L_n^{(0)}(x)$  is called the classical Laguerre polynomial of degree  $n$ .

- Generalized Laguerre polynomials are related to Bessel polynomials. Indeed

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



# Special types of Laguerre polynomials

- For  $\alpha = -n - 1$ ,  $L_n^{(-n-1)}(x)$  also has a familiar form given by

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

So  $L_n^{(-n-1)}(x)$  is the  $n^{\text{th}}$  Taylor polynomial of the exponential function.

- For  $\alpha = 0$ ,  $L_n^{(0)}(x)$  has a simple form given by

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

$L_n^{(0)}(x)$  is called the classical Laguerre polynomial of degree  $n$ .

- Generalized Laguerre polynomials are related to Bessel polynomials. Indeed

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

# Examples of reducible Generalized Laguerre Polynomials

- For  $\alpha = -a$  where  $1 \leq a \leq n$  is an integer, it can be easily seen that

$$\begin{aligned}L_n^{(-a)}(x) &= \sum_{j=0}^n (-1)^{n-j} \frac{(n-a)(n-1-a)\cdots(j+1-a)}{(n-j)!j!} x^j \\ &= x^a L_{n-a}^{(a)}(x).\end{aligned}$$

Hence  $L_n^{(\alpha)}(x)$  is reducible for  $\alpha = -a$  where  $1 \leq a \leq n$ .

- One can also check that

$$\begin{aligned}L_2^{(2)}(x) &= \frac{1}{2}(x-2)(x-6), \\ L_2^{(23)}(x) &= \frac{1}{2}(x-20)(x-30), \\ L_4^{(23)}(x) &= \frac{1}{24}(x-30)(x^3 - 78x^2 + 1872x - 14040).\end{aligned}$$

# Examples of reducible Generalized Laguerre Polynomials

- For  $\alpha = -a$  where  $1 \leq a \leq n$  is an integer, it can be easily seen that

$$\begin{aligned}L_n^{(-a)}(x) &= \sum_{j=0}^n (-1)^{n-j} \frac{(n-a)(n-1-a)\cdots(j+1-a)}{(n-j)!j!} x^j \\ &= x^a L_{n-a}^{(a)}(x).\end{aligned}$$

Hence  $L_n^{(\alpha)}(x)$  is reducible for  $\alpha = -a$  where  $1 \leq a \leq n$ .

- One can also check that

$$\begin{aligned}L_2^{(2)}(x) &= \frac{1}{2}(x-2)(x-6), \\ L_2^{(23)}(x) &= \frac{1}{2}(x-20)(x-30), \\ L_4^{(23)}(x) &= \frac{1}{24}(x-30)(x^3 - 78x^2 + 1872x - 14040).\end{aligned}$$

# Known cases of irreducibility of $L_n^{(\alpha)}(x)$

It is known that  $L_n^{(\alpha)}(x)$  is **irreducible** for each  $n \geq 1$  for the following values of  $\alpha$ .

- I. Schur (1930) :  $\alpha \in \{0, 1, -n - 1\}$
- F. Hajir (1995) :  $\alpha = -n - 1 - r$  for  $r \in [1, 8]$
- M. Filaseta, O. Trifonov (2002) :  $\alpha = -2n - 1$
- M. Filaseta, T. Kidd, O. Trifonov (2012) :  $\alpha = n$  with  $n \equiv 2 \pmod{4}$
- S. Nair, T. N. Shorey (2015) :  $\alpha = -n - 1 - r$  for  $r \in [9, 22]$
- A. Jindal, S. Laishram, R. Sarma (2018) :  $\alpha = -n - 1 - r$  for  $r \in [23, 60]$
- A. Jindal, S. Laishram (2022) :  $\alpha = -2n$  with  $n \equiv 2 \pmod{4}$
- A. Jindal, S. Laishram (2022) :  $\alpha = -2n - \beta$  for  $\beta \in [1, 4]$
- A. Jindal, S. Nair, T. N. Shorey (2023) :  $\alpha = -n - 1 - r$  for  $r \in [61, 100]$



**Tarlok N. Shorey**



**Shanta Laishram**



**Fashid Hajir**



**Ritumoni Sarma**








**Saranya Nair**









**Ankita Jindal**







# References

-  G. Dumas, *Sur quelques cas d'irréductibilité des polynômes à coefficients rationnels*, Journal de Math. Pure et Appl. 2 (1906), 191-258.
-  I. Schur, *Einige Sätze über Primzahlen mit Anwendungen auf Irreduzibilitätsfragen, I*, Sitzungsber. Preuss. Akad. Wiss. Berlin Phys.-Math. Kl., 14 (1929), 125-136.
-  I. Schur, *Einige Sätze über Primzahlen mit Anwendungen auf Irreduzibilitätsfragen, II*, Sitzungsber. Preuss. Akad. Wiss. Berlin Phys.-Math. Kl., 14 (1929), 370-391.
-  I. Schur, *Gleichungen ohne Affekt*, Sitzungsberichte der Preussischen Akademie der Wissenschaften, Physikalisch-Mathematische Klasse (1930), 443-449.
-  I. Schur, *Affektlose Gleichungen in der Theorie der Laguerreschen und Hermiteschen Polynome*, Journal für die reine und angewandte Mathematik 165 (1931), 52-58.

# References





-  Ø. Ore, *Newtonsche Polygone in der Theorie der algebraischen Körper*, Mathematische Annalen, 99 (1928) 84-117.
-  R. F. Coleman, *On the Galois groups of the exponential Taylor polynomials*, L'Enseignement Math. 33 (1987) 183-189.
-  F. Hajir, *Some  $\tilde{A}_n$ -extensions obtained from generalized Laguerre polynomials*, J. Number Theory 50 (1995) 206-212.
-  M. Filaseta, *The irreducibility of all but finitely many Bessel polynomials*, Acta Math., 174 (1995) 383-397.
-  M. Filaseta and O. Trifonov, *The Irreducibility of the Bessel polynomials*, J. Reine Angew. Math. 550 (2002) 125-140.
-  R. Brown, *Roots of generalized Schönemann polynomials in henselian extension fields*, Indian J. Pure Appl. Math. 39 (2008) 403-4102.

# References

-  A. Bishnoi and S. K. Khanduja, *On Eisenstein - Dumas and Generalized Schoneman polynomials*, Commun. Algebra 38 (2010) No. 9, 3163-3173.
-  R. Khassa and S. K. Khanduja, *A generalization of Eisenstein-Schönemann Irreducibility Criterion*, Manuscr. Math 134 (2011) 215-224.
-  S. K. Khanduja and S. Kumar, *On prolongations of valuations via Newton polygons and liftings of polynomials*, J. Pure Appl. Algebra, 216 (2012) 2648-2656.
-  M. Filaseta, T. Kidd and O. Trifonov, *Laguerre polynomials with Galois group  $A_m$  for each  $m$* , J. Number Theory 132 (2012) 776–805.
-  S. G. Nair and T. N. Shorey, *Irreducibility of Laguerre Polynomial  $L_n^{(-1-n-r)}(x)$* , Indagationes Mathematicae, 26 (2015) 615-625.
-  B. Jhorar and S. K. Khanduja, *A Generalization of the Eisenstein-Dumas-Schönemann Irreducibility Criterion*, Proc. Edinburgh Math. Soc. 60 (2017) 937-945.



# References

-  A. Jindal, S. Laishram and R. Sarma, *Irreducibility and Galois groups of Generalised Laguerre Polynomials  $L_n^{(-1-n-r)}(x)$* , J. Number Theory 183 (2018) 388-406.
-  A. Jindal and S. Laishram, *Families of Laguerre polynomials with Alternating group as Galois group*, J. Number Theory 241 (2022) 387-429.
-  A. Jindal and S. K. Khanduja, *An extension of Schur's irreducibility result*, <https://arxiv.org/abs/2305.04781>.
-  A. Jindal, S. G. Nair and T. N. Shorey, *Extension of Irreducibility results on Generalised Laguerre Polynomials  $L_n^{(-1-n-s)}(x)$* , preprint (2023).

