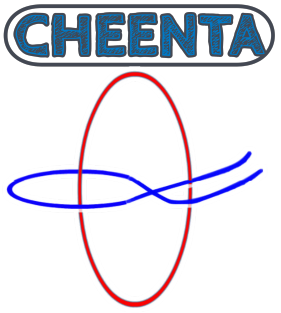

Cheenta

IOQM Concepts Revisited

Created By :
J V Raghunath

Topic : Polynomial with integer coefficients

Overview

We will learn about,

1. Polynomial
2. Monic Polynomial

1 Polynomial

Polynomial is an algebraic expression that is of the form

$$f(x) = a_n x^n + a^{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0$$

where $a_0, a_1, \ldots, a_n \in \mathbb{F}$ (or in $\mathbb{Z}$) are called *coefficients* of the polynomial and $n \in \mathbb{N}_0$ is the degree of the polynomial, if $a_n \neq 0$. Here $\mathbb{F}$ denotes anyone of $\mathbb{C}$ (or) $\mathbb{R}$ (or) $\mathbb{Q}$, i.e., Complex numbers, Real numbers, Rational numbers respectively. A polynomial *over* $\mathbb{Z}$ means that its coefficients are integers represented by $f(x) \in \mathbb{Z}[x]$. Here is an interesting property particularly for *Polynomials over* $\mathbb{Z}$.

Theorem 1.1. *If $P(x)$ is a polynomial over $\mathbb{Z}$, then for any distinct $u, v \in \mathbb{Z}$,*

$$u - v \mid P(u) - P(v)$$

Proof. Let $P(x) = a_n x^n + a^{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0$, where $a_0, a_1, \ldots, a_n \in \mathbb{Z}$. Now for any distinct $u, v \in \mathbb{Z}$,

$$\begin{aligned} P(u) &= a_n u^n + a^{n-1}u^{n-1} + a_{n-2}u^{n-2} + \cdots + a_1 u + a_0 \\ P(v) &= a_n v^n + a^{n-1}v^{n-1} + a_{n-2}v^{n-2} + \cdots + a_1 v + a_0 \\ \Rightarrow P(u) - P(v) &= a_n(u^n - v^n) + a_{n-1}(u^{n-1} - v^{n-1}) + a_{n-2}(u^{n-2} - v^{n-2}) + \cdots + a_1(u - v) \end{aligned}$$

But we know, $a^m - b^m = (a - b)(a^{m-1} + a^{m-2}b + a^{m-3}b^2 + \cdots + ab^{m-2} + b^{m-1})$

$\Rightarrow u - v$ divides all the terms in the expression of $P(u) - P(v)$

$\Rightarrow u - v \mid P(u) - P(v)$

Notice that $P(x) \in \mathbb{Z}[x] \Rightarrow P(u) - P(v) \in \mathbb{Z}$. So we need, $P(x) \in \mathbb{Z}[x]$. □

Question 1.1. *Let $P(x)$ be a polynomial with integer coefficients. Prove that if $P(P(\cdots P(x)\cdots)) = x$ for some integer x (where P is iterated n times, for any $n \in \mathbb{N}$), then $P(P(x)) = x$.*

Sol. Let us say that the integer x such that $\underbrace{P(P(\cdots P}_{n\ times}(x)\cdots)) = x$ is "a".
Now by the Theorem 1.1, $P(a) - a \mid P(P(a)) - P(a)$
$\Rightarrow |P(a)-a| \leq |P(P(a))-P(a)|$, since absolute value of divisor is always less than (or) equal to the absolute value of dividend to get an integer quotient. Continuing this way we get,

$$|P(a) - a| \leq |P(P(a)) - P(a)| \leq |P(P(P(a))) - P(P(a))| \leq \cdots$$

$$\cdots \leq |\underbrace{P(P(P(\cdots P}_{n+1\ times}(a)\cdots))) - \underbrace{P(P(\cdots P}_{n\ times}(a)\cdots))|$$

$$= |P(a) - a|$$

Hence,

$$|P(a) - a| = |P(P(a)) - P(a)| = |P(P(P(a))) - P(P(a))| = \cdots$$

$$\cdots = |\underbrace{P(P(P(\cdots P}_{n+1\ times}(a)\cdots))) - \underbrace{P(P(\cdots P}_{n\ times}(a)\cdots))| = |P(a) - a|$$

CASE 1:
If above equation is equal to 0, then $P(P(a)) = P(a) = a$.
CASE 2:
If numbers in first equality have opposite signs, then
$P(a) - a = P(a) - P(P(a)) \Rightarrow P(P(a)) = a$, we are done.
CASE 3:
If numbers inside both modulus in first equality have the same sign, then we take some equality in which adjacent numbers inside modulus have opposite signs. Obviously they have to switch sign because $(P(a) - a) + (P(P(a)) - P(a)) + (P(P(P(a))) - P(P(a))) + \cdots + (\underbrace{P(P(P(\cdots P}_{n\ times}(a)\cdots))) - \underbrace{P(P(\cdots P}_{n-1\ times}(a)\cdots))) = 0$ and all of them cannot have the same sign.
Let us represent $\underbrace{P(P(P(\cdots P}_{k\ times}(x)\cdots))) = P^k(x)$.
Hence, $P^k(a) - P^{k-1}(a) = -(P^{k+1}(a) - P^k(a))$, for some $k \in \mathbb{N} \leq n$
$\Rightarrow P^{k-1}(a) = P^{k+1}(a)$. Now take "$P$" function both sides for $n - k + 1$ times to get,
$P^{n-k+1}(P^{k-1}(a)) = P^{n-k+1}(P^{k+1}(a)) \Rightarrow P^n(a) = P^{n+2}(a) \Rightarrow \boxed{P(P(a)) = a}$.

Question 1.2. *Polynomial $P(x) \in \mathbb{Z}[x]$ takes values ± 1 at three different integer points. Prove that it has no integer zeros.*
[Hint : Divisibility condition of polynomials over $\mathbb{Z}$]

2 Monic Polynomial

Let $f(x) = a_n x^n + a^{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0$, with $a_n \neq 0$, then $f(x)$ is said to have degree n with leading coefficient a_n. If the leading coefficient of a polynomial is 1, then it is said to be a *Monic polynomial.*

Theorem 2.1 (Division Algorithm)**.** *Let $f(x)$ and $g(x)$ be polynomials with coefficients in $\mathbb{F}$ (or in $\mathbb{Z}$) and let $g(x)$ be non-zero. Then there exist unique polynomials $q(x)$ and $r(x)$ with coefficients in $\mathbb{F}$ (or in $\mathbb{Z}$) such that,*

$$f(x) = q(x)g(x) + r(x),$$

where $r(x)$ is either the zero polynomial or a non-zero polynomial of degree less than the degree of $g(x)$.
Here $q(x)$ is called the quotient and $r(x)$ the remainder, obtained on dividing $f(x)$ by $g(x)$. If $r(x)$ is the zero polynomial, we say that $f(x)$ is divisible by $g(x)$ over $\mathbb{F}$ (or in $\mathbb{Z}$) or that $g(x)$ is a factor of $f(x)$ over $\mathbb{F}$ (or in $\mathbb{Z}$).

Proof. Consider the set $S = \{f(x) - p(x)g(x) \mid p(x) \in \mathbb{F}(x)\}$ of polynomials and by the *Well-ordering principle*, the set S contains a polynomial of least degree, say m. Note that $m < deg\ g$, otherwise we can manipulate $p(x)$ in such a way that $f(x) - p(x)g(x)$ has degree less than m, which would be a contradiction. Hence, there exists polynomials $q(x), r(x)$ such that $f(x) = q(x)g(x) + r(x)$ and $deg\ r < deg\ g$ (or) $deg\ r = 0$.

For the uniqueness proof, let there be some other pair of polynomial $q'(x), r'(x)$, such that $q(x)g(x) + r(x) = q'(x)g(x) + r'(x) \Rightarrow g(x)(q(x) - q'(x)) = r'(x) - r(x)$. But the degrees of LHS and RHS do not match unless $q(x) - q'(x) = 0$ because $deg\ r < deg\ g \Rightarrow q(x) = q'(x),\ r(x) = r'(x)$. □

Theorem 2.2. *Let $f(x), g(x)$ be two polynomial with integer coefficients with $g(x)$ being a monic polynomial. By the Division Algorithm, there exist unique polynomial $q(x), r(x)$, such that $f(x) = q(x)g(x) + r(x)$, where $deg\ r < deg\ g$. Then $q(x), r(x)$ will also be polynomials with integer coefficients.*

Proof. Let $f(x) = a_m x^m + a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \cdots + a_1 x + a_0,\ g(x) = x^n + b^{n-1}x^{n-1} + b_{n-2}x^{n-2} + \cdots + b_1 x + b_0$, where $a_0, \ldots, a_m, b_0, \ldots, b_{n-1} \in \mathbb{Z}$. Now just

by comparing coefficients, we get $q(x) = a_m x^{m-n} + (a_{m-1} - a_m b_{n-1})x^{m-n-1} + \cdots$, which can be proved to be a polynomial with integer coefficients by induction and hence $r(x) = f(x) - q(x)g(x)$ will be a polynomial with integer coefficients. □

Theorem 2.3 (Rational Root Theorem)**.** *If a polynomial with integer coefficients* $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ *has a rational root of the form* $r = \pm\frac{p}{q}$ *with* $\gcd(p, q) = 1$*, then* $p \mid a_0$ *and* $q \mid a_n$*.*

Proof. Suppose $\frac{p}{q}$ is a root of $f(x)$. Then

$$a_n \left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + \cdots + a_1\frac{p}{q} + a_0 = 0.$$

By shifting the a_0 term to the right hand side, and multiplying throughout by q^n, we obtain $a_n p^n + a_{n-1}p^{n-1}q + \ldots + a_1 pq^{n-1} = -a_0 q^n$. Notice that the left hand side is a multiple of p, and thus $p \mid a_0 q^n$. Since $\gcd(p, q) = 1$, Euclid's lemma implies $p \mid a_0$. Similarly, if we shift the a_n term to the right hand side and multiply throughout by q^n, we obtain

$$a_{n-1}p^{n-1}q + a_{n-2}p^{n-2}q^2 + \cdots + a_1 pq^{n-1} + a_0 q^n = -a_n p^n.$$

Note that the left hand side is a multiple of q, and thus $q \mid a_n p^n$. Since $\gcd(p, q) = 1$, Euclid's lemma implies $q \mid a_n$. In particular, this tells us that if we want to check for 'nice' rational roots of a polynomial $f(x)$, we only need to check finitely many numbers of the form $\pm\frac{p}{q}$, where $p \mid a_0$ and $q \mid a_n$. This is a great tool for factorizing polynomials. □

This also tells us that for monic polynomial with integer coefficients, every rational root is an integer root.

Question 2.1. *Let* $p(x)$ *be a monic polynomial of degree four with distinct integer roots* a, b, c *and* d*. If* $p(r) = 4$ *for some integer* r*, prove that* $r = \frac{1}{4}(a + b + c + d)$
[*Hint : Use Factor Theorem*]

Question 2.2. *Find all rational zeroes of* $P(x) = 2x^4 + x^3 - 19x^2 - 9x + 9$*.*
[*Answer :* $-3, -1, \frac{1}{2}, 3$]

Question 2.3. *How many rational roots does* $x^{1000} - x^{500} + x^{100} + x + 1 = 0$ *have?*
[*Answer : 0, why?*]