Computational Number Theory

HW 2

Ahmik Virani
ES22BTECH11001

Q1) (a) $x^2 = 5$ in $\mathbb{Z}_{103}$

No solution

- $5^{\frac{103-1}{2}} = 5^{51} = -1$ in $\mathbb{Z}_{103} \Rightarrow$ ~~soln exists~~

- ~~$102 = 2^1 \times 51 \Rightarrow l = 1, m = 51$~~

- ~~$b = 5^{51} = 1 \Rightarrow$ To solve $y^2 = 1$~~

~~$\Rightarrow y = \pm 1$~~

~~Solution to $x = \pm \frac{5^{\frac{52}{2}}}{1} = \pm 5^{26} = \pm 1$~~

~~$x = 1$ and $x = 102$~~

(b) $x^2 = 2$ in $\mathbb{Z}_{103}$

- $2^{51} = 1 \Rightarrow$ solution exists in $\mathbb{Z}_{103}$

$\therefore$ $102 = 2^1 \times 51 \Rightarrow l = 1, m = 51$

- $b = 2^{51} = 1 \Rightarrow$ To solve $y^2 = 1$

$\Rightarrow y = \pm 1$

$\therefore$ Solution to $x = \pm \frac{2^{\frac{52}{2}}}{1} = \pm 2^{26} = \pm 38$

$\therefore$ $x = 38$ and $x = 65$

(c) $x^2 = 6$ in $\mathbb{Z}_{101}$

- $6^{50} = 1 \Rightarrow$ solution exists in $\mathbb{Z}_{101}$

- $100 = 2^2 \cdot 25 \Rightarrow l = 2, m = 25$

- $b = 6^{25} = 100$

$\Rightarrow$ solve $y^2 = 100$

$\Rightarrow y = \pm 10$

Solution to $x = \pm \frac{6^{13}}{10}$, $6^{13} = 14$, $10^{-1} = 91$

$\Rightarrow x = \pm 14 \times 91 = \pm 62$

$\therefore x = 62$ and $x = 39$

Q2) (a) $A = \{(x,y) \in \mathbb{Z}_p^2 : x+y = 1\}$

Let us fix $x = r$ where $r \in \{0, 1, \dots p-1\}$

$\therefore$ In $\mathbb{Z}_p$, $y = 1 - r$ has a unique solution (it will be a value $= 1-r$)

$\Rightarrow$ for each x we have unique y

$\Rightarrow$ Size of A , $|A| = p$

(b) $B = \{(x,y) \in \mathbb{Z}_p^2 : xy = 1\}$

Fix $x = r$ as above $\Rightarrow$ $ry = 1$ $\Rightarrow$ $y = 1 \cdot r^{-1}$

since $r \in \mathbb{Z}_p$, r^{-1} exists and is unique ~~(exists in pairs as seen in class)~~

since $\gcd(r,p) = 1$

except $r = 0$ $\leftarrow$ has no solution

$\Rightarrow$ Size of B, $|B| = p-1$

(c) $C = \{(x,y) \in \mathbb{Z}_p^2 : x^2 - y^2 = 1\}$

Write this as $(x-y)(x+y) = 1$

let $a = x - y$ and $b = x + y$

$\Rightarrow$ $x = \frac{a+b}{2}$, $y = \frac{b-a}{2}$ (we know 2^{-1} exists because p is odd prime)

This forms a bijection, $\therefore$ # of (x,y) = # of (u,v)

from part (b), We know it is $p-1$

$\therefore$ $|C| = p-1$

Proof of bijection: Say (x_1, y_1) and (x_2, y_2) map to (a,b)

$\Rightarrow x_1 - y_1 = x_2 - y_2$ and $x_1 + y_1 = x_2 + y_2$

① Adding both: $2x_1 = 2x_2$

but p is an odd prime, $\therefore$ divide by 2

$x_1 = x_2$

② Subtracting: $2y_1 = 2y_2$

divide by 2 as p is odd

$y_1 = y_2$

$\therefore$ $(x_1, y_1) = (x_2, y_2)$

Q3) $dk = (p-1)$. $a \in \mathbb{Z}_p$, then $x^d = a$ has Solution $\Leftrightarrow$ $a^k = 1$

(1) If ~~$dk = p-1$~~ $x^d = a$

raise both sides by power of k

$\Rightarrow (x^d)^k = a^k$

$\Rightarrow x^{dk} = a^k$

$\Rightarrow x^{p-1} = a^k$

$\Rightarrow a^k = 1$ (Fermat's little theorm)

$x^d = a \Rightarrow a^k = 1$

(2) $a^k = 1$

We know $x^{p-1} = 1$

$\Rightarrow x^{dk} = a^k$

$\Rightarrow x^{dk} - a^k = 0$

But $(x^d - a)$ is a factor of $x^{dk} - a^k$

$$x^{dk} - a^k = (x^d - a)(x^{dk-d} + a x^{dk-2d} + a^2 x^{dk-3d} + \cdots + a^{k-1} x^{dk-kd})$$

But $x^{dk} - a^k = x^{p-1} - 1$

~~St~~ We know that $x^{p-1} - 1$ has $(p-1)$ roots

$\therefore$ ~~By~~ Following the fact that if $f(x)$ has $\deg(f)$ roots and $g(x) | f(x)$ then $g(x)$ has $\deg(g)$ roots

Here $(x^d - a) | (x^{p-1} - 1) \Rightarrow x^d - a$ has $\deg(x^d - a) = d$ roots

$\Rightarrow x^d = a$ has a solution

□