Computational Number Theory : CS5610

Q2) Let $k = \text{ord}(a)$

$\Rightarrow$ k is the least power such that $a^k = e$

Let $d = qk + r$ ~~and~~ $r < k$

$\Rightarrow$ $a^d = a^{qk} \cdot a^r$

but $a^{qk} = e$ $\Rightarrow$ $a^d = a^r$

but by definition of order, if $r < k$ and $a^r = e$

then $r = 0$

$\therefore$ $d = qk$ or $k \mid d$ i.e. $\text{ord}(a) \mid d$

Q4) We have $f(x)(2x+1) \equiv 1 \mod (x^2+1)$

We basically need $(2x+1)^{-1} \mod (x^2+1)$

Let us write ~~$g(x)(x^2+1)$~~

$$f(x)(2x+1) - g(x)(x^2+1) \equiv 1$$

a	b	q	-g	f	u	v
x^2+1	$2x+1$	$4x+5$	1	0	0	1
$2x+1$	3	$3x+5$	0	1	1	$-4x-5$
3	0	-	1	$-4x-5$		

$\Rightarrow$ $g(x) = -1$ $\quad f(x) = -4x-5 = 3x+2$

but this is solution for $f(x)(2x+1) - g(x)(x^2+1) = 3$

$\therefore$ Multiply $3^{-1} = 5$ $\rightarrow f(x) = x+3$

$\therefore$ $f(x) = x+3$

Q6) $x^2 = 3 \mod p$ has a solution if $\left(\frac{3}{p}\right) = 1$

Case 1 | Case 2

Case 1: $p = 1 \mod 4$

$\hookrightarrow \left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$

(i) $p \mod 3 = 0$ Not possible since p is prime

(ii) $p \mod 3 = 1$ ok

(iii) $p \mod 3 = 2$ No since $\left(\frac{2}{3}\right) = -1$

$\therefore p = 1 \mod 4$ and $p = 1 \mod 3$

$\Downarrow$ $\Downarrow$

$p = 4x+1 = 3y+1$

$\Rightarrow 4x = 3y$

$x = 3k,\ y = 4k$

$\Rightarrow p = 4(3k)+1 = 12k+1$

i.e. $p \equiv 1 \mod 12$

Case 2: $p = 3 \mod 4$

$\Rightarrow -\left(\frac{p}{3}\right) = \left(\frac{3}{p}\right)$

Illy here only

$p \mod 3 = 2$ would word

$\Rightarrow p \equiv 3 \mod 4$ and $p \equiv 2 \mod 3$

$\Rightarrow p = 4x+3 = 3y+2$

$\Rightarrow \cancel{4x-3} \cancel{3y-4y} \ 3y - 4x = 1$

$(x,y) = (-1,-1)$ satisfies

general : $(-1-3k, -1-4k)$

$\therefore p = 4(-3k-1)+3$

$= -12k-1$

$\Rightarrow p \equiv -1 \mod 12$

$\therefore p \equiv \pm 1 \mod 12$

Q7) $\mathbb{Z}_{15} \cong \mathbb{Z}_3 \times \mathbb{Z}_5$

$\therefore$ We find solutions in $\mathbb{Z}_3$ and $\mathbb{Z}_5$ seperately and multiply

\# Solutions in $\mathbb{Z}_3$ ~~can~~ $\in \{0,1,2,3\}$

\# Solutions in $\mathbb{Z}_5$ $\in \{0,1,2,3,5\}$ (5 because if $f(x) \mod 5 \equiv 0$)

$\therefore$ We have $d = \{0,1,2,3,4,5,6,9,10,15\}$