④ (a). Show that the arithmetic function τ is multiplicative.

Pf :- For $m=n=1$, the result is trivially true.
Let $m>1$ & $n>1$ be two relatively prime integers, i.e. $(m,n)=1$.
Let $m = p_1^{a_1} \cdot p_2^{a_2} \cdots p_r^{a_r}$
& $n = q_1^{b_1} \cdot q_2^{b_2} \cdots q_s^{b_s}$ be prime factorizations of m & n. Since $(m,n)=1$, no p_i & q_j will be same. Therefore, the prime factorization of mn will be given by.

$$mn = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} \cdot q_1^{b_1} q_2^{b_2} \cdots q_s^{b_s}$$

Hence

$$\tau(mn) = [(a_1+1)(a_2+1)\cdots(a_r+1)][(b_1+1)\cdots(b_s+1)]$$
$$= \tau(m) \cdot \tau(n)$$

$\Rightarrow \tau$ is multiplicative.

Hence proved.

④ (b). If p is prime, then prove that

$$(p-1)! \equiv -1 \pmod{p}$$

Name the theorem.

Ans: Wilson's theorem.

(5) (b) Evaluate $\phi(5186)$

Ans: We have $5186 = 2 \times 2593$

$$\phi(5186) = \phi(2 \times 2593)$$
$$= \phi(2) \cdot \phi(2593)$$
$$= (2^1 - 2^0) \cdot (2593^1 - 2593^0)$$
$$= (2-1)(2593-1)$$
$$= 1 \cdot 2592$$
$$= 2592$$ Ans

(6) (a) State and prove Euler's theorem.

Ans: Statement -

If a & $n > 0$ are integers s.t. $(a,n) = 1$ then $a^{\phi(n)} \equiv 1 \pmod{n}$

Pf: If $n = 1$ then $\phi(1) = 1$ & $a^1 = a \equiv 1 \pmod{1}$

Now we assume $n > 1$.

Let $a_1, a_2, \ldots, a_{\phi(n)}$ be positive integers less than n which are relatively prime to n ie. $(a_i, n) = 1$.

We consider $aa_1, aa_2, \ldots, aa_{\phi(n)}$. For each i, $1 \le i \le \phi(n)$, $aa_i \not\equiv 0 \pmod{n}$ because $n \mid aa_i$, $(a,n) = 1$

$\Rightarrow n \mid a_i$ which is not possible

because $aa_i \equiv aa_j \pmod{n}$.

Also $aa_i \not\equiv aa_j \pmod{n}$

$\Rightarrow n \mid (aa_i - aa_j) = a(a_i - a_j)$ & $(a,n) = 1$.

$\Rightarrow n \mid a_i - a_j$

$\Rightarrow a_i \equiv a_j \pmod{n}$ which is again not possible.

⑤ (a) State & prove Mobius Inversion formula.

⇒. let

$$F(n) = \sum_{d/n} f(d)$$

then

$$f(n) = \sum_{d/n} \mu(d)\, F(n/d) = \sum_{d/n} \mu(n/d)\cdot F(d)$$

Pf:-

We have -

$$\sum_{d/n} \mu(d)\, F(n/d) = \sum_{d/n} \left[\mu(d) \sum_{c/(n/d)} f(c) \right]$$

$$= \sum_{d/n} \left[\sum_{c/(n/d)} \mu(d) f(c) \right]$$

$$= \sum_{c/n} \left[\sum_{d/(n/c)} f(c)\, \mu(d) \right]$$

[$\because$ d/n & $c/(n/d) \Leftrightarrow c/n$ & $d/(n/c)$]

$$= \sum_{c/n} \left[f(c) \sum_{d/(n/c)} \mu(d) \right]$$

$$= \sum_{c=n} f(c) \cdot 1$$

$$= f(n)$$

& by replacing d by n/d, we get -

$$F(n) = \sum_{d/n} f(d).$$

Hence proved.

⑤ (b)

Ans

⑥ (a

Ans

Pf

Thus, $aa_1, aa_2, \ldots, aa_{\phi(n)}$ are $\phi(n)$ mutually congruent integers & therefore

$aa_1 \equiv aa_1' \pmod n$

$aa_2 \equiv aa_2' \pmod n$

$\vdots$

$aa_{\phi(n)} \equiv aa'_{\phi(n)} \pmod n$

where $a_1', a_2', \ldots$ are a_1, a_2 in some other order.

Multiplying these relations we get -

$aa_1 \cdot aa_2 \cdots aa_{\phi(n)} \equiv a_1' a_2' \cdots a'_{\phi(n)} \pmod n$.

or $a^{\phi(n)} \cdot a_1 a_2 \cdots a_{\phi(n)} \equiv a_1 a_2 \cdots a_{\phi(n)} \pmod n$

since each a_i is coprime to n, so we have -

$a_1, a_2, \ldots, a_{\phi(n)}$ is coprime to n.

Therefore, $a^{\phi(n)} \equiv 1 \pmod n$.

Hence proved

⑥ (b) Solve the congurence.

$$3x^2 + 5x + 9 \equiv 0 \pmod{11}.$$

Sol^n: We have $3x^2 + 5x + 9 \equiv 0 \pmod{11}$ — ①

Multiplying ① by $3 \times 4 = 12$, we get -

$$36x^2 + 60x + 108 \equiv 0 \pmod{11}$$

or, $(6x+5)^2 \equiv 5 \pmod{11}$ — ②

Putting $6x + 5 = y$ in ②, we get.

$$y^2 \equiv 5 \pmod{11}$$
$$\equiv (5+11) \pmod{11}$$
$$\equiv 4^2 \pmod{11}$$
$$\Rightarrow y \equiv \pm 4 \pmod{11}$$
$$\Rightarrow 6x + 5 \equiv \pm 4 \pmod{11}$$
$$\Rightarrow 6x \equiv (2, 10) \pmod{11}$$
$$\Rightarrow x \equiv 4, 9 \pmod{11}$$

Ans.

① (a) Show that

$$\bar{\phi}(n) = \frac{1}{2} \sum_{x=1}^{n} \mu(x) \left[\left[\frac{n}{x}\right]^2 + \left[\frac{n}{x}\right] \right]$$

Pf:- We have

$$\bar{\phi}(n) = \phi(1) + \phi(2) + \cdots + \phi(n)$$

$$= 1 \sum_{d|1} \frac{\mu(d)}{d} + 2 \sum_{d|2} \frac{\mu(d)}{d} + \cdots + n \sum_{d|n} \frac{\mu(d)}{d}.$$

This can be written as -

$$\bar{\phi}(n) = a_1 \mu(1) + a_2 \mu(2) + \cdots + a_n \mu(n)$$
$$= \sum_{x=1}^{n} a_x \mu(x).$$

We see that $\mu(x)$ appears once in the following terms of (1) :-

$$x \sum_{d|x} \frac{\mu(d)}{d}, \quad 2x \sum_{d|2x} \frac{\mu(d)}{d}, \quad \ldots, \quad \left[\frac{n}{x}\right] x \sum_{d|[n/x]x} \frac{\mu(d)}{d}$$

Therefore :-

$$a_x = x \cdot \frac{1}{x} + 2x \cdot \frac{1}{x} + \cdots + \left[\frac{n}{x}\right] \cdot x \cdot \frac{1}{x}$$

$$= 1 + 2 + \cdots + \left[\frac{n}{x}\right]$$

$$= \frac{1}{2}\left[\left[\frac{n}{x}\right]^2 + \left[\frac{n}{x}\right]\right]$$

Hence,

$$\phi(n) = \frac{1}{2} \sum_{x=1}^{n} \mu(x) \left[\left[\frac{n}{x}\right]^2 + \left[\frac{n}{x}\right]\right]$$

Hence proved.

(7) (b) Construct the index table for 17 with primitive root 5.

Ans: We have $\phi(17) = 16$

& 5 is the primitive root.

Now, we have-

$5^0 = 1$, $5^1 = 5$, $5^2 \equiv 8 \pmod{17}$,

$5^3 \equiv 6 \pmod{17}$,

$5^4 \equiv 13 \pmod{17}$,

$5^5 \equiv 14 \pmod{17}$,

$5^6 \equiv 2 \pmod{17}$,

$5^7 \equiv 10 \pmod{17}$, $5^8 \equiv 16 \pmod{17}$,
$5^9 \equiv 12 \pmod{17}$, $5^{10} \equiv 9 \pmod{17}$,
$5^{11} \equiv 11 \pmod{17}$, $5^{12} \equiv 4 \pmod{17}$,
$5^{13} \equiv 3 \pmod{17}$, $5^{14} \equiv 15 \pmod{17}$
$5^{15} \equiv 7 \pmod{17}$.

Thus we have the following index $5^{16} \equiv 1 \pmod{}$ table :

a	1	2	3	4	5	6	7	8	9	10
ind a	0	6	13	12	1	3	15	2	10	7

a	11	12	13	14	15	16
ind a	11	9	4	5	14	8

Q.E.D.

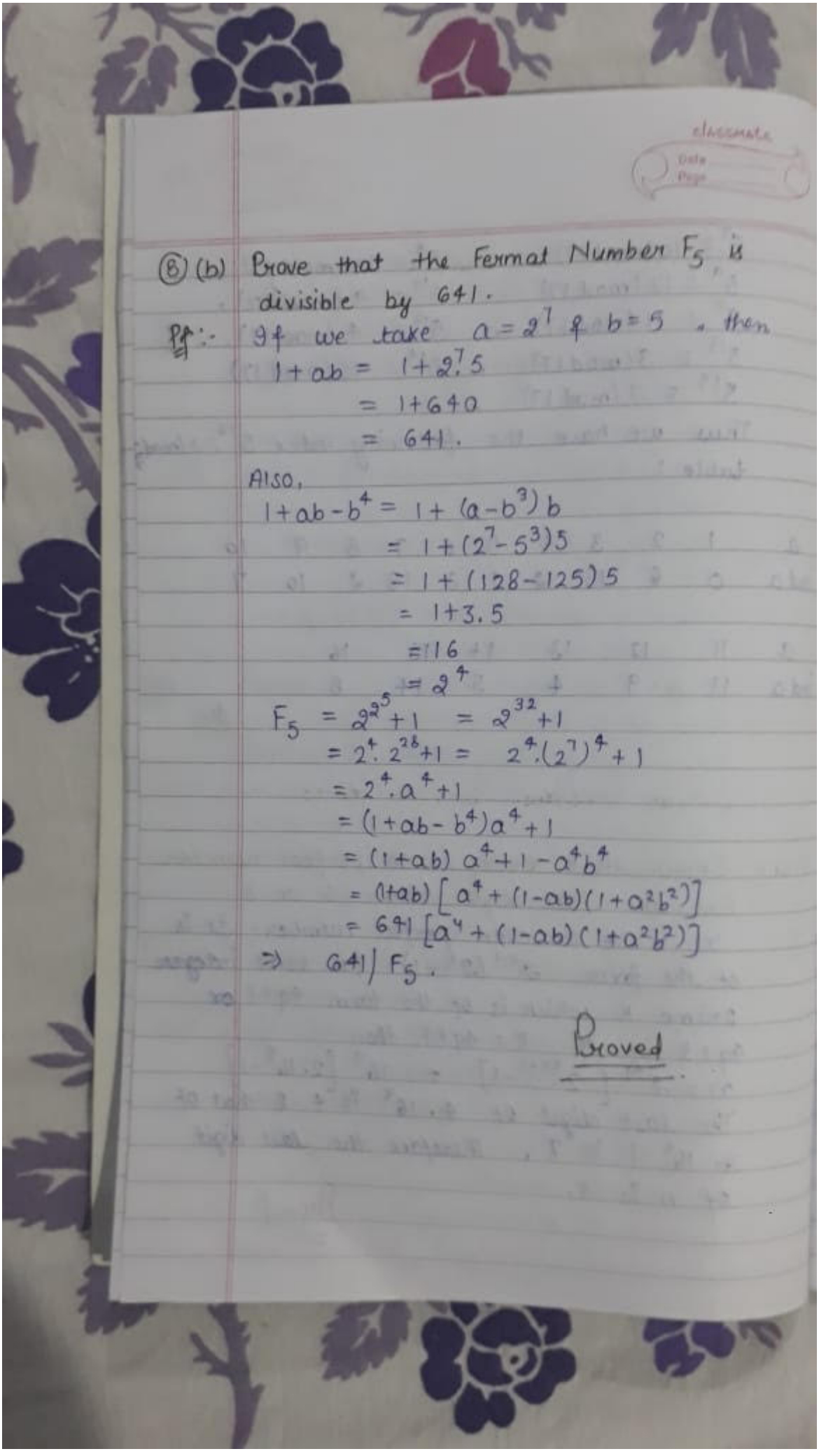
(B) (a). Show that every even perfect number has the last digit either 6 or 8.

Pf: Let n be an even perfect number. It is of the form $2^{k-1}(2^k - 1)$ for some integer prime k which is of the form $4q+1$ or $4q+3$. If $k = 4q+1$ then

$n = 2^{4q}\left[2^{4q+1} - 1\right] = 16^q\left[2 \cdot 16^q - 1\right]$

The last digit of $4 \cdot 16^q$ is 4 & that of $8 \cdot 16^q - 1$ is 7. Therefore the last digit of n is 8.

Proved.



⑧ (b) Prove that the Fermat Number F_5 is divisible by 641.

Pf:- If we take $a = 2^7$ & $b = 5$, then

$$1 + ab = 1 + 2^7 5$$
$$= 1 + 640$$
$$= 641.$$

Also,

$$1 + ab - b^4 = 1 + (a - b^3) b$$
$$= 1 + (2^7 - 5^3)5$$
$$= 1 + (128 - 125)5$$
$$= 1 + 3.5$$
$$= 16$$
$$= 2^4$$

$$F_5 = 2^{2^5} + 1 = 2^{32} + 1$$
$$= 2^4 . 2^{28} + 1 = 2^4 . (2^7)^4 + 1$$
$$= 2^4 . a^4 + 1$$
$$= (1 + ab - b^4) a^4 + 1$$
$$= (1 + ab) a^4 + 1 - a^4 b^4$$
$$= (1 + ab) [a^4 + (1 - ab)(1 + a^2 b^2)]$$
$$= 641 [a^4 + (1 - ab)(1 + a^2 b^2)]$$

$\Rightarrow 641 \mid F_5$.

Proved

③ (b) Find the remainder when 2^{340} is divided by 341.

Ans: We have $341 = 11 \times 31$
& $340 = 68 \times 5$.

Now,

$2^5 = 32 \equiv -1 \pmod{11}$

$\Rightarrow 2^{340} = (2^5)^{68} \equiv [-1 \pmod{11}]^{68}$

$\equiv (-1)^{68} \pmod{11}$

$\equiv 1 \pmod{11}$

Similarly,

$(2^5) = 32 \equiv 1 \pmod{31}$

$\Rightarrow 2^{340} \equiv (2^5)^{68} \equiv [1 \pmod{31}]^{68}$

$\equiv 1 \pmod{31}$

$\Rightarrow 2^{340} = [1 \pmod{11}] \cdot [1 \pmod{31}]$

$= (1 \cdot 1) \pmod{11 \cdot 31}$

$= 1 \pmod{341}$.

$\Rightarrow$ 1 is the remainder when 2^{340} is divided by 341.

Ans.