(1)

Number Theory:

Number Theory is the study of set of positive whole numbers.

e.g

1, 3, 5, 7, . . . Odd Numbers

2, 4, 6, 8, . . . Even numbers

Divisibility: An integer b is divisible by an integer a written as $a|b$ if there is an integer x such that

$b = ax$.

(2)

Proposition: Let a, b, c be integers.

i) $a|0$, $1|a$, $a|a$

ii) $a|1$ iff $a = \pm 1$

(iii) $a|b$ & $c|d$ then $ac|bd$

(iv) If $a|b$ and $b \neq 0$ then $|a| \leq |b|$

(v) If $a|b$ then $a|bc$

(VI) If $a|b$ and $b|c$ then $a|c$

(VII) If $c|a$ and $c|b$ then $c|ax+by$ $\forall$ x and y.

(VIII) If $a|b$ & $b|a$ then $a = \pm b$

(IX) Assume $c \neq 0$, then $a|b$ iff $ac|bc$.

(3)

Well Ordering Principle:

Every non-empty set S of non-negative integers contains a least element, i.e., there is some integer a in S such that $a \leq b \ \forall \ b \in S$.

Division Algorithm in $\mathbb{Z}$: Given integers a, b with $b > 0$ $\exists$ two unique integers q and r such that $a = bq + r$ and $0 \leq r < b$.

The number q is called the quotient and r is called the remainder.

Note: q and r are unique.

(4)

Proof: consider

$$S = \{ a - xb \mid x \text{ is an integer}; \ a - xb \geq 0 \}$$

$S \neq \phi$ as $b > 0$

$\therefore b \geq 1$, so $|a| b \geq |a|$

$$a - (-|a| b) = a + |a| b \geq a + |a| \geq 0$$

$\Rightarrow a - xb \in S$ for $x = -|a|$

By well ordering principle $\exists \ r \in S$ such that $r \leq c \ \forall \ c \in S$.

$r = a - qb$ (By definition of S $\exists$ integer q)

$r \geq 0$

To Prove : $r < b$

On Contrary if $r \geq b$, then

$r - b \geq 0 \Rightarrow a - qb - b = a - (q+1) b \geq 0$

$\Rightarrow r - b < r \in S$

Contradiction $\Rightarrow r < b$.

(5)

Uniqueness:

Suppose $a = qb + r = q'b + r'$

$0 \leq r < b$

$0 \leq r' < b$

$r' - r = b(q - q')$

$|r' - r| = b|q - q'|$

As $|r' - r| < b \Rightarrow b|q - q'| < b$

$\Rightarrow 0 \leq |q - q'| \leq 1$

$\Rightarrow q - q' = 0$

$\Rightarrow q = q' \Rightarrow r = r'$

GCD: Let a and b be two integers not both zero. The g.c.d of a and b is the positive integer d satisfying the following

(a) $d|a$ and $d|b$

(b) If $c|a$ and $c|b$ then $c \leq d$

Notation : $(a,b) = d$

Note: If $(a,b)=1$, a and b are relatively prime. (6)

Result: $(a,b) = (a-nb, b)$

Let $(a,b) = d \Rightarrow d|a$ and $d|b$

and $(a-nb, b) = d' \Rightarrow d' | a-nb$

$\&\quad d'|b$

$d|a-nb \Rightarrow d|d'$ (as $d|b$)

$\Rightarrow d \leq d' \quad -(1)$

Similarly $d'|a-nb \;\&\; d'|b$

$\Rightarrow d'|a \;\&\; d'|b$

$\Rightarrow d'|d$

$\Rightarrow d' \leq d \quad -(2)$

From (1) & (2)

$d = d'$

$\therefore (a,b) = (a-nb, b)$

Theorem: Given integers a and b (7) not both of which are Zero, ∃ integers x and y such that

$$\gcd(a,b) = d = ax + by$$

Proof: Consider

$$S = \{ au + bv \mid au + bv > 0, u, v \in Z \}$$

$S \neq \phi$ as if $a \neq \phi$ then

$$a = a \cdot u + b \cdot 0 \in S$$

($u = 1$ if $a > 0$ + $u = -1$ if $a < 0$)

By well ordering Principle

$\exists\ d \in S$ such that $d \leq t\ \forall\ t \in S$

Now $d = ax + by$ by definition of S

$x, y \in Z$.

To claim $d = (a,b)$

Apply division algorithm to ~~a and b~~ a and d.

(8)

$\exists$ integers q and r such that

$$a = qd + r, \qquad 0 \le r < d$$

$$\therefore \quad r = a - qd$$

$$= a - q(ax + by)$$

$$= a(1 - qx) + b(-qy)$$

If $r > 0$ then $r \in S$

A contradiction to the fact that the d is the least integer in $S\ (r < d)$

$$\therefore \quad r = 0$$

$$\Rightarrow \quad a = qd \Rightarrow d \mid a$$

Similarly $d \mid b$

If c is any arbitrary +ve integer s.t $c \mid a$ and $c \mid b$ then $c \mid ax + by$

$$\Rightarrow \quad c \mid d \Rightarrow c \le d$$

$$\Rightarrow \quad d = g.c.d\ (a, b)$$

(9)

Theorem: Let a and b be integers not both zero. Then a and b are relatively prime iff $\exists$ integers x and y such that

$$1 = ax + by$$

Proof: If $(a, b) = 1$

$\Rightarrow \exists\ x + y \in Z'$ s.t $1 = ax + by$

Conversely Let $1 = ax + by$

$+ \quad d = (a, b)$

$\Rightarrow d|a$ and $d|b \Rightarrow d|ax + by = 1$

$+ \quad d > 0 \Rightarrow d = 1$

$\Rightarrow$ a and b are relatively prime.

Excercise: $\rightarrow$ If $(a, b) = d$

then $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$

$\rightarrow$ If $a|c$ + $b|c$ with $(a, b) = 1$ then $ab|c$

(10)

Euclid's Lemma: If $a \mid bc$ with $(a, b) = 1$ then $a \mid c$.

Proof: $(a, b) = 1$

$\Rightarrow \exists\ x, y \in \mathbb{Z}$ such that

$$1 = ax + by$$

Now $c = 1 \cdot c$

$$= (ax + by) \cdot c = acx + bcy$$

$a \mid ac$ & $a \mid bc \Rightarrow a \mid acx + bcy$

$$\Rightarrow a \mid c$$

(14)

Lemma: If $a = bq + r$

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

Proof: Let $d = gcd(a,b)$

$\Leftrightarrow$ $d|a$ and $d|b \Rightarrow d|a-bq$

$\Rightarrow d|r$

$\Leftrightarrow$ d is a common multiple of b and r

Let c be any common multiple of b and r

$\Leftrightarrow$ $c|b$ and $c|r$

$\Leftrightarrow$ $c|bq+r$

$\Leftrightarrow$ $c|a$

Now $c|a$ and $c|b \Rightarrow c \leq d$

$\Leftrightarrow$ $d = (b,r)$

(12)

Euclidean Algorithm :

Let a and b be two integers, not both zero, $a \geq 1, b > 0$.

Apply Division algorithm to a and b to get

$$a = q_1 b + r_1, \quad 0 \leq r_1 < b$$

If $r_1 = 0$ then $b \mid a \Rightarrow (a, b) = b$

When $r_1 \neq 0$, divide b by r_1

$$b = q_2 r_1 + r_2 \; ; \quad 0 \leq r_2 < r_1$$

If $r_2 = 0$ then stop. Otherwise,

$$r_1 = q_3 r_2 + r_3 \; ; \quad 0 \leq r_3 < r_2$$

$$\vdots$$

$$r_{n-2} = q_n r_{n-1} + r_n \; ; \quad 0 \leq r_n < r_{n-1}$$

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

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

(13)

Proof

$$(a,b) = (b, r_1)$$
$$= (r_1, r_2)$$
$$= \cdots$$
$$= (r_n, 0) = r_n \quad (\text{By Lemma})$$

Example: $(12378, 3054) = ?$

$a = 12378, \quad b = 3054$

$12378 = 4 \cdot 3054 + 162$

$3054 = 18 \cdot 162 + 138$

$162 = 1 \cdot 138 + 24$

$138 = 5 \cdot 24 + 18$

$24 = 1 \cdot 18 + 6$

$18 = 3 \cdot 6 + 0$

$(12378, 3054) = 6$