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 $\mathbb{Z}_5$.

(a) The sum of any two congruence classes in $\mathbb{Z}_n$ is a congruence class in $\mathbb{Z}_n$. Addition is associative since

$$[a] + ([b] + [c]) = [a] + [b + c] = [a + b + c] = [a + b] + [c] = ([a] + [b]) + [c].$$

The element $[0]$ is an identity, since $[0]+[a] = [0+a] = [a]$ and similarly in the other order. There are inverses, namely $[-a] + [a] = [-a + a] = [0]$.
(b) $[0]$ has order 1; $[1]$ and $[3]$ have order 4; and $[2]$ has order 2.
(c) $[0]$ has order 1; and the rest have order 5.
(d) Yes.

(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 $\mathbb{Z}_8^\times$.

[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.

(a) First the product of units is a unit: if $[a]$ has inverse $[c]$ and $[b]$ has inverse $[d]$, then $[a][b][c][d] = [1]$. Associativity is similar to above. $[1]$ is a unit and is the identity. We have inverses by definition.
(b) $[1]$ has order 1; $[6]$ has order 2; $[2]$ and $[4]$ have order 3; and $[3]$ and $[5]$ have order 6.
(c) $[1]$ has order 1; and $[3]$, $[5]$, and $[7]$ have order 2.
(d) Yes.

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.

(a) Every element of $\mathbb{Z}_p$ except $[0]$ has an inverse, since every number that is not a multiple of p is coprime to p.
(b) Let e be the order of $[a]$, so $[a]^e = [1]$. Then $p-1 = ef$ for some f, so $[a]^{p-1} = [a]^{ef} = ([a]^e)^f = [1]$.
(c) If p does not divide a, then $[a] \neq [0]$ and $[a] \in \mathbb{Z}_p^\times$. Then $[a]^{p-1} = [1]$ implies that $a^{p-1} \equiv 1 \pmod{p}$.

(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) $7^{12} \equiv 1 \pmod{13}$ by FLT.
(2) $7^{96} \equiv (7^{12})^8 \equiv 1 \pmod{13}$
(3) $7^{98} \equiv (7^{12})^8 7^2 \equiv 7^2 \equiv 10 \pmod{13}$
(4) $1505 = 125 \cdot 12 + 5$, so $7^{1505} \equiv 7^5 \equiv 11 \pmod{13}$.

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 the Proposition above to compute the following:
- $\varphi(41) = 40$.
- $\varphi(27) = \varphi(3^3) = 3^2(3-1) = 18$.
- $\varphi(15) = \varphi(3)\varphi(5) = 2 \cdot 4 = 8$.
- $\varphi(100) = \varphi(2^2)\varphi(5^2) = 2(2-1)5(5-1) = 40$.

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

Since $\varphi(100) = 40$, we know $7^{40} \equiv 1 \pmod{100}$. Then
$$7^{2003} = 7^{50\cdot 40+3} \equiv (7^{40})^{50}7^3 \equiv 7^3 \equiv 343 \equiv 43 \pmod{100},$$
so the last two digits are 43.

(8) 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
$$\mathbb{Z}_{mn} \xrightarrow{\pi} \mathbb{Z}_m \times \mathbb{Z}_n$$
$$[a]_{mn} \mapsto ([a]_m, [a]_n)$$
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.

(a) Similar to Lagrange implies FLT.
(b) Every congruence class is represented by nonnegative number less than n. The class of zero is not a unit, so any possible unit is represented by a positive integer less than n. We saw last time that $[a]$ is a unit if and only if a and n are coprime.
(c) a is coprime with p^n if and only if p does not divide n. We count the number of positive integers less than p^n that are not multiples of p, and get the formula above.
(d) Note first that this is a well defined function: if two numbers are congruent modulo mn, they are congruent modulo m and modulo n. CRT says that any pair of residues modulo m and n correspond to a unique congruence class modulo mn; i.e., π is bijective.
(e) For the forward direction, let $[b]$ be an inverse of $[a]$, so $ab \equiv 1 \pmod{mn}$. Then $ab \equiv 1 \pmod{m}$ and $ab \equiv 1 \pmod{n}$, so $[a]$ is a unit in $\mathbb{Z}_m$ and $\mathbb{Z}_n$. For the reverse, let c, d be such that $ac \equiv 1 \pmod{m}$ and $ad \equiv 1 \pmod{n}$. By CRT, there is a b such that $b \equiv c \pmod{m}$ and $b \equiv d \pmod{n}$. Then $ab \equiv ac \equiv 1 \pmod{m}$ and $ab \equiv ad \equiv 1 \pmod{n}$. By the uniqueness part of CRT, $ab \equiv 1 \pmod{mn}$, so a has an inverse mod mn.
(f) By (d) and (e), every unit in $\mathbb{Z}_{mn}$ corresponds to a pair consisting of a unit in $\mathbb{Z}_m$ and a unit in $\mathbb{Z}_n$. Thus, the number of elements of $\mathbb{Z}_{mn}^\times$ is the product of the number of elements in $\mathbb{Z}_m^\times$ and $\mathbb{Z}_n^\times$.

(9) 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 $1, g, \dots, g^{e-1}$. Explain why these elements are all distinct.
(b) If $G = \{1, g, \dots, g^{e-1}\}$, explain why Lagrange's Theorem holds.

[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.

(c) If $h_1 \in G \setminus \{1, g, \ldots, g^{e-1}\}$, 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.

(a) If $g^a = g^b$ with $a < b < e$, then $1 = (g^{-1})^a g^a = (g^{-1})^a g^b = g^{b-a}$, which contradicts that e is the smallest exponent with $g^e = 1$.

(b) Because the number of elements of G is the order of g.

(c) If $hg^a = hg^b$ with $a < b < e$, then $g^a = h^{-1}hg^a = h^{-1}hg^b = g^b$, which we saw was impossible. If $g^a = hg^b$, then $g^{a-b} = g^a g^{-b} = hg^b g^{-b} = h$. But $g^{a-b} = g^{e+a-b}$ is on the first list.

(d) Along similar lines, we get an array like this with the rows all distinct. Eventually we must have the whole group, because it is finite. Then the cardinality of G is $(t+1)e$.