Gourav Dhanwar

1) Every composite no. can be written as a product of its prime factor

$N = p_1^{e_1} \ldots p_r^{e_r}$ where $p_r \leq n$

Ans:- Proof by contradiction,

let $n = p^i p_1 \ldots p_r = p^j q_1 q_2 \ldots q_r$ be 2 prime factorizations of the no. n

p is a common prime factor in both nos
$i \geq 0$ & $j > i$

Since $\gcd(p_i, p) = 1$ (∵ 2 prime nos are always relatively prime)

$[p_i] \in U_p \rightarrow$ where U_p is the residual set of P.

∴ $[p_1 \ldots p_r] \in U_p$ (∵ product of nos in a residual set also lies in that residual set)

Also, we know that
$p_1 \ldots p_r = p^{j-i} q_1 \ldots q_r$ — (i)
∴ $[p^{j-i} q_1 \ldots q_r] = [0]$

& from [i] $[p_1 p_2 \ldots p_r] = [0]$

$[0] \notin U_p$ but $[p_1 p_2 \ldots p_r] \in U_p$

There is a contradiction

Thus every comp has a unique prime factorization

(8-2)

(i) $S_i \cap S_j = \phi \quad (i \neq j)$

Assume $i \neq j$ & $S_i \cap S_j \neq \phi$
without loss of generality, let

$c \in S_i - S_j$
& $d \in S_i \cap S_j$
$\Rightarrow$ i. $c \sim d \quad (\because c, d \in S_i)$
d. $c \sim b \quad (\because \sim$ is transistive$)$ $\Big\}$ $c \in S_j$

$c \in S_i - S_j$

which proves that our assumption is wrong

$S_i \cap S_j = \phi$ — (3)

Also, we know for a fact, that, for any partition S_i of S, there is equivalence rely on S whose equivalence classes form partition S_i — (4)

using (3) & (4) we can claim that

$S_1 \cup S_2 \cup S_3 \ldots \cup S_4 = S$

(ii) if $a, b \in S_i$, $a \sim b$
for any partition S_i of S, there is equivalence relation on S whose equivalence

classes form the partition s_i

$\Rightarrow$ If $a, b \in s_i$
$a \sim b$

(iii) if $a \in s_i$, $b \in s_j$ $(i \neq j)$ then $a \nsim b$

From ①, we know that $\forall i \neq j$

$s_i \cap s_j = \phi$ — ②
If $a \in s_i$ & $b \in s_j$ where

$a \sim b$ would imply $s_i \cap s_j \neq \phi$
Hence $a \nsim b$

(iv) $S_1 \cup S_2 \cdots \cup S_n = S$

We know that $\forall i, j \in \{1, 2, \ldots 4\}$
w/ $i \neq j$

$s_i \cap s_j = \phi$ → ③
Also, we know for a fact, that for any partition S_i of S, there is an eq. rel^n ④

using ③ & ④, we can claim that

$$\boxed{S_1 \cup S_2 \cup S_3 \cdots \cup S_4 = S}$$

Q-3 Show that

(i) $[a]_n + [b]_n = [a+b]_n$
(ii) $[a]_n [b]_n = [ab]_n$
(iii) $[a]_n - [b]_n = [a-b]_n$

(i) $[a]_n \Rightarrow nq_1 + r_1 = a$ $\quad [a]_n = r_1 \quad 0 \leq r_1 \leq n$
$[b]_n \Rightarrow nq_2 + r_2 = b$ $\quad [b]_n = r_2 \quad 0 \leq r_2 \leq n$

$(a+b) = n(q_1+q_2) + (r_1+r_2)$

$[a+b]_n = [r_1+r_2]_n$ — ①

$[a]_n + [b]_n = [r_1+r_2]_n$ — ② [∵ we are considering modular arthimatic)

from ① & ②
$[a]_n + [b]_n = [a+b]_n$

(ii) When consider
$[a]_n$ & $[b]_n$ we can say that

→ $a = nq_1 + r_1$ & $[a]_n = r_1$ where $0 \leq r_1 < n$

→ $b = nq_2 + r_2$ & $[b]_n = r_2$ where $0 \leq r_2 < n$

Now, $[a]_n [b]_n = [r_1 r_2]_n$ — ①

Also, $a \cdot b = (nq_1 + r_1)(nq_2 + r_2)$

$= nq_1(nq_2 + r_2) + nr_1 q_2 + r_1 r_2$

$= n[q_1(nq_2 + r_2) + r_1 q_2] + r_1 r_2$

$[ab]_n = [r_1 r_2]_n$ —②

Hence from ① & ②

$[a]_n [b]_n = [ab]_n$

(iii) $a = nq_1 + r_1$ where $0 \le r_1 \le n$ $[a]_n = r_1$

$b = nq_2 + r_2$ where $0 \le r_2 \le n$ $[b]_n = r_2$

Now,

$[a]_n - [b]_n = [r_1 - r_2]_n$ ①

Also,

$a - b = n[q_1 - q_2] + r_1 - r_2$

$[a-b]_n = [r_1 - r_2]_n$ —②

from ① & ②

$[a-b]_n = [a]_n - [b]_n$

Q4) Chinese remainder theorem

Given $p_0, p_1 \ldots p_{n-1}$ are relatively prime integers & given any integer

Now,

for $u \bmod p_i = u_i$

then $r_u = (u_0, u_1 \ldots u_{n-1})$

Let $p = \prod_{i=0}^{n-1} p_i$ then there exists a 1-1 correspondence

$\{0, \ldots p-1\} \Leftrightarrow \{r_u \mid u = \{0 \ldots p-1\}\}$

<u>Proof:-</u>

Proof is done by contradiction

Suppose u, v are in $0 \ldots p-1$ such that $r_u = r_v$

$\therefore (u_0 \ldots u_{n-1}) = (v_0 \ldots v_{n-1})$

$\therefore u_i = v_i \quad \forall i$

or $u_i = u \pmod{p_i} = v_i = v \bmod p_i$

$\therefore p_i \mid u - u_i = u - v_i$

$p_i \mid v - v_i$

$\therefore$ p_i ~~$u-v_i$~~ must divide $(v-v_i)-(v-v_i)$

$p \mid u-v \quad \forall i$

since p_is are co-prime

$$\prod_{i=0}^{n-1} p_i \mid u-v = p \mid u-v$$

but u & v are in range $0 \ldots p-1$

$\therefore u=v$

$\therefore u-v=0$

which establishes one to one correspondance & proves that there exists a unique set r_u.

q-5) Prove using Euclidean algorithm that given (m,n) there exists (a,b) such that

$$\gcd(m,n) = am+bn$$

Also prove that a & b are unique

Proof:- From the euclidean algorithm we know that given $m \geq n$

$$\gcd(m,n) = \gcd([m]_n, n]$$

Hence we can say that if m is represented as

$m = nq_1 + r_1$ where q_1, r_1 are quotient & remainder
$0 < r_1 < n$

$n = r_1 q_2 + r_2$

$r_{k-2} = r_{k-1} q_k + r_k$

$r_{k-1} = r_k q_{k+1}$

$\therefore \gcd(m,n) = \gcd(r_{k-1}, r_k) = r_k$

$\therefore\ r_k = r_{k-2} - r_{k-1} q_k$

$r_k = r_{k-2} - (r_{k-3} - r_{k-1} q_{k-1}) q_n$

Rearranging we get,

$r_k = r_{k-2} a + r_{k-3} b$

$r_k = r_{k-2} a + r_{k-3} b$

where $a = 1 + q_{k-1} q_k$

$b = q_k$

We go on repeating this process of going backwards until we obtain

$r_k = am + bn$

where a & b are integers that are unique

$\therefore$ Hence a & b are the integers that are unique

Q6) Write the proof that $\phi(mn) = \phi(m)\phi(n)$

if $\gcd(m,n) = 1$

proof:-

To prove this we make a rectangular table of numbers 1 to mn with m rows & n coloumns

1	$m+1$	$(n-1)m+1$
2	$m+2$	$(n-1)m+2$
3	$m+3$	$(n-1)m+3$
⋮	⋮	⋮
m	$2m$	nm

The nos in the r^{th} row of this table

$km+r$ runs from 0 to $m-1$

let $d = \gcd(r,m)$, if $d > 1$ then no number in the r^{th} row is relatively prime to mn

$\because d \mid km+r$ for $\forall\, k \in \mathbb{Z}$

So, to count the residues relatively prime to mn we need to take a look at those row indexed by values & such that

$\gcd(r,m) = 1$
There are $\phi(m)$ such rows

If $\gcd(r,m) = 1$, then every entry in the r^{th} row is relatively prime to m.

Now, in the r^{th} row.

considering 2 element
$km+r \equiv (tm+r) \bmod n$

* This means that $km+r$ & $tm+r$ fall in the same residual class of n

But $(k-t)m \equiv 0 \bmod n$

& m can't divide n as we know $\gcd(m,n) = 1$

$\therefore k = t$ fall nos in the r^{th} row where

$\gcd(r,m) = 1$ have to lie in seperate residual

classes of n

Hence out of these nos $\phi(n)$ will have such value of $\gcd = 1$. Thus,

$\phi(m,n) = \phi(m) \cdot \phi(n)$ → No. of elements in each row.

no. of rows