① Given $a \in \mathbb{Z}$, $n \geq 1$ satisfing -

$$a^{n-1} \equiv 1 \pmod{n} \quad \text{but}$$

$$a^m \not\equiv 1 \pmod{n} \quad \text{for each } m \mid (n-1) \text{ \& } m < (n-1)$$

we know that if h is the smallest number

s.t. $a^h \equiv 1 \pmod{n}$

and k any other integer satisfying

$$a^k \equiv 1 \pmod{n}$$

$$\Rightarrow \quad h \mid k$$

Since for all divisor m of $n-1$ other than itself

$$a^m \not\equiv 1 \pmod{n}$$

$\Rightarrow$ $n-1$ is the smallest integer satisfying

$$a^{n-1} \equiv 1 \pmod{n}$$

or $\quad \text{ord}_n a = n-1$

By Euler th^m

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

$$\Rightarrow \quad n-1 \mid \phi(n) \quad \Rightarrow \quad n-1 \leq \phi(n) \quad - ①$$

But if n is not a prime then

$$\phi(n) < n-1$$

which contradicts ①. Hence n has to be a prime and $\phi(n) = n-1$.

② Given, n is not a Pseudoprime to base bb'

$(b, b') = 1$,

$\Rightarrow (bb')^{n-1} \not\equiv 1 \pmod{n}$ — ①

Let n is a Pseudoprime to base b, then

$b^{n-1} \equiv 1 \pmod{n}$ — ②

from ① -

$(bb')^{n-1} - b^{n-1} + b^{n-1} \not\equiv 1 \pmod{n}$

$\Rightarrow b^{n-1}(b'^{n-1} - 1) + b^{n-1} - 1 \equiv 0 \pmod{n}$

$\Rightarrow b^{n-1}(b'^{n-1} - 1) \not\equiv 0 \pmod{n}$ [from 2)

$\Rightarrow n \nmid b^{n-1}(b'^{n-1} - 1)$

$\Rightarrow n \nmid b^{n-1}$ and $n \nmid (b'^{n-1} - 1)$

$n \nmid b^{n-1}$ true from ②.

$\Rightarrow n \nmid (b'^{n-1} - 1)$

$\Rightarrow b'^{n-1} \not\equiv 1 \pmod{n}$

$\Rightarrow n$ is not a Pseudoprime to base b'.

Similarly, we know show if n is a Pseudoprime to base b', then n can not be Pseudoprime to base b.

③ (a) $1105 = 5 \times 13 \times 17$

Let $(a, 1105) = 1$

$\Rightarrow (a,5) = (a,13) = (a,17) = 1$

By Eular's thm -

$$a^4 \equiv 1 \pmod 5$$

$$a^{1104} = (a^4)^{276} \equiv 1 \pmod 5 \quad -①$$

Similarly,

$$a^{12} \equiv 1 \pmod{13}$$

$$\Rightarrow a^{1104} \equiv (a^{12})^{92} \equiv 1 \pmod{13} \quad -②$$

and $a^{16} \equiv 1 \pmod{17}$

$$a^{1104} \equiv (a^{16})^{69} \equiv 1 \pmod{17} \quad -③$$

from ①, ② & ③ and chinese remainder thm, we have-

$$a^{1104} \equiv 1 \pmod{1105} \text{ for all } (a, 1105) = 1$$

Hence, 1105 is a carmichael number.

(b) $1729 = 7 \times 13 \times 19$

Let $(a, 1729) = 1$

$\Rightarrow (a,7) = 1, (a,13) = 1, (a,19) = 1$

By Eular's thm -

$$a^6 \equiv 1 \pmod 7$$

$$\Rightarrow a^{1728} = (a^6)^{288} \equiv 1 \pmod 7 \quad -①$$

$$a^{12} \equiv 1 \pmod{13}$$

$\therefore$ $a^{1728} = (a^{12})^{144} \equiv 1 \pmod{13}$ — ②

$$a^{18} \equiv 1 \pmod{19}$$

$a^{1728} = (a^{18})^{86} \equiv 1 \pmod{19}$ — ③

from ①, ② & ③ and chinese remainder thm, we have-

$$a^{1728} \equiv 1 \pmod{1729} \text{ for all } (a, 1729) = 1$$

Hence, 1729 is a carmichael number.

④ $756 = 3^3 \times 2^2 \times 7$

Let $(a, 756) = 1$

$\therefore$ $(a, 3^3) = 1$, $(a, 2^2) = 1$, $(a, 7) = 1$

By euler thm

$$a^{\phi(27)} \equiv a^{18} \equiv 1 \pmod{3^3} \text{ — ①}$$

$$a^{\phi(4)} \equiv a^2 \equiv 1 \pmod{2} \text{ — ②}$$

$$a^{\phi(7)} = a^6 \equiv 1 \pmod{7} \text{ — ③}$$

Since- $\text{lcm}(18, 2, 6) = 1$, so -

from ①, ② & ③ and chinese remainder thm we have-

$$a^{18} \equiv 1 \pmod{756}$$

$\Rightarrow$ $K = 18$ is the smallest number s.t.

$$a^K \equiv 1 \pmod{756} \quad \forall \ (a, 756) = 1$$

(5) (a) $N = 49601$, $S = 247$

$N = 49601 = 257 \times 193$

$\phi(N) = \phi(257) \times \phi(193)$

$= 256 \times 192$ (257 & 193 are primes)

$= 49152$

We need to find private key t, s.t.

$$St \equiv 1 \mod(\phi(N))$$

$$\Rightarrow 247t \equiv 1 \mod(49152)$$

$$\Rightarrow 247t - 49152K = 1 \text{ (for some } k) \text{ — } ①$$

By Euclidean Algorithm, we have -

$$49152 = 198 \times 247 + 246$$

$$247 = 1 \times 246 + 1$$

$$\Rightarrow 1 = 247 - 1 \times 246$$

$$1 = 247 - 1(49152 - 198 \times 247)$$

$$1 = 199 \times 247 - 49152 \text{ — } ②$$

compare ① & ②, we have -

$$\boxed{t = 199}$$

(b) E = Encrypted message

$$E \equiv M^S \pmod N$$

M = No = 1415

$$E \equiv (1415)^{247} \pmod{49601}$$

$$49601 = 257 \times 193$$

$$(1415)^{247} \equiv (130)^{247} \pmod{257}$$

$$(1415)^{247} \equiv (64)^{247} \equiv (64)^{55} \pmod{193}$$

$$\equiv 64 \times (64^2)^{27} \equiv 64 \times (43)^{27}$$

$$\equiv 64 \times 43 \times (43^2)^{13}$$

$$\equiv 64 \times 43 \times (112)^{13}$$

$$\equiv 64 \times 43 \times 112 \times 81^6$$

$$\equiv 64 \times 43 \times 112 \times (-1)^6$$

$$\equiv 50 \times 112 \equiv 3 \pmod{193}$$

And-

$$(130)^{247} \equiv K \pmod{257}$$

$$\Rightarrow (130)^{256} \equiv K \times (130)^9 \pmod{257}$$

$$K \times (130)^9 \equiv 1 \pmod{257}$$

$$\Rightarrow K \times 130 \times (195)^4 \equiv 1 \pmod{257}$$

$$K \times 130 \times (246)^2 \equiv 1 \pmod{257}$$

$$\Rightarrow K \times 130 \times (-11)^2 \equiv 1 \pmod{257}$$

$$\Rightarrow K \times 130 \times 121 \equiv 1 \pmod{257}$$

$$K \times 53 \equiv 1 \pmod{257}$$

$$\Rightarrow K \times 53 - 257t = 1 \quad \text{— (*)}$$

$$257 = 4 \times 53 + 45$$

$$53 = 45 \times 1 + 8$$

$$45 = 8 \times 5 + 5$$

$$8 = 5\times 1 + 3$$

$$5 = 3\times 1 + 2$$

$$3 = 2\times 1 + 1$$

$$1 = 3 - 2$$

$$= 3 - (5 - 3)$$

$$= 2\times 3 - 5$$

$$= 2\times(8 - 5) - 5$$

$$= 2\times 8 - 3\times 5$$

$$= 2\times 8 - 3(45 - 8\times 5)$$

$$= 17\times 8 - 3\times 45$$

$$= 17(53 - 45) - 3\times 45$$

$$= 17\times 53 - 20\times 45$$

$$= 17\times 53 - 20(257 - 4\times 53)$$

$$1 = 97\times 53 - 20\times 257 \quad \cdots (**)$$

compare (*) and (**) we have -

$$k = 97$$

By CRT, we get -

$$193\, b_1 \equiv 1 \pmod{257}$$

$$257\, b_2 \equiv 64\, b_2 \equiv 1 \pmod{193}$$

By Euclidean algorithm, we get -

$$b_1 = 4, \quad b_2 = -3$$

e) $E = 257 \times (-3) \times 3 + 193 \times 4 \times 97$

$E \equiv 72571 \equiv 22970 \pmod{49601}$

So, $E = 22970$

To varify, we find

$$E' = E^t \pmod{N}$$

$(22970)^{199} \equiv 3^{199} \pmod{193}$

$\equiv 3^7 \pmod{193}$

$\equiv 9 \times 50 \equiv 64 \pmod{193}$

$(22970)^{199} \equiv (97)^{199} \pmod{257}$

$\equiv 97 \times (97^2)^{99}$

$\equiv 97 \times (157)^{99} \equiv 97 \times 157 \times (-23)^{49}$

$\equiv 66 \times (-23) \times (15)^{24}$

$\equiv 24 \times (225)^{12}$

$\equiv 24 \times (-32)^{12} = 24 \times 2^{60}$

$= 24 \times 2^4 \times (1)^7$

$\equiv -127 \pmod{257}$

By CRT, we have -

$E' = 257 \times (-3) \times 64 + 193 \times 4 \times (-127)$

$\equiv 1415 \pmod{N}$

$E' = E^t \equiv M \pmod{N}$.

(6) Let $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$

We know

$d(n)$ is multiplicative

$\Rightarrow \sum_{m|n} d(m)$, $d^3(n)$ and so $\sum_{m|n} d^3(m)$

are multiplicative functions.

$$d(p_i^{\alpha_i}) = \alpha_i + 1$$

$$\Rightarrow \sum_{m | p_i^{\alpha_i}} d(m) = \sum_{j=0}^{\alpha_i} d(p_i^j)$$

$$= \sum_{j=0}^{\alpha_i} (j+1)$$

$$= \frac{(\alpha_i+1)(\alpha_i+2)}{2}$$

and $$\sum_{m | p_i^{\alpha_i}} d^3(m) = \sum_{j=0}^{\alpha_i} d^3(p_i^j)$$

$$= \sum_{j=0}^{\alpha_i} (j+1)^3$$

$$= \left(\frac{(\alpha_i+1)(\alpha_i+2)}{2}\right)^2$$

$$= \left(\sum_{m | p_i^{\alpha_i}} d(m)\right)^2$$

Hence -

$$\left(\sum_{m|n} d(m)\right)^2 = \sum_{m|n} d^3(m).$$

(7) $N = 3^{10!} - 1$

$\phi(125) = 125 - 25 = 100$

By Euler thm -

$3^{100} \equiv 1 \pmod{125}$ $((3,125) = 1)$

Since $100 \mid 10!$

$\Rightarrow 3^{10!} \equiv 1 \pmod{125}$.

(8) (a) # of primitive roots

$= \phi(\phi(29))$

$= \phi(28) = \phi(4) \cdot \phi(7)$

$= 2 \times 6 = 12$

(b) $2^2 \equiv 4 \pmod{29}$

$2^7 \equiv 2^5 \cdot 2^2 \equiv -3 \times 4 \equiv -12 \pmod{29}$

$2^{14} \equiv (-12)^2 \equiv 144 \equiv -1 \pmod{29}$

$2^{28} \equiv 1 \pmod{29}$

$\Rightarrow$ 2 is a primitive root modulo 29.

(c) We know that. If a is a primitive root of n then a^k is a primitive root of n iff $gcd(k, \phi(n)) = 1$.

$\Rightarrow$ In this case $\phi(29) = 28$

$\Rightarrow$ $K = \{1, 3, 5, 9, 11, 13, 15, 17, 19, 23, 25, 27\}$

So, primitive roots are -

$2^1 \equiv 2$

$2^3 \equiv 8$

$2^5 \equiv 8 \times 4 \equiv 3$,

$2^7 \equiv 3 \times 4 \equiv 12$

$2^9 \equiv 12 \times 4 \equiv 19$

$2^{11} \equiv 3 \times 3 \times 2 \equiv 18$

$2^{13} \equiv 18 \times 4 \equiv 72 \equiv 14$

$2^{15} \equiv 14 \times 4 \equiv 56 \equiv -2 \equiv 27$

$2^{17} \equiv -2 \times 4 \equiv -8 \equiv 21$

$2^{19} \equiv (-8) \times 4 \equiv -3 \equiv 26$

$2^{23} \equiv -3 \times 16 \equiv -48 \equiv 10$

$2^{25} \equiv 10 \times 4 \equiv 40 \equiv 11$

$2^{27} \equiv 11 \times 4 \equiv 44 \equiv 15$

(9) Let $\exists$ integer x_1, y_1 s.t.

$$x_1^2 - 67 y_1^2 = 31$$

$$\Rightarrow x_1^2 = 31 + 67 y_1^2$$

$$\Rightarrow x_1^2 \equiv 31 \pmod{67}$$

$$\Rightarrow \left(\frac{31}{67}\right) = 1$$

$31, 67 \rightarrow$ primes

and $31 \equiv 3 \mod 4$

$67 \equiv 3 \pmod 4$

By Quadratic reciprocity -

$$\left(\frac{31}{67}\right) = -\left(\frac{67}{31}\right) = -\left(\frac{5}{31}\right)$$

$$= -\left(\frac{31}{5}\right) \quad \{ \because 5 \equiv 1 (4) \}$$

$$= -\left(\frac{1}{5}\right) = -1$$

which is a contradiction.

$\Rightarrow$ $X^2 - 67y^2 = 31$ has no integer sol^n.

(10) $12^{100} = 2^{200} \times 3^{100}$

$\Rightarrow$ no primitive roots modulo 12^{100} because it is not of the form $1, 2, 4, p^k$ or p^{2k}. $(2 \neq p$ prime$)$.

(11) (*) Every +ve integer is the sum of 4 squares.

(*) n is +ve integer. Then n can be expressed as sum of 2 squares iff all prime factors of n of the form $4t+3$ have even exponents in the factorization of n.

(*) n can be sum of 3 squares iff n is not of the form $4^r(8t+7)$.

(a) $n = 39470 = 2 \times 5 \times \underbrace{3947}_{\text{prime}}$

$3947 \equiv 3 \ (4)$, $39470 \equiv 6 \ (8)$

Not sum of 2 squares.

Exponent of 3947 is 1 (odd)

n can be sum of 3 squares

(b) $55555 = 5 \times 41 \times 271$

$271 \equiv 3 \ (4)$

Not sum of 2 squares.

$55555 \equiv 3 \ (8)$

can be sum of 3 square.

(c) $121_0 = 2^{10} \times 3^5 \times 5^2 \times 7 \times 11$

$7 \equiv 3 \ (4)$

Not sum of 2 square.

$3^5 \times 5^2 \times 7 \times 11 \equiv 4 \times 3 \times 7$

$\equiv 5 \times 7 \equiv 3 \pmod 8$

can be sum of 3 squares.

(d) b^2+2

$p^2+2 = p^2+1^2+1^2$

can be written as sum of 3 squares.

$p=2$

$\Rightarrow 2^2+2=6$ can't be sum of 2 squares.

Let p be an odd prime.

Case-1:- If $p = 4K+1$

$\Rightarrow p^2+2 = 16K^2+1+8K+2$

$\equiv 3 \pmod 4$

Case-2:- if $p = 4K+3$

$p^2+2 \equiv 3 \pmod 4$

Now suppose that p^2+2 can be written as sum of 2 square and

$$p^2+2 = p_1^{k_1} \cdot p_2^{k_2} \cdots p_r^{k_r}$$

$\Rightarrow$ Either p_i are of the form

$4k+1$ or if there is any prime p_j of the form $4k+3$ then k_j will be an even number.

if $p_i \equiv 1 \pmod 4$ then for every k_i, $p_i^{k_i} \equiv 1 \pmod 4$

and if $p_j \equiv 3 \pmod 4$, then

$$p_j^{k_j} \equiv 1 \pmod 4 \quad k_j \text{ even}$$

$$\equiv 3 \pmod 4 \quad k_j \text{ odd}$$

$\Rightarrow$ If p^2+2 can be written as sum of 2 squares then

$$p^2+2 \equiv 1 \pmod 4$$

which is not true from case ① and case ②.

$\Leftarrow$ p^2+2 can not be written as sum of 2 squares.