

LAGRANGE'S THEOREM - A BRIEF INTRODUCTION AND HISTORY

Ryan McElhatton, Ruairi Dennehy, Enda Daly and Ross Treaty†

†National University of Ireland, Galway



Introduction to Lagrange's Theorem

This poster takes a look at mathematician Joseph Louis Lagrange, and his most famous work, 'Lagrange's Theorem'. Born in 1766, in Turin, Italy, Lagrange made huge contributions to the field of mathematics. One of his most important findings came in Group Theory where he proved a theorem that states if H is a subgroup of a finite group G , then, the size of H divides the size of G . We will take a look at Lagrange himself, his theorem, and some applications of the theorem.

Joseph Louis Lagrange

Giuseppe Luigi Lagrangia was born in Turin on the 25th of January 1766. He made for significant contributions to many areas of mathematics including analysis, number theory and mechanics. Areas in mathematics such as Lagrangian in mechanics and the Euler-Lagrange equation in calculus have been given his name as testament to his work. He passed away in Paris on the 10th of April 1813, aged 77.

The Theorem of Lagrange

Lagrange's theorem states, If a function $f(x_1, x_2, \dots, x_n)$ at $n!$ variables is acted on by all possible permutations of the variables and these permuted functions take only r distinct values then r is a division of $n!$.

Lagrange discovered this while he was trying to find an algebraic formula solution for a 5th degree polynomial and more generally for the n th degree polynomial where $n > 4$. He observed that the solution for quartic and cubic equations could be solved by finding an equation of a lower degree. These types of polynomials are known as resolvent polynomials. For this example we will write the roots as:

$$\frac{x_1x_2 + x_3x_4}{2}, \frac{x_1x_3 + x_2x_4}{2}, \frac{x_1x_4 + x_2 + x_3}{2}$$

where x_1, x_2, x_3, x_4 are roots of the original polynomial. In addition, he observed that all of the 4 roots are permuted in $4! = 24$ ways and only these 3 values would occur. Lagrange then said that in order to solve a quintic equation, we would need a function which only takes 4 values when the variable is permuted in $5! = 120$ ways.

Proof of Lagrange's Theorem

Theorem:

If G is a finite group of order n and H is a subgroup of G of order k , then $k|n$ and $\frac{n}{k}$ is the number of distinct cosets of H in G

Proof:

To prove this theorem we start by considering the 3 lemmas outlined below.

- **Lemma 1:** If G is a group with subgroup H , then there is a one to one correspondence between H and any coset of H
- **Lemma 2:** If G is a group with subgroup H , then the left coset relation, $g_1 \sim g_2$ if and only if $g_1 * H = g_2 * H$ is an equivalence relation.
- **Lemma 3:** Let S be a set and \sim be an equivalence relation on S . If A and B are two equivalence classes with $A \cap B \neq \emptyset$, then $A = B$.

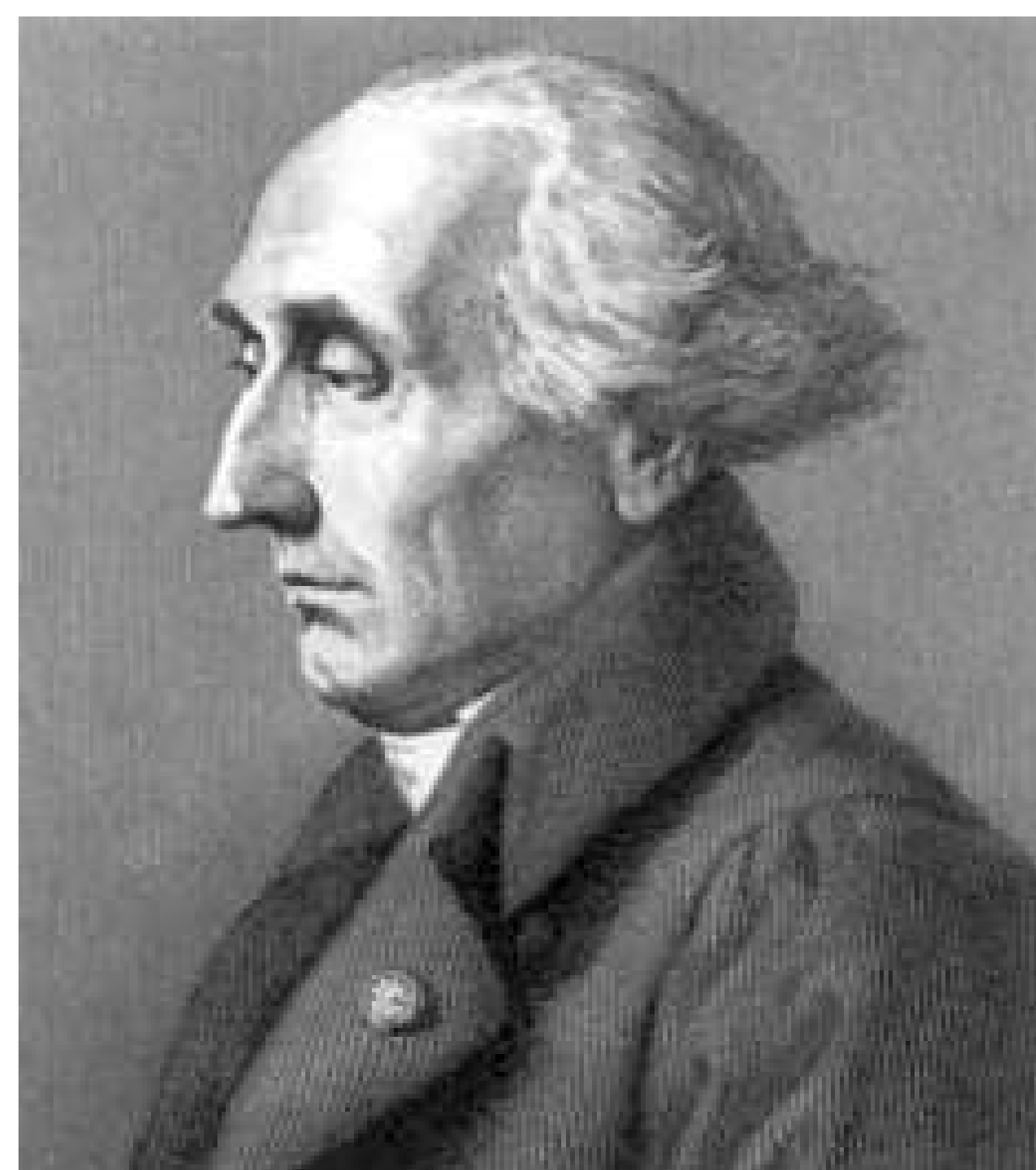


Fig. 1: Joseph Louis Lagrange

Let \sim be the left coset equivalence relation defined in Lemma 2.

It follows from Lemma 2 that \sim is an equivalence relation and by Lemma 3 any two distinct cosets of \sim are disjoint. Hence, we can write

$$G = (g_1 * H) \cup (g_2 * H) \cup \dots \cup (g_n * H)$$

where the $g_i * H$, $i = 1, 2, \dots$ are the disjoint left cosets of H guaranteed by Lemma 3. By Lemma 1, the cardinality of each of these cosets is the same as the order of H , and so

$$\begin{aligned} |G| &= |g_1 * H| + |g_2 * H| + \dots + |g_n * H| \\ |G| &= |H| + |H| + \dots + |H| \\ |G| &= n * |H| = n * k. \end{aligned}$$

where k = the order of H

Q.E.D

Applications

Lagrange's theorem is often used to prove the special cases of Fermat's little theorem and its generalization, Euler's theorem, which were already known before Lagrange's theorem. Lagrange's theorem can also be used to show that there are an infinite number of primes. The theorem is also very important in the field of cryptography. With the rise of cryptocurrencies such as Bitcoin and our move towards a cashless society, work in cryptography is sure to be very important in the coming years. Bitcoin has recently reached its all time high of over 20,000 USD further proving our shift towards cryptocurrencies. Having a good knowledge of Lagrange's theorem may help you get into the world of cryptography!

Lagrange Fun Facts

Here are a few fun facts around Lagrange and his theorem

- Lagrange's interest in mathematics began by chance after reading a memoir by Edmond Halley
- In 1764, Lagrange was awarded a prize by the French Academy of Science for an essay on how apparent oscillation causes insignificant yet tangible changes in position of lunar features on the visible face of the moon. This essay included the famous equations we use today.

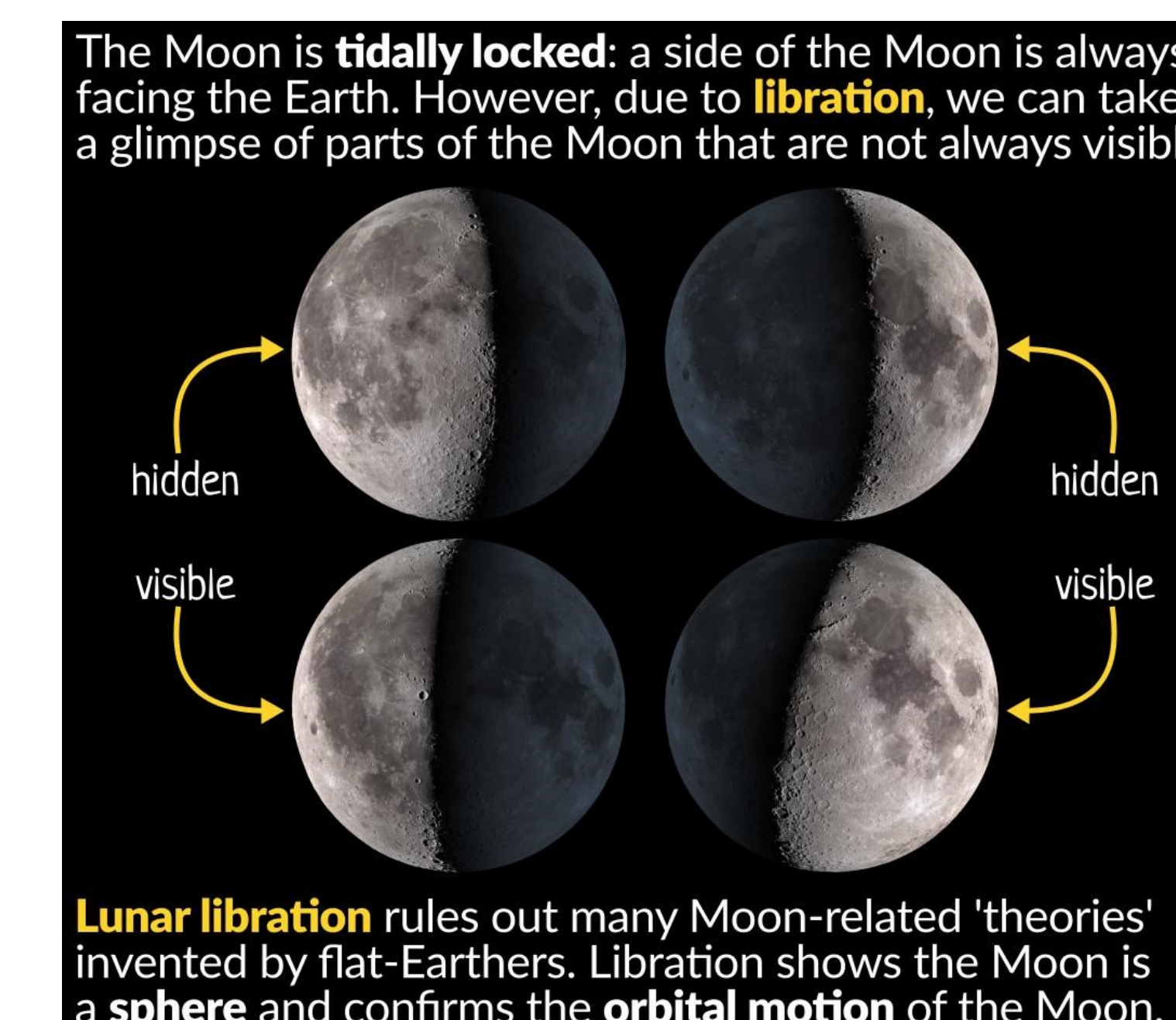


Fig. 2: The basis of one of Lagrange's famous papers

- Lagrange, at Leonhard Euler's recommendation, was made Director of Mathematics at the Berlin Academy in 1766.
- Despite being both an academic, and a foreigner, Lagrange survived the French Revolution and Reign of Terror.