MA-222

Note Title 12-08-2021

Lec-7.

Division Algo:

Thm: Given $a, b \in \mathbb{N}$ (TRI) there exist unique $q, r \in \mathbb{Z}$ such that

$$a = bq + r \quad \& \quad 0 \le r < b$$

Pf: $S = \{ a - bq \mid a - bq \ge 0 \ \& \ q \in \mathbb{Z} \} \neq \emptyset$.

By WOP, $\exists$ least elt say r.

$\mathbb{Z}_p[x]$

$r = a - bq$ for some $q \in \mathbb{Z}$

$a = bq + r$

$r \geq 0$

$r < b$

$r \geq b$ ✗

$(q_1, r_1) \neq (q_2, r_2)$

$a = bq_1 + r_1 = bq_2 + r_2$

$0 \leq r_1, r_2 < b$

$b(q_1 - q_2) = r_2 - r_1$

$r_2 \geq r_1$

$0 \leq r_2 - r_1 < b$

$b \mid r_2 - r_1 \Rightarrow r_2 - r_1 = 0 \Rightarrow r_1 = r_2$ □

Def: $GCD(a,b) = d$ (say)

$a, b \in \mathbb{Z}$

$d \mid a$ $\quad d \mid b$ & d is (largest such)

$e \mid a$ $\quad e \mid b$ $\quad e \le d$.

$\Rightarrow e \mid d$.

$\square$

$\gcd(a,b)$

(a,b)

$\gcd(a,0) = |a|$ ←

$\gcd(0,0) = 0$ convention.

↳ undefined.

$d = lcm(a,b)$ ≥ 0

$a \mid l$. $b \mid l$ & l is smallest such

$a \mid k$ $b \mid k$ then $d \leq k$

$d \mid k$.

Thm:

$gcd(a,b) = d$ $l = lcm(a,b)$.

then $d \cdot l = |a| \cdot |b|$.

$[a,b]$

$lcm(0,b) = ?$

$lcm(a,0) = ?$

Pf.

$a = \gcd(a, b)$

$\Leftrightarrow$ $a \mid b$

$\Leftrightarrow$ a is a common divisor of a & b.

$\Leftarrow$ $a = \gcd(a, b)$

$\Rightarrow$ a is the smallest common divisor of a & b.

$\Rightarrow$ $a \mid \gcd(a, b)$

$\Rightarrow$ $a \mid b$

$\Rightarrow$ a is a common divisor of a & b.

$\Rightarrow$ $a \le \gcd(a, b)$

$\Rightarrow$ $a = \gcd(a, b)$

□

Euclidean Algo

$ax+by$? $\forall x, y$.

Thm: $a, b \in \mathbb{N}$. then $d = \gcd(a,b) = \gcd(a+\alpha b, b)$ $\forall \alpha \in \mathbb{Z}$.

Que: $\gcd(a,b) \stackrel{?}{=} \gcd(ax+by, b)$ $\forall x, y \in \mathbb{Z}$.

Pf:

$d \mid a,\ d \mid b \Rightarrow d \mid a+\alpha b$. $\forall \alpha \in \mathbb{Z}$.

$e \mid a+\alpha b$ & $e \mid b \Rightarrow e \mid (a+\alpha b) - \alpha \cdot b$.

$\Rightarrow e \mid a$ $\Rightarrow e \mid d$.

Corollary

$a, b \in \mathbb{Z}$ $\exists\ q, r \in \mathbb{Z}$ s.t. $a = bq + r$.

then $\gcd(a, b) = \gcd(b, r)$.

$= \gcd(b, a - bq)$

Thm: $a, b \in \mathbb{N}$. $a \geq b$.

Define $r_0 = a$ $r_1 = b$ $s_0 = 1$ $s_1 = 0$ $t_0 = 0$ $t_1 = 1$.

Applying div. algo repeatedly, define

$$r_i = r_{i+1} q_{i+1} + r_{i+2} \qquad 0 \leq r_{i+2} < r_{i+1} \quad \forall\, 0 \leq i \leq n-2$$

where n is such that $r_{n+1} = 0$.

Then $\gcd(a, b) = r_n$.

In the process also define.

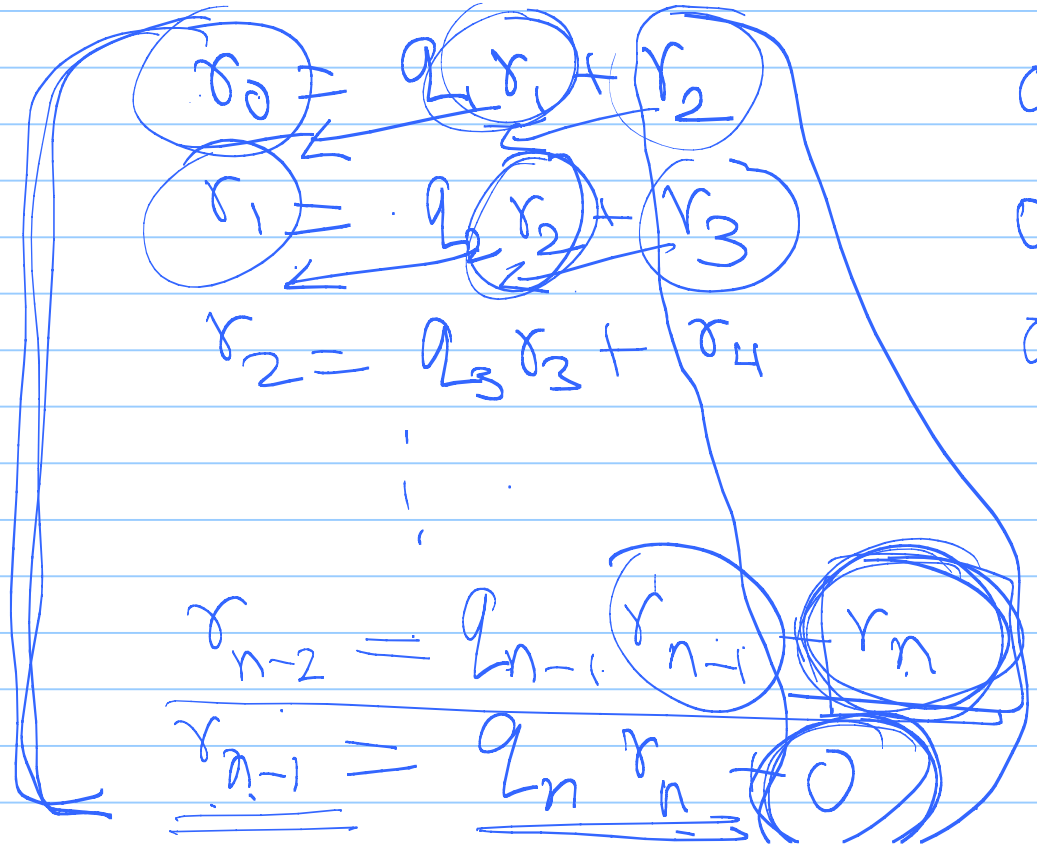
$$s_{i+1} = s_{i-1} - q_{i+1} s_i \quad \& \quad t_{i+1} = t_{i-1} - q_{i+1} t_i$$

$$0 \le i \le n-2$$

Further

$$\gcd(a,b) = r_n = s_{n+1} a + t_{n+1} b$$

Pf: $a = r_0 = q_1 b + r_2 = q_1 r_1 + r_2$. $0 \le r_2 < r_1$.



$r_0 = q_1 r_1 + r_2$ $\quad 0 \le r_2 < r_1$.

$r_1 = q_2 r_2 + r_3$ $\quad 0 \le r_3 < r_2$.

$r_2 = q_3 r_3 + r_4$ $\quad 0 \le r_4 < r_3$.

n-steps

$r_{n-2} = q_{n-1} r_{n-1} + r_n$ $\quad 0 \le r_n < r_{n-1}$

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

$r_0 \geq r_1 > r_2 > r_3 > \cdots > r_{n-1} > r_n \geq 0.$

$$\gcd(a,b) = \gcd(r_0, r_1) = \gcd(r_1, r_2)$$
$$= \gcd(r_2, r_3)$$
$$\vdots$$
$$= \gcd(r_n, 0)$$
$$= r_n.$$