(1) If in a Group G there is an element a of order 360; what is the order of a^{220}? Show that If G is cyclic group of order n and m divids n, then G has a subgroup of order m. (10)

Sol- we know that for a group G

$$o(a^n) = \frac{o(a)}{(o(a), n)} \quad \forall a \in G$$

Given $o(a) = 360$

$$\therefore o(a^{220}) = \frac{360}{(360, 220)}$$

$$= \frac{360}{20}$$

$$\Rightarrow o(a^{220}) = 18$$

let G is a cyclic group generated by a of order n.

$$\therefore G = \langle a \rangle$$

$$a^n = e$$

let m divids n $\Rightarrow$ $n = mk$

we claim that

$H = \langle a^k \rangle$ is a subgroup of order m.

$\because$ H is cyclic group generated by a^k

hence it's a subgroup of G.

we have to show $o(H) = m$

i.e. $o(a^k) = m$

now $(a^k)^m$

$= a^{km}$

$= a^n = e$ $\because$ as $o(a) = n$

suppose now,

$(a^k)^t = e$

$\Rightarrow a^{kt} = e$

$\Rightarrow o(a) \mid kt$

$\Rightarrow n \mid kt$

$\Rightarrow mk \mid kt$

$\Rightarrow m \mid t$

$\therefore$ m is the least + integer for which

$(a^k)^m = e$

$\therefore o(a^k) = m$

$\therefore$ Hence H is subgroup having order m.

Q-2] a] If p is a prime no. and e a positive integer what are the elements 'a' in the ring $\mathbb{Z}_{p^e}$ of integers modulo p^e $\ni$ $a^2 = a$?
Hence determine the elements in $\mathbb{Z}_{35}$ $\ni$ $a^2 = a$. (14)

Sol^n:- we know that

$$\frac{\mathbb{Z}}{\langle p^e \rangle} \cong \mathbb{Z}_{p^e}$$

Let $p^e = n$

$\therefore$ consider $\langle n \rangle + m$ be an idempotent element of $\frac{\mathbb{Z}}{\langle n \rangle}$

then $(\langle n \rangle + m)^2 = \langle n \rangle + m$

$\Rightarrow \langle n \rangle + m^2 = \langle n \rangle + m$

$\Rightarrow m^2 - m \in \langle n \rangle$

$\Rightarrow n \mid m^2 - m$

$\Rightarrow n \mid m(m-1)$

$\Rightarrow p^e \mid m(m-1)$

$\because (m, m-1) = 1$

$\Rightarrow p^e \mid m$ or $p^e \mid m-1$

if $n = p^e \mid m$ then $m = rn$.

$\Rightarrow \langle m \rangle + \langle n \rangle = \langle rn \rangle + \langle n \rangle = \langle n \rangle$

if $n = p^e \mid (m-1)$

then $m-1 = nk$.

$\Rightarrow \langle n \rangle + m$

$= \langle n \rangle + nk + 1$

$= \langle n \rangle + 1$

$\therefore$ zero and unity are the only idempotents of $\frac{Z}{\langle n \rangle}$

$\therefore \bar{0}, \bar{1}$ are idempotent of Z_{p^e}.

in Z_{35}

$\bar{0}$ and $\bar{1}$ are idempotent

$= \bar{0} \cdot \bar{0} = 0$

$\bar{1} \cdot \bar{1} = \bar{1}$

now in Z_{35} —— $\{35 = 5 \times 7$

$35 = 5 \times 7$

$(5, 7) = 1$

$\therefore$ any solⁿ to the

$x \equiv 1 \bmod (5)$ and $x \equiv 0 \pmod 7$

Possible choices	6	0
	11	7
	16	14
	21	21
	26	28
	31	
	1	
	~~0~~	

taking common solⁿ we find $\overline{21}$ is idempotent if we revers this process

i.e $x \equiv 1 \bmod 7$ and $x \equiv 0 \bmod 5$

8	0
15	5
22	10
29	15
1	20
	25
	30

we find $\overline{15}$ is idempotent element

$\therefore$ $\overline{0}, \overline{1}, \overline{15}$ and $\overline{21}$ are idempotent element

Q-3] a] What is the maximum possible order of a permutation in S_8 the group of the eight numbers $\{1, 2, 3, \cdots 8\}$? Justify your answer. (Majority of marks will be given for the justification). (13)

Soln:- Let $f \in S_8$ $\therefore$ it can be expressed as $f = C_1 C_2, \cdots C_K$ where C_i are disjoint cycle of length $n_1, n_2, \cdots n_K$ respectively. If $n_1 + n_2 + \cdots + n_K = n$ then $\{n_1, n_2, \cdots n_K\}$ is called cyclic decomposition of f.

and the order of a permutation of a finite set written in disjoint cycle form is the least common multiple of the length of the cycle.

	possible cyclic decomposition of 8 (C.D.)	max. order / Max order
1]	1 1 1 1 1 1 1 1	1
2]	2 11 11 11	2
3]	3 1 11 11	3
4]	4 11 11	4
5]	5 11 1	5
6]	6 11	6
7)	7 1	7
8]	8	8
9]	2 2 11 11	2
10]	2 2 2 11	2
11]	2 2 2 2	2

Date /

	C.D	Max. order
10)	3 2 1 1 1	6
11)	3 2 2 1	6
12)	3 3 1 1	3
13)	3 3 2	6
14)	4 2 1 1	4
15)	4 2 2	4
16)	4 3 1	12
17)	4 4	4
18)	5 2 1	10
19)	5 3	15
20)	6 2	6

{wrong number}

there the maximum possible order is 15 whose cyclic decomposition is {5 3}

eg:- (1 3 2 4 6) (7 8 5)