Reference Book:- Contemporary Abstract Algebra (Auth:- Joseph Gallian)

Assignments

# Well Ordering Principle:-

→ Every set of Positive integers contain a smallest member.

# Division Algorithm:-

→ let $a$ be any integer and $b > 0$ Then $\exists$ unique $q, r \in \mathbb{Z}$ s.t. $a = bq + r$ where $0 \leq r < b$.

# Theorem:- $\gcd(a,b) = at + bs$ for some $s,t \in \mathbb{Z}$.

Proof:- $A = \{ am + bn > 0 \mid m, n \in \mathbb{Z} \}$

let $d = at + bs$ be the smallest element of set $A$. By W.O.P.

claim:- $d$ is $\gcd(a,b)$

let $a = dq + r \quad 0 \leq r < d$

$a = (at + bs)q + r$

$r = a - atq - bsq$

$r = a(1 - tq) + b(-sq)$

$\therefore r$ is a linear combination of $a$ and $b$.

$r \in A$

$\therefore d \leq r$

contradiction

Similarily $d$ divides $b$.

let $r'$ be a common divisor, i.e., $r'|a$ and $r'|b$

$a = r'q_1$ , $b = r'q_2$

$d = r'q_1 t + r'q_2 s$

$d = r'(q_1 t + q_2 s)$

$\Rightarrow r' | d$

$\therefore$ $d$ is the greatest common divisor of $a$ and $b$.

$\gcd(4, 15) = 1$

$1 = 4 \times 4 + 15 \times -1$

# Euclidean Algorithm:-

let $a > b$,

$\gcd(a,b)$

$a = bq_1 + r_1 \qquad 0 \le r_1 < b$

$b = r_1 q_2 + r_2 \qquad 0 \le r_2 < r_1$

$r_1 = r_2 q_3 + r_3 \qquad 0 \le r_3 < r_2$

$\vdots$

$r_{k-1} = r_k q_{k+1} + r_{k+1} \qquad 0 \le r_{k+1} < r_k$

$r_k = r_{k+1} q_{k+2} + 0$

Claim:- $r_{k+1}$ is the gcd.

proof:- $r_{k+1}$ is a common divisor of $a$ and $b$.

let $r'$ be any common divisor of $a$ and $b$.

As $r'|a$ and $r'|b$, we can say $r'|r_1$

similarily $r'|r_2, \dots, r'|r_{k+1}$

Hence Proved

# Euclid's Lemma : $a, b \in \mathbb{Z} \setminus \{0\}$

Let $p$ be a prime. $p | ab \Rightarrow p|a$ or $p|b$

Proof by contradiction:-

$$a = pq_1 + r_1 \quad , r_1 \neq 0 \quad , r_1 < p$$
$$b = pq_2 + r_2 \quad , r_2 \neq 0 \quad , r_2 < p$$

$ab = kp + r_1 r_2$

$r_1 r_2$ does not divide $p$ hence $ab \nmid p$

$\Rightarrow$ contradiction.

Proof 2:-

suppose $p \nmid a$ then To show:- $p|b$

$\gcd(p, a) = 1$ using $p$ is prime

$1 = ps + at$

$b = psb + atb$

R.H.S. $| p \Rightarrow b | p$

else $p|a$

Hence proved

# Fundamental Theorem of Arithmetic :-

→ Every integer greater than 1 is a prime or product of prime. This product is unique upto the order of the factors.

Thus if $n = p_1 p_2 \dots p_r$, and $n = q_1 q_2 \dots q_s$ where $p_i$'s and $q_i$'s are prime

Then $r = s$ and $p_i = q_i \;\forall i$ after renumbering.

# Least Common Multiple :-

$lcm(a,b)$

suppose $d$ is a common multiple of $a$ and $b$ then $lcm(a,b) \mid d$

Proof :- $c = lcm(a,b)$

$d = cq + r \qquad 0 \leq r < c$

$\Rightarrow$ $r$ is a common multiple of $a$ and $b$

$\therefore r > c$

$\rightarrow\leftarrow$