Assignment 2

Q1) Show that $n^7 - n$ is divisible by 42 for every natural number.

Ans) $f(n) = n^7 - n$
$= n(n^6 - 1)$
$= n(n-1)(n^5 + n^4 + n^3 + n^2 + n + 1)$
$= n(n-1)(n+1)(n^4 + n^2 + 1)$

* To show that $42 | n^7 - n$, it is enough to show that
① $2 | n^7 - n$
② $3 | n^7 - n$ as $42 = 2 \times 3 \times 7$
③ $7 | n^7 - n$

→ ① Claim: $2 | (n-1)n \quad \forall n \in N$
Proof: If $n \equiv 0 \pmod 2 \Rightarrow 2 | n$
$n \equiv 1 \pmod 2 \Rightarrow 2 | (n-1)$
$\therefore 2 | (n-1)n \ \forall n \in N$
$\Rightarrow 2 | n^7 - n \ \forall n \in N$ as $n^7 - n = n(n-1)(n+1)(n^4 - n^2 + 1)$

→ ② Claim: $3 | (n-1)n(n+1) \ \forall n \in N$
Proof: If $n \equiv 0 \pmod 3 \Rightarrow 3 | n$
$n \equiv 1 \pmod 3 \Rightarrow 3 | (n-1)$
$n \equiv 2 \pmod 3 \Rightarrow 3 | (n+1)$
$\therefore 3 | (n-1)n(n+1) \ \forall n \in N$
$\Rightarrow 3 | n^7 - n \ \forall n \in N$

→ ③ Claim: $7 | n^7 - n$
Proof: As 7 is prime, using Fermat's Little Theorem, $a^p \equiv a \pmod p$
$\Rightarrow n^7 \equiv n \pmod 7$
$\Rightarrow (n^7 - n) \equiv 0 \pmod 7$
$\Rightarrow 7 | (n^7 - n) \ \forall n \in N$

$\therefore 42 | (n^7 - n) \ \forall n \in N$

Q2) Show that if $\gcd(m,n)=1$, then $m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{mn}$

Ans) • Since $\gcd(m,n)=1$, to show that

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

it is enough to show that

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

and

$$m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{n} \quad — ②$$

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

$\Rightarrow m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{m}$ (By Euler's Theorem)

$\rightarrow$ ② $(m^{\phi(n)} + n^{\phi(m)}) \pmod{n} \equiv m^{\phi(n)} \pmod{n}$

$\Rightarrow m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{n}$ (By Euler's Theorem)

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

H.P.

Q3) Solve the simultaneous congruences

$x \equiv 3 \pmod{6}$,
$x \equiv 5 \pmod{10}$,
$x \equiv 1 \pmod{17}$

Ans) ~~Using CRT~~

* $x \equiv 3 \pmod{6}$
  $x \equiv 5 \pmod{10}$

$\Rightarrow x = 6y_1 + 3 = 10y_2 + 5$

$\Rightarrow 6y_1 - 10y_2 = 2$

$\Rightarrow 3y_1 - 5y_2 = 1$

$\Rightarrow (y_1, y_2) = (2+5k, 1+3k)$

$\Rightarrow x = 6(2+5k)+3 = 10(1+3k)+5$

$x = 30k + 15$

$\therefore x \equiv 15 \pmod{30}$

* $x \equiv 15 \pmod{30}$
  & $x \equiv 1 \pmod{17}$

Since $\gcd(17,30)=1$, By CRT.

$x \equiv 375 \pmod{30 \times 17}$

$x \equiv 375 \pmod{510}$

($30y_1 + 15 = 17y_2 + 1$
$\Rightarrow (y_1, y_2) = (4, 7) \cdot (-14) = (-56, -98)$)

$\therefore x \equiv 375 \pmod{510}$ satisfies $x \equiv 3 \pmod{6}$, $x \equiv 5 \pmod{10}$, $x \equiv 1 \pmod{17}$

Q4) Find all $x \in \mathbb{Z}_{35}$ s.t. $(x-1)(x-2)=0$

Ans) → By the CRT, we need to solve for

$$(x-1)(x-2) \equiv 0 \pmod 7$$

and $(x-1)(x-2) \equiv 0 \pmod 5$

→ ⇒ $x = 1, 2 \pmod 7$ and $x = 1, 2 \pmod 5$ by Lagrange's Th^n

→ By the CRT, each congruence relation would have a unique sol^n modulo $(5 \times 7 = 35)$

⇒ $x \equiv 1 \pmod 7$ & $x \equiv 1 \pmod 5$ ⇒ $x \equiv 1 \pmod{35}$

→ $x \equiv 1 \pmod 7$ & $x \equiv 2 \pmod 5$ ⇒ $x \equiv 22 \pmod{35}$

→ $x \equiv 2 \pmod 7$ & $x \equiv 1 \pmod 5$ ⇒ $x \equiv 16 \pmod{35}$

→ $x \equiv 2 \pmod 7$ & $x \equiv 2 \pmod 5$ ⇒ $x \equiv 2 \pmod{35}$

∴ $\boxed{x \equiv 1, 2, 16, 22}$ are the only sol^n in $\mathbb{Z}_{35}$

Q5) Find all $x \in \mathbb{Z}_{29}$ such that $x^{11} = 2$.

Ans) → We need to solve $x^{11} \equiv 2 \pmod{29}$

→ By Fermat's Little Theorem,

$$x^{29} \equiv x \pmod{29}$$

→ Hence we try to find k s.t.

$(x^{11})^k \equiv 2^k \pmod{29}$ and $11k \equiv 29 \pmod{28}$ → $k-1$

⇒ $11k \equiv 1 \pmod{28}$

∴ $11k \equiv 1 \pmod{28}$

⇒ $11k = 28y + 1$

⇒ $(k, y) = (23, 9)$ is a sol^n.

⇒ $k = 23$.

→ ∴ $(x^{11})^{23} \equiv 2^{23} \pmod{29}$

⇒ $x \equiv 2^{23} \pmod{29}$

⇒ $\underline{x \equiv 10 \pmod{29}}$ $(2^1 \to 2, 2^2 \to 4, 2^4 \to 16, 2^8 \to 24, 2^{16} \to 25)$

$\therefore 2^{23} = 2^{16} \times 2^4 \times 2^2 \times 2^1 = 10 \pmod{29}$.

Q4) Find the number of pairs $(x,y) \in \mathbb{Z}_p^2$ s.t. $x^2 - y^2 = 1$

Ans) → For $p = 2$, we can easily see that $(0,1)$ & $(1,0)$ are the only solutions i.e. no. of sol^n = 2

→ For $p \neq 2$, consider any $a \in \mathbb{Z}_p - \{0\}$

* Since p is prime, every a will have a unique inverse b s.t. $ab \equiv 1 \pmod{p}$

* Now let $x \equiv (a+b) \times 2^{-1} \pmod{p}$ and $y \equiv (a-b) \times 2^{-1} \pmod{p}$

$$\Rightarrow (x+y)(x-y) = x^2 - y^2$$
$$= \left(2^{-1}(a+b) + (a-b)\right)\left(2^{-1}(a+b) - (a-b)\right)$$
$$= (2^{-1} \cdot 2(a)) \times (2^{-1} \cdot 2(b))$$
$$= ab$$
$$= 1$$

* ∴ for each $a \in \mathbb{Z}_p$ we get one pair

$\boxed{\therefore \text{ Total number of sol}^n = p - 1}$