MODULE I

- Number Theory: $(\mathbb{N}, \mathbb{Z})$

Well-ordering Principle: Any subset S of $\mathbb{N}$ has a minimum element.

Divisors, quotient, remainder, divisibility:

THEOREM 1.1

If $a \& b$ are integers and $b>0$, then there is a unique pair of integers $q \& r$ s.t $a = qb+r$ and $0 \le r < b$

Eg: $a=5$ $b=3$ $5 = q \cdot 3 + r$ $0 \le r < 3$ $r = 0, 1, 2$

$\hookrightarrow 1 \cdot 3 + 2$

$q \Rightarrow$ quotient

$r \Rightarrow$ remainder.

Proof: To prove: There is a pair (q, r) which satisfies the condition $a = qb+r$ and $0 \le r < b$.

It is a unique pair. $(q_1, r_1) \& (q_2, r_2)$ which satisfy $a = q_1 b + r_1 = q_2 b + r_2$ $0 \le r_1, r_2 < b$ then $q_1 = q_2$ & $r_1 = r_2$

Existence of the pair

Define $S = \{ a - ub \mid u \in \mathbb{Z} \} = \{ a, a \pm b, a \pm 2b, \dots a \pm ib, \dots \}$

S contains +ve integers. Therefore $S \cap \mathbb{N}$ is non-empty and obviously a subset of $\mathbb{N}$. By well ordering property $S \cap \mathbb{N}$ has a minimum element, r. Since $r \in \mathbb{N}$, $0 \le r$. and $r \in S$, $r = a - qb$ for some $q \in \mathbb{Z}$. $r < b$, for if $r > b$ then $0 \le r - b = a - qb - b = a - (q+1)b \in S \cap \mathbb{N}$ and $r - b < r$ contradicting the fact that r is the minimum element of $S \cap \mathbb{N}$. Now $a = qb + r$ and $0 \le r < b$.

Uniqueness

Let us say there are two pairs $(q_1, r_1) \& (q_2, r_2)$ which satisfy $a = qb + r$ & $0 \le r < b$.

ie $a = q_1 b + r_1 = q_2 b + r_2$.

$\therefore (q_1 - q_2) b = (r_2 - r_1)$ Since both $r_1 \& r_2$ satisfy $0 \le r < b$, the magnitude of the difference $|r_2 - r_1| < b$. Hence $r_2 - r_1$ cannot be a multiple of b. Therefore $r_1 = r_2$ and hence $q_1 = q_2$

∎

Eg: Any square n produces a remainder 0 or 1 with 4.

Proof: $n = a^2$, $a \in \mathbb{N}$.

Case 1: a is even: i.e. $a = 2k$ $k \in \mathbb{N}$

$n = a^2 = 4k^2 = 4q + r$ $\quad r = 0$, $q = k^2$

Case 2: a is odd i.e. $a = 2k+1$

$n = (2k+1)^2 = 4k^2 + 4k + 1 = 4(k^2+k) + 1$

$= 4q + r$

$r = 1$

$q = k^2 + k$.

Case: when $b < 0$

Since $b < 0$, we have $-b > 0$. and hence Theorem 1.1 applies to $-b$ and $a = q \times (-b) + r$ $\quad 0 \le r < -b = |b|$. Therefore a can be written as $a = (-q) \times b + r$ which is unique because (q, r) is unique by Theorem 1.1.

Divisors

→ a is a divisor of b if $b = qa$ for some integer q ($q \in \mathbb{Z}$)

a is referred to as a multiple of b (q)

Eg: 3 is a divisor of 6 ($6 = 2 \times 3$)

3 is a divisor of -6 ($-6 = -2 \times 3$)

→ Notation: $a|b \Rightarrow$ a divides b

(a is a divisor of b)

↳ a

(*) PROVE THE FOLLOWING (Home work)

(a) if $a|b$ and $b|c$ then $a|c$;

(b) if $a|b$ and $c|d$ then $ac|bd$;

(c) if $m \neq 0$, then $a|b$ if and only if $ma|mb$;

(d) if $d|a$ and $a \neq 0$ then $|d| \leq |a|$.

Theorem 1.3

(a) If c divides $a_1, \ldots, a_k$, then c divides $a_1u_1 + \cdots + a_ku_k$ for all integers $u_1, \ldots, u_k$.

(b) $a|b$ and $b|a$ if and only if $a = \pm b$.

Eg: $c = 3$ $\quad a_1 = 6$ $\quad a_2 = 18$ $\quad a_3 = 9$ $\quad 6u_1 + 18u_2 + 9u_3$ $\quad u_1, u_2, u_3 \in \mathbb{Z}$

PROOF:

(a) $c|a_1, c|a_2 \ldots c|a_k \Rightarrow$ Therefore $a_i = q_i c$ $\quad i = 1 \ldots k$

Hence $a_1u_1 + a_2u_2 + a_3u_3 + \cdots + a_ku_k$

$= c(q_1u_1 + q_2u_2 + \cdots + q_ku_k) = c\hat{q}$ $\quad \hat{q} = \sum_{i=1}^{k} q_iu_i \in \mathbb{Z}$.

$\therefore c|(a_1u_1 + a_2u_2 + \cdots a_ku_k)$ by the definition of divisibility

(b) If $a \neq 0, b \neq 0$

$a|b \Rightarrow b = q_1a \rightarrow (1)$ Similarly $b|a \Rightarrow a = q_2b \rightarrow (2)$

Plugging (2) into (1) we get $b = q_1q_2b$.

$q_1 q_2 = 1$ which is possible only if q_1 and q_2 satisfy ± 1.

On the other hand if $a=b=0$ then obviously $a=\pm b$

GREATEST COMMON DIVISOR

If $d|a$ & $d|b$ then d is called a common divisor.

The greatest common divisor (GCD) of a and b denoted by (a,b) is a number d which satisfies:

(i) If c is a common divisor of a & b then $c \le d$

(ii) d is a common divisor ($d|a$ & $d|b$)

Eg $(6,4)=2$ $\quad (100,75)=25$ $\quad (21,18)=3$

$0 = 0 \cdot q + 0$ (q, r)

Theorem (1) (Euclids Algorithm)

If $a = qb + r$ then $\gcd(a,b) = \gcd(b,r)$. $\Rightarrow$ Eg: $(27,18) = (18,9)$ (a, b; $r=9$)

$= (9,0) \Rightarrow 9$ ✓

PROOF:

Let c be any divisor of a & b. Now $r = a - qb$

By Theorem 1.3, $c \mid a - qb = r$. That is any common divisor of a & b is also a divisor of r. Hence c is a common divisor of b & r. GCD is also a divisor of a & b and hence of b & r. Hence

$(a,b) = (b,r)$ ∎

$54 = 36 \cdot 1 + 18$ (q_1, r_1)

$36 = 18 \cdot 2 + 0$ (q_2, r_2)

$a = 54 \quad b = 36$

$(a,b) = (54,36) = (36,18) = (18,0) = 18$

(a,b) $\longrightarrow$ Euclid's Algorithm steps:

$a = q_1 b + r_1 \quad \cdots \rightarrow (1) \quad (b, r_1)$

$b = q_2 r_1 + r_2 \quad \cdots \rightarrow (2) \quad (r_1, r_2)$

$r_1 = q_3 r_2 + r_3 \quad \cdots \rightarrow (3) \quad (r_2, r_3)$

$\vdots \qquad \vdots$

$r_{n-2} = q_{n-1} r_{n-1} + r_n \quad \cdots \rightarrow (n) \quad (r_{n-1}, r_n) = (r_{n-1}, 0)$ ($r_n = 0$)

$= r_{n-1}$

THEOREM

In the above procedure $d = (a,b) = r_{n-1}$.

PROOF:

From Theorem (1) applied on eq: (1), $(a,b) = (b, r_1)$. Similarly applying it on (2), $(b, r_1) = (r_1, r_2)$. Progressively applying on the rest of the equations we get $d = (a,b) = (r_1, r_2) = (r_2, r_3) = \cdots = (r_{n-1}, r_n) = (r_{n-1}, 0) = r_{n-1}$ ▨

Bezout's Identity

If a and b are integers (not both 0), then there exist integers u and v such that

$$\gcd(a,b) = au + bv.$$

Eg: 54 36 $\quad 18 = 54 \cdot 1 + 36 \cdot -1$, $u=1$, $v=-1$

$(54, 37) = 1 \quad 1 = 54u + 37v$

Euclid's Alg:

$54 = 37 \cdot 1 + 17 \rightarrow 17 = 54 - 37$ ✓

$37 = 17 \cdot 2 + 3 \rightarrow 37 = (54-37)\cdot 2 + 3$

$37 = 2 \cdot 54 - 2 \cdot 37 + 3$

$-2 \cdot 54 + 3 \cdot 37 = 3$ ✓

$17 = 3 \cdot 5 + 2$

$54 - 37 = (2 \cdot 54 + 3 \cdot 37) \cdot 5 + 2$

$= -10 \cdot 54 + 15 \cdot 37 + 2$

$11 \cdot 54 - 16 \cdot 37 = 2$ ✓

$3 = 2 \cdot 1 + 1$

$2 = 2 \cdot 1 + 0$

$-2 \cdot 54 + 3 \cdot 37 = (11 \cdot 54 - 16 \cdot 37) \cdot 1 + 1$

$-13 \cdot 54 + 19 \cdot 37 = 1$

$u = -13$

$v = 19$

Every intermediate r_i was expressed as $au_i + bv_i$

Therefore $r_{n-1} = d = au_{n-1} + bv_{n-1} = au + bv$.

PROOF: Writing the Euclid's Alg step by step:

$a = bq_1 + r_1 \rightarrow (1)$

$b = r_1 q_2 + r_2 \rightarrow (2)$

$r_1 = r_2 q_3 + r_3 \rightarrow (3)$

$\vdots \quad \vdots \quad \vdots$

$r_{n-2} = r_{n-1} q_n + r_n \rightarrow (n)$ $(r_n = 0)$

From (1) we get $r_1 = a - bq_1 = au_1 + bv_1$ where $u_1 = 1$ & $v_1 = -q_1$. Now plugging this into (2) we get $b = q_1(au_1 + bv_1) + r_2$

Rearranging $r_2 = au_2 + bv_2$. $(u_2 = -q_1 u_1,\ v_2 = 1 - q_1 v_1)$. Proceeding Similarly we can express every r_i as $au_i + bv_i$.

Hence $d = r_{n-1} = au_{n-1} + bv_{n-1} = au + bv$ $(u = u_{n-1},\ v = v_{n-1})$

Corollary: $d = (a,b)$ is the smallest positive integer that can be written as $au + bv$ where $u, v \in \mathbb{Z}$ and at least one of a & b is non-zero.

 → Think it over.

Eg: $(105, 45) = 15$

$\cos u + 45v$

$0 - 14$ X

(A) **Extended Euclid's Algorithm** (Reading assignment)

↓

Finding out a pair (u,v) s.t $au + bv = (a,b)$

Least Common Multiple (LCM)

Consider two integers a, b.

Common Multiple (CM)

An integer c is a CM of a & b if $a|c$ & $b|c$.

Eg $a = 3,\ b = 4$ common multiples $\{12, 24, 36, -12, -24, \ldots\}$

If you take, the set of all the +ve common multiples of a and b then by Well Ordering Principle, the set has a minimum element, called LCM.

Eg: +ve Common multiples of 3 & 4

$\{12, 24, 36, 48, 60, \ldots\} \subseteq \mathbb{N}$

↑ LCM

Notation: $[a,b] = LCM(a,b)$

Property: If c is any CM of a & b. Then $l = [a,b] \mid c$.

PROOF:

Suppose $l \nmid c$. Obviously $l \leq c$. Since $l \nmid c$ by division theorem we can write $c = lq + r$ where $0 < r < l$. $a \mid c$ implies $a \mid (lq + r)$. Now since $a \mid l$, a should divide r also. Therefore r is a multiple of a. Arguing in the same way $b \mid r$ and hence r is a CM of a & b, contradicting the fact that l is the LCM. Hence $l \mid c$.

THEOREM: If $d = (a,b)$ and $l = [a,b]$ then $dl = ab$.

Eg: $(12,16) = 4$ $\quad [12,16] = 48$ $\quad 12 \times 16 = 4 \times 48$

$192 \qquad 192$

PROOF:

Consider a and b are non-negative.

PART I — Establish $ld \mid ab$

Define $e = a/d$ & $f = b/d$. Now $\frac{ab}{d} = \frac{de \cdot df}{d} = def$

But $def = af$ Hence $a \mid def$. Similarly $def = be$ and hence $b \mid def$. Therefore def is a common multiple of a & b. Since def is a CM of a & b lcm $l \mid def = \frac{ab}{d}$, This implies that $ld \mid ab$.

Establish $ab \mid ld$

$d = au + bv$ by Bezout's Identity. Therefore

$ld = alu + blv$. Hence $\frac{ld}{ab} = \left(\frac{ld}{ab}\right)u + \left(\frac{bl}{ab}\right)v$

where $\hat{u} = l/b$ & $\hat{v} = l/a$ $(\in \mathbb{Z})$ $\quad = \hat{u}u + \hat{v}v \in \mathbb{Z}$

Therefore $ab \mid ld$

Since $ld \mid ab$ and $ab \mid ld$ we have $ab = ld$. ∎

SOLVING DIOPHANTINE EQUATION

$ax + by = c$ $\quad a,b,c,x,y \in \mathbb{Z}$.

Solve for x & y given a,b,c.

Eg: $3x + 15y = 17 \rightarrow$ No Solution.

$3x + 15y = 21 \rightarrow$ Infinitely many Solutions

(Brahmagupta - Around 600 AD)

Theorem: The equation $ax+by=c$ has solution if and only if $d=(a,b) \mid c$. in which case there are infinitely many solutions.

PROOF: Let $d \mid c$. Therefore $c=dq$ where $q \in \mathbb{Z}$. By Bezout's identity we have $d=au+bv$. Plugging this into $c=dq$ we get $c = aqu + bqv = ax_0 + by_0$ where $x_0 = qu$ & $y_0 = qv$.

$(e,f)=1$

PROOF: $d=au+bv$
Dividing both sides by d: we get
$1 = eu + fv$.
$\therefore (e,f)=1$
[COPRIME]

Take any x,y st $ax+by=c$. Subtracting ax_0+by_0 from $ax+by$ we get $a(x-x_0)+b(y-y_0)=0 \longrightarrow (1)$

Dividing (1) by d we get $\frac{a}{d}(x-x_0)+\frac{b}{d}(y-y_0)=0$

Denote a/d as e & b/d as f we get $e(x-x_0)+f(y-y_0)=0$

Rearranging we get $e(x-x_0) = f(y_0-y)$. Since $(e,f)=1$
$e \mid (y-y_0) \Rightarrow y-y_0 = eu$ ($x-x_0 \in \mathbb{Z}$, $y_0-y \in \mathbb{Z}$)

$$y = y_0 + eu = y_0 + \frac{a}{d}u$$

$$e(x-x_0) = -f\frac{au}{d} = -feu$$

$$x = x_0 - fu = x_0 - \frac{b}{d}u$$

The General set of Solutions from the particular Solution (x_0, y_0) is $\left(x_0 - \frac{b}{d}u,\ y_0 + \frac{a}{d}u\right)$ $u \in \mathbb{Z}$.

Converse is obvious and follows from an earlier theorem proved.

∎