IRREDUCIBILITY CRITERIA FOR POLYNOMIALS OVER THE FIELD OF RATIONALS

PRADEEP MAAN, AMIT SEHGAL, AND ARCHANA MALIK

Abstract. In this paper we discuss , (i) $f(x) \in \mathbb{Z}[x]$ be a polynomial of degree n having all zeros in the set D_r for some $r \in N - \{1\}$ and there exists an integer m with $|m| \geq r + t$ where $t \in N$ such that $|f(m)|$ is t-times product of s primes (which may or may not be distinct), then $f(x)$ has at most s irreducible factors in $\mathbb{Z}[x]$ and (ii) Let $f(x) \in \mathbb{Z}[x]$ be a polynomial of degree n having all zeros in the set OD_r for some $r \in N - \{1\}$. If $|f(m)|$ is product of r primes where $|m| < r - 1$, then $f(x)$ has at most r irreducible factors in $\mathbb{Z}[x]$.

1. Introduction

There has been a close relationship between prime numbers and irreducibility. Establishing the relationship firstly $A\ Cohn's$ Irreducibility Criterion for base-10 version was introduced in [1].A classical Cohn's irreducibility criteria stated:- If a prime number p is expressed in base-10 as $p = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1\ 10 + a_0$ (where $0 \leq a_i \leq 9$) then the polynomial $f(x) = a_k x^k + a_{k-1} x^{k-1} + \cdots + a_1\ x + a_0$ is irreducible in $\mathbb{Z}$[x]. The generalisation of $A\ Cohn's$ irreducibility criterion for base-b is given by Brillhart, Filesta and Odlyzko in [2] which is stated as:- If a prime number p is expressed in base-b as $p = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1\ b + a_0$ (where $0 \leq a_i \leq b - 1$) then the polynomial $f(x) = a_k x^k + a_{k-1} x^{k-1} + \cdots + a_1\ x + a_0$ is irreducible in $\mathbb{Z}[x]$.R.Murthy gave a simplified proof and history of the result in [3]. There exists various results on prime b-adiac expansion and polynomials having prime or prime power value. The well known Eisenstein's irreducibility criterion is a sufficient condition to check irreducibility of polynomials but this criterion is not applicable to all polynomials with integer coefficients that are irreducible over the rational numbers.Being a sufficient condition its domain is restricted. Furthermore all these results available are sufficient conditions for irreducibility of polynomials. So, many researchers are working towards new irreducibility criteria on different domains.

2. Preliminary Results

Let the set $\{z \in \mathbb{C} | |z| < r, r \in N\}$ and $\{z \in C | |z| > r, r \in N\}$ are denoted by D_r and OD_r,where $\mathbb{C}$ denotes the set of complex numbers.

2000 *Mathematics Subject Classification.* Primary 12E05; Secondary 11R09.
Key words and phrases. Field; Polynomials; Reducibility and irreducibility of polynomials; Polynomial factorization.

A region D_r which denoted above is simply connected because every closed curve which lies entirely in D_r can be pulled to a single point in D_r.

Now we prove two lemmas which are extension of lemma 2.1 from [4].

Lemma 2.1. *Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ be a polynomial such that $0 < a_0 \le a_1 \le \cdots \le a_{k-1} < a_k \le \cdots \le a_n$ for some $0 < k \le n$ then $f(x) \in Z[x]$ is a polynomial having all zeros in the set D_r for some $r \in N - \{1\}$.*

Proof:- Suppose on the contrary $f(x)$ has a zero α with $|\alpha| \ge r$. Then α is a root of $F(x) = (x-1)f(x) = a_n x^{n+1} + (a_{n-1} - a_n)x^n + \cdots + (a_0 - a_1)x - a_0$. α being root of $F(x)$, we have $a_n\alpha^{n+1} = (a_n - a_{n-1})\alpha^n + \cdots + (a_1 - a_0)\alpha + a_0$. Now, $|\alpha| \ge r > 1$, we get $|a_n\alpha^{n+1}| < (a_n - a_{n-1})|\alpha^n| + \cdots + (a_1 - a_0)|\alpha^n| + a_0|\alpha^n| = |a_n\alpha^n|$ which leads to a contradiction $|\alpha| < 1$ because $a_n > 0$. Hence, $f(x) \in \mathbb{Z}[x]$ is a polynomial having all zeros in the set D_r.

Lemma 2.2. *Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ be a polynomial of degree n such that $-[\frac{r-1}{2}]|a_n| < a_0 \le a_1 \le \cdots \le a_{k-1} < a_k \le \cdots a_n$ for some $0 < k \le n$, then $f(x) \in \mathbb{Z}[x]$ be a polynomial having all zeros in the set D_r for some $r \in N - \{1\}$.*

Proof:-Suppose on the contrary $f(x)$ has a zero α with $|\alpha| \ge r$. Then α is a root of $F(x) = (x-1)f(x) = a_n x^{n+1} + (a_{n-1} - a_n)x^n + \cdots + (a_0 - a_1)x - a_0$. α being root of $F(x)$, we have $a_n\alpha^{n+1} = (a_n - a_{n-1})\alpha^n + \cdots + (a_1 - a_0)\alpha + a_0$.

Case 1:-None of a_i is negative (means positive or zero)

Now, using $|\alpha| \ge r > 1$, we get $|a_n\alpha^{n+1}| < (a_n - a_{n-1})|\alpha^n| + \cdots + (a_1 - a_0)|\alpha^n| + a_0|\alpha^n| = |a_n\alpha^n|$ which leads to a contradiction $|\alpha| < 1$ because $a_n > 0$. Hence $f(x) \in \mathbb{Z}[x]$ is a polynomial having all zeros in the set D_r.

Case 2:- Some of a_i may negative or zero but $a_n \ne 0$

Now using the concept that $|\alpha| \ge r > 1$, we have $|a_n\alpha^{n+1}| < (a_n - a_{n-1})|\alpha^n| + \cdots + (a_1 - a_0)|\alpha^n| + (-a_0)|\alpha^n| = (a_n - 2a_0)|\alpha^n| < (|a_n| + 2|a_0|)|\alpha^n|$ implies $|\alpha| < 1 + \frac{2|a_0|}{|a_n|} < 1 + 2[\frac{r-1}{2}] \le r$ which leads to a contradiction $|\alpha| < r$ because $-[\frac{r-1}{2}]|a_n| < a_0$.Hence, $f(x) \in \mathbb{Z}[x]$ is a polynomial having all zeros in the set D_r. Redefining lemma 1 from [3].

Lemma 2.3. *Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ be a polynomial of degree n such that $a_n > 0$ and $r > \max(\max_{0 \le i \le n-1} |\frac{n a_i}{a_n}|, 1)$ then $f(x) \in \mathbb{Z}[x]$ is a polynomial having all zeros in the set D_r for some $r \in N - \{1\}$.*

Proof:-Suppose to the contrary that $f(x)$ has a zero α with $|\alpha| \ge r$. Then $a_n\alpha^n = (-a_{n-1})\alpha^{n-1} + \cdots + (-a_1)\alpha - a_0$.

$|a_n\alpha^n| = |(-a_{n-1})\alpha^{n-1} + \cdots + (-a_1)\alpha - a_0| \le (|a_{n-1}||\alpha^{n-1}| + \cdots + |a_1||\alpha| + |a_0|)$.

$|\alpha^n| \le (\frac{|a_{n-1}|}{|a_n|}|\alpha|^{n-1} + \cdots + \frac{|a_1|}{|a_n|}|\alpha| + \frac{|a_0|}{|a_n|}) \le \max_{0 \le i \le n-1} |\frac{a_i}{a_n}|(|\alpha|^{n-1} + \cdots + |\alpha|^{n-1} + |\alpha|^{n-1})$

By use of $|\alpha| \ge r > 1$, we get $|\alpha^n| \le \max_{0 \le i \le n-1} |\frac{a_i}{a_n}|(|\alpha|^{n-1})$.

Now, we have $|\alpha| \le \max_{0 \le i \le n-1} |\frac{a_i}{a_n}| < r$ which leads to a contradiction $|\alpha| < r$. Hence, $f(x) \in \mathbb{Z}[x]$ be a polynomial having all zeros in the set D_r.

Next lemma is extension of previous one.

Lemma 2.4. *Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ be a polynomial of degree n such that $a_n > 0$ and $r > \max(|\frac{|a_{n-1}|+|a_{n-2}|+\cdots+|a_1|+|a_0|}{a_n}|, 1)$ then $f(x) \in \mathbb{Z}[x]$ is a polynomial having all zeros in the set D_r for some $r \in N - \{1\}$.*

Proof:-Suppose to the contrary that $f(x)$ has a zero α with $|\alpha| \geq r$. Then $a_n\alpha^n = (-a_{n-1})\alpha^{n-1} + \cdots + (-a_1)\alpha - a_0$.
$|a_n\alpha^n| = |(-a_{n-1})\alpha^{n-1} + \cdots + (-a_1)\alpha - a_0| \leq (|a_{n-1}||\alpha^{n-1}| + \cdots + |a_1||\alpha| + |a_0|)$.
$|\alpha^n| \leq (\frac{|a_{n-1}|}{|a_n|}|\alpha|^{n-1} + \cdots + \frac{|a_1|}{|a_n|}|\alpha| + \frac{|a_0|}{|a_n|}) \leq (|\frac{a_i}{a_n}||\alpha|^{n-1}| + \cdots + |\frac{a_1}{a_n}||\alpha|^{n-1}| + |\frac{a_0}{a_n}||\alpha|^{n-1}|)$
$|\alpha^n| \leq \frac{|a_{n-1}|+|a_{n-2}|+\cdots+|a_1|+|a_0|}{|a_n|}|\alpha^{n-1}|$.
By use of $|\alpha| \geq r > 1$, we get $|\alpha^n| \leq \frac{|a_{n-1}|+|a_{n-2}|+\cdots+|a_1|+|a_0|}{|a_n|}|\alpha^{n-1}|$.
Now, we have $|\alpha| \leq \frac{|a_{n-1}|+|a_{n-2}|+\cdots+|a_1|+|a_0|}{|a_n|} < r$ which leads to a contradiction $|\alpha| < r$.
Hence, $f(x) \in \mathbb{Z}[x]$ is a polynomial having all zeros in the set D_r.

Theorem 2.5. *(Rouche's Theorem) If we have functions f and g which are analytic on a simple closed contour C, and meromorphic inside the contour C, and if $|g| < |f|$ on contour C, then both f and $f + g$ have same number of zeros in C,where each zero is counted as many times as its multiplicity.*

3. Main Theorems

Now we extend Lemma 2.2 from [4].

Theorem 3.1. *Let $f(x) \in \mathbb{Z}[x]$ be a polynomial having all zeros in the set D_r for some $r \in N - \{1\}$. If there exists an integer m with $|m| \geq r + t$ where $t \in N$ such that $|f(m)|$ is $t-$times of the prime number, then $f(x)$ is irreducible over the field of rationals.*

Proof:-Suppose to the contrary that $f(x) = g(x)h(x)$ where $g(x), h(x) \in \mathbb{Z}[x]$. In view of hypothesis at least one of $|g(m)|, |h(m)|$ is divisor of t . Without loss of generality, assume that $|g(m)||t$.

Write $g(x) = c\prod_{i=1}^{k}(x - \alpha_i)$ where $\alpha_i \in D_r \forall\ i = 1, 2, \cdots, k$

Keeping in mind that $|\alpha_i| < r$ and $|m| \geq r+t \implies |m|-|\alpha_i| > t \;\forall\, i = 1, 2, \cdots, k$

By use of $|a - b| \geq |a| - |b|$, we have

$|g(m)| = |c|\prod_{i=1}^{k}|(m - \alpha_i)| \geq |c|\prod_{i=1}^{k}(|m| - |\alpha_i|) > t$ which is a contradiction to the fact that $f(x)$ is reducible over $\mathbb{Z}[x]$, hence we get $f(x)$ is irreducible over $\mathbb{Z}[x]$ and consequently irreducible over $Q[x]$.

Theorem 3.2. *Let $f(x) \in \mathbb{Z}[x]$ be a polynomial of degree n having all zeros in the set D_r for some $r \in N - \{1\}$. If there exists an integer m with $|m| \geq r + 1$ such that $|f(m)|$ is a product of s primes (which may or may not be distinct), then $f(x)$ has at most s irreducible factors in $\mathbb{Q}[x]$.*

Proof:-Suppose to the contrary that $f(x) = g_1(x)g_2(x)g_3(x)\cdots g_{s+1}(x)$ where $g_1(x), g_2(x), \cdots, g_{s+1}(x) \in \mathbb{Q}[x]$. In view of hypothesis at least one of $|g_i(m)|$ where

$1 \leq i \leq s+1$ is equal to 1. Without loss of generality, assume that $|g_1(m)| = 1$. Write $g_1(x) = c\prod_{i=1}^{k}(x - \alpha_i)$ where $\alpha_i \in D_r \forall\ i = 1, 2, \cdots, k$

Keeping in mind that $|\alpha_i| < r$ and $|m| \geq r+1 \implies |m| - |\alpha_i| > 1\ \forall\ i = 1, 2, \cdots, k$

By use of inequality $|a-b| \geq |a| - |b|$, we have

$|g_1(m)| = |c|\prod_{i=1}^{k}|(m - \alpha_i)| \geq |c|\prod_{i=1}^{k}(|m| - |\alpha_i|) > 1$ which is a contradiction with fact that $f(x)$ has more than s irreducible factors over $\mathbb{Q}[x]$, hence we get $f(x)$ has at most s irreducible factors in $\mathbb{Q}[x]$.

Theorem 3.3. *Let $f(x) \in \mathbb{Z}[x]$ be a polynomial of degree n having all zeros in the set D_r for some $r \in N - \{1\}$. If there exists an integer m with $|m| \geq r + t$ where $t \in N$ such that $|f(m)|$ is t-times product of s primes (which may or may not be distinct), then $f(x)$ has at most s irreducible factors in $\mathbb{Q}[x]$.*

Proof:-Suppose to the contrary that $f(x) = g_1(x)g_2(x)g_3(x)\cdots g_{s+1}(x)$ where $g_1(x)g_2(x)\cdots g_{s+1}(x) \in \mathbb{Q}[x]$. In view of hypothesis at least one of $|g_i(m)|$ where $1 \leq i \leq s+1$ is divisor of t. Without loss of generality, assume that $|g_1(m)||t$. Write $g_1(x) = c\prod_{i=1}^{k}(x - \alpha_i)$ where $\alpha_i \in D_r \forall\ i = 1, 2, \cdots, k$

Keeping in mind that $|\alpha_i| < r$ and $|m| \geq r+t \implies |m| - |\alpha_i| > t\ \forall\ i = 1, 2, \cdots, k$

By use of inequality $|a-b| \geq |a| - |b|$, we say that

$|g_1(m)| = |c|\prod_{i=1}^{k}|(m - \alpha_i)| \geq |c|\prod_{i=1}^{k}(|m| - |\alpha_i|) > t$ which is a contradiction with fact that $f(x)$ has more than s irreducible factors over $\mathbb{Z}[x]$, hence we get $f(x)$ has at most s irreducible factors over $\mathbb{Z}[x]$.

Theorem 3.4. *Let $f(x) \in \mathbb{Z}[x]$ be a polynomial of degree n having all zeros in the set OD_r for some $r \in N - \{1\}$. If $|f(m)$ is t-times a prime where $|m| < r - t$ where t is a positive integer less than p, then $f(x)$ is irreducible in $\mathbb{Q}[x]$.*

Proof:-Suppose to the contrary that $f(x) = g_1(x)g_2(x)$ where $g_1(x), g_2(x) \in \mathbb{Z}[x]$. In view of hypothesis at least one of $|g_i(m)|$ where $1 \leq i \leq 2$ is equal to 1. Without loss of generality, assume that $|g_1(m)||t$. Write $g_1(x) = c\prod_{i=1}^{k}(x - \alpha_i)$ where $\alpha_i \in OD_r \forall\ i = 1, 2, \cdots, k$

Keeping in mind that $|\alpha_i| > r > 1 \forall\ i = 1, 2, \cdots, k$. Using $|m| < p - t$, we get $-|m| > t - p$.

Now $|\alpha_i| - |m| > t \forall\ i = 1, 2, \cdots, k$

By use of inequality $|a-b| \geq |a| - |b|$, we say that

$|g_1(m)| = |c|\prod_{i=1}^{k}|(m - \alpha_i)| \geq |c|\prod_{i=1}^{k}(|\alpha_i| - |m|) > t$ which is a contradiction with fact that $f(x)$ is irreducible over $\mathbb{Z}[x]$.

Theorem 3.5. *Let $f(x) \in \mathbb{Z}[x]$ be a polynomial of degree n having all zeros in the set OD_r for some $r \in N - \{1\}$. If $|f(m)|$ is t-times product of two prime where $|m| < r - t$ where t is a positive integer less than p, then $f(x)$ has at most two irreducible factors in $\mathbb{Q}[x]$.*

Proof:-Suppose to the contrary that $f(x) = g_1(x)g_2(x)g_3(x)$ where $g_1(x), g_2(x)$ and $g_3(x) \in \mathbb{Z}[x]$. In view of hypothesis at least one of $|g_i(m)|$ where $1 \leq i \leq 3$ is equal to 1. Without loss of generality, assume that $|g_1(m)||t$. Write $g_1(x) = c\prod_{i=1}^{k}(x - \alpha_i)$ where $\alpha_i \in OD_r \forall\ i = 1, 2, \cdots, k$

Keeping in mind that $|\alpha_i| > r > 1 \forall\ i = 1, 2, \cdots, k$. Using $|m| < r - t$, we get $-|m| > t - r$.
Now $|\alpha_i| - |m| > t \forall\ i = 1, 2, \cdots, k$

By use of inequality $|a - b| \geq |a| - |b|$, we say that

$|g_1(m)| = |c| \prod_{i=1}^{k} |(m - \alpha_i)| \geq |c| \prod_{i=1}^{k}(|\alpha_i| - |m|) > t$ which is a contradiction with fact that $f(x)$ is irreducible over $\mathbb{Z}[x]$.

Theorem 3.6. *Let $f(x) \in \mathbb{Z}[x]$ be a polynomial of degree n having all zeros in the set OD_r for some $r \in N - \{1\}$. If $|f(m)$ is product of r primes where $|m| < r - 1$, then $f(x)$ has at most r irreducible factors in $\mathbb{Z}[x]$.*

Proof:-Suppose to the contrary that $f(x) = g_1(x)g_2(x)g_3(x) \cdots g_{r+1}(x)$ where $g_1(x), g_2(x), g_3(x), \cdots, g_{r+1}(x) \in \mathbb{Z}[x]$. In view of hypothesis at least one of $|g_i(m)|$ where $1 \leq i \leq r+1$ is equal to 1. Without loss of generality, assume that $|g_1(m)||t$. Write $g_1(x) = c \prod_{i=1}^{k}(x - \alpha_i)$ where $\alpha_i \in OD_r \forall\ i = 1, 2, \cdots, k$

Keeping in mind that $|\alpha_i| > r > 1 \forall\ i = 1, 2, \cdots, k$. Using $|m| < r - 1$, we get $-|m| > 1 - r$.
Now $|\alpha_i| - |m| > 1 \forall\ i = 1, 2, \cdots, k$

By use of inequality $|a - b| \geq |a| - |b|$, we say that

$|g_1(m)| = |c| \prod_{i=1}^{k} |(m - \alpha_i)| \geq |c| \prod_{i=1}^{k}(|\alpha_i| - |m|) > 1$ which is a contradiction with fact that $f(x)$ is irreducible over $\mathbb{Z}[x]$ hence over $\mathbb{Q}[x]$.

4. Example

Example 4.1. Polynomial $f(x) = x^5 + x^4 + 2x^3 + 2x^2 + 2x + 3 \in Z[x]$ satisfies all conditions of lemma 2.1, there exist some $r \in N - \{1\}$ such all the zeros of $f(x)$ lies in D_r. Now we search value for r using Rouche's Theorem. Set $\gamma(x) = -x^4 - 2x^3 - 2x^2 - 2x - 3$ and $g(x) = x^5$.
For $|x| = 3$, we have $|\gamma(x)| \leq 3^4 + 2.3^3 + 2.3^2 + 2.3 + 3 = 162 < |3^5| = |g(x)|$.
By Rouche's Theorem, the number of roots of $g(x)$ in $|x| < 3(= 5)$ coincides with ones of $x^5 + x^4 + 2x^3 + 2x^2 + 2x + 3in|x| < 2$. Therefore, $f(x) = x^5 + x^4 + 2x^3 + 2x^2 + 2x + 3$ has 5 roots in D_3.So we get $r = 3$.

Here $f(4) = 1451$ is a prime number. If assume $t = 1$ and $m = 4$, then by using Theorem 3.1 we say that $f(x)$ has at one irreducible factor. So we conclude that $f(x)$ is irreducible over $Q[x]$.

References

[1] G. *Pólya* and G. *Szegö*, Problems and Theorems in Analysis, Vol. 2, Springer-Verlag, 1976, Problem VIII.128.

[2] Brillhart, John; Filaseta, Michael; Odlyzko, Andrew (1981). "On an irreducibility theorem of A. Cohn". Canadian Journal of Mathematics.

[3] Murty, Ram (2002). "Prime Numbers and Irreducible Polynomials". American Mathematical Monthly. 109 (5): 452–458

[4] Anuj Jakhar and Neeraj Sangwan (2016)."An irreducibility criterion for integer polynomials". arXiv:1612.01712

Pradeep Maan: Department of Mathematics, Pt. Neki Ram Sharma Government College, Rohtak (Haryana), India
Email address: pradeepmaan89@gmail.com

Amit Sehgal: Department of Mathematics, Pt. Neki Ram Sharma Government College, Rohtak (Haryana), India
Email address: amit_sehgal_iit@yahoo.com

Archana Malik: Department of Mathematics, Maharshi Dayanand University, Rohtak (Haryana), India
Email address: archanamalik67@gmail.com