Lagrange's Theorem and Euler's Totient Theorem

Well, only part of it :)

Anand Narasimhan

SoS Beamer

July 2022

Intro to Groups

I can't go talking about Lagrange's Theorem without explaining what a group is :)

Definition 1 (Groups)

A **group** is an ordered pair $(G, *)$ where G is a set and $*$ is a binary operation on G satisfying the following axioms :

1. $(a * b) * c = a * (b * c)$, for all $a, b, c \in G$, i.e., $*$ is **associative**,
2. There exists an element $e \in G$, called an identity of G such that for all $a \in G$ we have $a * e = e * a = a$,
3. For each $a \in G$ there is an element $a^{-1} \in G$, called an **inverse** of a, such that $a * a^{-1} = a^{-1} * a = e$.

Some useful terms and properties of Groups

Definition 2 (Orders)

Let G be a group.

1. The order of a group is the number of distinct elements in the group
2. Let x be an element in G. The order of x is defined as the smallest positive integer n such that $x^n = 1$, where 1 is the identity element of G.

Proposition 1 (Cancellation Laws)

Let G be a group and let $a, b \in G$. The equations $ax = b$ and $ya = b$ have unique solutions for $x, y \in G$. In particular, left and right cancellation laws hold in G, i.e.

1. If $au = av$, then $u = v$
2. If $ub = vb$, then $u = v$

Subgroups

Now let's define a subgroup :

Definition 3 (Subgroup)

Let G be a group. The subset H of G is a **subgroup** of G if H is nonempty and H is closed under products and inverses ($x, y \in H \implies x^{-1} \in H$ and $xy \in H$).

Basically, a subgroup of a group is just a subset which is itself a group with respect to the operation of that group.

Example

Any group has at least 2 subgroups, one is the identity element of the group and the other is the full group itself.

Lagrange's Theorem, not fully though

Theorem 1 (Lagrange's Theorem, incomplete)

If G is a finite group and H is a subgroup of G, then the order of H divides the order of G.

I've left out a major part of the theorem, but this part is all we need in our discussion.

Let's define some terms that we will need later

Definition 4 (Euler's totient function (φ-function))

$\varphi(n)$, for $n \in \mathbb{Z}^+$, is the number of positive integers $a \leq n$ such that a is relatively prime to n, i.e., their GCD is 1.

Definition 5 ($\mathbb{Z}/n\mathbb{Z}$ - The Integers Modulo n)

This can be thought of as the set of remainders that can be obtained when any number is divided by n, i.e., the set $\{0, 1, 2, \ldots, n-1\}$

This set can be thought of as a group under addition, since it satisfies all the criteria for it to be a group : Addition modulo n is associative, the identity is the element 0 and the inverse of the element k will be the element $n - k$.

Number Theory (contd)

An important subset of $\mathbb{Z}/n\mathbb{Z}$ consists of the collection of elements which have a multiplicative inverse in $\mathbb{Z}/n\mathbb{Z}$:

$$(\mathbb{Z}/n\mathbb{Z})^{\times} = \{a \in \mathbb{Z}/n\mathbb{Z} \mid \text{there exists } c \in \mathbb{Z}/n\mathbb{Z} \text{ with } a \cdot c = 1\}$$

Proposition 2 (Condition for Multiplicative Inverse)

$(\mathbb{Z}/n\mathbb{Z})^{\times} = \{\, \overline{a} \in \mathbb{Z}/n\mathbb{Z} \mid (a, n) = 1 \,\}$.

In simpler words, only those elements which are **coprime** with n have a multiplicative inverse in $\mathbb{Z}/n\mathbb{Z}$.
It can be seen that the set $(\mathbb{Z}/n\mathbb{Z})^{\times}$ is a **group under multiplication**, since every element has an inverse, the element 1, which is it's own inverse, is the identity, and multiplication is associative.

Euler's Totient Theorem

Before talking about the theorem, it is important to generalise the definition of $\mathbb{Z}/n\mathbb{Z}$ not just to positive integers less than n, but to all integers. So the elements of the group are no longer just elements, they are **residue classes** or **equivalence classes** containing all the numbers leaving the same remainder mod n. So for example, the residue class $\bar{1}$ contains all integers $1 + kn, k \in \mathbb{Z}$. Now, let's go ahead!

Theorem 2 (Euler's Totient Theorem)

If n and a are coprime positive integers, and $\varphi(n)$ is Euler's totient function, then

$$a^{\varphi(n)} \equiv 1(\text{ mod } n)$$

Unlikely as it sounds, we're going to use Group Theory and Lagrange's Theorem to help prove this theorem!

Proving Euler's Totient Theorem

Let's start with the group $(\mathbb{Z}/n\mathbb{Z})^\times$ (Why?)[1], and let's find the order of the group. Since the group contains all the elements (residue classes) coprime to n, by the definition of the Euler totient function, $\varphi(n)$ is also the number of coprime residue classes, therefore it is the order of the group.

Now, let's observe a random element $\bar{a}$ from the group $(\mathbb{Z}/n\mathbb{Z})^\times$. Let it's order be k. We first prove that the order is finite. An overkill proof would just be to use Lagrange's Theorem directly, (which we're anyway going to use), but let's do a more involved proof. Let us assume that the order of a is infinite and let us take the set of the powers of a, namely, $\{1, a, a^2, \ldots, a^m, \ldots, a^{m+l}, \ldots\}$

[1] Observe that it contains all the elements coprime to n, which is related to the Theorem

Proving Euler's Totient Theorem (contd)

We see that all these powers must be in the group $(\mathbb{Z}/n\mathbb{Z})^\times$, since it is closed under multiplication. Since the group itself is finite, some elements must repeat, since otherwise they all can't be in the group. Let $a^m = a^{m+l}$. Using the cancellation laws, we get that $a^l = 1$, which shows that there is an integer l such that $a^l = 1$, which is a contradiction to the claim that the order is infinite. Therefore, the order must be finite.

Of course, we could have proved this using Lagrange Theorem, by making an additional observation that the set of powers of a is actually a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$ (This is called a cyclic subgroup, and can easily be verified), and in that case, the order of that subgroup would be the order of $\bar{a}$ (logical since there can only be k distinct powers of a before it cycles back to 1 again) and since the order of the subgroup divides the order of the group, the order of $\bar{a}$ has to be finite.

Proving Euler's Totient Theorem (contd)

But wait! We said that the order of the element $\bar{a}$ is the order of the cyclic subgroup (set of powers of $\bar{a}$), which divides the order of the group itself! Let the order of that random element $\bar{a}$ be k. We already know that the order of the group is $\varphi(n)$, so let's write $\varphi(n) = km$, where $m \in \mathbb{N}$.

We know that if k is the order of the element a, $a^k \equiv 1 \bmod n$. Simply taking both sides to power m gives

$$a^{km} = a^{\varphi(n)} \equiv 1^m \bmod n = 1 \bmod n$$

This is the proof I wanted to show you, a proof of Euler's Totient Theorem using Group Theory, while in the process taking you through some basic Group Theory terms, Number Theory and Lagrange's Theorem (not the full thing :))