THE UNIT GROUP, FERMAT'S LITTLE THEOREM, AND EULER'S THEOREM

DEFINITION: A **group** is a set G equipped with a product operation

$$G \times G \to G \qquad (g,h) \mapsto gh$$

and an **identity** element $1 \in G$ such that

- the product is associative: $(gh)k = g(hk)$ for all $g, h, k \in G$,
- $g1 = 1g = g$ for all $g \in G$, and
- for every $g \in G$, there is an inverse element $g^{-1} \in G$ such that $gg^{-1} = g^{-1}g = 1$.

A group is **abelian** if the product is commutative: $gh = hg$ for all $g, h \in G$. A **finite group** is a group G that is a finite set.

DEFINITION: Let G be a group and $g \in G$. The **order** of g is the smallest positive integer n such that $g^n = e$, if some such n exists, and ∞ if no such integer exists.

LAGRANGE'S THEOREM: Let G be a finite group and $g \in G$. Then the order of g is finite and divides the cardinality of the group G.

(1) The additive group $\mathbb{Z}_n$: Let n be a positive integer.
  (a) Show[1] that the set $\mathbb{Z}_n$ with the addition operation and identity element $[0]$ is a group. We will write $\mathbb{Z}_n$ to denote this group with this operation in general.
  (b) Find the order of each element in $\mathbb{Z}_4$.
  (c) Find the order of each element in $\mathbb{Z}_5$.
  (d) Check that Lagrange's theorem holds for $\mathbb{Z}_4$ and $\mathbb{Z}_5$.

(2) The group $\mathbb{Z}_n^\times$: Let n be a positive integer.
  (a) Show that the set

$$\mathbb{Z}_n^\times := \{a \in \mathbb{Z}_n \mid a \text{ is a unit in } \mathbb{Z}_n\}$$

  with the multiplication operation and identity element $[1]$ is a group. We will write $\mathbb{Z}_n^\times$ to denote this group with this operation in general.
  (b) Find the order of each element in $\mathbb{Z}_7^\times$.
  (c) Find the order of each element in $\mathbb{Z}_8^\times$.
  (d) Check that Lagrange's theorem holds for $\mathbb{Z}_7^\times$ and $\mathbb{Z}_8^\times$.

FERMAT'S LITTLE THEOREM: Let p be a prime number and a an integer. If p does not divide a, then

$$a^{p-1} \equiv 1 \pmod{p}.$$

(3) Lagrange's Theorem implies Fermat's Little Theorem:
  (a) Show that $\mathbb{Z}_p^\times$ has exactly $p-1$ elements.
  (b) Use Lagrange's theorem to show that if $[a] \in \mathbb{Z}_p^\times$, then $[a]^{p-1} = [1]$ in $\mathbb{Z}_p$.
  (c) Deduce Fermat's Little Theorem.

(4) Use Fermat's Little Theorem to find the smallest nonnegative integer congruent to each of the following: (a) $7^{12} \pmod{13}$, (b) $7^{96} \pmod{13}$, (c) $7^{98} \pmod{13}$, (d) $7^{1505} \pmod{13}$.

[1] Even though we are saying "product" operation, write gh for the typical group operation, and 1 for the typical identity element, we can take $(g,h) \mapsto g + h$ here. We just need to check the three rules above.

DEFINITION: Let n be a positive integer. We define $\varphi(n)$ to be the number of elements of $\mathbb{Z}_n^\times$. We call this **Euler's phi function**.

PROPOSITION: Euler's phi function satisfies the following properties.

(1) If p is a prime and n is a positive integer, then $\varphi(p^n) = p^{n-1}(p-1)$.
(2) If m, n are coprime positive integers, then $\varphi(mn) = \varphi(m)\varphi(n)$.

EULER'S THEOREM: Let a, n be coprime integers, with n positive. Then

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

(5) Use the Proposition above to compute the following:
- $\varphi(41)$
- $\varphi(27)$
- $\varphi(15)$
- $\varphi(100)$.

(6) Use Euler's Theorem to compute the last two digits of 7^{2003}.

(7) Euler's phi function and Euler's Theorem.
  (a) Explain why Lagrange's Theorem implies Euler's Theorem.
  (b) Explain why $\varphi(n)$ is equal to the number of positive integers less than n that are coprime to n.
  (c) Prove the first part of the Proposition above.
  (d) Use CRT to explain why the map

$$\begin{aligned} \mathbb{Z}_{mn} &\xrightarrow{\pi} \mathbb{Z}_m \times \mathbb{Z}_n \\ [a]_{mn} &\mapsto ([a]_m, [a]_n) \end{aligned}$$

  is bijective.
  (e) Show[2] that $[a]_{mn}$ is a unit in $\mathbb{Z}_{mn}$ if and only if $[a]_m$ is a unit in $\mathbb{Z}_m$ and $[a]_n$ is a unit in $\mathbb{Z}_n$.
  (f) Conclude the proof of the second part of the Proposition above.

(8) Proof of Lagrange's Theorem: Let G be a finite group and $g \in G$. Let e be the order of g.
  (a) Consider the list $1, g, \ldots, g^{e-1}$. Explain why these elements are all distinct.
  (b) If $G = \{1, g, \ldots, g^{e-1}\}$, explain why Lagrange's Theorem holds.
  (c) If $h_1 \in G \smallsetminus \{1, g, \ldots, g^{e-1}\}$, explain why the list of elements $h_1, h_1 g, \ldots, h_1 g^{e-1}$ are all distinct. Then explain why $\{1, g, \ldots, g^{e-1}\}$ and $\{h_1, h_1 g, \ldots, h_1 g^{e-1}\}$ are disjoint.
  (d) Continue this process to form a table

$$\begin{array}{cccc} 1 & g & \ldots & g^{e-1} \\ h_1 & h_1 g & \ldots & h_1 g^{e-1} \\ \vdots & \vdots & \ddots & \vdots \\ h_t & h_t g & \ldots & h_t g^{e-1} \end{array}$$

  Conclude the proof of the theorem.

[2] For the forward direction, take an inverse $[b]_{mn}$ for $[a]_{mn}$ is a unit in $\mathbb{Z}_{mn}$ and consider $[b]_m$ and $[b]_n$. For the reverse, take inverses $[c]_m$ and $[d]_n$ for $[a]_m$ and $[a]_n$ respectively, and apply CRT.