# Prime Numbers & Irreducible Polynomials

Saikat Goswami

*Department of Mathematics*, Ramakrishna Mission Vidyamandira, Belur Math


July 23,2021

# Overview

1. **Buniakowski Conjecture**
   - Investigating the assumptions in the Conjecture
   - Extracting an Irreducibility criterion from the Conjecture
2. **Murty's Irreducibility Criterion (M.I.C.)**
   - Root Capturing Lemma (1)
   - Proving Murty's Irreducibility Criterion
   - Generalizing Murty's Irreducibility Criterion
3. **Constructing Irreducible Poly. using Prime numbers**
   - Cohn's Irreducibility Criterion
   - Root Capturing Lemma (2)
   - Proving Cohn's Irreducibility Criterion

# Section 1

# Buniakowski Conjecture [1854]

## Aim:

To produce prime numbers from irreducible polynomials.

# Buniakowski Conjecture [1854]

## Aim:

To produce prime numbers from irreducible polynomials.

## Statement:

# Buniakowski Conjecture [1854]

## Aim:

To produce prime numbers from irreducible polynomials.

## Statement:

If $f(x) \in \mathbb{Z}[X]$ with the following properties:

1. The leading coefficient of $f$ is positive.

# Buniakowski Conjecture [1854]

## Aim:

To produce prime numbers from irreducible polynomials.

## Statement:

If $f(x) \in \mathbb{Z}[X]$ with the following properties:

1. The leading coefficient of $f$ is positive.
2. $f(x)$ is irreducible.

# Buniakowski Conjecture [1854]

## Aim:

To produce prime numbers from irreducible polynomials.

## Statement:

If $f(x) \in \mathbb{Z}[X]$ with the following properties:

1. The leading coefficient of $f$ is positive.
2. $f(x)$ is irreducible.
3. The set $\{f(n) : n \in \mathbb{N}\}$ has no common divisor $> 1$.

# Buniakowski Conjecture [1854]

## Aim:

To produce prime numbers from irreducible polynomials.

## Statement:

If $f(x) \in \mathbb{Z}[X]$ with the following properties:

1. The leading coefficient of $f$ is positive.
2. $f(x)$ is irreducible.
3. The set $\{f(n) : n \in \mathbb{N}\}$ has no common divisor $> 1$.

Then the sequence $(f(n))_{n\in\mathbb{N}}$ contain primes infinitely often.

# Buniakowski Conjecture [1854]

## Aim:

To produce prime numbers from irreducible polynomials.

## Statement:

If $f(x) \in \mathbb{Z}[X]$ with the following properties:

1. The leading coefficient of $f$ is positive.
2. $f(x)$ is irreducible.
3. The set $\{f(n) : n \in \mathbb{N}\}$ has no common divisor $> 1$.

Then the sequence $(f(n))_{n\in\mathbb{N}}$ contain primes infinitely often.

## Example:

$f(x) = x^2 + 1 \implies (f(n))_{n\in\mathbb{N}}$ contains primes infinitely often (i.o.).

This Conjecture is still one of the major unsolved problems in Number Theory when $\deg f > 1$.

This Conjecture is still one of the major unsolved problems in Number Theory when $\deg f > 1$.

When $f$ is linear, the conjecture is true, and follows from Dirichlet's theorem on infinitude of primes in arithmetic progressions.

This Conjecture is still one of the major unsolved problems in Number Theory when $\deg f > 1$.

When $f$ is linear, the conjecture is true, and follows from Dirichlet's theorem on infinitude of primes in arithmetic progressions.

**Dirichlet's Prime Number Theorem:**

$a, d \in \mathbb{N}$ with $(a, d) = 1$

This Conjecture is still one of the major unsolved problems in Number Theory when $\deg f > 1$.

When $f$ is linear, the conjecture is true, and follows from Dirichlet's theorem on infinitude of primes in arithmetic progressions.

**Dirichlet's Prime Number Theorem:**

$a, d \in \mathbb{N}$ with $(a, d) = 1$ there are infinitely many primes of the form $a + nd$ where $n$ is a positive integer.

# Investigating the assumptions in the Conjecture

# Investigating the assumptions in the Conjecture

**$(f(n))_{n\in\mathbb{N}}$ contains prime i.o. $\implies$ $a_n > 0$**

# Investigating the assumptions in the Conjecture

**$(f(n))_{n\in\mathbb{N}}$ contains prime i.o. $\implies$ $a_n > 0$**

If the leading coefficient $a_n < 0$ then $f(x) < 0$ for all large $x$. Then $f(n)$ would be prime for atmost finitely many $n$.

# Investigating the assumptions in the Conjecture

**$(f(n))_{n\in\mathbb{N}}$ contains prime i.o. $\implies$ $a_n > 0$**

If the leading coefficient $a_n < 0$ then $f(x) < 0$ for all large $x$. Then $f(n)$ would be prime for atmost finitely many $n$.

**$(f(n))_{n\in\mathbb{N}}$ contains prime i.o. $\implies$ $f$ is irreducible**

# Investigating the assumptions in the Conjecture

**$(f(n))_{n\in\mathbb{N}}$ contains prime i.o. $\implies a_n > 0$**

If the leading coefficient $a_n < 0$ then $f(x) < 0$ for all large $x$. Then $f(n)$ would be prime for atmost finitely many $n$.

**$(f(n))_{n\in\mathbb{N}}$ contains prime i.o. $\implies f$ is irreducible**

If $f$ were reducible with $f(x) = g(x)h(x)$. Then $f(n) = g(n)h(n)\ \forall n \in \mathbb{N}$. So $g(x)$ and $h(x)$ takes the value $\pm 1$ infinitely many times ; Contradiction! So $f(n)$ is composite for all large $n$.

# Investigating the assumptions in the Conjecture

**$(f(n))_{n\in\mathbb{N}}$ contains prime i.o. $\implies$ $a_n > 0$**

If the leading coefficient $a_n < 0$ then $f(x) < 0$ for all large $x$. Then $f(n)$ would be prime for atmost finitely many $n$.

**$(f(n))_{n\in\mathbb{N}}$ contains prime i.o. $\implies$ $f$ is irreducible**

If $f$ were reducible with $f(x) = g(x)h(x)$. Then $f(n) = g(n)h(n)\ \forall n \in \mathbb{N}$. So $g(x)$ and $h(x)$ takes the value $\pm 1$ infinitely many times ; Contradiction! So $f(n)$ is composite for all large $n$.

Do (1) & (2) $\implies$ there are primes infinitely often in $(f(n))_{n\in\mathbb{N}}$ ?

**$a_n > 0$ & $f$ : irreducible $\not\Rightarrow$ $(f(n))_{n\in\mathbb{N}}$ contains prime i.o.**

**$a_n > 0$ & $f$ : irreducible $\not\Rightarrow$ $(f(n))_{n\in\mathbb{N}}$ contains prime i.o.**

$f(x) = x^2 + x + 2$ ; but $f(n)$ is even for all $n \in \mathbb{N}$.

**$a_n > 0$ & $f$ : irreducible $\not\Longrightarrow$ $(f(n))_{n\in\mathbb{N}}$ contains prime i.o.**

$f(x) = x^2 + x + 2$ ; but $f(n)$ is even for all $n \in \mathbb{N}$.

So the $3rd$ assumption is very crucial in the generation of primes infinitely often in $(f(n))_{n\in\mathbb{N}}$.

**$(f(n))_{n\in\mathbb{N}}$ contains prime i.o. $\Longrightarrow$ $\{f(n) : n \in \mathbb{N}\}$ has no common divisor $d > 1$**

**$a_n > 0$ & $f$ : irreducible $\not\Longrightarrow$ $(f(n))_{n\in\mathbb{N}}$ contains prime i.o.**

$f(x) = x^2 + x + 2$ ; but $f(n)$ is even for all $n \in \mathbb{N}$.

So the $3rd$ assumption is very crucial in the generation of primes infinitely often in $(f(n))_{n\in\mathbb{N}}$.

**$(f(n))_{n\in\mathbb{N}}$ contains prime i.o. $\Longrightarrow$ $\{f(n) : n \in \mathbb{N}\}$ has no common divisor $d > 1$**

If $\{f(n) : n \in \mathbb{N}\}$ has a common divisor $d > 1 \implies d \mid f(n)\ \forall\ n \in \mathbb{N}$.
Hence $(f(n))_{n\in\mathbb{N}}$ cannot contain primes i.o.

# Extracting an Irreducibility Criterion

# Extracting an Irreducibility Criterion

**An Irreducibility Criterion: $f(x) \in \mathbb{Z}[X]$ s.t.**

# Extracting an Irreducibility Criterion

**An Irreducibility Criterion: $f(x) \in \mathbb{Z}[X]$ s.t.**

$(f(n))_{n\in\mathbb{N}}$ containing primes infinitely often $\implies$ $f$ : irreducible

# Extracting an Irreducibility Criterion

**An Irreducibility Criterion: $f(x) \in \mathbb{Z}[X]$ s.t.**

$(f(n))_{n\in\mathbb{N}}$ containing primes infinitely often $\implies$ $f$ : irreducible

The applicability of this result is very poor.

# Extracting an Irreducibility Criterion

**An Irreducibility Criterion: $f(x) \in \mathbb{Z}[X]$ s.t.**

$(f(n))_{n\in\mathbb{N}}$ containing primes infinitely often $\implies$ $f$ : irreducible

The applicability of this result is very poor.

**A stronger version of the above criterion (M.I.C.)**

$(f(n))_{n\in\mathbb{N}}$ contains a prime for sufficiently large $n$ $\implies$ $f$ : irreducible

# Section 2

# Formal statement of M.I.C.

## Murty's Irreducibility Criterion (M.I.C.)

$f(x) = a_m x^m + a_{m-1} x^{m-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[X]$ with

$$H := \max_{0 \leq i \leq m-1} \left| \frac{a_i}{a_m} \right|$$

# Formal statement of M.I.C.

## Murty's Irreducibility Criterion (M.I.C.)

$f(x) = a_m x^m + a_{m-1} x^{m-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[X]$ with

$$H := \max_{0 \leq i \leq m-1} \left| \frac{a_i}{a_m} \right|$$

$f(n)$ is prime for some $H + 2 \leq n$

# Formal statement of M.I.C.

## Murty's Irreducibility Criterion (M.I.C.)

$f(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[X]$ with

$$H := \max_{0 \leq i \leq m-1} \left| \frac{a_i}{a_m} \right|$$

$f(n)$ is prime for some $H + 2 \leq n \implies f(x)$ : irreducible in $\mathbb{Z}[X]$.

# Formal statement of M.I.C.

## Murty's Irreducibility Criterion (M.I.C.)

$f(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[X]$ with

$$H := \max_{0 \leq i \leq m-1} \left| \frac{a_i}{a_m} \right|$$

$f(n)$ is prime for some $H + 2 \leq n \implies f(x)$ : irreducible in $\mathbb{Z}[X]$.

## Example: $f(x) = x^3 - x + 7$

# Formal statement of M.I.C.

## Murty's Irreducibility Criterion (M.I.C.)

$f(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[X]$ with

$$H := \max_{0 \leq i \leq m-1} \left| \frac{a_i}{a_m} \right|$$

$f(n)$ is prime for some $H + 2 \leq n \implies f(x)$ : irreducible in $\mathbb{Z}[X]$.

## Example: $f(x) = x^3 - x + 7$

$H = 7$

# Formal statement of M.I.C.

## Murty's Irreducibility Criterion (M.I.C.)

$f(x) = a_m x^m + a_{m-1} x^{m-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[X]$ with

$$H := \max_{0 \leq i \leq m-1} \left| \frac{a_i}{a_m} \right|$$

$f(n)$ is prime for some $H + 2 \leq n \implies f(x)$ : irreducible in $\mathbb{Z}[X]$.

## Example: $f(x) = x^3 - x + 7$

$H = 7$ ; $f(10) = 10^3 - 10 + 7 = 997$

# Formal statement of M.I.C.

## Murty's Irreducibility Criterion (M.I.C.)

$f(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[X]$ with

$$H := \max_{0 \leq i \leq m-1} \left| \frac{a_i}{a_m} \right|$$

$f(n)$ is prime for some $H + 2 \leq n \implies f(x)$ : irreducible in $\mathbb{Z}[X]$.

## Example: $f(x) = x^3 - x + 7$

$H = 7$ ; $f(10) = 10^3 - 10 + 7 = 997$ ; $H + 2 \leq 10$

# Formal statement of M.I.C.

## Murty's Irreducibility Criterion (M.I.C.)

$f(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[X]$ with

$$H := \max_{0 \leq i \leq m-1} \left| \frac{a_i}{a_m} \right|$$

$f(n)$ is prime for some $H + 2 \leq n \implies f(x)$ : irreducible in $\mathbb{Z}[X]$.

## Example: $f(x) = x^3 - x + 7$

$H = 7$ ; $f(10) = 10^3 - 10 + 7 = 997$ ; $H + 2 \leq 10 \implies f$ : irreducible

# Main Tool used in the proof of M.I.C.

## A Root Capturing Lemma:

# Main Tool used in the proof of M.I.C.

## A Root Capturing Lemma:

$f(x) = a_m x^m + a_{m-1} x^{m-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[X]$ ; $\alpha \in \mathbb{C}$ is a root.

# Main Tool used in the proof of M.I.C.

## A Root Capturing Lemma:

$f(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[X]$ ; $\alpha \in \mathbb{C}$ is a root.

$$\text{Then} \quad |\alpha| < H + 1 \quad \text{where} \quad H := \max_{0 \leq i \leq m-1} \left| \frac{a_i}{a_m} \right|$$

# Main Tool used in the proof of M.I.C.

## A Root Capturing Lemma:

$f(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[X]$ ; $\alpha \in \mathbb{C}$ is a root.

$$\text{Then} \quad |\alpha| < H + 1 \quad \text{where} \quad H := \max_{0 \leq i \leq m-1} \left| \frac{a_i}{a_m} \right|$$

## Proof:

# Main Tool used in the proof of M.I.C.

## A Root Capturing Lemma:

$f(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[X]$ ; $\alpha \in \mathbb{C}$ is a root.

$$\text{Then} \quad |\alpha| < H + 1 \quad \text{where} \quad H := \max_{0 \leq i \leq m-1} \left| \frac{a_i}{a_m} \right|$$

## Proof:

$$f(\alpha) = 0 \implies -\alpha^m = \frac{a_{m-1}}{a_m}\alpha^{m-1} + \cdots + \frac{a_1}{a_m}\alpha + \frac{a_0}{a_m}$$

# Main Tool used in the proof of M.I.C.

## A Root Capturing Lemma:

$f(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[X]$ ; $\alpha \in \mathbb{C}$ is a root.

$$\text{Then } |\alpha| < H + 1 \text{ where } H := \max_{0 \leq i \leq m-1} \left| \frac{a_i}{a_m} \right|$$

## Proof:

$$f(\alpha) = 0 \implies -\alpha^m = \frac{a_{m-1}}{a_m}\alpha^{m-1} + \cdots + \frac{a_1}{a_m}\alpha + \frac{a_0}{a_m}$$

$$\implies |\alpha|^m \leq H\left(|\alpha|^{m-1} + \cdots + |\alpha| + 1\right) = H\left(\frac{|\alpha|^m - 1}{|\alpha| - 1}\right)$$

$$\text{Then } |\alpha| > 1 \implies |\alpha|^{\mathbf{m}}\left(|\alpha| - \mathbf{1}\right) < H\,|\alpha|^m - H < \mathbf{H}\,|\alpha|^{\mathbf{m}}$$

# Proof of M.I.C.

## A proof by contradiction !

# Proof of M.I.C.

## A proof by contradiction !

- $f(x) = g(x)h(x)$, where $g(x)$ and $h(x)$ are of positive degree.

  $f(n)$ is prime $\Rightarrow$ $g(n)$ or $h(n) = \pm 1$. WLOG we assume it to be $g(n)$

# Proof of M.I.C.

## A proof by contradiction !

- $f(x) = g(x)h(x)$, where $g(x)$ and $h(x)$ are of positive degree.

  $f(n)$ is prime $\Rightarrow$ $g(n)$ or $h(n) = \pm 1$. WLOG we assume it to be $g(n)$

- $$g(x) = c\prod_i (x - \alpha_i)$$

  $c$ : leading coefficient of $g$ & $\alpha_i$ runs over a subset of zeros of $f$.

# Proof of M.I.C.

## A proof by contradiction !

- $f(x) = g(x)h(x)$, where $g(x)$ and $h(x)$ are of positive degree.

  $f(n)$ is prime $\Rightarrow$ $g(n)$ or $h(n) = \pm 1$. WLOG we assume it to be $g(n)$

- $$g(x) = c\prod_i (x - \alpha_i)$$

  $c$ : leading coefficient of $g$ & $\alpha_i$ runs over a subset of zeros of $f$.

- Now we arrive at a contradiction (since $|g(n)| = 1$).

$$\mathbf{|g(n)|} \geq \prod_i (n - |\alpha_i|) \;>\; \prod_i (n - (H+1)) \geq \mathbf{1}$$

# Application of M.I.C.

**An Infinite family of $f$ which are reducible mod $p$ $\forall$ $p$.**

# Application of M.I.C.

**An Infinite family of $f$ which are reducible mod $p$ $\forall$ $p$.**

For any $a \in \mathbb{N}$ ; $f(x) = x^4 + (4a+2)x^2 + 1$ is reducible mod $p$ for all $p$.

# Application of M.I.C.

**An Infinite family of $f$ which are reducible mod $p$ $\forall$ $p$.**

For any $a \in \mathbb{N}$ ; $f(x) = x^4 + (4a+2)x^2 + 1$ is reducible mod $p$ for all $p$.

$a = 1$ ; $f(x) = x^4 + 6x^2 + 1$ ; $H = 6$

# Application of M.I.C.

**An Infinite family of $f$ which are reducible mod $p$ $\forall$ $p$.**

For any $a \in \mathbb{N}$ ; $f(x) = x^4 + (4a+2)x^2 + 1$ is reducible mod $p$ for all $p$.

$a = 1$ ; $f(x) = x^4 + 6x^2 + 1$ ; $H = 6$

$f(8) = 4481$ is a prime

# Application of M.I.C.

**An Infinite family of $f$ which are reducible mod $p$ $\forall$ $p$.**

For any $a \in \mathbb{N}$ ; $f(x) = x^4 + (4a+2)x^2 + 1$ is reducible mod $p$ for all $p$.

$a = 1$ ; $f(x) = x^4 + 6x^2 + 1$ ; $H = 6$

$f(8) = 4481$ is a prime ; $H + 2 \leq 8$

# Application of M.I.C.

**An Infinite family of $f$ which are reducible mod $p$ $\forall$ $p$.**

For any $a \in \mathbb{N}$ ; $f(x) = x^4 + (4a+2)x^2 + 1$ is reducible mod $p$ for all $p$.

**$a = 1$ ; $f(x) = x^4 + 6x^2 + 1$ ; $H = 6$**

$f(8) = 4481$ is a prime ; $H + 2 \leq 8 \implies f$ irreducible.

# Application of M.I.C.

**An Infinite family of $f$ which are reducible mod $p$ $\forall$ $p$.**

For any $a \in \mathbb{N}$ ; $f(x) = x^4 + (4a+2)x^2 + 1$ is reducible mod $p$ for all $p$.

**$a = 1$ ; $f(x) = x^4 + 6x^2 + 1$ ; $H = 6$**

$f(8) = 4481$ is a prime ; $H + 2 \leq 8 \implies f$ irreducible.

**$a = 2$ ; $f(x) = x^4 + 10x + 1$ ; $H = 10$**

# Application of M.I.C.

**An Infinite family of $f$ which are reducible mod $p$ $\forall$ $p$.**

For any $a \in \mathbb{N}$ ; $f(x) = x^4 + (4a+2)x^2 + 1$ is reducible mod $p$ for all $p$.

**$a = 1$ ; $f(x) = x^4 + 6x^2 + 1$ ; $H = 6$**

$f(8) = 4481$ is a prime ; $H + 2 \leq 8 \implies f$ irreducible.

**$a = 2$ ; $f(x) = x^4 + 10x + 1$ ; $H = 10$**

$f(18) = 108217$ is a prime

# Application of M.I.C.

**An Infinite family of $f$ which are reducible mod $p$ $\forall$ $p$.**

For any $a \in \mathbb{N}$ ; $f(x) = x^4 + (4a+2)x^2 + 1$ is reducible mod $p$ for all $p$.

**$a = 1$ ; $f(x) = x^4 + 6x^2 + 1$ ; $H = 6$**

$f(8) = 4481$ is a prime ; $H + 2 \leq 8 \implies f$ irreducible.

**$a = 2$ ; $f(x) = x^4 + 10x + 1$ ; $H = 10$**

$f(18) = 108217$ is a prime ; $H + 2 \leq 18$

# Application of M.I.C.

**An Infinite family of $f$ which are reducible mod $p$ $\forall$ $p$.**

For any $a \in \mathbb{N}$ ; $f(x) = x^4 + (4a+2)x^2 + 1$ is reducible mod $p$ for all $p$.

**$a = 1$ ; $f(x) = x^4 + 6x^2 + 1$ ; $H = 6$**

$f(8) = 4481$ is a prime ; $H + 2 \leq 8 \implies f$ irreducible.

**$a = 2$ ; $f(x) = x^4 + 10x + 1$ ; $H = 10$**

$f(18) = 108217$ is a prime ; $H + 2 \leq 18 \implies f$ irreducible.

# Application of M.I.C.

**An Infinite family of $f$ which are reducible mod $p$ $\forall$ $p$.**

For any $a \in \mathbb{N}$ ; $f(x) = x^4 + (4a+2)x^2 + 1$ is reducible mod $p$ for all $p$.

**$a = 1$ ; $f(x) = x^4 + 6x^2 + 1$ ; $H = 6$**

$f(8) = 4481$ is a prime ; $H + 2 \leq 8 \implies f$ irreducible.

**$a = 2$ ; $f(x) = x^4 + 10x + 1$ ; $H = 10$**

$f(18) = 108217$ is a prime ; $H + 2 \leq 18 \implies f$ irreducible.

**$a = 5$ ; $f(x) = x^4 + 22x + 1$ ; $H = 22$**

# Application of M.I.C.

**An Infinite family of $f$ which are reducible mod $p$ $\forall$ $p$.**

For any $a \in \mathbb{N}$ ; $f(x) = x^4 + (4a+2)x^2 + 1$ is reducible mod $p$ for all $p$.

**$a = 1$ ; $f(x) = x^4 + 6x^2 + 1$ ; $H = 6$**

$f(8) = 4481$ is a prime ; $H + 2 \leq 8 \implies f$ irreducible.

**$a = 2$ ; $f(x) = x^4 + 10x + 1$ ; $H = 10$**

$f(18) = 108217$ is a prime ; $H + 2 \leq 18 \implies f$ irreducible.

**$a = 5$ ; $f(x) = x^4 + 22x + 1$ ; $H = 22$**

$f(204) = 1732807009$ is a prime

# Application of M.I.C.

**An Infinite family of $f$ which are reducible mod $p$ $\forall$ $p$.**

For any $a \in \mathbb{N}$ ; $f(x) = x^4 + (4a+2)x^2 + 1$ is reducible mod $p$ for all $p$.

**$a = 1$ ; $f(x) = x^4 + 6x^2 + 1$ ; $H = 6$**

$f(8) = 4481$ is a prime ; $H + 2 \leq 8 \implies f$ irreducible.

**$a = 2$ ; $f(x) = x^4 + 10x + 1$ ; $H = 10$**

$f(18) = 108217$ is a prime ; $H + 2 \leq 18 \implies f$ irreducible.

**$a = 5$ ; $f(x) = x^4 + 22x + 1$ ; $H = 22$**

$f(204) = 1732807009$ is a prime ; $H + 2 \leq 204$

# Application of M.I.C.

**An Infinite family of $f$ which are reducible mod $p$ $\forall$ $p$.**

For any $a \in \mathbb{N}$ ; $f(x) = x^4 + (4a+2)x^2 + 1$ is reducible mod $p$ for all $p$.

**$a = 1$ ; $f(x) = x^4 + 6x^2 + 1$ ; $H = 6$**

$f(8) = 4481$ is a prime ; $H + 2 \leq 8 \implies f$ irreducible.

**$a = 2$ ; $f(x) = x^4 + 10x + 1$ ; $H = 10$**

$f(18) = 108217$ is a prime ; $H + 2 \leq 18 \implies f$ irreducible.

**$a = 5$ ; $f(x) = x^4 + 22x + 1$ ; $H = 22$**

$f(204) = 1732807009$ is a prime ; $H + 2 \leq 204 \implies f$ irreducible

# Application of M.I.C.

**An Infinite family of $f$ which are reducible mod $p$ $\forall$ $p$.**

For any $a \in \mathbb{N}$ ; $f(x) = x^4 + (4a+2)x^2 + 1$ is reducible mod $p$ for all $p$.

**$a = 1$ ; $f(x) = x^4 + 6x^2 + 1$ ; $H = 6$**

$f(8) = 4481$ is a prime ; $H + 2 \leq 8 \implies f$ irreducible.

**$a = 2$ ; $f(x) = x^4 + 10x + 1$ ; $H = 10$**

$f(18) = 108217$ is a prime ; $H + 2 \leq 18 \implies f$ irreducible.

**$a = 5$ ; $f(x) = x^4 + 22x + 1$ ; $H = 22$**

$f(204) = 1732807009$ is a prime ; $H + 2 \leq 204 \implies f$ irreducible

**They are the smallest $H + 2 \leq n$ for which $f(n)$ is prime**

# Can we refine the bound from "$H+2$" to "$H+1$"?

# Can we refine the bound from "$H+2$" to "$H+1$"?

## M.I.C.

$f(n)$ is prime for some $H+2 \leq n \implies f(x)$ : irreducible in $\mathbb{Z}[X]$

$$\text{where} \quad H := \max_{0 \leq i \leq m-1} \left| \frac{a_i}{a_m} \right|$$

**The lowerbound "$H+2$" obtained is the best possible.**

# Can we refine the bound from "$H+2$" to "$H+1$"?

## M.I.C.

$f(n)$ is prime for some $H+2 \leq n \implies f(x)$ : irreducible in $\mathbb{Z}[X]$

$$\text{where} \quad H := \max_{0 \leq i \leq m-1} \left| \frac{a_i}{a_m} \right|$$

**The lowerbound "$H+2$" obtained is the best possible.**

**Counterexample:** $f(x) = x^3 - 9x^2 + x - 9 = (x-9)(x^2+1)$

# Can we refine the bound from "$H+2$" to "$H+1$"?

## M.I.C.

$f(n)$ is prime for some $H+2 \leq n \implies f(x)$ : irreducible in $\mathbb{Z}[X]$

$$\text{where} \quad H := \max_{0 \leq i \leq m-1} \left| \frac{a_i}{a_m} \right|$$

**The lowerbound "$H+2$" obtained is the best possible.**

**Counterexample:** $f(x) = x^3 - 9x^2 + x - 9 = (x-9)(x^2+1)$

$H = 9$ ;

# Can we refine the bound from "$H+2$" to "$H+1$"?

## M.I.C.

$f(n)$ is prime for some $H+2 \leq n \implies f(x)$ : irreducible in $\mathbb{Z}[X]$

$$\text{where} \quad H := \max_{0 \leq i \leq m-1} \left| \frac{a_i}{a_m} \right|$$

**The lowerbound "$H+2$" obtained is the best possible.**

**Counterexample:** $f(x) = x^3 - 9x^2 + x - 9 = (x-9)(x^2+1)$

$H = 9$ ; $f(10) = 101$ (prime)

# Can we refine the bound from "$H+2$" to "$H+1$"?

## M.I.C.

$f(n)$ is prime for some $H+2 \leq n \implies f(x)$ : irreducible in $\mathbb{Z}[X]$

$$\text{where} \quad H := \max_{0 \leq i \leq m-1} \left| \frac{a_i}{a_m} \right|$$

**The lowerbound "$H+2$" obtained is the best possible.**

## Counterexample: $f(x) = x^3 - 9x^2 + x - 9 = (x-9)(x^2+1)$

$H = 9$ ; $f(10) = 101$ (prime) & $H + 1 \leq 10$

# Can we refine the bound from "$H+2$" to "$H+1$"?

## M.I.C.

$f(n)$ is prime for some $H+2 \leq n \implies f(x)$ : irreducible in $\mathbb{Z}[X]$

$$\text{where} \quad H := \max_{0 \leq i \leq m-1} \left| \frac{a_i}{a_m} \right|$$

**The lowerbound "$H+2$" obtained is the best possible.**

## Counterexample: $f(x) = x^3 - 9x^2 + x - 9 = (x-9)(x^2+1)$

$H = 9$ ; $f(10) = 101$ (prime) & $H+1 \leq 10 \not\implies f$ : irreducible.

Given by Kurt Girstmair in 2005 :

## Genralized Murty's Irreducibility Criterion:

Given by Kurt Girstmair in 2005 :

## Genralized Murty's Irreducibility Criterion:

$f(x) = a_m x^m + \cdots + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[X]$ with

$$H := \max_{0 \leq i \leq m-1} \left| \frac{a_i}{a_m} \right|$$

Given by Kurt Girstmair in 2005 :

## Genralized Murty's Irreducibility Criterion:

$f(x) = a_m x^m + \cdots + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[X]$ with

$$H := \max_{0 \leq i \leq m-1} \left| \frac{a_i}{a_m} \right|$$

For some natural number $d$ , $n$ and a prime $p$

Given by Kurt Girstmair in 2005 :

## Genralized Murty's Irreducibility Criterion:

$f(x) = a_m x^m + \cdots + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[X]$ with

$$H := \max_{0 \leq i \leq m-1} \left| \frac{a_i}{a_m} \right|$$

For some natural number $d$ , $n$ and a prime $p$

$f(n) = \pm d.p \ ; \ H + d + 1 \leq n \ \ \& \ \ p \nmid d \implies f(x)$ : irreducible in $\mathbb{Z}[X]$

# Proving the Generalized M.I.C.

**Tool:** Each complex root $\alpha$ of $f(x)$ satisfies $|\alpha| < H + 1$

# Proving the Generalized M.I.C.

**Tool:** Each complex root $\alpha$ of $f(x)$ satisfies $|\alpha| < H + 1$

## Preparation

# Proving the Generalized M.I.C.

**Tool:** Each complex root $\alpha$ of $f(x)$ satisfies $|\alpha| < H + 1$

## Preparation

- $f(x) = g(x)h(x)$, where $g(x)$ and $h(x)$ are of positive degree.

$$f(n) = g(n)h(n) = \pm d \cdot p \quad \text{and} \quad p \nmid d$$

$p$ cannot divide both $g(n)$ and $h(n)$. WLOG let $p \nmid g(n)$

$\implies$ All factors of $g(n)$ are present in $d$ i.e $g(n) \mid d$

# Proving the Generalized M.I.C.

**Tool:** Each complex root $\alpha$ of $f(x)$ satisfies $|\alpha| < H + 1$

## Preparation

- $f(x) = g(x)h(x)$, where $g(x)$ and $h(x)$ are of positive degree.

$$f(n) = g(n)h(n) = \pm d \cdot p \quad \text{and} \quad p \nmid d$$

$p$ cannot divide both $g(n)$ and $h(n)$. WLOG let $p \nmid g(n)$

$\implies$ All factors of $g(n)$ are present in $d$ i.e $g(n) \mid d$

## $g(x)$ is of the form:

$$g(x) = c\prod_i (x - \alpha_i)$$

$c$ : leading coefficient of $g$ & $\alpha_i$ runs over a subset of zeros of $f$.

## $g(x)$ is of the form:

$$g(x) = c\prod_i (x - \alpha_i)$$

$c$ : leading coefficient of $g$ & $\alpha_i$ runs over a subset of zeros of $f$.

**Note:** $H + d + 1 \leq n$ & $|\alpha| < H + 1$

## $g(x)$ is of the form:

$$g(x) = c\prod_i (x - \alpha_i)$$

$c$ : leading coefficient of $g$ & $\alpha_i$ runs over a subset of zeros of $f$.

**Note:** $H + d + 1 \leq n$ & $|\alpha| < H + 1$

## Arriving at a Contradiction!

## $g(x)$ is of the form:

$$g(x) = c\prod_i (x - \alpha_i)$$

$c$ : leading coefficient of $g$ & $\alpha_i$ runs over a subset of zeros of $f$.

**Note:** $H + d + 1 \leq n$ & $|\alpha| < H + 1$

## Arriving at a Contradiction!

For each root $\alpha$ of $f(x)$ we have

$$|\,\mathbf{n} - \alpha\,| \geq n - |\alpha| \;>\; H + d + 1 - (H + 1) = \mathbf{d}$$

## $g(x)$ is of the form:

$$g(x) = c\prod_i (x - \alpha_i)$$

$c$ : leading coefficient of $g$ & $\alpha_i$ runs over a subset of zeros of $f$.

**Note:** $H + d + 1 \leq n$ & $|\alpha| < H + 1$

## Arriving at a Contradiction!

For each root $\alpha$ of $f(x)$ we have

$$|\,\mathbf{n} - \alpha\,| \geq n - |\alpha| \;>\; H + d + 1 - (H + 1) = \mathbf{d}$$

Therefore we contradict the fact $g(n) \mid d$ as

$$|\mathbf{g(n)}| = |c|\prod_i |n - \alpha_i| \;>\; \mathbf{d}$$

# The Use of Generalized M.I.C.:

## Generalized M.I.C.:

$f(n) = \pm d.p \;\; ; \;\; H + d + 1 \leq n \;\; \& \;\; p \nmid d \implies f(x)$ : irreducible in $\mathbb{Z}[X]$

$f(x) = x^4 + (4a+2)x^2 + 1 \;\; ; \; a \in \mathbb{N}$

# The Use of Generalized M.I.C.:

## Generalized M.I.C.:

$f(n) = \pm d.p \;\; ; \;\; H + d + 1 \leq n \;\; \& \;\; p \nmid d \implies f(x)$ : irreducible in $\mathbb{Z}[X]$

$f(x) = x^4 + (4a+2)x^2 + 1 \;\; ; \;\; a \in \mathbb{N}$

$a = 2 \;\; ; \;\; f(x) = x^4 + 10x + 1 \;\; ; \;\; H = 10$

# The Use of Generalized M.I.C.:

## Generalized M.I.C.:

$f(n) = \pm d.p \;\; ; \;\; H + d + 1 \leq n \;\; \& \;\; p \nmid d \implies f(x)$ : irreducible in $\mathbb{Z}[X]$

$f(x) = x^4 + (4a+2)x^2 + 1 \; ; \; a \in \mathbb{N}$

$a = 2 \; ; \; f(x) = x^4 + 10x + 1 \; ; \; H = 10$

$f(18) = 108217$ is a prime ; $H + 2 \leq 18 \implies f$ irreducible.

# The Use of Generalized M.I.C.:

## Generalized M.I.C.:

$f(n) = \pm d.p \;\; ; \;\; H + d + 1 \leq n \;\; \& \;\; p \nmid d \implies f(x)$ : irreducible in $\mathbb{Z}[X]$

$f(x) = x^4 + (4a+2)x^2 + 1 \;\; ; \;\; a \in \mathbb{N}$

$a = 2 \;\; ; \;\; f(x) = x^4 + 10x + 1 \;\; ; \;\; H = 10$

$f(18) = 108217$ is a prime ; $H + 2 \leq 18 \implies f$ irreducible.

$f(15) = 4 \cdot 13219$

# The Use of Generalized M.I.C.:

## Generalized M.I.C.:

$f(n) = \pm d.p \;\; ; \;\; H + d + 1 \leq n \;\; \& \;\; p \nmid d \implies f(x)$ : irreducible in $\mathbb{Z}[X]$

$f(x) = x^4 + (4a+2)x^2 + 1 \;\; ; \;\; a \in \mathbb{N}$

$a = 2 \;\; ; \;\; f(x) = x^4 + 10x + 1 \;\; ; \;\; H = 10$

$f(18) = 108217$ is a prime ; $H + 2 \leq 18 \implies f$ irreducible.

$f(15) = 4 \cdot 13219 \;\; ; \;\; d = 4$

# The Use of Generalized M.I.C.:

## Generalized M.I.C.:

$f(n) = \pm d.p \;\; ; \;\; H + d + 1 \leq n \;\; \& \;\; p \nmid d \implies f(x)$ : irreducible in $\mathbb{Z}[X]$

$f(x) = x^4 + (4a+2)x^2 + 1 \;\; ; \;\; a \in \mathbb{N}$

$a = 2 \;\; ; \;\; f(x) = x^4 + 10x + 1 \;\; ; \;\; H = 10$

$f(18) = 108217$ is a prime ; $H + 2 \leq 18 \implies f$ irreducible.

$f(15) = 4 \cdot 13219 \;\; ; \;\; d = 4 \;\; ; \;\; H + d + 1 \leq 15$

# The Use of Generalized M.I.C.:

## Generalized M.I.C.:

$f(n) = \pm d.p \;\; ; \;\; H + d + 1 \leq n \;\; \& \;\; p \nmid d \implies f(x)$ : irreducible in $\mathbb{Z}[X]$

$f(x) = x^4 + (4a+2)x^2 + 1 \;\; ; \;\; a \in \mathbb{N}$

$a = 2 \;\; ; \;\; f(x) = x^4 + 10x + 1 \;\; ; \;\; H = 10$

$f(18) = 108217$ is a prime ; $H + 2 \leq 18 \implies f$ irreducible.

$f(15) = 4 \cdot 13219 \;\; ; \;\; d = 4 \;\; ; \;\; H + d + 1 \leq 15 \;\; ; \;\; p \nmid d$

# The Use of Generalized M.I.C.:

## Generalized M.I.C.:

$f(n) = \pm d.p \;\; ; \;\; H + d + 1 \leq n \;\; \& \;\; p \nmid d \implies f(x)$ : irreducible in $\mathbb{Z}[X]$

$f(x) = x^4 + (4a+2)x^2 + 1 \;\; ; \;\; a \in \mathbb{N}$

$a = 2 \;\; ; \;\; f(x) = x^4 + 10x + 1 \;\; ; \;\; H = 10$

$f(18) = 108217$ is a prime ; $H + 2 \leq 18 \implies f$ irreducible.

$f(15) = 4 \cdot 13219$ ; $d = 4$ ; $H + d + 1 \leq 15$ ; $p \nmid d \implies f$ irreducible.

# The Use of Generalized M.I.C.:

## Generalized M.I.C.:

$f(n) = \pm d.p \;\; ; \;\; H + d + 1 \leq n \;\; \& \;\; p \nmid d \implies f(x)$ : irreducible in $\mathbb{Z}[X]$

$f(x) = x^4 + (4a+2)x^2 + 1 \;\; ; \;\; a \in \mathbb{N}$

$a = 2 \;\; ; \;\; f(x) = x^4 + 10x + 1 \;\; ; \;\; H = 10$

$f(18) = 108217$ is a prime ; $H + 2 \leq 18 \implies f$ irreducible.

$f(15) = 4 \cdot 13219$ ; $d = 4$ ; $H + d + 1 \leq 15$ ; $p \nmid d \implies f$ irreducible.

$a = 5 \;\; ; \;\; f(x) = x^4 + 22x + 1 \;\; ; \;\; H = 22$

# The Use of Generalized M.I.C.:

## Generalized M.I.C.:

$f(n) = \pm d.p \;\; ; \;\; H + d + 1 \leq n \;\; \& \;\; p \nmid d \implies f(x)$ : irreducible in $\mathbb{Z}[X]$

$f(x) = x^4 + (4a+2)x^2 + 1 \;\; ; \;\; a \in \mathbb{N}$

$a = 2 \;\; ; \;\; f(x) = x^4 + 10x + 1 \;\; ; \;\; H = 10$

$f(18) = 108217$ is a prime ; $H + 2 \leq 18 \implies f$ irreducible.

$f(15) = 4 \cdot 13219$ ; $d = 4$ ; $H + d + 1 \leq 15$ ; $p \nmid d \implies f$ irreducible.

$a = 5 \;\; ; \;\; f(x) = x^4 + 22x + 1 \;\; ; \;\; H = 22$

$f(204) = 1732807009$ is a prime ; $H + 2 \leq 204 \implies f$ irreducible.

# The Use of Generalized M.I.C.:

## Generalized M.I.C.:

$f(n) = \pm d.p \;\; ; \;\; H + d + 1 \leq n \;\; \& \;\; p \nmid d \implies f(x)$ : irreducible in $\mathbb{Z}[X]$

$f(x) = x^4 + (4a+2)x^2 + 1 \;\; ; \;\; a \in \mathbb{N}$

$a = 2 \;\; ; \;\; f(x) = x^4 + 10x + 1 \;\; ; \;\; H = 10$

$f(18) = 108217$ is a prime ; $H + 2 \leq 18 \implies f$ irreducible.

$f(15) = 4 \cdot 13219$ ; $d = 4$ ; $H + d + 1 \leq 15$ ; $p \nmid d \implies f$ irreducible.

$a = 5 \;\; ; \;\; f(x) = x^4 + 22x + 1 \;\; ; \;\; H = 22$

$f(204) = 1732807009$ is a prime ; $H + 2 \leq 204 \implies f$ irreducible.

$f(30) = 7 \cdot 118543$

# The Use of Generalized M.I.C.:

## Generalized M.I.C.:

$f(n) = \pm d.p \;\; ; \;\; H + d + 1 \leq n \;\; \& \;\; p \nmid d \implies f(x)$ : irreducible in $\mathbb{Z}[X]$

$f(x) = x^4 + (4a+2)x^2 + 1 \;\; ; \;\; a \in \mathbb{N}$

$a = 2 \;\; ; \;\; f(x) = x^4 + 10x + 1 \;\; ; \;\; H = 10$

$f(18) = 108217$ is a prime ; $H + 2 \leq 18 \implies f$ irreducible.

$f(15) = 4 \cdot 13219$ ; $d = 4$ ; $H + d + 1 \leq 15$ ; $p \nmid d \implies f$ irreducible.

$a = 5 \;\; ; \;\; f(x) = x^4 + 22x + 1 \;\; ; \;\; H = 22$

$f(204) = 1732807009$ is a prime ; $H + 2 \leq 204 \implies f$ irreducible.

$f(30) = 7 \cdot 118543$ ; $d = 7$

# The Use of Generalized M.I.C.:

## Generalized M.I.C.:

$f(n) = \pm d.p \;\; ; \;\; H + d + 1 \leq n \;\; \& \;\; p \nmid d \implies f(x)$ : irreducible in $\mathbb{Z}[X]$

$f(x) = x^4 + (4a+2)x^2 + 1 \;\; ; \;\; a \in \mathbb{N}$

## $a = 2 \;\; ; \;\; f(x) = x^4 + 10x + 1 \;\; ; \;\; H = 10$

$f(18) = 108217$ is a prime ; $H + 2 \leq 18 \implies f$ irreducible.

$f(15) = 4 \cdot 13219$ ; $d = 4$ ; $H + d + 1 \leq 15$ ; $p \nmid d \implies f$ irreducible.

## $a = 5 \;\; ; \;\; f(x) = x^4 + 22x + 1 \;\; ; \;\; H = 22$

$f(204) = 1732807009$ is a prime ; $H + 2 \leq 204 \implies f$ irreducible.

$f(30) = 7 \cdot 118543$ ; $d = 7$ ; $H + d + 1 \leq 30$

# The Use of Generalized M.I.C.:

## Generalized M.I.C.:

$f(n) = \pm d.p \;\; ; \;\; H + d + 1 \leq n \;\; \& \;\; p \nmid d \implies f(x)$ : irreducible in $\mathbb{Z}[X]$

$f(x) = x^4 + (4a+2)x^2 + 1 \;\; ; \;\; a \in \mathbb{N}$

$a = 2 \;\; ; \;\; f(x) = x^4 + 10x + 1 \;\; ; \;\; H = 10$

$f(18) = 108217$ is a prime ; $H + 2 \leq 18 \implies f$ irreducible.

$f(15) = 4 \cdot 13219$ ; $d = 4$ ; $H + d + 1 \leq 15$ ; $p \nmid d \implies f$ irreducible.

$a = 5 \;\; ; \;\; f(x) = x^4 + 22x + 1 \;\; ; \;\; H = 22$

$f(204) = 1732807009$ is a prime ; $H + 2 \leq 204 \implies f$ irreducible.

$f(30) = 7 \cdot 118543$ ; $d = 7$ ; $H + d + 1 \leq 30$ ; $p \nmid d$

# The Use of Generalized M.I.C.:

## Generalized M.I.C.:

$f(n) = \pm d.p \;\; ; \;\; H + d + 1 \leq n \;\; \& \;\; p \nmid d \implies f(x)$ : irreducible in $\mathbb{Z}[X]$

$f(x) = x^4 + (4a+2)x^2 + 1 \;\; ; \;\; a \in \mathbb{N}$

$a = 2 \;\; ; \;\; f(x) = x^4 + 10x + 1 \;\; ; \;\; H = 10$

$f(18) = 108217$ is a prime ; $H + 2 \leq 18 \implies f$ irreducible.

$f(15) = 4 \cdot 13219$ ; $d = 4$ ; $H + d + 1 \leq 15$ ; $p \nmid d \implies f$ irreducible.

$a = 5 \;\; ; \;\; f(x) = x^4 + 22x + 1 \;\; ; \;\; H = 22$

$f(204) = 1732807009$ is a prime ; $H + 2 \leq 204 \implies f$ irreducible.

$f(30) = 7 \cdot 118543$ ; $d = 7$ ; $H + d + 1 \leq 30$ ; $p \nmid d \implies f$ irreducible.

# Section 3

# Irreducible Polynomials from Prime numbers

# Irreducible Polynomials from Prime numbers

**Fix $b \geq 2$ ; for any $k \in \mathbb{N}$ : $k = a_n b^n + a_{n-1} b^{n-1} + \cdots + a_1 b + a_0$**

# Irreducible Polynomials from Prime numbers

**Fix $b \geq 2$ ; for any $k \in \mathbb{N}$ : $k = a_n b^n + a_{n-1} b^{n-1} + \cdots + a_1 b + a_0$**

$111 = 10^2 + 10 + 1 \quad ;$

# Irreducible Polynomials from Prime numbers

**Fix $b \geq 2$ ; for any $k \in \mathbb{N}$ : $k = a_n b^n + a_{n-1} b^{n-1} + \cdots + a_1 b + a_0$**

$111 = 10^2 + 10 + 1 \quad ; \quad 53 = 7^2 + 4 \quad ;$

# Irreducible Polynomials from Prime numbers

**Fix $b \geq 2$ ; for any $k \in \mathbb{N}$ :** $k = a_n b^n + a_{n-1} b^{n-1} + \cdots + a_1 b + a_0$

$111 = 10^2 + 10 + 1 \quad ; \quad 53 = 7^2 + 4 \quad ; \quad 53 = 3^3 + 2 \cdot 3^2 + 2 \cdot 3 + 2$

# Irreducible Polynomials from Prime numbers

**Fix $b \geq 2$ ; for any $k \in \mathbb{N}$ : $k = a_n b^n + a_{n-1} b^{n-1} + \cdots + a_1 b + a_0$**

$111 = 10^2 + 10 + 1 \quad ; \quad 53 = 7^2 + 4 \quad ; \quad 53 = 3^3 + 2 \cdot 3^2 + 2 \cdot 3 + 2$

## Cohn's Irreducibility Criterion:

$b \geq 2$ be any natural number and $p$ a prime with

$$p = a_n b^n + a_{n-1} b^{n-1} + \cdots + a_1 b + a_0 \quad \text{where } 0 \leq a_i \leq b - 1$$

# Irreducible Polynomials from Prime numbers

**Fix $b \geq 2$ ; for any $k \in \mathbb{N}$ : $k = a_n b^n + a_{n-1} b^{n-1} + \cdots + a_1 b + a_0$**

$111 = 10^2 + 10 + 1 \quad ; \quad 53 = 7^2 + 4 \quad ; \quad 53 = 3^3 + 2 \cdot 3^2 + 2 \cdot 3 + 2$

## Cohn's Irreducibility Criterion:

$b \geq 2$ be any natural number and $p$ a prime with

$$p = a_n b^n + a_{n-1} b^{n-1} + \cdots + a_1 b + a_0 \quad \text{where } 0 \leq a_i \leq b - 1$$

$$\implies f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \text{ is irreducible in } \mathbb{Z}[X].$$

# Irreducible Polynomials from Prime numbers

**Fix $b \geq 2$ ; for any $k \in \mathbb{N}$ : $k = a_n b^n + a_{n-1} b^{n-1} + \cdots + a_1 b + a_0$**

$111 = 10^2 + 10 + 1 \quad ; \quad 53 = 7^2 + 4 \quad ; \quad 53 = 3^3 + 2 \cdot 3^2 + 2 \cdot 3 + 2$

## Cohn's Irreducibility Criterion:

$b \geq 2$ be any natural number and $p$ a prime with

$$p = a_n b^n + a_{n-1} b^{n-1} + \cdots + a_1 b + a_0 \quad \text{where } 0 \leq a_i \leq b - 1$$

$$\implies f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \text{ is irreducible in } \mathbb{Z}[X].$$

## Example:

$b = 10$ ;

# Irreducible Polynomials from Prime numbers

**Fix $b \geq 2$ ; for any $k \in \mathbb{N}$ : $k = a_n b^n + a_{n-1} b^{n-1} + \cdots + a_1 b + a_0$**

$111 = 10^2 + 10 + 1 \quad ; \quad 53 = 7^2 + 4 \quad ; \quad 53 = 3^3 + 2 \cdot 3^2 + 2 \cdot 3 + 2$

## Cohn's Irreducibility Criterion:

$b \geq 2$ be any natural number and $p$ a prime with

$$p = a_n b^n + a_{n-1} b^{n-1} + \cdots + a_1 b + a_0 \quad \text{where } 0 \leq a_i \leq b - 1$$

$$\implies f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \text{ is irreducible in } \mathbb{Z}[X].$$

## Example:

$b = 10$ ; $997 = 9 \cdot 10^2 + 9 \cdot 10 + 7$

# Irreducible Polynomials from Prime numbers

**Fix $b \geq 2$ ; for any $k \in \mathbb{N}$ : $k = a_n b^n + a_{n-1} b^{n-1} + \cdots + a_1 b + a_0$**

$111 = 10^2 + 10 + 1 \quad ; \quad 53 = 7^2 + 4 \quad ; \quad 53 = 3^3 + 2 \cdot 3^2 + 2 \cdot 3 + 2$

## Cohn's Irreducibility Criterion:

$b \geq 2$ be any natural number and $p$ a prime with

$$p = a_n b^n + a_{n-1} b^{n-1} + \cdots + a_1 b + a_0 \quad \text{where } 0 \leq a_i \leq b - 1$$

$$\implies f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \text{ is irreducible in } \mathbb{Z}[X].$$

## Example:

$b = 10$ ; $997 = 9 \cdot 10^2 + 9 \cdot 10 + 7 \implies f(x) = 9x^2 + 9x + 7$ is irreducible.

# 9 Irreducible Polynomials using a single prime number

## 9 Irreducible Polynomials using a single prime number

$$101 = 2^6 + 2^5 + 2^3 + 1$$

## 9 Irreducible Polynomials using a single prime number

$$101 = 2^6 + 2^5 + 2^3 + 1$$

$$101 = 3^4 + 2 \cdot 3^2 + 2$$

$$101 = 4^3 + 2 \cdot 4^2 + 4 + 1$$

## 9 Irreducible Polynomials using a single prime number

$$101 = 2^6 + 2^5 + 2^3 + 1$$

$$101 = 3^4 + 2 \cdot 3^2 + 2$$

$$101 = 4^3 + 2 \cdot 4^2 + 4 + 1$$

$$101 = 4 \cdot 5^2 + 1$$

$$101 = 2 \cdot 6^2 + 4 \cdot 6 + 5$$

$$101 = 2 \cdot 7^2 + 3$$

## 9 Irreducible Polynomials using a single prime number

$$101 = 2^6 + 2^5 + 2^3 + 1$$

$$101 = 3^4 + 2 \cdot 3^2 + 2$$

$$101 = 4^3 + 2 \cdot 4^2 + 4 + 1$$

$$101 = 4 \cdot 5^2 + 1$$

$$101 = 2 \cdot 6^2 + 4 \cdot 6 + 5$$

$$101 = 2 \cdot 7^2 + 3$$

$$101 = 8^2 + 4 \cdot 8 + 5$$

$$101 = 9^2 + 2 \cdot 9 + 2$$

$$101 = 10^2 + 1$$

## 9 Irreducible Polynomials using a single prime number

| | |
|---|---|
| $101 = 2^6 + 2^5 + 2^3 + 1$ | $f(x) = x^6 + x^5 + x^3 + 1$ |
| $101 = 3^4 + 2 \cdot 3^2 + 2$ | $f(x) = x^4 + 2x^2 + 2$ |
| $101 = 4^3 + 2 \cdot 4^2 + 4 + 1$ | $f(x) = x^3 + 2x^2 + x + 1$ |
| $101 = 4 \cdot 5^2 + 1$ | $f(x) = 4x^2 + 1$ |
| $101 = 2 \cdot 6^2 + 4 \cdot 6 + 5$ | $f(x) = 2x^2 + 4x + 5$ |
| $101 = 2 \cdot 7^2 + 3$ | $f(x) = 2x^2 + 3$ |
| $101 = 8^2 + 4 \cdot 8 + 5$ | $f(x) = x^2 + 4x + 5$ |
| $101 = 9^2 + 2 \cdot 9 + 2$ | $f(x) = x^2 + 2x + 2$ |
| $101 = 10^2 + 1$ | $f(x) = x^2 + 1$ |

## Cohn's Irreducibility Criterion

$$p = a_n b^n + a_{n-1} b^{n-1} + \cdots + a_1 b + a_0 \quad \text{where } 0 \leq a_i \leq b-1$$

$$\implies f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \text{ is irreducible in } \mathbb{Z}[X].$$

## An important Note:

The positivity of the coefficient's plays a crucial role in Cohn's Theorem.

## Cohn's Irreducibility Criterion

$$p = a_n b^n + a_{n-1} b^{n-1} + \cdots + a_1 b + a_0 \quad \text{where } 0 \leq a_i \leq b-1$$

$$\implies f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \text{ is irreducible in } \mathbb{Z}[X].$$

## An important Note:

The positivity of the coefficient's plays a crucial role in Cohn's Theorem.

$$\mathbf{101} = 10^3 - 9 \cdot 10^2 + 10 - 9 \quad \text{is a prime number}$$

but the corresponding $\mathbf{f(x) = x^3 - 9x^2 + x - 9} = (x-9)(x^2+1)$ is reducible in $\mathbb{Z}[X]$.

# Main tool used in proving Cohn's Claim

# Main tool used in proving Cohn's Claim

## Another Root Capturing Lemma (2)

# Main tool used in proving Cohn's Claim

## Another Root Capturing Lemma (2)

$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[X]$.

# Main tool used in proving Cohn's Claim

## Another Root Capturing Lemma (2)

$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[X]$.Suppose that

$$a_n \geq 1 \ , \ a_{n-1} \geq 0 \text{ and } |a_i| < H \ \text{ for } \ i = 0, 1, ..., n-2$$

where $H$ is some positive constant.

# Main tool used in proving Cohn's Claim

## Another Root Capturing Lemma (2)

$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[X]$.Suppose that

$$a_n \geq 1 \ , \ a_{n-1} \geq 0 \text{ and } |a_i| < H \ \text{ for } \ i = 0, 1, ..., n-2$$

where $H$ is some positive constant.

Then any complex zero of $f$ either has nonpositive real part or satisfies

$$|\alpha| < \frac{1 + \sqrt{1 + 4H}}{2} = K \ (say)$$

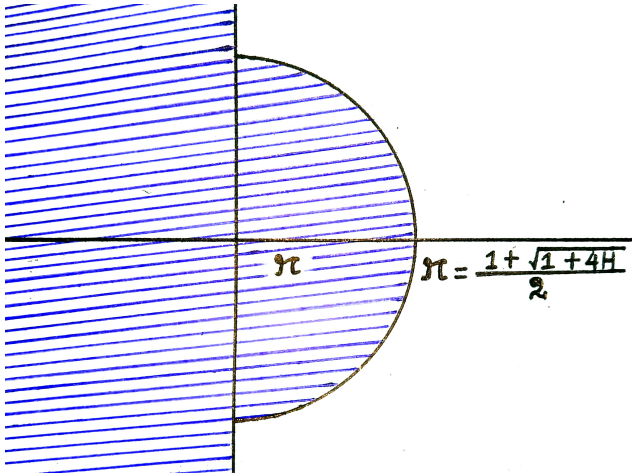



**Figure:** All the roots of $f(x)$ will lie in the shaded region.

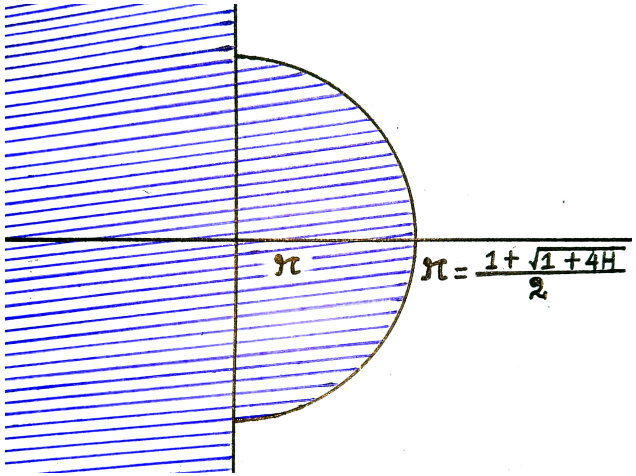



**Figure:** All the roots of $f(x)$ will lie in the shaded region.

## Strategy:

We show that for any complex number $z$ which lies

on the Right-half Plane & outside the Open Disc of radius $\frac{1+\sqrt{1+4H}}{2}$

we have $f(z) \neq 0$.

# Proving Cohn's Irreducibility Criterion

# Proving Cohn's Irreducibility Criterion

## Preparation

# Proving Cohn's Irreducibility Criterion

## Preparation

- $f(x) = g(x)h(x)$, where $g(x)$ and $h(x)$ are of positive degree.

  $f(b)$ is prime $\Rightarrow$ $g(b)$ or $h(b) = \pm 1$. WLOG we assume it to be $g(b)$.

# Proving Cohn's Irreducibility Criterion

## Preparation

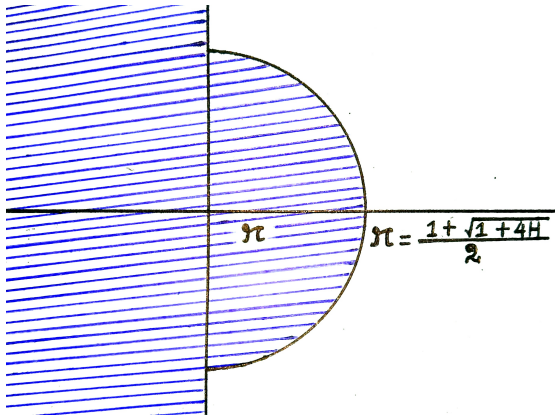
- $f(x) = g(x)h(x)$, where $g(x)$ and $h(x)$ are of positive degree.

  $f(b)$ is prime $\Rightarrow$ $g(b)$ or $h(b) = \pm 1$. WLOG we assume it to be $g(b)$.

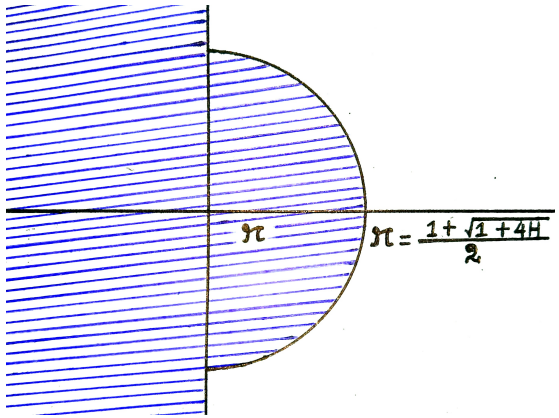
- Now $g$ is of the form

$$g(x) = c\prod_i (x - \alpha_i)$$

  $c$ : leading coefficient of $g$ & $\alpha_i$ runs over a subset of the zeros of $f$.



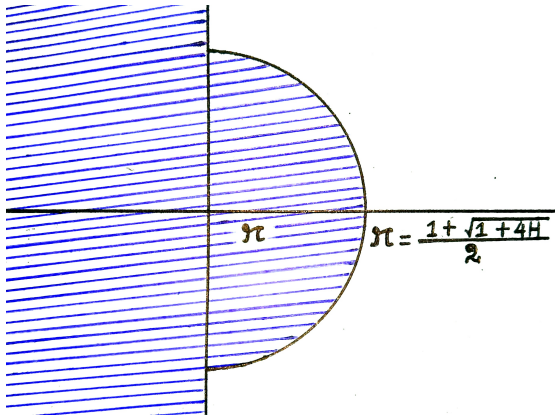

## Deploying the $2^{nd}$ Root Capturing Lemma




## Deploying the $2^{nd}$ Root Capturing Lemma

Every zeros say $(\alpha)$ of $f$ either has

1) $\Re(\alpha) \leq 0$ ; i.e. $\alpha$ lies on the left half plane.




## Deploying the $2^{nd}$ Root Capturing Lemma

Every zeros say $(\alpha)$ of $f$ either has

**1)** $\Re(\alpha) \leq 0$ ; i.e. $\alpha$ lies on the left half plane.

OR

**2)** $|\alpha| < \frac{1+\sqrt{1+4(b-1)}}{2}$ ; i.e. If it lies on the right half plane, it lies inside the mentioned disc.

## Arriving at a Contradiction!

## Arriving at a Contradiction!

We consider the mentioned two cases seperately:

## Arriving at a Contradiction!

We consider the mentioned two cases seperately:

1) As $\alpha$ lies on the Left-half Plane we immediately have $|\mathbf{b} - \alpha| \geq b > \mathbf{1}$

## Arriving at a Contradiction!

We consider the mentioned two cases seperately:

1) As $\alpha$ lies on the Left-half Plane we immediately have $|\mathbf{b} - \alpha| \geq b > \mathbf{1}$
2) In the second case we have

$$|\alpha| < \frac{\mathbf{1} + \sqrt{\mathbf{1} + \mathbf{4(b-1)}}}{\mathbf{2}} \leq \mathbf{b - 1} \implies 1 < |b - \alpha|$$

## Arriving at a Contradiction!

We consider the mentioned two cases seperately:

1) As $\alpha$ lies on the Left-half Plane we immediately have $|\mathbf{b} - \alpha| \geq b > \mathbf{1}$
2) In the second case we have

$$|\alpha| < \frac{\mathbf{1} + \sqrt{\mathbf{1} + \mathbf{4(b-1)}}}{\mathbf{2}} \leq \mathbf{b - 1} \implies 1 < |b - \alpha|$$

So $|b - \alpha_i| > 1$ for each $i$.

## Arriving at a Contradiction!

We consider the mentioned two cases seperately:

1) As $\alpha$ lies on the Left-half Plane we immediately have $|\mathbf{b}-\alpha| \geq b > \mathbf{1}$
2) In the second case we have

$$|\alpha| < \frac{\mathbf{1}+\sqrt{\mathbf{1}+\mathbf{4(b-1)}}}{\mathbf{2}} \leq \mathbf{b-1} \implies 1 < |b-\alpha|$$

So $|b-\alpha_i| > 1$ for each $i$. Hence we contradict the fact $|g(b)| = 1$ as

$$g(x) = c\prod_i (x-\alpha_i) \implies |\mathbf{g(b)}| = |c|\prod_i |b-\alpha_i| > \mathbf{1}$$

## Arriving at a Contradiction!

We consider the mentioned two cases seperately:

1) As $\alpha$ lies on the Left-half Plane we immediately have $|\mathbf{b}-\alpha| \geq b > \mathbf{1}$
2) In the second case we have

$$|\alpha| < \frac{\mathbf{1}+\sqrt{\mathbf{1}+\mathbf{4(b-1)}}}{\mathbf{2}} \leq \mathbf{b-1} \implies 1 < |b-\alpha|$$

So $|b-\alpha_i| > 1$ for each $i$. Hence we contradict the fact $|g(b)| = 1$ as

$$g(x) = c\prod_i (x-\alpha_i) \implies |\mathbf{g(b)}| = |c|\prod_i |b-\alpha_i| > \mathbf{1}$$

The proof BREAKS DOWN in the highlighted inequality when $b = 2$

To extend the proof of `Cohn's Claim` so as to cover the case $b = 2$.

We need to develop a new tool.

To extend the proof of `Cohn's Claim` so as to cover the case $b = 2$.

We need to develop a new tool.

## The strategy will be

- To take a non-trivial factor $g(x)$ of $f(x)$ with $\mid g(2) \mid = 1$

To extend the proof of `Cohn's Claim` so as to cover the case $b = 2$.

We need to develop a new tool.

## The strategy will be

- To take a non-trivial factor $g(x)$ of $f(x)$ with $\mid g(2) \mid = 1$
- Then after investigating the properties of all the complex roots of $g(x)$ we will obtain the inequality $\mid g(2) \mid > 1$, giving a contradiction.

To extend the proof of `Cohn's Claim` so as to cover the case $b = 2$.

We need to develop a new tool.

## The strategy will be

- To take a non-trivial factor $g(x)$ of $f(x)$ with $\mid g(2) \mid = 1$
- Then after investigating the properties of all the complex roots of $g(x)$ we will obtain the inequality $\mid g(2) \mid > 1$, giving a contradiction.
- Hence coming to the conclusion that $f(x)$ is irreducible for the case $b = 2$

# References

M. Ram Murty (2002)

Prime numbers and Irreducible Polynomials

*The American Mathematical Monthly;* 109:05, 452 — 458.

Kurt Gritzman (2005)

On an irreducibility criterion of M. Ram Murty

*The American Mathematical Monthly;* 112:3, 269 — 270.

M. A. Lee (1969)

Some irreducible polynomials which are reducible mod $p$ for all $p$

*The American Mathematical Monthly;* 76, 1125.

$f(x) = x^4 + (4a + 2)x + 1$ is reducible mod $p$ for all prime $p$.

`https://math.stackexchange.com/questions/4202911`

*Thank You for listening!*