Irreducibility of Polynomials

Masum Billal

February 23, 2015

1. Introduction

Definition. A polynomial P in $\mathbb{Z}$[1] for the variable X is:

$$P(X) = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0 = \sum_{i=0}^{n} a_i X_i$$

where $a_i \in \mathbb{Z}$.

First we discuss some ideas on polynomials.

Definition (Irreducible Polynomial)**.** A polynomial $P(X)$ is *irreducible* if it can't be written as product of two non-constant polynomials of degree at least one.

Definition (Root Of A Polynomial)**.** The numbers α that satisfy $P(\alpha) = 0$ are called the *roots* or *zeros* of P.

Definition (Monic Polynomial)**.** If the leading coefficient, $a_n = 1$, then P is called a *monic* polynomial.

Definition (Primitive Polynomial)**.** A polynomial with integer coefficients is called *primitive* if its coefficients are relatively prime.

Example. $2x^2 + 4$ is not primitive, whereas $x^3 - 4$ is. A monic polynomial is always a primitive one.

As you can see, a_0 is the *constant* term. In practice, we always assume that if P has degree n, i.e. $\deg(P) = n$, then $a_n \neq 0$. Otherwise, it doesn't remain a valid polynomial of degree n. For example,

Lemma 1. *For integers a, b:*

$$a - b | P(a) - P(b)$$

Proof. This is merely an exercise, straight enough. ☐

[1] the set of integers

The following theorem may be the first non-trivial theorem in polynomials.

Theorem 1.1 (Gauss's Lemma)**.** *If a polynomial with integer coefficients can be factored into polynomials with rational coefficients, it can also be factored into primitive polynomials with integer coefficients.*

I think you can prove them yourself. Use the following idea:

Lemma 2. *Prove that the product of two primitive polynomials is primitive.*

Theorem 1.2 (Rational Root Theorem)**.** *If a polynomial $P(x)$ with integral coefficients has a rational zero $x = \frac{a}{b}$, where a and b are in co-prime, then the leading coefficient of $P(x)$ is a multiple of b, and the constant term is a multiple of a.*

Proof. Let $\alpha = \frac{u}{v}$ be any root of the polynomial P with $\gcd(u, v) = 1$. Then

$$\begin{aligned} a_n \left(\frac{u}{v}\right)^n + \ldots + a_1 \frac{u}{v} + a_0 &= 0 \\ a_n u^n + \ldots + a_1 u v^{n-1} + a_0 v^n &= 0 \\ -v(a_{n-1}u^{n-1} + \ldots + a_1 u v^{n-2} + a_0 v^{n-1}) &= a_n u^n \end{aligned}$$

So v divides[2] $a_n u^n$. But $\gcd(u, v) = 1$, therefore, v must divide a_n. Prove the other part yourself in a similar manner. □

Corollary 1.1 (Special Case For Monic Polynomial)**.** Any rational zero of a monic polynomial must be an integer. Conversely, if a number is not an integer but is a zero of a monic polynomial, it must be irrational.

Theorem 1.3 (Fundamental Theorem Of Algebra)**.** *A polynomial of degree n can have at most n distinct zeros.*

Corollary 1.2. If two polynomials $P(X)$ and $Q(X)$ are equal for $n+1$ different X-values where $\deg(P) = \deg(Q) = n$, then $P = Q$ must occur.

Theorem 1.4. *If a polynomial has real coefficients, then its zeros come in complex conjugate pairs, in other words, if $\alpha = a + bi$ is a solution to P, then so is $\beta = a - bi$.*

Prove them yourself.

Theorem 1.5 (Vieta's Formulas)**.** *Consider $z_1, z_2, ..., z_n$ be the roots of P. Then,*

$$\begin{aligned} z_1 + z_2 + \ldots + z_n &= -\frac{a_{n-1}}{a_n} \\ z_1 z_2 + \ldots + z_n z_1 &= \frac{a_{n-2}}{a_n} \\ &\vdots \\ z_1 z_2 \cdots z_n &= \frac{a_0}{a_n} \end{aligned}$$

Here the signs come alternating.

Now let's get to the irreducibility of polynomials.

[2] From now on, we assume $a|b$ implies a divides b.

2. Theorems On Irreducibility

This is probably the most known theorem in this field.

Theorem 2.1 (Eisenstein Criterion). *If P is a polynomial in $\mathbb{Z}$ such that for a particular prime p, $p|a_i$ for $0 \leq i \leq n-1$ but $p \not| a_n, p^2 \not| a_0$, then P is irreducible.*

Proof. Here we just give the idea to prove this. If

$$P = FG$$

with F and G non-constant polynomial, and b and c are constant terms of them respectively, $a_0 = bc$.[3] Now try to prove that b and c both are divisible by p, hence p^2 would divide a_0 which contradicts the fact that $p^2 \not| a_0$. Thus such F and G doesn't exist. □

This theorem can be generalized with the same type of proof.

Theorem 2.2 (Extended Eisenstein). *If $p|a_i$ for $0 \leq i \leq k$, $p \not| a_{k+1}$, and also $p^2 \not| a_0$ for $0 \leq k < n$ then P has an irreducible factor of degree greater than k.*

The following theorems more involves the roots of P in proving P irreducible. Particularly, the following lemma involves an idea that may be applicable to many problems. For brevity, we call it *CTL*, short for lemma involving the constant.

Lemma 1 (CTL). *If $|a_0|$ is a prime and*

$$|a_0| > |a_1| + |a_2| + \ldots + |a_n|$$

then P is irreducible.

Proof. We consider a complex root z of P. Assume that, $|z| \leq 1$. But then,

$$\begin{aligned} |a_0| &= |a_1 z + \ldots + a_n z^n| \\ &\leq |a_1 z| + \ldots + |a_n z^n| \\ &= |a_1| \cdot |z| + \ldots + |a_n| \cdot |z^n| \\ &\leq |a_1| + \ldots + |a_n| \end{aligned}$$

which leaves a contradiction. Thus, $|z| > 1$. Let's suppose that,

$$P(X) = G(X)H(X)$$

Then, $a_0 = G(0)H(0)$. Since $|a_0|$ is a prime, we have $|G(0)| = 1$ or $|H(0)| = 1$. Without loss of generality, we take $|G(0)| = 1$ and say, b is the leading coefficient of G. The crucial move: Since G is a factor of P, it must have some same roots $z_1, z_2, ..., z_k$. From Vieta's formulas,

$$z_1 z_2 \cdots z_k = \frac{1}{a} \leq 1$$

where a is the leading co-efficient of G. It forces us to $|z_i| \leq 1$, a contradiction. □

[3] Note that, $b = G(0), c = G(0)$.

Note 1.

$$|a+b| \leq |a| + |b|$$

This is actually the *triangle inequality.*

Theorem 2.3 (PERRON CRITERION). *If $a_0 \neq 0$ and*

$$|a_{n-1}| > 1 + |a_{n-2}| + \ldots + |a_0|$$

where $|X|$ denotes the absolute value of X, then P is irreducible.

The proof uses the lemma stated below, and the idea is putting bounds on the roots of P.

Lemma 2. *If P is a monic polynomial with*

$$|a_{n-1}| > 1 + |a_{n-2}| + \ldots + |a_0|$$

then exactly one zero z_1 of P satisfy $|z_1| > 1$ and the others $z_i, i \geq 2$ satisfy $|z_i| < 1$.

Proof. Without loss generality, assume that a_0 is non-zero. Next, we prove $|z| = 1$ is not a valid root of P under these conditions. Re-write the polynomial equation as:

$$-a_{n-1}z^{n-1} = z^n + a_{n-2}z^{n-2} + \ldots + a_1 z + a_0$$

Therefore, we get:

$$\begin{aligned}
|a_{n-1}| &= |-a_{n-1}z^{n-1}| \\
&= |z^n + a_{n-2}z^{n-2} + \ldots + a_1 z + a_0| \\
&\leq |z^n| + \ldots + |a_1 z| + |a_0| \\
&\leq 1 + |a_{n-2}| + \ldots + |a_0|
\end{aligned}$$

This is a clear contradiction against the given condition. Since

$$|z_1 z_2, ..., z_n| = |a_0| \geq 1$$

at least one of the roots must have an absolute value greater than 1. Let $|z_1| > 1$. Take the polynomial Q with

$$Q(X) = X^{n-1} + b_{n-2}X^{n-2} + \ldots + b_1 X + b_0$$

with roots $z_2, ..., z_n$. Then,

$$\begin{aligned}
P(X) &= (X - z_1)Q(X) \\
&= X^n + (b_{n-2} - z_1)X^{n-1} + (b_{n-3} - b_{n-2}z_1)X^{n-2} + \ldots + (b_0 - b_1 z_1)X - b_0 z_1
\end{aligned}$$

Hence, $b_{n-1} = 1, a_0 = -b_0 z_1$ and $a_i = b_{i-1} - b_i z_1$ for $1 \leq i \leq n-1$. Then, from the inequality assumed,

$$\begin{aligned}
|b_{n-2} - z_1| = a_{n-1} &> 1 + |a_{n-2}| + \ldots + |a_0| \\
&= 1 + |b_{n-3} - b_{n-2}z_1| + \ldots + |b_0 z_1| \\
&\geq 1 + |b_{n-1}z_1| - |b_{n-3}| + |b_{n-3}|z_1 - |b_{n-4}| + \ldots + |b_1||z_1| - |b_0| + |b_0||z_1| \\
&= 1 + |b_{n-2}| + (|z_1| - 1)(|b_{n-2}| + \ldots + |b_1| + |b_0|
\end{aligned}$$

It's obvious that, $|b_{n-2} - z_1| \leq |b_{n-2}| + |z_1|$, hence,

$$|b_{n-2}| + |z_1| > |b_{n-2}| + (|z_1| - 1)(|b_{n-2}| + \ldots + |b_1| + |b_0|$$

yielding that,

$$|b_{n-2}| + |b_{n-3}| + \ldots + |b_0| < 1$$

This is the step of contradiction step. We show that, $Q(z_1)$ is non-zero i.e. z_1 can't be a root of Q. In fact, we are going to prove $Q(z_1) > 0$. I intend to give it away as an exercise.

□

We use the following theorem without proof.

Theorem 2.4 (*Rouchés Theorem*)**.** *Let f and g be two analytic functions on and inside a simple closed curve C. Let $|f(x)| > |g(x)|$ for all points $x \in C$. Then f and g has the same number of roots interior to C.*

This produces another important result.

Corollary 2.1. Let P be a polynomial such that,

$$|a_k| > |a_0| + \ldots + |a_{k-1}| + |a_{k+1}| + \ldots + |a_n|$$

for some $0 \leq k \leq n$. Then exactly k roots of P lie strictly inside the unit circle, and the other strictly outside the unit circle.

As you can see, the fundamental theorem of algebra can be a special case of this result.

Theorem 2.5 (*Extended Rouché*)**.** *Let f and g be analytic functions on and inside a simple closed curve C. Let*

$$|f(x) + g(x)| < |f(x)| + |g(x)|$$

for all point $x \in C$, then they have the same number of roots inside C.

The theorem we state next, is easy enough to prove yourself, at least after these much proofs we have done. So I will be just giving hints only to prove the theorem.

Theorem 2.6. *If*

$$P(x) = a_n x^n + \ldots + a_0$$

with a_i real number such that, $0 < a_0 \leq a_1 \leq ... \leq a_n$, then any complex root α of P satisfies $|\alpha| \leq 1$.

Hint 1. α is a root of $(1-x)P(x)$. Set this in the polynomial equation, and then bound $|a_n\alpha^n|$, to show that if the condition doesn't hold then we have $|a_n\alpha^n| < |a_n\alpha^n|$.

The next theorems combine irreducibility with the polynomial being prime.

Theorem 2.7 (Cohn's Criterion). *If a prime p is expressed in decimal system as*

$$p = a_n 10^n + \ldots + a_0$$

then

$$P(x) = a_n x^n + \ldots + a_0$$

is irreducible.

This result was generalized by Brillhart, Filaseta and Odlyzko.

Theorem 2.8 (Generalized Cohn Criterion). *If a prime p is expressed in b-base number system with $b \geq 2$,*

$$p = a_n b^n + \ldots + a_0$$

with $a_n \neq 0, 0 \leq a_i < b$, then

$$P(x) = a_n x^n + \ldots + a_0$$

is irreducible.

And Filaseta generalized this even more.

Theorem 2.9. *If a prime p and is a positive integer such that, $w < b, wp \geq b$ is expressed in b-base number system with $b \geq 2$,*

$$wp = a_n b^n + \ldots + a_0$$

with $a_n \neq 0, 0 \leq a_i < b$, then

$$P(x) = a_n x^n + \ldots + a_0$$

is irreducible.

They are irreducible even over $\mathbb{Q}$. But here, we prove the generalized Chon's theorem. The proof is due to M. Ram Murty[4].

Proof. We need two lemmas to finish the proof off.

Lemma 3.

Lemma 4.

□

[4] M. Ram Murty, Prime Numbers and Irreducible Polynomials, Amer. Math. Monthly. 109 (2002) 452-458

3. Problems

The problems may be of different class of difficulty.

Problem 3.1. Prove that $\sqrt{2}$ is an irrational number.

Solution 1. We make the use of the special case of Rational Root Theorem for monic polynomial. Consider the polynomial

$$P(x) = x^2 - 2$$

If it has a rational zero x an integer. Therefore, x divides 2, which says $x = \pm 2$ and this doesn't satisfy the equation.

Problem 3.2. Find all polynomials P in $\mathbb{Z}$ with

$$P(7) = 11, P(11) = 13$$

Solution 2. There is no such polynomial. According to 1, we can say that,

$$11 - 7 | P(11) - P(7)$$

which gives us $4|2$, impossible.

Problem 3.3. Prove that, for a prime p,

$$P(x) = x^{p-1} + x^{p-2} + \ldots + x + 1$$

is irreducible.[5]

Solution 3. We solve this problem using Eisenstein criterion. But the solution uses an incredible idea. **You won't always find the criterion applicable straightly.** See how we tackle the situation in this case. And the same type of modification may be needed in other problems. Note that, it's enough to prove that $P(x+1)$ is irreducible. And due to the identity:

$$x^n - y^n = (x-y)(x^{n-1} + x^{n-2}y + \ldots + xy^{n-2} + y^{n-1})$$

we have,

$$\begin{aligned} P(x) &= \frac{x^p - 1}{x - 1} \text{ so} \\ P(x+1) &= \frac{(x+1)^p - 1}{x} \\ &= x^{p-1} + \binom{p}{1} x^{p-2} + \binom{p}{2} x^{p-3} + \ldots + \binom{p}{p-2} x + p \end{aligned}$$

Intuition suggests us that p is our desired prime for applying the criterion. Therefore, we need to prove another lemma.

[5]This polynomial is actually $\Phi_p(x)$, the cyclotomic polynomial for prime p. Cyclotomic polynomial $\Phi_n(X)$ is defined by:

$$\Phi_n(X) = \prod_{\gcd(k,n)=1, k \leq n} (X - e^{\frac{2i\pi}{n} k}$$

Lemma 5. *$p|\binom{p}{i}$ for $0 < i < p$.*

Proof. We have the identity

$$\binom{p}{i} = \frac{p}{i}\binom{p-1}{i-1}$$

Thus, $p|i\binom{p}{i}$. But since for $0 < i < p, \gcd(p,i) = 1$, it gives $p|\binom{p}{i}$. □

The rest is now straight.

Problem 3.4. Prove that

$$P(x) = x^n + 5x^{n-1} + 3$$

can not be expressed as a product of two non-constant polynomials.

First Solution. First we use Extended Eisenstein criterion. Consider the prime $p = 3$. Then $p|a_i$ for $0 \le i \le n-2$ and $p^2 \not| a_0, p \not| a_{n-1}$. Therefore, it must have an irreducible factor of degree greater than $n-1$ i.e. it must have an integer solution. But since it is monic polynomial and its solution must divide 3, we find that, it's impossible to write it as a product of two polynomials. □

Second Solution. Now, we use Perron criterion, and the problem is straight now. Since P satisfies

$$|a_{n-1} = 5| > 1 + |a_0| = 4$$

P is irreducible. □

Third Solution. The proposers solution was as follows. Suppose that,

$$P(x) = G(x)H(x)$$

Since $P(0) = G(0)H(0)$, either $|G(0)| = 1$ or $|H(0)| = 1$. We may assume $|G(0)| = 1$ and it has common roots $x_1, ..., x_k$ with P.

$$G(x) = (x - x_1)\cdots(x - x_k)$$

Note that, $x^{n-1}(x+5) = -3$ for any root, x of P. Then, $|G(-5)| = 3^k$. But since $P(5) = G(-5)H(-5) = 3$, we have $k \le 1$. This proves the theorem. □

Problem 3.5.