Soham Chatterjee
Email: sohamc@cmi.ac.in
Course: Algebra and Computation

Assignment - 1
Roll: BMC202175
Date: May 14, 2024

Problem 1 Problem Set 1: P5

For a prime p and a positive integer e, prove that $\mathbb{Z}_{p^e}^*$ is cyclic.

Solution: We will prove this in 3 stages: $e = 1$, $e = 2$, $e > 2$.

Case 1: $e = 1$

Lemma 1. $\sum\limits_{d|n} \varphi(d) = n$

Proof: Consider the list of numbers $S = \left\{\frac{1}{n}, \frac{2}{n}, \dots, \frac{n}{n}\right\}$. If we express every number in S as simplified form i.e. $\frac{p}{q}$ form where $gcd(p,q) = 1$. Then the denominators are all the divisors of n.

Then for any $k \in [n]$ we have

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

Denote $d_k := \frac{n}{gcd(k,n)}$ then d_k is a factor of n. And since $gcd\left(\frac{k}{gcd(k,n)}, \frac{n}{gcd(k,n)}\right) = 1$ we have $\frac{k}{gcd(k,n)} \in \mathbb{Z}_{d_k}^*$. Let $k \in \mathbb{Z}_d^*$ then suppose l is such that $d \times l = n$ then the fraction $\frac{k}{d} = \frac{k \times l}{n} \in S$ and its simplified form is infact $\frac{k}{d}$.

Hence for any $d \mid n$, the number of fractions with denominator d is $\varphi(d)$, since for all such fractions the numerators are the elements of $\mathbb{Z}_d^*$. Therefore we have $\sum\limits_{d|n} \varphi(d) = n$. □

Now define for d such that $d \mid p-1$, $S_d = \{a \in \mathbb{Z}_p^* \mid ord(a) = d\}$. Then we have the following lemma:

Lemma 2. $|S_d| = \varphi(d)$

Proof: First we will show that $|S_d| \in \{0, \varphi(d)\}$ then we will show that $|S_d| = \varphi(d)$. Now if $|S_d| \neq 0$ then $\exists\ a \in S_d$ such that $ord(a) = d$. Then consider the polynomial $x^d - 1$ over $\mathbb{F}_p$. $1, a, a^2, \dots, a^{p-1}$ are its distinct roots. Since the degree is d these are the only roots of the polynomial. Now a^k has order $\frac{d}{gcd(d,k)}$. Then the elements which has order d are a^k where $gcd(k,d) = 1$. Hence there are $\varphi(d)$ many powers of a which has order d. Therefore $|S_d| \in \{0, \varphi(d)\}$.

Now we have by Lemma 1

$$\sum_{d|p-1} \varphi(d) = p - 1$$

Now $\{S_d \mid d \mid p-1\}$ is a partition of $\mathbb{Z}_p^*$. Therefore $\sum\limits_{d|p-1} |S_d| = p - 1$. Hence

$$p - 1 = \sum_{d|p-1} |S_d| \leq \sum_{d|p-1} \varphi(d) = p - 1 \iff |S_d| = \varphi(d)\ \forall\ d \text{ such that } d \mid p-1$$

□

Hence the number of elements in $\mathbb{Z}_p^*$ which has order d such that $d \mid p-1$

Now we will introduce another definition. Let H be a group. Then Exponent of H is the smallest number n such that $\forall a \in H$, $a^n = 1$. Now we will show that every finite abelian group has an element which has the order to be exponent of the group. Then we will show that $\mathbb{Z}_p^*$ has exponent $p-1$. With that we can say $\mathbb{Z}_p^*$ has an element which has order $p-1$. Therefore $\mathbb{Z}_p^*$ is cyclic since $|\mathbb{Z}_p^*| = p - 1$ because $\mathbb{Z}_p^*$ is a finite abelian group.

Lemma 3. *If G is a finite abelian group with exponent n then $\exists\ g \in G$ such that $ord(g) = n$.*

Proof: By structure theorem we have

$$G \cong \mathbb{Z}_{q_1} \times \cdots \times \mathbb{Z}_{q_m}$$

where $q_1, \ldots, q_m$ are primes powers. Now $\forall\, g \in G$, $ord(g) \mid lcm(q_1, \ldots, q_m)$. The element in $\mathbb{Z}_{q_1} \times \cdots \times \mathbb{Z}_{q_m}$, $(1, 1, \ldots, 1)$ has order $lcm(q_1, \ldots, q_m)$. So the exponent of G is $lcm(q_1, \ldots, q_m)$ and the corresponding element of $(1, \ldots, 1)$ has order $lcm(q_1, \ldots, q_m)$. □

Lemma 4. *$\mathbb{Z}_p^*$ has exponent $p-1$.*

Proof: Over $\mathbb{F}_p$ the equation $x^{p-1} - 1$ has $p-1$ roots which are all the elements of $\mathbb{Z}_p^*$. There does not exists any polynomial of lower degree which satisfies this property. Hence the exponent of $\mathbb{Z}_p^*$ is $p-1$. □

Therefore there exists an element of $\mathbb{Z}_p^*$ which has order $p-1$. Therefore the group $\mathbb{Z}_p^*$ is cyclic.

Case 2: $e = 2$

Lemma 5. *Let g be generator of the group $\mathbb{Z}_p^*$. Then either g or $g+p$ is generator for $\mathbb{Z}_{p^2}^*$.*

Proof: We have $|\mathbb{Z}_{p^2}^*|\varphi(p^2) = p(p-1)$. Let g has order m in $\mathbb{Z}_{p^2}^*$. Then $g^p \equiv 1 \bmod p$. Hence $p-1 \mid m$. Therefore $m = p(p-1)$ or $m = p-1$ since $m \mid p(p-1)$. If its the first case then we are done. For the later take the element $g+p$. Again let its order is m'. Then $(g+p)^{m'} \equiv 1 \bmod p$. So $p-1 \mid m'$. Hence m' can be either $p-1$ or $p(p-1)$. If it is also $p-1$ then we have

$$\begin{aligned} 1 \equiv (g+p)^{p-1} &\equiv g^{p-1} + (p-1)g^{p-2}p + p^2(\cdots) \bmod p^2 \\ &\equiv g^{p-1} + p(p-1)g^{p-2} \bmod p^2 \\ &\equiv 1 + p(p-1)g^{p-2} \bmod p^2 \end{aligned}$$

Therefore

$$p(p-1)g^{p-2} \equiv 0 \bmod p^2 \iff p \mid (p-1)g^{p-2}$$

which is not possible since $gcd(p, p-1) = 1$ and $gcd(p, g) = 1$. Contradiction. Hence at least one of g and $g+p$ has order $p(p-1)$. □

With this lemma we have an element of $\mathbb{Z}_{p^2}^*$ which has order $p(p-1) = |\mathbb{Z}_{p^2}^*|$. So $\mathbb{Z}_{p^2}^*$ is cyclic.

Case 3: $e > 2$

Lemma 6. $(1+p)^{p^k} \equiv 1 + p^{k+1} \bmod p^{k+2}$

Proof:

$$\begin{aligned} (1-p)^{p^k} &\equiv ((1+p)^p)^{p^{k-1}} \\ &\equiv \left(1 + p^2 + \binom{p}{2} p^2\right)^{p^{k-1}} \bmod p^{k+2} \\ &\equiv 1 + p^2 \times p^{k-1} \bmod p^{k+2} \\ &\equiv 1 + p^{k+1} \bmod p^{k+2} \end{aligned}$$

□

□

Problem 2 Problem Set 1: P6

For a prime p and a positive integer e, prove that $\mathbb{Z}_{p^e}^*$ is cyclic.

Solution:

□

Problem 3 Problem Set 1: P7

For a prime p and a positive integer e, prove that $\mathbb{Z}_{p^e}^*$ is cyclic.

Solution:

□

Problem 4 Problem Set 1: P13

For a prime p and a positive integer e, prove that $\mathbb{Z}_{p^e}^*$ is cyclic.

Solution:

□

Problem 5 Problem Set 1: P14

For a prime p and a positive integer e, prove that $\mathbb{Z}_{p^e}^*$ is cyclic.

Solution:

□