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

$1 \cdot 3 + 2$

$q \Rightarrow$ quotient
$r \Rightarrow$ remainder.

PROOF: have 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 $S = \{a - nb \mid n \in \mathbb{Z}\} = \{a, a \pm b, a \pm 2b, \dots a \pm ib, \dots\}$
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 $q_1 = q_2$

$\blacksquare$

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

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

Case 0: a is even: i.e. $a = 2k$ $k \in \mathbb{N}$

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

Case 1: 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 $a = q_1 \times (-b) + r$ $0 \le r < -b = |b|$. Therefore a can be written as $a = (-q_1) \times b + r$ 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

Eg: 3 is a divisor of 6 $(6 = \overset{(q)}{2} \times 3)$
3 is a divisor of -6 $(-6 = -2 \times 3)$

→ Notation: $a|b \Rightarrow$ a divides b
(a is a divisor of b)

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

PROOF:

(a) $c|a_1, c|a_2 \ldots c|a_k \Rightarrow$ Therefore $a_i = q_ic$ $i = 1..k$
Hence $a_1u_1 + a_2u_2 + a_3u_3 + \cdots + a_ku_k$
$= c(q_1u_1 + q_2u_2 + \cdots + q_ku_k) = c\hat{q}$ $\hat{q} = \sum_{i=1}^{k} q_iu_i \in \mathbb{Z}.$
$\therefore c|(a_1u_1 + a_2u_2 + \cdots a_ku_k)$ 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 <u>common divisor</u>.

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 $c \leq d$

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

Eg $(6,4) = 2$ $\quad (100,75) = 25$ $\quad (21,18) = 3$ $\quad 0 = \underset{q}{0} \cdot 9 + \underset{r}{0}$

Theorem (1) (Euclid's Algorithm)

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

$= (9,0) \Rightarrow \underline{9}$

PROOF:

Let c be any divisor of a & b. Now $r = a - qb$. By Theorem 1.3, $c \,|\, a - qb = r$. 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 $(a,b) = (b,r)$ ☒

—— × ——

$a = 54 \qquad b = 36$

$$\overset{\qquad q_1 \quad r_1}{54 = 36 \cdot 1 + 18}$$
$$\underset{\qquad q_2 \quad r_2}{36 = 18 \cdot 2 + 0}$$

$(a,b) = (54,36) = (36,18) = (18,0) = \underline{\underline{18}}$

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

$a = q_1 b + r_1 \dashrightarrow (1) \qquad (b, r_1)$

$b = q_2 r_1 + r_2 \dashrightarrow (2) \qquad (r_1, r_2)$

$r_1 = q_3 r_2 + r_3 \dashrightarrow (3) \qquad (r_2, r_3)$

$\vdots \qquad \vdots \qquad \vdots$

$r_{n-2} = q_{n-1} r_{n-1} + r_n \longrightarrow (n) \qquad (r_{n-1}, r_n) = (r_{n-1}, 0) = \underline{\underline{r_{n-1}}}$

$(r_n = 0)$

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 $\quad 18 = 54\cdot 1 + 36\cdot -1$

$u = 1 \quad v = -1$

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

Euclid's Alg:

$54 = \overset{b}{37}\cdot \overset{q_1}{1} + \overset{r_1}{17} \to 17 = \underline{\underline{54 - 37}}$ ✓

$\overset{b}{37} = \overset{r_1}{17}\cdot \overset{q_2}{2} + \overset{r_2}{3} \to 37 = (54-37)\cdot 2 + 3$

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

$\boxed{-2\cdot 54 + 3\cdot 37 = 3}$

$\overset{r_1}{17} = \overset{r_2}{3}\cdot \overset{q_3}{5} + \overset{r_3}{2}$

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

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

$\boxed{11\cdot 54 - 16\cdot 37 = 2}$ ✓

$\overset{r_2}{3} = \overset{r_3}{2}\cdot \overset{q_4}{1} + \overset{r_4}{1}$

$\overset{r_3}{2} = \overset{r_4}{1}\cdot \overset{q_5}{2} + \overset{r_5}{0}$

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

$\boxed{-13\cdot 54 + 19\cdot 37 = 1}$

$u = -13$
$v = 19$

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:

$a = bq_1 + r_1 \to$ ①

$b = r_1 q_2 + r_2 \to$ ②

$r_1 = r_2 q_3 + r_3 \to$ ③

$\vdots$

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

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: $(105, 45) = 15$ $\quad \underline{\underline{105u + 45v}}$

~~0~~ ~~14~~ ×

(☆) 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 $\{12, 24, 36, -12, -24, \dots\}$

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

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

$\boxed{\text{LCM}}$

$\boxed{\text{Notation: } [a,b] = LCM(a,b)}$

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: $(12, 16) = 4$ $\quad [12,16] = 48$ $\quad \underbrace{12 \times 16}_{192} = \underbrace{4 \times 48}_{192}$

PROOF:

Consider a and b are non-negative.

PART I

Establish $ld \mid ab$

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

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 $ld = al\,u + bl\,v$. Hence $\frac{ld}{ab} = \left(\frac{al}{ab}\right)u + \left(\frac{bl}{ab}\right)v = \hat{u}u + \hat{v}v \in \mathbb{Z}$

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

Therefore $ab \mid ld$

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

SOLVING DIOPHANTINE EQUATION

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

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 $c = aqu + b\,qv = a x_0 + b y_0$ where $x_0 = qu$ & $y_0 = qv$.

$(e,f)=1$

PROOF: $d = au+bv$ Dividing both sides by d: we get $1 = eu + fv$.

Take any x, y st $ax+by=c$. Substracting 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 $e(x-x_0) + f(y-y_0) = 0$

$\therefore (e,f)=1$ [COPRIME]

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

$e \mid (y-y_0) \Rightarrow y - y_0 = eu$

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

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

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

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. ∎

x-special/nautilus-clipboard
copy
file:///media/ameya/Ubuntu%2020.04%20LTS%20amd641/trisquel_9.0_amd64.iso

MODULAR ARITHMETIC

Congruence Relations

Recap
- → Divisibility
- → Euclid's Alg.
- → GCD
- → LCM
- → Bezout's Id.
- → Diophantine (Linear) eqns.

(1) Given $n \in \mathbb{N}$ we say $x \in \mathbb{Z}$, $y \in \mathbb{Z}$ $\boxed{x \equiv y \mod n}$ if both x & y produce the same remainder when divided by n.

x is congruent to y modulo n.

Eg: $8 \equiv 13 \mod 5$

(2) This is equivalent to saying that $x \equiv y \mod n$ iff $n \mid x-y$

$8 \equiv 13 \mod 5 \Rightarrow 5 \mid 8-13 = -5$

(1) $\Leftrightarrow$ (2) $n \mid x-y$ iff x & y produce the same remainder modulo n.

$\Downarrow$

- $n \mid x-y \Rightarrow x-y = kn \quad k \in \mathbb{Z}$

Let $x = nq_x + r_x \qquad 0 \leq r_x < n$

$y = nq_y + r_y. \qquad 0 \leq r_y < n$

$x-y = n(q_x-q_y) + (r_x-r_y)$

$\Rightarrow kn = n(q_x-q_y) + (r_x-r_y)$

$\Rightarrow (k-q_x+q_y)n = (r_x-r_y)$

$\Rightarrow n \mid (r_x-r_y)$ (n divides r_x-r_y)

This is possible only if $r_x-r_y=0$ or $r_x=r_y$! since $|r_x-r_y| < n$

Both x and y produce the same remainders.

- Both x & y produce the same remainder wrt. n.

i.e. $x = nq_x + r$

$y = nq_y + r$

$x-y = n(q_x-q_y)$

Therefore $n \mid (x-y)$

→ Addition & Subtraction.

$a, b \in \mathbb{Z}$ $n \in \mathbb{N}$
$c, d \in \mathbb{Z}$

$$a \equiv b \mod n$$
$$c \equiv d \mod n$$
$$\overline{a \pm c = b \pm d \mod n}$$

Eg:
$$5 \equiv 13 \mod 8$$
$$12 \equiv 36 \mod 8$$

Addition: $17 \equiv 49 \mod 8$

remainder = 1 remainder 1

Subtract: $-7 \equiv -23 \mod 8$

$\boxed{\text{rem} = 1}$

PROOF

From $a \equiv b \mod n$ we have $a - b = k_1 n$

||ly from $c \equiv d \mod n$ we have $c - d = k_2 n$

$k_1, k_2 \in \mathbb{Z}$

$$a-b + c-d = (a+c) - (b+d)$$
$$= (k_1 + k_2) n$$
$$= kn$$
$$a+c \equiv b+d \mod n.$$

Prove subtraction similarly

→ Multiplication

$$a \equiv b \mod n$$
$$c \equiv d \mod n$$
$$\overline{ac \equiv bd \mod n.}$$

$$12 \equiv 36 \mod 8$$
$$5 \equiv 29 \mod 8$$
$$\overline{60 \equiv 1044 \mod 8}$$

remainder = 4   4

PROOF

$a - b = k_1 n \rightarrow (1)$

$c - d = k_2 n \rightarrow (2)$

Multiplying (1) by c on both sides

$ac - bc = c k_1 n \rightarrow (3)$

Multiplying (2) by b on both sides

$bc - bd = b k_2 n \rightarrow (4)$

(3) + (4)

$$ac - bd = (ck_1 + bk_2) n$$
$$= kn$$
$$ac \equiv bd \mod n.$$

→ Division is not defined in modular arithmetic:

$$10 \equiv 16 \mod 6$$

If you divide both sides by 2

$$5 \not\equiv 8 \mod 6$$

You loose congruence b/w LHS & RHS

We define x/y $(x, y \in \mathbb{Z})$ by finding another integer z s.t $x \equiv yz \bmod n$. (This is not always defined)

Eg: $n = 7$

$$\boxed{5/3 \to 4} \quad 5 \equiv 3 \times 4 \bmod 7$$

$$5 \equiv 12 \bmod 7$$

$\Rightarrow$ Congruence is an equivalence relation on $\mathbb{Z}$

(i) $\forall\, x \in \mathbb{Z}$ $\quad x \equiv y \bmod n \Rightarrow y \equiv x \bmod (n)$ [Symmetry]

(ii) $\forall\, x, y, z$ $\quad$ if $x \equiv y \bmod n$ & $y \equiv z \bmod n$ then $x \equiv y \bmod n$ [Transitive]

(iii) $\forall\, x$ $\quad x \equiv x \bmod n$

Therefore it divides $\mathbb{Z}$ into n equivalence classes.
(a because division by n can produce n remainders $0 \ldots (n-1)$)

Eg: $n = 5$

Notation:

$[0] \to$ remainder $0 \Rightarrow \{0, \pm 5, \pm 10, \pm 15, \pm 20, \ldots\}$

$[1] \to$ remainder $1 \Rightarrow \{\pm 1, \pm 6, \pm 11, \pm 16, \ldots\}$

$[2] \to$ remainder $2 \Rightarrow \{\pm 2, \pm 7, \pm 12, \pm 17, \ldots\}$

$[3] \to$ remainder $3 \Rightarrow \{\pm 3, \pm 8, \pm 13, \ldots\}$

$[4] \to$ remainder $4 = \{\pm 4, \pm 9, \pm 14, \pm 19, \ldots\}$

$$\boxed{\mathbb{Z}_n \triangleq \{[0], [1], [2], [3], [4] \ldots [n-1]\}}$$

MODULE II

Prime Numbers

Prime Number : Definition

→ $p \in \mathbb{N}$ is called prime if only 1 and p divides p.

1 is not prime

2 is prime and the only even number which is a prime

THEOREM

Let p be prime and a and b be integers.

① → Either $p|a$ or $(a,p) = 1$

② → If $p|ab$ then $p|a$ or $p|b$.

PROOF -

① → Since p is prime, only 1 & p are its factors. Therefore either $(a,p) = 1$ or p. If $(a,p) = 1$ we are done. else $(a,p) = p$. This implies $p|a$.

② If $p|a$ then it is done.

If $p \nmid a$ then $(a,p) = 1$. Then by Bezouts' identity

$$ax + py = 1, \text{ where } x, y \in \mathbb{Z}$$

Multiplying both sides by b

$$abx + pby = b.$$

Since $p|ab$ and $p|pb$ the Left Hand side is a multiple of p. Hence $p|b$.

Corollary

If $p \mid a_1 a_2 a_3 \cdots a_n$, $n \geq 2$ then it $p|a_i$ for at least one $i \in 1 \cdots n$.

PROOF Use induction

Basis : $n = 2$; we have proved this case.

Hypothesis : The corollary holds for $n \leq n_0$. consider the product $t = a_1 a_2 a_3 a_4 \cdots \cdots a_{n_0} a_{n_0+1}$

Define $a = a_1 \cdots a_{n_0}$; $b = a_{n_0+1}$

Therefore $p \mid t = p \mid ab$ and hence $p \mid a_1 \cdots a_{n_0}$ or $p \mid a_{n_0+1}$. But since $p \mid a_1 \cdots a_{n_0}$ by Ind. Hypothesis $p \mid a_1$ or $p \mid a_2 \mid \cdots p \mid a_{n_0}$. Therefore $p \mid a_1$ or $p \mid a_2 \cdots \cdots p \mid a_{n_0+1}$ (Combining all)

Eg: $p = 5$ $\qquad 10 \times 7 \times 8 \Rightarrow p \mid 560 \Rightarrow p \mid 10$

Prime Power Factorization

Fundamental Theorem of Arithmetic

Given any integer $n > 1$, can be written as a product of prime-powers.

$(p^e : p \text{ is Prime})$

Eg: $100 = 2^2 \times 5^2$ $\qquad P_1, P_2$ = Prime Numbers

$= P_1^2 \, P_2^2$

Prime Power Factorization

$$\boxed{n = p_1^{e_1} \cdot p_2^{e_2} \cdot \cdots \cdot p_k^{e_k} \qquad e_i > 0}$$

Theorem

Every integer $n > 1$ can be factorized into prime-powers and the factorization is unique.

PROOF: Use mathematical Induction to prove the theorem.

⇒ If $n = 2$, then $n = 2^1$ which is of the required form.

⇒ Let us say every integer from 2 to $n-1$ can be factorized into prime powers

⇒ Consider n, if n is prime then n satisfies the theorem

If n is Composite then $n = ab$ $\qquad 1 < a, b < n$

Since $1 < a, b < n$ both are prime-power factorizable by induction.

Let $a = p_1^{e_1} \, p_2^{e_2} \cdots p_k^{e_k}$ $\qquad e_i \geq 0$

& $b = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}$ $\quad f_k \geq 0$

Therefore

$n = ab = \prod_{i=1}^{k} p_i^{e_i+f_i}$ which is a prime power factorization.

$21 = 3 \times 7$ $\quad 3,5,7$

$35 = 5 \times 7$

$21 = 3^1 \times 5^0 \times 7^1$

$35 = 3^0 \times 5^1 \times 7^1$

Since n is arbitrary it implies any integer greater than 1 is prime factorizable.

Uniqueness (upto permutation of the primes)

Suppose there are two prime-power factorizations for $n>1$

Say $p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots p_k^{e_k}$ & $q_1^{f_1} q_2^{f_2} \cdots q_\ell^{f_\ell}$

Let us denote by R the set of all the primes present in both the factorizations together i.e. $R = \{p_1 \cdots p_k\} \cup \{q_1 \cdots q_\ell\}$

Let $R = \{r_1, r_2, \cdots r_m\}$, $r_i \neq r_j$ $\quad r_i$'s are all primes

Therefore the factorization $\prod_{i=1}^{m} p_i^{e_i} = \prod_{j=1}^{m} r_j^{\hat{e}_j}$; $\hat{e}_j \geq 0$

$|||^{ly}$ the factorization $\prod_{i=1}^{\ell} q_i^{f_i} = \prod_{j=1}^{m} r_j^{\hat{f}_j}$; $\hat{f}_j \geq 0$

$$1 = \frac{n}{n} = \frac{\prod_{j=1}^{m} r_j^{\hat{e}_j}}{\prod_{j=1}^{m} e_j^{\hat{f}_j}} = \prod_{j=1}^{m} r_j^{(\hat{e}_j - \hat{f}_j)}$$

which implies that $\hat{e}_j = \hat{f}_j$ $\forall j \in \{1 \cdots m\}$

This proves that both the factorizations are the same ☒

DISTRIBUTION OF PRIMES

THEOREM There are infinite no: of primes

PROOF: Prove it by contradiction.

Let us assume there are only finite no: of primes.

Since there are only finite no: of primes, there is a largest prime, P. Let us define $Q = 1.2.3.4.5 \cdots .P + 1$. obviously $Q > P$.

If Q is prime then it contradicts the fact that P is the largest prime.

If Q is composite, then none of the primes in 1 to P divides Q. Hence this leads to contradiction with the assumption since there has to a prime greater than P which divides Q. Hence $\therefore$ prime nos. have to be infinite in nos.

GCD and LCM in terms of prime factorization:

Let a & b be two natural numbers. Then a & b, by Fundamental theorem of arithmetic can be written as:

$$a = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_k^{e_k}$$

$$b = p_1^{f_1} \, p_2^{f_2} \ldots p_k^{f_k} \qquad e_i, f_i \geq 0$$

$$gcd(a,b) = (a,b) = p_1^{min(e_1,f_1)} \, p_2^{min(e_2,f_2)} \ldots p_k^{min(e_k,f_k)}$$

Eg:

$$54 = 2 \times 3^3$$
$$16 = 2^4$$

$p_1 = 2$, $p_2 = 3$

$$54 = p_1^1 \cdot p_2^3$$
$$16 = p_1^4 \cdot p_2^0$$

$$(54,16) = 2^{min(1,4)} \cdot 3^{min(0,3)}$$

$$= \underline{\underline{2}}$$

LCM

$$[a,b] = \prod_{i=1}^{k} p_i^{max(e_i,f_i)}$$

$$[54,16] = 2^4 \cdot 3^3 = 16 \times 27 = 6^3 \times 2$$
$$= 216 \times 2 = \underline{\underline{432}}$$

$$(a,b)\,[a,b] = \prod_{i=1}^{k} p_i^{min(e_i,f_i)} \prod_{j=1}^{k} p_j^{max(e_j,f_j)}$$

Collect the terms of the same prime and write the expression as

$$\prod_{i=1}^{k} p_i^{[\,min(e_i,f_i) + max(e_i,f_i)\,]} = \prod_{i=1}^{k} p_i^{e_i+f_i}$$

Say $min(e_i,f_i) = e_i$

then $\max(e_i, f_i) = f_i$

$\therefore$ Sum is $e_i + f_i$.

$$= \prod_{i=1}^{k} p_i^{e_i} \prod_{j=1}^{k} p_j^{f_j}$$

$$= \underline{\underline{a \cdot b}}$$

Fermat and Mersenne Primes

$2^m \pm 1$

There are many small primes which are of this form

Eg: 3, 5, 7, 17 ....

$3 = 2^1 + 1$, $m=1$; 2^2+1, $m=2$; 2^3-1, $m=3$; 2^4+1, $m=4$

Fermat considered numbers of the 2^m+1.

Theorem If 2^m+1 is a prime then m is a power of 2.

Eg: $3 = 2^1 + 1 \Rightarrow m = 1 = 2^0$

$5 = 2^2 + 1 \Rightarrow m = 2 = 2^1$

$17 = 2^4 + 1 \Rightarrow m = 4 = 2^2$

Proof: Suppose m is not a power of 2. Then m can be written as $2^n q$. (where $n \geq 0$, $q > 1$ and q is odd)

(Any no: not a pow. of 2 can be written this way. Eg. $15 = 2^0 \times \underline{\underline{15}}$, $26 = 2^1 \times \underline{\underline{13}}$, $20 = 2^2 \times \underline{\underline{5}}$)

Consider the polynomial $f(t) = t^q + 1$. Since q is odd $t=-1$ is a solution (root). Hence $t+1$ is a factor of $f(t)$. Put $t = x^{2^n}$, then $f(t) = f(x^{2^n}) = (x^{2^n})^q + 1 = x^{2^n q} + 1 = x^m + 1$. This has $t+1 = x^{2^n}+1$ as a factor. In particular if you put $x=2$ you get $(2^{2^n}+1)$ is a factor of 2^m+1. Therefore

2^m+1 is Composite.

$2^{2^n}+1 \Rightarrow F_n$ (Fermat Number).

Fermat nos. F_n which are prime are called Fermat primes.

$n=0$	$n=1$	$n=2$	$n=3$	$n=4$
$F_0=3$	$F_1=5$	$F_2=17$	$F_3=257$	$F_4=65537$

All primes

Euler proved that $F_5 = 4294967297$ is Composite.

Consider nos. of the form a^m-1 (which is a generalization of 2^m-1)

What are the conditions a & m should satisfy for a^m-1 to be a prime?

THEOREM If a^m-1 is a prime then $a=2$ and m is prime.

PROOF

Condition on a: Consider the polynomial $f(a) = a^m-1$. This has 1 as a root (Soln.). Therefore $a-1$ is a factor of $f(a)$. If $a>2$ then $a-1>1$ and hence a^m-1 is composite. If $a=1$ then $f(a)=0$ is invariably 0 for every m and hence not prime for any m. Therefore $a=2$ is the possibility for $f(a)$ to be prime for some m.

Condition on m: Suppose m is Composite. Then $m=pq$, where $1<p,q<m$. Therefore $2^m-1 = 2^{pq}-1 = (2^p)^q-1$. Taking $t=2^p$, 2^m-1 can be written as t^q-1. This clearly has $t-1$

as a factor. Resubstituting 2^p for t we get $2^p - 1$ as a factor for $2^m - 1$. But $2^p - 1 > 1$ hence $2^m - 1$ is composite. Therefore for $2^m - 1$ to be prime m has to be prime too.

$\boxtimes$

Nos. of the form $2^p - 1$ (p is prime) are called Mersenne Numbers. If it is a prime then it is called Mersenne Prime.

M_p

$p = 2 \quad M_2 = 3$

$p = 3 \quad M_3 = 7$

$p = 5 \quad M_5 = 31$

$p = 7 \quad M_7 = 127$

M_{11}
2047
(not prime)
(23×89)

PRIMALITY TESTING

Given a number n, how can we determine if it is prime?

→ Naivest algorithm: Take all integers 2 to $(n-1)$ and divide n by those numbers. If at least one of them produces a remainder 0, then n is composite. Else it is prime

→ Exponentially complex $(\Theta(n))$ → input size is $\log(n)$

THEOREM: n is composite if & only if there exists a prime $p \leq \sqrt{n}$ s.t $p | n$.

→ search $2 \ldots \sqrt{n}$

PROOF: If there exists a prime $p \leq \sqrt{n}$, then obviously n is composite.

Converse

If n is composite then $n = ab$. At least one of a & b has to be $\leq \sqrt{n}$ (otherwise $a > \sqrt{n}$ & $b > \sqrt{n} \Rightarrow a \cdot b > n$). without loss of generality let $a \leq \sqrt{n}$. If a is prime the theorem is proved, else if a is composite it has a prime factor $p < a \leq \sqrt{n}$. Now p is a factor of n. This proves the theorem. $\boxtimes$

This theorem improves the time complexity to $\Theta(\lfloor \sqrt{n} \rfloor)$