Number Theory 3

20 August 2023 11:03

GCD of polynomials.–

$$P(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

$$P(x) = 0 \Rightarrow a_0 = 0, a_1 = 0, \ldots, a_n = 0$$

$$P(x) = 1 \Rightarrow a_0 = 1, a_1 = 0, \ldots a_n = 0$$

$$\underset{\text{degree } \alpha_1}{P_1(x)} = \underset{\text{degree } \alpha_d}{d(x)}\, \underset{\text{degree } \alpha_{q_1}}{q_1(x)} + \underset{\text{degree } \alpha_{r_1}}{r_1(x)}$$

$$\alpha_{r_1} < \alpha_d$$

$$\underset{\text{degree } \alpha_2}{P_2(x)} = \underset{\text{degree } \alpha_d}{d(x)}\, \underset{\text{degree } \alpha_{q_2}}{q_2(x)} + \underset{\text{degree } \alpha_{r_2}}{r_2(x)}$$

$$\alpha_{r_2} < \alpha_d$$

If $r_1(x) = r_2(x) = 0$ & $\gcd(q_1(x), q_2(x)) = 1$ coprime polynomials

then $\gcd(P_1(x), P_2(x)) = d(x)$

Q:– Find gcd of $P_1(x) = x^3 - 3x^2 + x + 1$

$P_2(x) = x - 1$

Ans:– $P_2(x) =$ 1-degree polynomial

With x's coefficient 1 only $(x-1)$ divides $(x-1)$

$$x^2(x-1) - 2x(x-1) - 1(x-1)$$

$$= x^3 - x^2 - 2x^2 + 2x - x + 1$$

$$P_1(x) = (x-1)(x^2 - 2x - 1) \qquad P_2(x) = (x-1)$$

$$\alpha_{r_1} = 0 < \alpha_d = 1$$

$$\alpha_{r_2} = 0 < \alpha_d = 1$$

$$\Rightarrow \gcd(P_1, P_2) = (x-1) \; //$$

Q: If p is prime then show that $\gcd(a, p) \in \{1, p\}$.

$x \in [a, b]$

$\downarrow$

$a \leq x \leq b$

$x \in (a, b)$

$\downarrow$

$a < x < b$

$x \in \{a, b\}$

Ans:– Case 1:– $p \nmid a$ and $a \nmid p \Rightarrow \gcd(a, p) = 1$

Case 2:– $p \mid a \Rightarrow \gcd(a, p) = 1$

$\Rightarrow \gcd(a, p) \in \{1, p\}$

Case 2:- $p \nmid a \Rightarrow gcd(a,p) = 1$

Case 3:- $a \mid p \Rightarrow a = 1$ or $p \Rightarrow gcd(a,p) \in \{1, p\}$

$x \in \{a, b\}$

$x = a$ or $x = b$

Euclid's Division Algorithm:- → Think of gcd in terms of common prime factors

$m = p^2 q$ $\quad gcd(m,n) = pq$

$n = pq^2 r$

$m+n = p^2 q + pq^2 r = pq(p + qr)$

In general, the part we can take common outside of $m+n$ is $gcd(m,n)$

Q:- $gcd(a+b, b) = gcd(a,b)$ → True or false?
$a, b \in \mathbb{Z}$

Q:- $gcd(a+3b, b) = gcd(a,b)$ → True or false?
$a, b \in \mathbb{Z}$

Generalizing:-

Lemma:- Let a, b be integers. We can write $a = bq + r$ for integers q, r and $0 \leq r < b$. Then we can say that,

$$gcd(a,b) = gcd(r,b)$$

$(a - qb, b)$

Proof:- As in notes Number Theory 1.

$$\boxed{gcd(a,b) = gcd(bq+r, b) = gcd(bq + r - bq, b) = gcd(r,b)}$$

This process is called Euclid's Division Algorithm (iterated until $r=0$)

$gcd(\underset{a_0}{210}, \underset{b_0}{50}) \rightarrow 210 = 50 \times 4 + 10$

$= gcd(\underset{a_1}{50}, \underset{b_1}{10}) \rightarrow 50 = 10 \times 5 + 0$

$= gcd(0, 10) = 10$

$\gcd(a_0, b_0) \longrightarrow a_0 = b_0 q_0 + r_0$

$b_0 = r_0 q_1 + r_1$

$r_0 = r_1 q_2 + r_2$

$\vdots$

$r_{n-2} = r_{n-1} q_n + r_n$ until $r_n = 0$

Then $\gcd(a_0, b_0) = r_{n-1}$

$\gcd(137, 5) = 1$

$$\begin{array}{l} 5)\,137\,(27 \\ \;\;-10 \\ \;\;\;\;37 \\ \;\;-35 \\ \;\;\;\;\;2)\,5\,(2 \\ \;\;\;\;\;\;-4 \\ \;\;\;\;\;\;\;\;1)\,2\,(2 \\ \;\;\;\;\;\;\;\;\;\;-2 \\ \;\;\;\;\;\;\;\;\;\;\;\;0. \end{array}$$

Q:- Prove that Euclid's Division Algorithm terminates in finite step for finite $a, b \in \mathbb{Z}$.

Ans:- $0 \le r < b$ for $a = bq + r$

r is decreasing in each step by at least 1.

This means r will be 0 in finite step

This means as a, b are finite so r will be 0 in finite step

That's when this algorithm stops.

Q:- $\gcd(-120, 10) = \gcd(0, 10) = 10$

Q:- $\gcd(-120, 7) = \gcd(6, 7) = \gcd(1, 6) = \gcd(0, 1) = 1$

$-120 = 7 \times (-18) + 6$

Q:- $\gcd(-120, -7) = (\gcd(120, 7)) = 1$

H.W:- Q:- Show that $\gcd(4n+3, 2n) \in \{1, 3\}$

Q:- Let $a, b \in \mathbb{Z}$. Then we can write $a = bq + r$, $0 \le r < b$

$q, r \in \mathbb{Z}$. Then is $\operatorname{lcm}(a, b) = \operatorname{lcm}(r, b)$ — True or false?

In your solution

$\gcd(12k+7, 6k+2)$

Easy Solution:-

3) In your solution

$\gcd(12k+7, 6k+2)$

$= \gcd(6k+5, 6k+2)$

$= \gcd(3, 6k+2) \in \{1, 3\}$

Easy Solution:-

$\gcd(4n+3, 2n)$

$= \gcd(3, 2n)$

$\in \{1, 3\}$

$\text{lcm}(b^2+1, b) = (b^2+1)b$

$\text{lcm}(1, b) = b$ ⇒ not equal

So $\text{lcm}(a,b) \neq \text{lcm}(r,b)$

$\gcd(b^2+1, b) = \gcd(1, b) = 1$