Theory Assignment 2

Aayush Patel
CS20BTECH11001

1. $x^2 - 1 \equiv 0 \bmod n \qquad n = 17 \times 19$

$\downarrow$

$(x^2-1) \equiv 0 \bmod 17$ AND $(x^2-1) \equiv 0 \bmod 19$

$x = +1, -1$ in Z_{17} $\qquad$ $x = +1, -1$ in Z_{19}

$x = 17d_1 + 1, 17d_1 - 1 \quad \forall d_1 \in Z$ $\qquad$ $x = 19d_2 + 1, 19d_2 - 1 \quad \forall d_2 \in Z$

I] $x = 17d_1 + 1$ & $x = 19d_2 + 1$

$x \equiv 1 \bmod 17$ & $x = 1 \bmod 19$

Using CRT, there is a unique solution in $Z_{19 \times 17}$

$\boxed{x = 1}$

Similarly for other 3 cases.

II] & $x \equiv +1 \bmod 17$ & $x \equiv -1 \bmod 19 \implies \boxed{x = 19*17 - 1}$

III] $x \equiv 1 \bmod 17$ & $x \equiv +1 \bmod 19$

$x - 1 = 17d_1, \quad x + 1 = 19d_2 \implies 2 = 19d_2 - 17d_1$

$d_2 = 1, \quad d_1 = 1$

~~$x = 18$~~ $\qquad$ $\boxed{x = 17d_1 + 1 = 18}$

IV] $x \equiv +1 \bmod 17$ & $x \equiv 1 \bmod 19$

$x + 1 = 17d_1$ & $x - 1 = 19d_2 \implies 17d_1 - 19d_2 = 2$

$d_1 = -1, \quad d_2 < -1$

$\boxed{x = 17d_1 - 1 = -18 = 19*17 - 18}$

$\therefore \boxed{x = 1, 18, 19*17-18, 19*17-1}$

classmate ~~x~~ 1, 18, 305, 324

DATE

2. $x^7 \equiv 2 \pmod{41}$

By Fermat's Little Theorem, $x^{40} \equiv 1 \pmod{41} \quad \forall \ 41 \nmid x$

$x^7 \equiv 2 \implies x^{42} \equiv 2^6 \quad \longleftarrow (1)$

$x^{40} \equiv 1$

$\Downarrow$

$x^2 \equiv 2^6$

$x \equiv \pm 2^3 \implies x \equiv \pm 8$

But $\gcd(p-1, d) = \gcd(40, 7) = 1$

There is either 0 or 1 solution

→ For $x \equiv -8$, $(-8)^7 = -(64)^3\, 8$

$= -(23)^3\, 8$

$= -(529)(194)$

$= -(119)(20)$

$\equiv -80$

$\equiv 2$

→ For $x \equiv +8$, $8^7 \equiv 80 \equiv -2 \not\equiv +2$

$\therefore x \equiv 8$ is an invalid solution (Extra solution added due to (1))

$\therefore$ $x \equiv -8$ only for

$x \equiv -8 \equiv 33$ only solution in $\mathbb{Z}_{41}$

DATE

3. $A = \{ a \in \mathbb{Z}_p : a^d = 1 \}$ To prove: $A = B$

$B = \{ a^{\frac{p-1}{2}} : a \in \mathbb{Z}_p^* \}$

I] To prove: $B \subseteq A$

Consider $x \in B$, $x = a^{\frac{p-1}{2}}$ for some $a \in \mathbb{Z}_p^*$

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

$x^d = 1$ (By Fermat's Little Theorem, also $p \nmid a$ since $a \in \mathbb{Z}_p^*$)

$\therefore x \in A$

$x \in B \longrightarrow x \in A \Rightarrow B \subseteq A$

q & 4

(4)

DATE

II) $A \subseteq B$

Say we have $a \in A$, i.e. $a^d = 1$, $a \in \mathbb{Z}_p$

To prove: $\exists\, x \in \mathbb{Z}_p^*$ s.t. $a = x^{\frac{p-1}{d}}$

$x^{\frac{p-1}{d}} = a$ has soln $\iff a^{\left(\frac{p-1}{\frac{p-1}{d}}\right)} = 1$

$a^{\left(\frac{p-1}{\frac{p-1}{d}}\right)} = a^d = 1$

$\therefore x^{\frac{p-1}{d}}$ has a soln.

$\therefore A \subseteq B$

$\therefore A \subseteq B$ & $B \subseteq A \longrightarrow A = B$

∴ $|B| = |A|$ & $B \subseteq A$ ⟶ $A = B$

4(a) $d \in [1, 2, \ldots n]$

$S = \{x \mid dx \equiv 0 \bmod n\}$

$dx = dn$

$x = \frac{dn}{d}$ for $d \in [1, n]$ & $x \in [0, n-1]$

$\Rightarrow 0 \leq \frac{dn}{d} \leq (n-1)$

$0 \leq d \leq \frac{d(n-1)}{n} \Rightarrow \boxed{0 \leq d \leq d-1}$

$x = d\left(\frac{n}{d}\right) = d\left[\frac{\frac{n}{\gcd(n,d)}}{\frac{d}{\gcd(n,d)}}\right]$

$\because \frac{n}{\gcd(n,d)}$ & $\frac{d}{\gcd(n,d)}$ are coprimes,

possible values of d : $\{0, \frac{d}{\gcd(n,d)}, \frac{2d}{\gcd(n,d)} \ldots\ldots (\gcd(n,d)-1)\frac{d}{\gcd(n,d)}\}$

i.e. multiples of $\frac{d}{\gcd(n,d)} < d$

DATE

Possible values of $x = S$

$$\left\{0, \frac{n}{\gcd(n,d)}, \frac{2n}{\gcd(n,d)} \cdots\cdots \frac{(\gcd(n,d)-1)n}{\gcd(n,d)}\right\}$$

$$\therefore |S| = \gcd(n,d)$$

(b) Let a be the primitive root of Z_p

$Z_p^* = \{1, a, a^2 \cdots a^{p-2}\}$

q ∧ Z_p^* $x^d = 1$, Let $x = a^k \Rightarrow a^{dk} \equiv 1 \bmod p = a^0 \bmod p$

∵ a is a primitive root, this eqn is same as $\boxed{dk \equiv 0 \bmod p-1}$

Number of values of k in Z_p = number of solutions of $x^d = 1$ = gcd(d, p-1) (from (a))

5. $x^2 \equiv 4 \bmod 7^3 \Rightarrow x^2 \equiv 4 \bmod 7^2 \Rightarrow x^2 \equiv 4 \bmod 7 \Rightarrow$

$x = 7k \pm 2$

$\Rightarrow$ ~~$(7k+2)^2 \equiv 4 \bmod 7^3$~~ $(7k+2)^2 \equiv 4 \bmod 7^2$ | $(7k-2)^2 \equiv 4 \bmod 7^2$

~~$49k^2 + 28 \equiv 0 \bmod 7^3$~~ $28k \equiv 0 \bmod 7^2$ | $-28k \equiv 0 \bmod 7^2$

$k \equiv 0 \bmod 7$ | $k \equiv 0 \bmod 7$

$\Rightarrow$ Solution to $x^2 \equiv 4 \bmod 7^2 \Rightarrow x = 7k \pm 2, \ \forall k \equiv 0 \bmod 7$

$= 49d \pm 2, \ \forall d \in Z$

$\Rightarrow$ $(7k+2)^2 \equiv 4 \bmod 7^3$ | $(7k-2)^2 \equiv 4 \bmod 7^3$

$7^2k^2 + 28k \equiv 0 \bmod 7^3$ | $7^2k^2 - 28k \equiv 0 \bmod 7^3$

$0 + 28 \times 7d \equiv 0 \bmod 7^3 \quad (k = 7d)$ | $-28 \times 7d \equiv 0 \bmod 7^3$

$d \equiv 0 \bmod 7$ | $d \equiv 0 \bmod 7$

$\Rightarrow$ Solution to $x^2 \equiv 4 \bmod 7^3 \Rightarrow 7^3d \pm 2 \Rightarrow \{\pm 2, $ PAGE B41 $\square$