(11) $\left(\frac{46}{83}\right)$

$46 = 2 \times 23$

and 83 is a prime.

$$\left(\frac{46}{83}\right) = \left(\frac{2}{83}\right)\left(\frac{23}{83}\right) \quad -(i)$$

$\left[\because \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\right]$

for a prime p. we know

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} \quad -(2)$$

$$\left(\frac{2}{83}\right) = (-1)^{(6889-1)/8}$$

$$= (-1)^{861} = -1 \quad -(3)$$

and by Quadratic reciprocity law -

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{(p-1)(q-1)/4} \quad -(4)$$

$$\therefore \left(\frac{23}{83}\right) = \left(\frac{83}{23}\right)(-1)^{41 \cdot 11}$$

$$= -\left(\frac{83}{23}\right)$$

$$= -\left(\frac{14}{23}\right) \quad \left(\because \left(\frac{m}{p}\right) = \left(\frac{a}{p}\right)\right.$$
where $m \equiv a \bmod p$)

$$= -\left(\frac{2}{23}\right)\left(\frac{7}{23}\right) \quad \left(\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\right) \quad -(5)$$

$$\left(\frac{2}{23}\right) = (-1)^{23^2-1/8} \quad [\text{from } (2)]$$

$$= (-1)^{66} = 1 \quad -(6)$$

$$\left(\frac{7}{23}\right) = \left(\frac{23}{7}\right)(-1)^{\frac{22 \times 11 \times 3}{4}} \quad [\text{from } (4)]$$

$$= -\left(\frac{2}{7}\right)$$

$$= -(-1)^{48/8} \quad [\text{from } (2)]$$

$$= -1 \quad -(7)$$

from (1), (3), (5), (6) & (7), we have

$$\left(\frac{46}{83}\right) = -1$$

② By Euclidean Algorithm-

$$1155 = 182 \times 6 + 63 \quad -①$$

$$182 = 63 \times 2 + 56 \quad -②$$

$$63 = 56 \times 1 + 7 \quad -③$$

$$56 = 7 \times 8$$

Hence, $\gcd(1155, 182) = 7$

from ③

$$7 = 63 - 56 \times 1$$

from ②

$$7 = 63 - (182 - 2 \times 63)$$

$$= 3 \times 63 - 182$$

from ① -

$$7 = 3(1155 - 6 \times 182) - 182$$

$$7 = 3 \times 1155 - 19 \times 182$$

Thus- $x = -19$, $y = 3$.

③ Since $\gcd(m,n) = 1$, $m, n \geq 1$

By Euler's th^m $\Rightarrow \phi(m), \phi(n) \geq 1$

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

&

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

$\Rightarrow$ $n \mid m^{\phi(n)} - 1$, $m \mid n^{\phi(m)} - 1$

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

$\Rightarrow$ $mn \mid (m^{\phi(n)} - 1)(n^{\phi(m)} - 1)$

$\Rightarrow$ $m^{\phi(n)} \cdot n^{\phi(m)} - m^{\phi(n)} - n^{\phi(m)} + 1$

$\equiv 0 \pmod{mn}$

Since $m \mid m^{\phi(n)}$ & $n \mid n^{\phi(m)}$

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

$\Rightarrow$ $mn \mid m^{\phi(n)} \cdot n^{\phi(m)}$

$\Rightarrow$ $-m^{\phi(n)} - n^{\phi(m)} + 1 \equiv 0 \pmod{mn}$

$\Rightarrow$ $m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{mn}$.

(4) $2730 = 2 \times 3 \times 5 \times 7 \times 13$

By Fermat's th^m -

for Every $n \in \mathbb{Z}$

$$n^2 \equiv n \pmod 2$$

$$\Rightarrow n^{13} \equiv n \pmod 2 \quad -(1)$$

$$n^3 \equiv n \pmod 3$$

$$n^{13} \equiv (n^3)^4 \cdot n \equiv n^4 \cdot n \equiv n^3 \cdot n^2$$

$$\equiv n^3 \equiv n \pmod 3 \quad -(2)$$

$$n^5 \equiv n \pmod 5$$

$$\Rightarrow n^{13} \equiv (n^5)^2 \cdot n^3 \equiv n^5 \equiv n \pmod 5 \quad -(3)$$

$$n^7 \equiv n \pmod 7$$

$$\Rightarrow n^{13} \equiv n^7 \cdot n^6 \equiv n^7 \equiv n \pmod 7 \quad -(4)$$

$$n^{13} \equiv n \pmod{13} \quad -(5)$$

Since $\gcd(2,3,5,7,13) = 1$

Hence from (1), (2), (3), (4) & (5), we have

$$n^{13} \equiv n \pmod{2730}$$

Ques-5:- $x \equiv 4 \pmod{91}$

$x \equiv 5 \pmod{31}$

$\because \gcd(91, 31) = 1$, So use Chinese Remainder theorem -

$M = 91 \times 31$

$m_1 = 31$, $m_2 = 91$

$m_1 b_1 \equiv 1 \pmod{91}$

$31 b_1 \equiv 1 \pmod{91}$

$\Rightarrow 31 b_1 - 91 y = 1$

by Euclidean Algorithm -

$91 = 2 \times 31 + 29$

$31 = 1 \times 29 + 2$

$29 = 2 \times 14 + 1$

$1 = 2 \times 1$

$\Rightarrow 1 = 29 - 2 \times 14$

$= 29 - 14(31 - 29)$

$= 15 \times 29 - 14 \times 31$

$$= 15(91 - 2\times 31) - 14\times 31$$

$$= 15\times 91 - 44\times 31$$

$$b_1 \equiv -44 \pmod{91}$$

or $$b_1 \equiv 47 \pmod{91} \quad \text{--- (1)}$$

and $$m_2 b_2 \equiv 1 \pmod{31}$$

$$91 b_2 \equiv 1 \pmod{31}$$

$$-2b_2 \equiv 1 \pmod{31}$$

$$\Rightarrow b_2 \equiv 15 \pmod{31}$$

and $$X \equiv m_1 a_1 b_1 + m_2 a_2 b_2 \pmod{91\times 31}$$

$$X = 31\times 4\times 47 + 91\times 15\times 5$$

$$\equiv 12653 \pmod{91\times 31}$$

□

(6) $$f(X) = x^3 + x^2 - 5 \equiv 0 \pmod{7^j} \quad \text{--- (1)}$$

for $j = 1$

$$f(X) \equiv 0 \pmod{7}$$

$$x^3 + x^2 - 5 \equiv 0 \pmod 7$$

$x = 0$, $f(x) = 0$

$x = 1$, $f(x) = -3$

$x = 2$, $f(x) = 8 + 4 - 5 = 7 \equiv 0 \pmod 7$

$x = 3$, $f(x) = 27 + 9 - 5 = 31$

$x = -3$, $f(x) = -27 + 9 - 5 = -23$

$\equiv -2 \equiv 5 \pmod 7$

$x = -2$, $f(x) = -8 + 4 - 5 \equiv 5 \pmod 7$

$x = -1$, $f(x) = -1 + 1 - 5 \equiv 2 \pmod 7$

$\Rightarrow$ $x = 2$ is the unique soln.

Let $x_1 = 2 + 7t$

then- By Taylor Expansion.

$$f(2+7t) \equiv f(2) + 7t f'(2) \pmod{7^2}$$

$f'(x) = 3x^2 + 2x$, $f(2) = 7$

$f'(2) = 16$

Since $7 \mid f(2)$ and $7 \nmid f'(2)$

$\Rightarrow$ $t f'(2) \equiv \frac{f(2)}{7} \pmod 7$ has a unique soln.

$\Rightarrow$ $16t \equiv 1 \pmod 7$

$\Rightarrow$ $2t \equiv 1 \pmod 7$

$\Rightarrow$ $t = 4 \pmod 7$ $x_1 \equiv 30 \pmod{7^2}$

Let $\exists$ a unique sol^n x_j of (i) for all $j \leq k$, such that $\nmid f'(x_j)$ $\forall$ $j \leq k$

Let $x_{k+1} = x_k + p^k t$

then -

$$f(x_{k+1}) \equiv f(x_k) + p^k t f'(x_k) \pmod{p^{k+1}}$$

Since $p^k \mid f(x_k)$ and $p \nmid f'(x_k)$ [by induction hypothesis]

$\Rightarrow$ $\exists$ a unique $t \pmod p$ s.t.

$$t f'(x) = \frac{f(x_k)}{p^k} \pmod p$$

$\Rightarrow$ $f(x_{k+1}) \equiv 0 \pmod{p^{k+1}}$

Also, $p \nmid f'(x_{k+1})$, hence by Hensel's Lemma, (1) has a unique sol^n $\forall$ $\beta \in \mathbb{N}$.

(8) We know that

$$\left(\frac{c}{p}\right) = \begin{cases} 1 & \text{if } x^2 \equiv c \pmod p \text{ is solvable} \\ -1 & \text{otherwise.} \end{cases}$$

and

$$\left(\frac{c+kp}{p}\right) = \begin{cases} 1 & \text{if } x^2 \equiv c+kp \pmod p \text{ is solvable} \\ -1 & \text{o/w.} \end{cases}$$

but $x^2 \equiv c+kp \equiv c \pmod p$

$\Rightarrow$ $x^2 \equiv c+kp \pmod p$ is solvable iff $x^2 \equiv c \pmod p$ is solvable $\Rightarrow \left(\frac{c}{p}\right) = \left(\frac{c+kp}{p}\right)$. □

(9) $x^2 \equiv 150 \pmod{1009}$ is solvable iff $\left(\frac{150}{1009}\right) = 1$

1009 - prime

$150 = 25 \times 3 \times 2$

$\Rightarrow \left(\frac{150}{1009}\right) = \left(\frac{2}{1009}\right)\left(\frac{3}{1009}\right)\left(\frac{25}{1009}\right)$ — (1)

$\left(\frac{25}{1009}\right) = 1 \qquad [\because 25 = 5^2]$

$\left(\frac{2}{1009}\right) = (-1)^{\frac{1009^2-1}{8}}$

$= (-1)^{128260} = 1$

$\left(\frac{3}{1009}\right) = \left(\frac{1009}{3}\right)(-1)^{\frac{2 \times 1008}{4}} \qquad [QRL]$

$= \left(\frac{1009}{3}\right)$

$= \left(\frac{1}{3}\right) = 1$

from (i) $\left(\frac{150}{1009}\right) = 1$

$\Rightarrow x^2 \equiv 150 \pmod{1009}$ is solvable.

(10) (a) True

$3 \equiv 3 \pmod 7$

$3^2 \equiv 9 \equiv 2 \pmod 7$

$3^3 \equiv 27 \equiv -1 \equiv 6 \pmod 7$

$3^4 \equiv 6 \times 3 \equiv 4 \pmod 7$

$3^5 \equiv 4 \times 3 \equiv 12 \equiv 5 \pmod 7$

$3^6 \equiv 5 \times 3 \equiv 15 \equiv 1 \pmod 7$

$\Rightarrow \{3, 3^2, 3^3, 3^4, 3^5, 3^6\} \equiv$

$\{1, 2, 3, 4, 5, 6\} \pmod 7$ is some order.

$\therefore \{3, 3^2, 3^3, 3^4, 3^5, 3^6\}$ is a reduced residue system $\pmod 7$.

(b) True.

Case-1:- n is odd.

$\gcd(2, n) = 1$

$\Rightarrow \phi(2n) = \phi(2) \cdot \phi(n)$

$= \phi(n)$.

Case-2 :- n is even-

then- $n = 2^k \cdot m$

m is an odd integer.

$$\phi(n) = \phi(2^k) \cdot \phi(m)$$

$$= (2^k - 2^{k-1})\,\phi(m)$$

$$\phi(2n) = \phi(2^{k+1}) \cdot \phi(m)$$

$$= (2^{k+1} - 2^k)\,\phi(m)$$

$$= 2(2^k - 2^{k-1})\,\phi(m)$$

$$= 2\,\phi(n)$$ □.

(C) False.

A set forms complete residue system of 7 if the elements of the set are congruent to $\{0,1,2,3,4,5,6\}$ modulo 7 in

some order.

⇒ A complete residue system of 7 contains exactly 7 numbers but we have $\{-13, -9, -1, 9, 18, 21\}$ only 6 numbers. So, This set can never form a complete residue system modulo 7.

(7) $\left(\frac{1}{13}\right) = 1$ — QR

$\left(\frac{2}{13}\right) \equiv 2^{(13-1)/2} \equiv 2^6 \equiv 64 \equiv -1$

NR $\pmod{13}$

$\left(\frac{3}{13}\right) \equiv 3^6 \equiv 27 \times 27 \equiv 1 \pmod{13}$

QR

$\left(\frac{4}{13}\right) \equiv 1$ QR $[\because 4 = 2^2]$

$\left(\frac{5}{13}\right) \equiv 5^6 \equiv (25)^3 \equiv (-1)^3 \equiv -1 \pmod{13}$

NR

$\left(\frac{6}{13}\right) = \left(\frac{2}{13}\right)\left(\frac{3}{13}\right) = -1$ NR. $\left[\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\right.$

$\left(\frac{7}{13}\right) \equiv 7^6 \equiv (49)^3 \equiv (10)^3 \equiv 100 \times 10 \equiv 9 \times 10$

$\equiv 90 \equiv -1 \pmod{13}$

NR

$\left(\frac{8}{13}\right) \equiv 8^6 \equiv 2^{12} \cdot 2^6 \equiv -1 \pmod{13}$

NR

$\left(\frac{9}{13}\right) = 1$ QR $\left[\because 9 = 3^2\right]$

$\left(\frac{10}{13}\right) = \left(\frac{2}{13}\right)\left(\frac{5}{13}\right) = 1$ QR

$\left(\frac{11}{13}\right) \equiv (11)^6 \equiv (-2)^6 \equiv 2^6 \equiv -1 \pmod{13}$

NR.

$\left(\frac{12}{13}\right) \equiv (12)^6 \equiv (-1)^6 \equiv 1 \pmod{13}$ QR.

QR- 1, 3, 4, 9, 10, 12.