HW-2

1) x^2-1 in $\mathbb{Z}_n$, $n = 17\times 19 = 323$

in $\mathbb{Z}_{17}$, $x^2-1=0$

$\Rightarrow x = \pm 1 \Rightarrow x = 1, 16$ — ①

in $\mathbb{Z}_{19}$, $x^2-1=0 \Rightarrow x = \pm 1$

$\Rightarrow x = 1, 18$ — ②

In $\mathbb{Z}_{17\times 19}$, $x^2-1=0 \Rightarrow x = \pm 1$

$\Rightarrow x = 1, 322$

Also, from ① & ②,

on solving $x = 1 \,\%\, 17$

& $x = 18 \,\%\, 19$

we get $x = 18 \,\%\, 323$

$\Rightarrow x = 18, 305$

Since the eqn can have atmost 4 roots,

$\therefore$ $\boxed{x = 1, 18, 305, 322}$

2) $x^7 = 2$ in $\mathbb{Z}_{41}$ — ①

$x^{40} = 1$ — ②

$\Rightarrow x^{35} = 2^5 = 32$ — ③

$\Rightarrow x^5 = 2^{-5} = 9$ — ④ (from ②, ③)

$\Rightarrow x^2 = 2\times 9^{-1} = 23$ — ⑤ (from ①, ④)

$\Rightarrow x^6 = 23^3 = 31$ — ⑥

$\Rightarrow x = 2\times 31^{-1}$ (from ①, ⑥)

$\Rightarrow \boxed{x = 8}$

3) $p \to$ odd prime, $d \mid p-1$

$A = \{a \in \mathbb{Z}_p : a^d = 1\}$

$B = \{a^{(p-1)/d} : a \in \mathbb{Z}_p^*\}$

0 can not be a part of A, since $0^d = 0$.

Now, $x^{p-1} = 1 \Rightarrow (x^d)^{\frac{p-1}{d}} = 1$

$\Rightarrow (x^{\frac{p-1}{d}})^d = 1$

$\Rightarrow$ The elements of A are of the form $a^{\frac{p-1}{d}}$, $a \neq 0 \Rightarrow a \in \mathbb{Z}_p^*$. $\therefore \boxed{A \in B}$

In B, for any element $x = a^{p-1/d}$,

$x^d = a^{p-1} = 1$.

$\Rightarrow \boxed{B \in A}$

Since, $A \in B$ & $B \in A$

$\Rightarrow \boxed{A = B}$

4) a) $S = \{0 \leq K \leq n-1 : dK \equiv 0 \% n\}$

$dK \equiv 0 \% n$

$\Rightarrow n \mid dK$

$\Rightarrow \gcd(n, dK) = 0$

$$\Rightarrow \gcd\left(\frac{n}{\gcd(n,d)}, \frac{dk}{\gcd(n,d)}\right) = \frac{n}{\gcd(n,d)}$$

since $\frac{n}{\gcd(n,d)}$ & $\frac{d}{\gcd(n,d)}$ are coprime,

$$\gcd\left(\frac{n}{\gcd(n,d)}, k\right) = \frac{n}{\gcd(n,d)}$$

$\Rightarrow$ k is a multiple of $\frac{n}{\gcd(n,d)}$, $k \in \{0, 1, \dots, n-1\}$

$$\Rightarrow \# k = n / \left(n / \gcd(n,d)\right)$$
$$= \gcd(n,d)$$

$$\therefore |\{0 \leq k \leq n-1 : dk \equiv 0 \% n\}| = \gcd(n,d)$$

b) Consider $\gcd(x^d - 1, x^{p-1} - 1)$.

$$\gcd(x^d - 1, x^{p-1} - 1) = x^{\gcd(d, p-1)} - 1$$

$$\Rightarrow x^{p-1} - 1 = (x^{\gcd(d,p-1)} - 1) f(x)$$

x^{p-1} has $p-1$ roots, & $\gcd(d, p-1) \mid p-1$.

$\therefore$ $x^{\gcd(d,p-1)}$ has $\gcd(d, p-1)$ roots.

Now, $x^d - 1 = (x^{\gcd(d,p-1)} - 1) g(x)$

since $g(x)$ has no common factor with $x^{p-1} - 1$, it has no sol^n.

$\Rightarrow$ $x^d - 1$ has $\gcd(d, p-1)$ roots.

5) $x^2 - 4$ in $\mathbb{Z}_{343}$

In $\mathbb{Z}_7$,

$$x^2 - 4 = 0 \Rightarrow x = 2, 5$$

$\Rightarrow x = 7K + 5$

$\Rightarrow (7K+5)^2 = 4 \ \% \ 49$

$\Rightarrow 49K^2 + 70K + 25 = 4 \ \% \ 49$

$\Rightarrow 10k + 3 = 0 \ \% \ 7$

$\Rightarrow 10k + 3 = 7p$

$\Rightarrow K = -1, \ p = -1$

$\therefore x = -2 = 47$

other root $= 49 - 47 = 2$

$\Rightarrow$ On solving $x = 47 \ \% \ 49$

$x = 5 \ \% \ 7$

$\Rightarrow 47 + 49p = 5 + 7q$

$\Rightarrow 42 + 49p = 7q$

$\Rightarrow 6 + 7p = q$

$\Rightarrow p = -1, \ q = -1$

$\Rightarrow x = -2 \ \% \ 343$

$\Rightarrow \boxed{x = 2, 341}$