Euler's Theorem and Fermat's Little Theorem

Learning Objectives. By the end of class, students will be able to:

- Define and find a reduced residue system modulo m
- Define the Euler ϕ-function $\phi(n)$
- Prove Euler's Generalization of Fermat's Little Theorem .

Read Strayer, Section 2.5

Turn in Exercise 50. Prove that $9^{10} = 1 \pmod{11}$ by following the steps of the proof of Fermat's Little Theorem.

> **Solution:** Consider the 10 integers given by $9, 2(9), 3(9), \ldots, 9(10)$. Note that $11 \mid 9i$ for $i = 1, 2, \ldots, 10$ since 11 is prime and $11 \nmid 10$ and $11 \nmid i$. By **??**, since $(9, 11) = 1$ if $9i \equiv 9j \pmod{11}$ implies $i \equiv j \pmod{11}$. Therefore, no two of $9, 2(9), 3(9), \ldots, 9(10)$ are congruent modulo 11. So the least nonnegative residues modulo 11 of the integers $9, 2(9), 3(9), \ldots, 9(10)$, taken in some order, must be $1, 2, \ldots, p-1$. Then
>
> $$(9)(2(9))(3(9)) \cdots (9(10)) \equiv (1)(2) \cdots (10) \pmod{11}$$
>
> or, equivalently,
>
> $$9^{10} 10! \equiv 10! \pmod{11}.$$
>
> By **??**, the congruence above becomes $-9^{10} \equiv -1 \pmod{11}$, which is equivalent to $9^{10} \equiv 1 \pmod{11}$.

Quiz (10 min)

Euler's Generalization of Fermat's Little Theorem (40 min)

There are several different ways to present the material in Sections 2.4 through 2.6. In class, we will do the other order: Fermat's Little Theorem to prove Wilson's Theorem. I will keep the result numbering from the book, so they will be out of order.

Definition (reduced residue system modulo m)**.** Let m be a positive integer. We say that $\{r_1, r_2, \ldots, r_k\}$ is a *reduced residue system modulo* m if

- $(r_i, m) = 1$ for all $i = 1, 2, \ldots, k$,
- $r_i \not\equiv r_j \pmod{m}$ when $i \neq j$,
- for all $a \in \mathbb{Z}$ with $(a, m) = 1$, $a \equiv r_1 \pmod{p}$ for some $i = 1, 2, \ldots, k$.

Example 1.

- *The sets* $\{1, 2, 3, 4, 5, 6\}$ *and* $\{5, 10, 15, 20, 25, 30, 35\}$ *are both reduced residue systems modulo* 7.
- *If p is prime, then* $\{1, 2, \ldots, p-1\}$ *is a complete residue system modulo p. If $p \neq 5$,* $\{5, 10, \ldots, 5(p-1)\}$ *is a complete residue system modulo p.*
- *The sets* $\{1, 5, 7, 11\}$ *and* $\{5, 25, 35, 55\}$ *are both reduced residue systems modulo* 12.

Lemma 1 (Porism 2.18)**.** *Let m be a positive integer and let $\{r_1, r_2, \ldots, r_k\}$ be a reduced residue system modulo m. If $a \in \mathbb{Z}$ with $(a, m) = 1$, then $\{ar_1, ar_2, \ldots, ar_k\}$ is a reduced residue system modulo m.*

Learning outcomes:
Author(s): Claire Merriman

This result is also implicitly used in the proof of Fermat's Little Theorem since $\{1, 2, \ldots, p-1\}$ is a reduced residue system.

Proof Let $\{r_1, r_2, \ldots, r_k\}$ be a reduced residue system modulo m and $a \in \mathbb{Z}$ with $(a, m) = 1$. Since $\{r_1, r_2, \ldots, r_k\}$ and $\{ar_1, ar_2, \ldots, ar_k\}$ have the same number of elements, it suffices to show that $(ar_i, m) = 1$ and $ar_i \not\equiv ar_j \pmod{m}$ for $i \neq j$. If there exist some prime p such that $p \mid (ar_i, m)$ then $p \mid ar_i$ and $p \mid m$ by **??**. By **??**, $p \mid a$ or $p \mid r_i$, so either $p \mid (a, m)$ or $p \mid (r_i, m)$. which is a contradiction. Thus, $(ar_i, m) = 1$.

By **??**, $ar_i \equiv ar_j \pmod{m}$ if and only $r_i \equiv r_j \pmod{\frac{m}{(a,m)}}$. Since $(a, m) = 1$, $ar_i \not\equiv ar_j \pmod{m}$ when $i \neq j$. ■

Definition (Euler ϕ-function)**.** Let n be a positive integer. The *Euler ϕ-function* $\phi(n)$ is

$$\phi(n) = \#\{a \in \mathbb{Z} : a > 0 \text{ and } (a, m) = 1\}.$$

Remark 1. *For a positive integer m, $\phi(m)$ is the number of reduced residues modulo m*

Example 2.
- $\phi(7) = 6$
- *If p is prime, $\phi(p) = p - 1$*
- $\phi(12) = 4$

Theorem 1 (Euler's Generalization of Fermat's Little Theorem)**.** *Let $a, m \in \mathbb{Z}$ with $m > 0$. If $(a, m) = 1$, then*

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

Corollary (Fermat's Little Theorem)**.** *Let p be prime and $a \in \mathbb{Z}$. If $p \nmid a$, then*

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

Proof Let p be prime and $a \in \mathbb{Z}$, then $(a, p) = 1$ if and only if $p \nmid a$. Since $\phi(p) = p - 1$, $a^{p-1} \equiv 1 \pmod{p}$. ■

Warning 1. *The converse of both of these theorems is false. The easiest example is $1^k \equiv 1 \pmod{m}$ for all positive integers k, m. Also note that $2^{341} \equiv 2 \pmod{341}$. Since $(2, 341) = 1$, there exists an integer a such that $2a \equiv 1 \pmod{341}$. Thus*

$$a2^{341} \equiv (2a)2^{340} \equiv 2^{340} \equiv 2a \equiv 1 \pmod{341}.$$

However, $341 = (11)(31)$.

Proof of Euler's Generalization of Fermat's Little Theorem Let m be a positive integer and let $\{r_1, r_2, \ldots, r_{\phi(m)}\}$ be a reduced residue system modulo m. If $a \in \mathbb{Z}$ with $(a, m) = 1$, then $\{ar_1, ar_2, \ldots, ar_{\phi(m)}\}$ is a reduced residue system modulo m by Porism 2.18. Thus, for all $i = 1, 2, \ldots, \phi(m)$, then $r_i \equiv ar_j \pmod{m}$ for some $j = 1, 2, \ldots, \phi(m)$. Thus

$$r_1 r_2 \cdots r_{\phi(min)} \equiv ar_1 ar_2 \cdots ar_{\phi(min)} \equiv a^{\phi(m)} r_1 r_2 \cdots r_{\phi(m)} \pmod{m}.$$

Since $(r_i, m) = 1$, there exists $x_i \in \mathbb{Z}$ such that $r_i x_i \equiv 1 \pmod{m}$. Thus,

$$\begin{aligned} r_1 x_1 r_2 x_2 \cdots r_{\phi(min)} x_{\phi(m)} &\equiv a^{\phi(m)} r_1 x_1 r_2 x_2 \cdots r_{\phi(min)} x_{\phi(m)} \pmod{m} \\ 1 &\equiv a^{\phi(m)} \pmod{m}. \end{aligned}$$

■