# Order of elements modulo $m$

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

- Define the order of an element modulo $m$
- Find the order of an element modulo $m$
- Prove basic facts about the order of an element modulo $m$ .

## Review of $\phi$-function

**Remark 1.** *From before break, ?? states if $(m, n) = 1$ for positive integers $m$ and $n$, then $\phi(mn) = \phi(m)\phi(n)$.*

*Thus, $\phi(63) = \phi(9(7)) = \phi(9)\phi(7) = 6(6)$.*

**Homework Problem 1** *Using ?? and the ??*

(a) *Let $n$ be an integer not divisible by 3. Prove that $n^7 \equiv n \pmod{63}$.*

***Proof*** *Let $n$ be an integer that is not divisible by 3. By the ??,*

$$\begin{aligned} x &\equiv n^7 \pmod{7} \\ x &\equiv n^7 \pmod{9} \end{aligned}$$

*has a unique solution modulo 63. By ??, $n^7 \equiv n \pmod{7}$.*

*Since $(n, 9) = 1$ and $\phi(9) = 6$, ?? says that $n^6 \equiv 1 \pmod{9}$. Multiplying both sides of the congruence by $n$ gives $n^7 \equiv n \pmod{9}$. Thus, $7 \mid n^7 - n$ and $9 \mid n^7 - n$ by definition. Since $(7, 9) = 1$, $63 \mid n^7 - n$, so $n^7 \equiv n \pmod{63}$.* ■

(b) *Let $n$ be an integer divisible by 9. Prove that $n^7 \equiv n \pmod{63}$.*

**Remark 2.** *Reviewing the proof of part (a): ?? only requires the modulus is prime. ?? does require $(n, m) = 1$, so you cannot use it for this problem, but $n \equiv 0 \pmod{9}$.*

## Order of $a$ modulo $m$

**Definition 1** (order of $a$ modulo $m$)**.** *Let $a, m \in \mathbb{Z}$ with $m > 0$ and $(a, m) = 1$. Then the* order of $a$ modulo $m$*, denoted* $\operatorname{ord}_m a$*, is the smallest positive integer $n$ such that $a^n \equiv 1 \pmod{m}$.*

| $a^1$ | $a^2$ | $a^3$ | $a^4$ | $a^5$ | $a^6$ | $\operatorname{ord}_7 a$ |
|---|---|---|---|---|---|---|
| $\boxed{1}$ | $\boxed{1}$ | $\boxed{1}$ | $\boxed{1}$ | $\boxed{1}$ | $\boxed{1}$ | 1 |
| $\boxed{2}$ | $\boxed{4}$ | $\boxed{1}$ | $\boxed{2}$ | $\boxed{4}$ | $\boxed{1}$ | 3 |
| $\boxed{3}$ | $\boxed{2}$ | $\boxed{6}$ | $\boxed{4}$ | $\boxed{5}$ | $\boxed{1}$ | 6 |
| $\boxed{4}$ | $\boxed{2}$ | $\boxed{1}$ | $\boxed{4}$ | $\boxed{2}$ | $\boxed{1}$ | 3 |
| $\boxed{5}$ | $\boxed{4}$ | $\boxed{6}$ | $\boxed{2}$ | $\boxed{3}$ | $\boxed{1}$ | 6 |
| $\boxed{6}$ | $\boxed{1}$ | $\boxed{6}$ | $\boxed{1}$ | $\boxed{6}$ | $\boxed{1}$ | 2 |

Learning outcomes:

Author(s): Claire Merriman

Table 1: Table of exponents modulo 7

There are many patterns in this table that we will talk about in the future, but the first is that $\text{ord}_m a \mid \phi(m)$.

**Proposition 1.** *Let $a, m \in \mathbb{Z}$ with $m > 0$ and $(a, m) = 1$. Then $a^n \equiv 1 \pmod{m}$ for some positive integer $n$ if and only if $\text{ord}_m a \mid n$. In particular, $\text{ord}_m a \mid \phi(m)$.*

***Proof*** *Let $a, m \in \mathbb{Z}$ with $m > 0$ and $(a, m) = 1$.*

($\Rightarrow$) *We want to show if $a^n \equiv 1 \pmod{m}$ for some positive integer $n$, then $\text{ord}_m a \mid n$.*

*By the **??**, there exist unique integers $q, r$ such that $n = (\text{ord}_m a)q + r$ and $0 \le r < \text{ord}_m a$. Thus,*

$$1 \equiv a^n \equiv a^{(\text{ord}_m a)q+r} \equiv (a^{(\text{ord}_m a)})^q a^r \equiv a^r \pmod{m}$$

*since $a^{(\text{ord}_m a)} \equiv 1 \pmod{m}$ by definition of order of a modulo m. Since $a^r \equiv 1 \pmod{m}$ and $0 \le r < \text{ord}_m a$, if must be that $r = 0$, otherwise $\text{ord}_m a$ is not the smallest positive integer where $a^k \equiv 1 \pmod{m}$.*

($\Leftarrow$) *We want to show if $\text{ord}_m a \mid n$ for some positive integer $n$, then $a^n \equiv 1 \pmod{m}$.*

*If $\text{ord}_m a \mid n$, then there exists an integer $k$ such that $(\text{ord}_m a)k = n$. Thus,*

$$a^n \equiv (a^{\text{ord}_m a})^k \equiv 1 \pmod{m}$$

*by definition of order of a modulo m.*

■

**Proposition 2.** *Let $a, m \in \mathbb{Z}$ with $m > 0$ and $(a, m) = 1$. Then $a^i \equiv a^j \pmod{m}$ for nonnegative integers $i, j$ if and and only if $i \equiv j \pmod{\text{ord}_m a}$.*

**Example 1.** *Let $a = 2$ and $m = 7$. Since $\text{ord}_7 2 = 3$, $2^i \equiv 2^j \pmod{7}$ if and only if $i \equiv j \pmod{3}$.*

***Sketch of Proof*** *Let $a = 2$ and $m = 7$. Without loss of generality, assume that $i \ge j$.*

($\Rightarrow$) *Assume that $2^i \equiv 2^j \pmod{7}$. Then by exponent rules, $2^j 2^{i-j} \equiv 2^j \pmod{7}$. Since $(2^i, 7) = 1$, there exists a multiplicative inverse of $2^i$ modulo 7 by **??**, say $(2^j)'$. Multiplying both sides of the congruence by this inverse, we get,*

$$2^{i-j} \equiv (2^j)'2^j 2^{i-j} \equiv (2^j)'2^j \equiv 1 \pmod{7}.$$

*By , $\text{ord}_m a \mid i - j$. Thus, $i \equiv j \pmod{\text{ord}_m a}$ by definition.*

($\Leftarrow$) *Assume that $i \equiv j \pmod{3}$. Then $3 \mid i - j$ by definition. Since $\text{ord}_7 2 = 3$, states that $2^{i-j} \equiv 1 \pmod{7}$. Multiplying both sides of the congruence by $2^j$ gives $2^i \equiv 2^j \pmod{7}$.*

■

***Proof of Proposition 2*** Let $a, m \in \mathbb{Z}$ with $m > 0$ and $(a, m) = 1$. Without loss of generality, assume that $i \ge j$ for nonnegative integers $i$ and $j$.

($\Rightarrow$) Assume that $a^i \equiv a^j \pmod{m}$. Then by exponent rules, $a^j a^{i-j} \equiv a^j \pmod{m}$. Since $(a^i, m) = 1$ by assumption, there exists a multiplicative inverse of $a^i$ modulo $m$ by **??**, say $(a^j)'$. Multiplying both sides of the congruence by this inverse, we get,

$$a^{i-j} \equiv (a^j)'a^j a^{i-j} \equiv (a^j)'a^j \equiv 1 \pmod{m}.$$

By , $\text{ord}_m a \mid i - j$. Thus, $i \equiv j \pmod{\text{ord}_m a}$ by definition.

($\Leftarrow$) Assume that $i \equiv j \pmod{\text{ord}_m a}$. Then $\text{ord}_m a \mid i - j$ by definition, and states that $a^{i-j} \equiv 1 \pmod{m}$. Multiplying both sides of the congruence by $a^j$ gives $a^i \equiv a^j \pmod{m}$.

■