Prime Numbers & Irreducible Polynomials

Saikat Goswami

Department of Mathematics, Ramakrishna Mission Vidyamandira, Belur Math

July 23,2021

Overview

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 $f(x)\ 2\ Z[X]$ 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 $f(x)\ 2\ Z[X]$ 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 $f(x)\ 2\ \mathbb{Z}[X]$ with the following properties:

1. The leading coefficient of f is positive.
2. $f(x)$ is irreducible.
3. The set $f f(n) : n\ 2\ \mathbb{N}g$ 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 $f(x)\ 2\ \mathbb{Z}[X]$ with the following properties:

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

Then the sequence $(f(n))_{n2\mathbb{N}}$ contain primes infinitely often.

Example:

$f(x) = x^2 + 1\ =)\ \ (f(n))_{n2\mathbb{N}}$ 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:

$a; d\ 2$ 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:

$a; d\ 2$ 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

$(f(n))_{n2\mathbb{N}}$ contains prime i.o. $=)$ $a_n > 0$

Investigating the assumptions in the Conjecture

$(f(n))_{n2\mathbb{N}}$ contains prime i.o. $=)$ $a_n > 0$

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

$(f(n))_{n2\mathbb{N}}$ contains prime i.o. $=)$ $a_n > 0$

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.

$(f(n))_{n2\mathbb{N}}$ contains prime i.o. $=)$ f is irreducible

Investigating the assumptions in the Conjecture

$(f(n))_{n2\mathbb{N}}$ contains prime i.o. $=)$ $a_n > 0$

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.

$(f(n))_{n2\mathbb{N}}$ contains prime i.o. $=)$ f is irreducible

If f were reducible with $f(x) = g(x)h(x)$. Then $f(n) = g(n)h(n)$ $8n$ 2 N. So $g(x)$ and $h(x)$ takes the value 1 infinitely many times ; Contradiction! So $f(n)$ is composite for all large n.

Investigating the assumptions in the Conjecture

$(f(n))_{n2\mathbb{N}}$ contains prime i.o. $=)$ $a_n > 0$

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.

$(f(n))_{n2\mathbb{N}}$ contains prime i.o. $=)$ f is irreducible

If f were reducible with $f(x) = g(x)h(x)$. Then $f(n) = g(n)h(n)$ $8n$ 2 N. So $g(x)$ and $h(x)$ takes the value 1 infinitely many times ; Contradiction! So $f(n)$ is composite for all large n.

Do (1) & (2) $=)$ there are primes infinitely often in $(f(n))_{n2\mathbb{N}}$?

$a_n > 0$ & f : irreducible $\Rightarrow$ $(f(n))_{n \in \mathbb{N}}$ 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 $\Rightarrow$ $(f(n))_{n \in \mathbb{N}}$ contains prime i.o.

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

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. $\Rightarrow$ $\{f(n) : n \in \mathbb{N}\}$ has no common divisor $d > 1$

$a_n > 0$ & f : irreducible $\Rightarrow$ $(f(n))_{n \in \mathbb{N}}$ contains prime i.o.

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

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. $\Rightarrow$ $\{f(n) : n \in \mathbb{N}\}$ has no common divisor $d > 1$

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

Extracting an Irreducibility Criterion

Extracting an Irreducibility Criterion

An Irreducibility Criterion: $f(x)\ 2\ Z[X]$ s.t.

Extracting an Irreducibility Criterion

An Irreducibility Criterion: $f(x)\ 2\ Z[X]$ s.t.

$(f(n))_{n2\mathbb{N}}$ containing primes infinitely often $=)$ f : irreducible

Extracting an Irreducibility Criterion

An Irreducibility Criterion: $f(x)\ 2\ Z[X]$ s.t.

$(f(n))_{n2\mathbb{N}}$ containing primes infinitely often $=)$ f : irreducible

The applicability of this result is very poor.

Extracting an Irreducibility Criterion

An Irreducibility Criterion: $f(x)\ 2\ Z[X]$ s.t.

$(f(n))_{n2N}$ containing primes infinitely often $=)$ f : irreducible

The applicability of this result is very poor.

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

$(f(n))_{n2N}$ contains a prime for sufficiently large n $=)$ f : irreducible

Section 2

Formal statement of M.I.C.

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

$f(x) = a_m x^m + a_{m-1} x^{m-1} + \cdots + a_1 x + a_0 \; 2 \; \mathbb{Z}[X]$ with

$$H := \max_{0 \; i \; m-1} \frac{a_i}{a_m}$$

Formal statement of M.I.C.

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

$f(x) = a_m x^m + a_{m\ \ 1} x^{m\ \ 1} + \quad + a_1 x + a_0\ 2\ Z[X]$ with

$$H := \max_{0 \quad i \quad m \quad 1} \frac{a_i}{a_m}$$

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

Formal statement of M.I.C.

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

$f(x) = a_m x^m + a_{m\ 1} x^{m\ 1} + \quad + a_1 x + a_0\ 2\ Z[X]$ with

$$H := \max_{0 \quad i \quad m\ 1} \frac{a_i}{a_m}$$

$f(n)$ is prime for some $H + 2 \quad n \quad =)$ $f(x)$: irreducible in $Z[X]$.

Formal statement of M.I.C.

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

$f(x) = a_m x^m + a_{m\ 1} x^{m\ 1} + \quad + a_1 x + a_0\ 2\ Z[X]$ with

$$H := \max_{0 \quad i \quad m\ 1} \frac{a_i}{a_m}$$

$f(n)$ is prime for some $H + 2 \quad n \quad =)\ \ f(x)$: irreducible in $Z[X]$.

Example: $f(x) = x^3 \quad x + 7$

Formal statement of M.I.C.

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

$f(x) = a_m x^m + a_{m\ 1} x^{m\ 1} + \quad + a_1 x + a_0\ 2\ Z[X]$ with

$$H := \max_{0 \quad i \quad m \ 1} \frac{a_i}{a_m}$$

$f(n)$ is prime for some $H + 2 \quad n \quad =)$ $f(x)$: irreducible in $Z[X]$.

Example: $f(x) = x^3 \quad x + 7$

$H = 7$

Formal statement of M.I.C.

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

$f(x) = a_m x^m + a_{m\ 1} x^{m\ 1} + \quad + a_1 x + a_0\ 2\ Z[X]$ with

$$H := \max_{0 \quad i \quad m \quad 1} \frac{a_i}{a_m}$$

$f(n)$ is prime for some $H + 2 \quad n \quad =) \quad f(x)$: irreducible in $Z[X]$.

Example: $f(x) = x^3 \quad x + 7$

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

Formal statement of M.I.C.

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

$f(x) = a_m x^m + a_{m\ 1} x^{m\ 1} + \quad + a_1 x + a_0\ 2\ Z[X]$ with

$$H := \max_{0 \quad i \quad m \quad 1} \frac{a_i}{a_m}$$

$f(n)$ is prime for some $H + 2 \quad n \quad =) \quad f(x)$: irreducible in $Z[X]$.

Example: $f(x) = x^3 \quad x + 7$

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

Formal statement of M.I.C.

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

$f(x) = a_m x^m + a_{m\ 1} x^{m\ 1} + \quad + a_1 x + a_0\ 2\ Z[X]$ with

$$H := \max_{0 \quad i \quad m \quad 1} \frac{a_i}{a_m}$$

$f(n)$ is prime for some $H + 2 \quad n \quad =)\ f(x)$: irreducible in $Z[X]$.

Example: $f(x) = x^3 \quad x + 7$

$H = 7$; $f(10) = 10^3 \quad 10 + 7 = 997$; $H + 2 \quad 10 \quad =)\ f$: 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:

$f(x) = a_m x^m + a_{m-1} x^{m-1} + \quad + a_1 x + a_0 \; 2 \; \mathbb{Z}[X]$; 2 C is a root.

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

A Root Capturing Lemma:

$f(x) = a_m x^m + a_{m-1} x^{m-1} + \quad + a_1 x + a_0 \ 2 \ \mathbb{Z}[X]$; $2 \ \mathbb{C}$ is a root.

Then $j \ j < H + 1$ where $H := \max_{0 \ i \ m-1} \frac{a_i}{a_m}$

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

A Root Capturing Lemma:

$f(x) = a_m x^m + a_{m-1} x^{m-1} + \quad + a_1 x + a_0 \ 2 \ \mathbb{Z}[X]$; $\ 2 \ \mathbb{C}$ is a root.

Then $j \ j < H + 1$ where $H := \max_{0 \ i \ m-1} \frac{a_i}{a_m}$

Proof:

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

A Root Capturing Lemma:

$f(x) = a_m x^m + a_{m-1} x^{m-1} + \quad + a_1 x + a_0 \ 2 \ \mathbb{Z}[X]$; $\ 2 \ \mathbb{C}$ is a root.

Then $\ j \ j < H + 1$ where $H := \max_{0 \ i \ m-1} \frac{a_i}{a_m}$

Proof:

$f(\ ) = 0 \ =) \qquad {}^m = \frac{a_{m-1}}{a_m} {}^{m-1} + \quad + \frac{a_1}{a_m} + \frac{a_0}{a_m}$

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

A Root Capturing Lemma:

$f(x) = a_m x^m + a_{m-1} x^{m-1} + \quad + a_1 x + a_0 \; 2 \; \mathbb{Z}[X]$; $\; 2 \; \mathbb{C}$ is a root.

$$\text{Then } \; j \; j < H + 1 \; \text{ where } \; H := \max_{0 \; i \; m-1} \frac{a_i}{a_m}$$

Proof:

$$f(\;) = 0 \;\; =) \qquad {}^m = \frac{a_{m-1}}{a_m} \; {}^{m-1} + \quad + \frac{a_1}{a_m} \quad + \frac{a_0}{a_m}$$

$$=) \;\; j \; j^m \quad H \; j \; j^{m-1} + \quad + j \; j + 1 \;\; = H \;\; \frac{j \; j^m \quad 1}{j \; j \quad 1}$$

Then $j \; j > 1 \;\; =) \;\; j \; j^{\mathbf{m}} \; (j \; j \quad 1) < H \; j \; j^m \quad H < \mathrm{H} \; j \; j^{\mathbf{m}}$

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 & α_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 & α_i runs over a subset of zeros of f.

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

$$|g(n)| \prod_i |n - |\alpha_i|| > \prod_i (n - (H + 1)) \geq 1$$

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 8 p.

For any a 2 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 8 p.

For any a 2 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 8 p.

For any a 2 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 8 p.

For any a 2 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 ; $H + 2$ 8

Application of M.I.C.

An Infinite family of f which are reducible mod p 8 p.

For any a 2 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 ; $H + 2$ 8 $=)$ f irreducible.

Application of M.I.C.

An Infinite family of f which are reducible mod p 8 p.

For any a 2 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 ; $H + 2$ 8 $=)$ 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 8 p.

For any a 2 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 ; $H + 2$ 8 $=)$ 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 8 p.

For any a 2 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 ; $H + 2$ 8 $=)$ f irreducible.

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

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

Application of M.I.C.

An Infinite family of f which are reducible mod p 8 p.

For any a 2 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 ; $H + 2$ 8 $=)$ f irreducible.

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

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

Application of M.I.C.

An Infinite family of f which are reducible mod p $8\ p$.

For any $a\ 2$ 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 ; $H + 2 \quad 8 \ =) \quad f$ irreducible.

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

$f(18) = 108217$ is a prime ; $H + 2 \quad 18 \ =) \quad f$ 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 $8\ p$.

For any $a\ 2$ 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 ; $H + 2 \quad 8 \ =) \quad f$ irreducible.

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

$f(18) = 108217$ is a prime ; $H + 2 \quad 18 \ =) \quad f$ 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 $8\ p$.

For any $a\ 2$ 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 ; $H + 2 \quad 8 \ =) \quad f$ irreducible.

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

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

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

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

Application of M.I.C.

An Infinite family of f which are reducible mod p $8\ p$.

For any $a\ 2$ 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 ; $H + 2 \quad 8 \ =) \quad f$ irreducible.

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

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

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

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

Application of M.I.C.

An Infinite family of f which are reducible mod p 8 p.

For any a 2 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 ; $H + 2$ 8 $=)$ f irreducible.

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

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

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

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

They are the smallest $H + 2$ 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 $H + 2 \quad n \quad =) \quad f(x)$: irreducible in $\mathbb{Z}[X]$

$$\text{where} \quad H := \max_{0 \quad i \quad m \quad 1} \frac{a_i}{a_m}$$

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 $H + 2 \quad n \quad =) \quad f(x)$: irreducible in $\mathbb{Z}[X]$

$$\text{where} \quad H := \max_{0 \quad i \quad m \quad 1} \frac{a_i}{a_m}$$

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

Counterexample: $f(x) = x^3 \quad 9x^2 + x \quad 9 = (x \quad 9)(x^2 + 1)$

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

M.I.C.

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

$$\text{where} \quad H := \max_{0 \quad i \quad m \quad 1} \frac{a_i}{a_m}$$

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

Counterexample: $f(x) = x^3 \quad 9x^2 + x \quad 9 = (x \quad 9)(x^2 + 1)$

$H = 9$;

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

M.I.C.

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

$$\text{where} \quad H := \max_{0 \quad i \quad m \quad 1} \frac{a_i}{a_m}$$

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

Counterexample: $f(x) = x^3 \quad 9x^2 + x \quad 9 = (x \quad 9)(x^2 + 1)$

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

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

M.I.C.

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

$$\text{where} \quad H := \max_{0 \quad i \quad m \quad 1} \frac{a_i}{a_m}$$

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

Counterexample: $f(x) = x^3 \quad 9x^2 + x \quad 9 = (x \quad 9)(x^2 + 1)$

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

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

M.I.C.

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

$$\text{where} \quad H := \max_{0 \quad i \quad m \quad 1} \frac{a_i}{a_m}$$

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

Counterexample: $f(x) = x^3 \quad 9x^2 + x \quad 9 = (x \quad 9)(x^2 + 1)$

$H = 9$; $f(10) = 101$ (prime) & $H + 1$ 10 $=6)$ f : irreducible.

Given by Kurt Girstmair in 2005 :

Genralized Murty's Irreducibility Criterion:

Given by Kurt Girstmair in 2005 :

Genralized Murty's Irreducibility Criterion:

$f(x) = a_m x^m + \quad + a_{m\ 1} x^{m\ 1} + \quad + a_1 x + a_0\ 2\ Z[X]$ with

$$H := \max_{0 \quad i \quad m\ 1} \frac{a_i}{a_m}$$

Given by Kurt Girstmair in 2005 :

Genralized Murty's Irreducibility Criterion:

$f(x) = a_m x^m + \quad + a_{m\ 1} x^{m\ 1} + \quad + a_1 x + a_0\ 2\ Z[X]$ with

$$H := \max_{0 \quad i \quad m\ 1} \frac{a_i}{a_m}$$

For some natural number d , n and a prime p

Given by Kurt Girstmair in 2005 :

Genralized Murty's Irreducibility Criterion:

$f(x) = a_m x^m + \quad + a_{m\ 1} x^{m\ 1} + \quad + a_1 x + a_0\ 2\ Z[X]$ with

$$H := \max_{0 \quad i \quad m\ 1} \frac{a_i}{a_m}$$

For some natural number d , n and a prime p

$f(n) = \quad d{:}p \ ; \ H + d + 1 \quad n \ \& \ p\not| d =) \quad f(x)$: irreducible in $Z[X]$

Proving the Generalized M.I.C.

Tool: Each complex root of $f(x)$ satisfies j $j < H + 1$

Proving the Generalized M.I.C.

Tool: Each complex root of $f(x)$ satisfies j $j < H + 1$

Preparation

Proving the Generalized M.I.C.

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

Preparation

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

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

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

$\Rightarrow$) 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 of $f(x)$ satisfies $|\ | < H + 1$

Preparation

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

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

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

$\Rightarrow$) 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 & α_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 & α_i runs over a subset of zeros of f.

Note: $H + d + 1$ n & j $j < H + 1$

$g(x)$ is of the form:

$$g(x) = c \prod_{i} (x - \alpha_i)$$

c : leading coefficient of g & α_i runs over a subset of zeros of f.

Note: $H + d + 1$ n & j $j < H + 1$

Arriving at a Contradiction!

$g(x)$ is of the form:

$$g(x) = c \prod_{i} (x - \alpha_i)$$

c : leading coefficient of g & α_i runs over a subset of zeros of f.

Note: $H + d + 1$ n & j $j < H + 1$

Arriving at a Contradiction!

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

j n j n j j $>$ $H + d + 1$ $(H + 1) =$ d

$g(x)$ is of the form:

$$g(x) = c \prod_{i} (x \quad _i)$$

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

Note: $H + d + 1$ n & j $j < H + 1$

Arriving at a Contradiction!

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

$$j \, n \quad j \quad n \quad j \; j > H + d + 1 \quad (H + 1) = d$$

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

$$jg(n)j = jcj \prod_{i} jn \quad _ij > d$$

The Use of Generalized M.I.C.:

Generalized M.I.C.:

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

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

The Use of Generalized M.I.C.:

Generalized M.I.C.:

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

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

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

The Use of Generalized M.I.C.:

Generalized M.I.C.:

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

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

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

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

The Use of Generalized M.I.C.:

Generalized M.I.C.:

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

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

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

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

$f(15) = 4$ 13219

The Use of Generalized M.I.C.:

Generalized M.I.C.:

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

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

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

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

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

The Use of Generalized M.I.C.:

Generalized M.I.C.:

$f(n) = d:p$; $H + d + 1$ n & $p6 d$ $=)$ $f(x)$: irreducible in $Z[X]$

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

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

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

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

The Use of Generalized M.I.C.:

Generalized M.I.C.:

$f(n) = d:p \ ; \ H + d + 1 \quad n \ \& \quad p \nmid d \ ) \quad f(x)$: irreducible in $Z[X]$

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

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

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

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

The Use of Generalized M.I.C.:

Generalized M.I.C.:

$f(n) = d : p \;;\; H + d + 1 \quad n \;\&\; p \nmid d \Rightarrow f(x)$: 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 ; $H + 2 \quad 18 \Rightarrow f$ irreducible.

$f(15) = 4 \quad 13219 \;;\; d = 4 \;;\; H + d + 1 \quad 15 \;;\; p \nmid d \Rightarrow f$ irreducible.

The Use of Generalized M.I.C.:

Generalized M.I.C.:

$f(n) = d : p \;;\; H + d + 1 \quad n \;\&\; p \nmid d \Rightarrow f(x)$: 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 ; $H + 2 \quad 18 \Rightarrow f$ irreducible.

$f(15) = 4 \quad 13219 \;;\; d = 4 \;;\; H + d + 1 \quad 15 \;;\; p \nmid d \Rightarrow f$ irreducible.

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

The Use of Generalized M.I.C.:

Generalized M.I.C.:

$f(n) = \; d{:}p \;\; ; \;\; H + d + 1 \quad n \;\; \& \;\; p6j\, d \;\; =) \;\; f(x)$: irreducible in $Z[X]$

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

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

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

$f(15) = 4 \quad 13219$; $d = 4$; $H + d + 1 \quad 15$; $p6j\, d \;\; =) \;\; f$ irreducible.

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

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

The Use of Generalized M.I.C.:

Generalized M.I.C.:

$f(n) = d:p$; $H + d + 1 \quad n$ & $p \not| d$ $) f(x)$: irreducible in $Z[X]$

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

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

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

$f(15) = 4 \quad 13219$; $d = 4$; $H + d + 1 \quad 15$; $p \not| d$ $) f$ irreducible.

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

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

$f(30) = 7 \quad 118543$

The Use of Generalized M.I.C.:

Generalized M.I.C.:

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

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

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

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

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

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

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

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

The Use of Generalized M.I.C.:

Generalized M.I.C.:

$f(n) = d:p$; $H + d + 1$ n & $p \nmid d$ $\Rightarrow$ $f(x)$: 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 ; $H + 2$ 18 $\Rightarrow$ f irreducible.

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

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

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

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

The Use of Generalized M.I.C.:

Generalized M.I.C.:

$f(n) = d:p \;;\; H + d + 1 \quad n \;\&\; p \nmid d \Rightarrow f(x)$: 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 ; $H + 2 \quad 18 \Rightarrow f$ irreducible.

$f(15) = 4 \quad 13219$; $d = 4$; $H + d + 1 \quad 15$; $p \nmid d \Rightarrow f$ irreducible.

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

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

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

The Use of Generalized M.I.C.:

Generalized M.I.C.:

$f(n) = d:p \;;\; H + d + 1 \quad n \;\&\; p \nmid d \;) \; f(x)$: irreducible in $Z[X]$

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

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

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

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

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

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

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

Section 3

Irreducible Polynomials from Prime numbers

Irreducible Polynomials from Prime numbers

Fix b 2 ; for any k 2 N : $k = a_n b^n + a_{n\ 1} b^{n\ 1} +$ $+ a_1 b + a_0$

Irreducible Polynomials from Prime numbers

Fix b 2 ; for any k 2 N : $k = a_n b^n + a_{n\ 1} b^{n\ 1} +$ $+ a_1 b + a_0$

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

Irreducible Polynomials from Prime numbers

Fix b 2 ; for any k 2 N : $k = a_n b^n + a_{n\ 1} b^{n\ 1} + \quad + a_1 b + a_0$

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

Irreducible Polynomials from Prime numbers

Fix b 2 ; for any k 2 N : $k = a_n b^n + a_{n\ 1} b^{n\ 1} + \quad + a_1 b + a_0$

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

Irreducible Polynomials from Prime numbers

Fix $b \quad 2$; for any $k \; 2 \; \mathbb{N}$: $k = a_n b^n + a_{n \; 1} b^{n \; 1} + \quad + a_1 b + a_0$

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

Cohn's Irreducibility Criterion:

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

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

Irreducible Polynomials from Prime numbers

Fix b 2 ; for any k 2 N : $k = a_n b^n + a_{n\ 1} b^{n\ 1} + \quad + a_1 b + a_0$

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

Cohn's Irreducibility Criterion:

b 2 be any natural number and p a prime with

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

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

Irreducible Polynomials from Prime numbers

Fix b 2 ; for any k 2 N : $k = a_n b^n + a_{n\ 1} b^{n\ 1} + \quad + a_1 b + a_0$

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

Cohn's Irreducibility Criterion:

b 2 be any natural number and p a prime with

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

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

Example:

$b = 10$;

Irreducible Polynomials from Prime numbers

Fix b 2 ; for any k 2 N : $k = a_n b^n + a_{n\ 1} b^{n\ 1} + \quad + a_1 b + a_0$

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

Cohn's Irreducibility Criterion:

b 2 be any natural number and p a prime with

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

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

Example:

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

Irreducible Polynomials from Prime numbers

Fix b 2 ; for any k 2 N : $k = a_n b^n + a_{n\ 1} b^{n\ 1} +$ $+ a_1 b + a_0$

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

Cohn's Irreducibility Criterion:

b 2 be any natural number and p a prime with

$p = a_n b^n + a_{n\ 1} b^{n\ 1} +$ $+ a_1 b + a_0$ where 0 a_i b 1

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

Example:

$b = 10$; $997 = 9\ 10^2 + 9\ 10 + 7$ $=)$ $f(x) = 9x^2 + 9x + 7$ 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

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

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

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

9 Irreducible Polynomials using a single prime number

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

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

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

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

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

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

9 Irreducible Polynomials using a single prime number

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

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

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

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

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

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

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

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

$101 = 10^2 + 1$

9 Irreducible Polynomials using a single prime number

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

Cohn's Irreducibility Criterion

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

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

An important Note:

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

Cohn's Irreducibility Criterion

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

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

An important Note:

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

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

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

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)

$f(x) = a_n x^n + a_{n\ 1} x^{n\ 1} + \quad + a_1 x + a_0\ 2\ Z[X]$.

Main tool used in proving Cohn's Claim

Another Root Capturing Lemma (2)

$f(x) = a_n x^n + a_{n\ \ 1} x^{n\ \ 1} + \quad + a_1 x + a_0\ 2\ Z[X]$.Suppose that

$$a_n \quad 1\ ;\ a_{n\ \ 1} \quad 0 \text{ and } ja_i j < H \quad \text{for} \quad i = 0; 1; :::; n \quad 2$$

where H is some positive constant.

Main tool used in proving Cohn's Claim

Another Root Capturing Lemma (2)

$f(x) = a_n x^n + a_{n\ 1} x^{n\ 1} + \quad + a_1 x + a_0\ 2\ Z[X]$.Suppose that

$$a_n \quad 1\ ;\ a_{n\ 1} \quad 0 \text{ and } ja_i j < H \quad \text{for} \quad i = 0; 1; :::; n \quad 2$$

where H is some positive constant.

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

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

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 & α_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 ( ) of f either has

1) R( ) 0 ; i.e. lies on the left half plane.

Deploying the 2^{nd} Root Capturing Lemma

Every zeros say () of f either has

1) R( ) 0 ; i.e. lies on the left half plane.

OR

2) j j < $\frac{1+\sqrt{1+4(b\ \ 1)}}{2}$; 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 lies on the Left-half Plane we immediately have $|b| > 1$

Arriving at a Contradiction!

We consider the mentioned two cases seperately:

1) As lies on the Left-half Plane we immediately have $|jb| \leq |j| \quad b > 1$
2) In the second case we have

$$|j| \; |j| < \frac{1 + \sqrt{1 + 4(b \quad 1)}}{2} \quad b \quad 1 \; =) \quad 1 < |jb| \quad |j|$$

Arriving at a Contradiction!

We consider the mentioned two cases seperately:

1) As lies on the Left-half Plane we immediately hajvbe j b > 1
2) In the second case we have

$$j\ j < \frac{1 + \sqrt{1 + 4(b\ \ 1)}}{2} \quad b\ \ 1 =) \quad 1 < jb\ \ j$$

So jb ¡j > 1 for eachi.

Arriving at a Contradiction!

We consider the mentioned two cases seperately:

1) As lies on the Left-half Plane we immediately have $|b| \quad |\quad b > 1$
2) In the second case we have

$$|\ \ | < \frac{1 + \sqrt{1 + 4(b \quad 1)}}{2} \quad b \quad 1 \ =) \quad 1 < |b \quad |$$

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

$$g(x) = c \prod_i (x \quad _i) \ =) \ |\ g(b)| = |c| \prod_i |b \quad _i| > 1$$

Arriving at a Contradiction!

We consider the mentioned two cases seperately:

1) As lies on the Left-half Plane we immediately have $|b| \quad |b| > 1$
2) In the second case we have

$$|\ | < \frac{1 + \sqrt{1 + 4(b \quad 1)}}{2} \qquad b \quad 1 \ =) \quad 1 < |b \quad |$$

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

$$g(x) = c \prod_i (x \quad _i) \ =) \ |g(b)| = |c| \prod_i |b \quad _i| > 1$$

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

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 $j\ g(2)\ j = 1$

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 $|g(2)| = 1$

Then after investigating the properties of all the complex roots of $g(x)$ we will obtain the inequality $|g(2)| > 1$, 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 $|g(2)| = 1$

Then after investigating the properties of all the complex roots of $g(x)$ we will obtain the inequality $|g(2)| > 1$, 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!