

Primitive roots modulo a prime

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

- Find the order of an element modulo m using primitive roots.

Instructor Notes: Reading Uploaded notes

Turn in For each result in the scanned notes, identify the result in our textbook. If it is a special case of the theorem in the textbook, (ie, the reading only proves the theorem for primes or $d = q^s$), also note this.

Definition 1 (primitive root). Let $r, m \in \mathbb{Z}$ with $m > 0$ and $(r, m) = 1$. Then r is said to be a primitive root modulo m if $\text{ord}_m r = \phi(r)$.

We saw in the reading that primitive roots always exist modulo a prime. What about composites?

Example 1. • Since $\phi(4) = 2$, and $\text{ord}_4 3 = 2$, 3 is a primitive root modulo 4. The powers $\{3^1, 3^2\}$ are a reduced residue system modulo 4.

- Since $\phi(6) = \phi(3)\phi(2) = 2$ and $\text{ord}_6 5 = 2$, 5 is a primitive root modulo 6. The powers $\{5^1, 5^2\}$ are a reduced residue system modulo 6.
- There are no primitive roots modulo 8. By ??, $\phi(8) = 4$. Since every odd number squares to 1 modulo 8, $\text{ord}_8 1 = 1$ and $\text{ord}_8 3 = \text{ord}_8 5 = \text{ord}_8 7 = 2$.
- Since $\phi(9) = 3^1(3 - 1) = 6$ by ??, we check:

$$2^1 = 1, \quad 2^2 = 4, \quad 2^3 = 8, \quad 2^4 \equiv 7 \pmod{9}, \quad 2^5 \equiv 5 \pmod{9}, \quad 2^6 \equiv 1 \pmod{9}$$

So 2 is a primitive root modulo 9, but are there more?

$$4^1 = 4, \quad 4^2 = 2^4 \equiv 7 \pmod{9}, \quad 4^3 = 2^6 \equiv 1 \pmod{9}$$

We can also use exponent rules and ?? to simplify some calculations. For example, $5 \equiv 2^5 \pmod{9}$, so $5^i \equiv 2^{5i} \equiv 2^j \pmod{9}$ if and only if $5i \equiv j \pmod{6}$.

$$\begin{aligned} 5^1 &\equiv 5 \pmod{9}, & 5^2 &\equiv 2^{10} \equiv 2^4 \equiv 7 \pmod{9}, & 5^3 &\equiv 2^{15} \equiv 2^3 \equiv 8 \pmod{9}, \\ 5^4 &\equiv 2^{20} \equiv 2^2 \equiv 4 \pmod{9}, & 5^5 &\equiv 2^{25} \equiv 2^1 \equiv 2 \pmod{9}, & 5^6 &\equiv 1 \pmod{9}, \end{aligned}$$

$$7^1 \equiv (-2) \equiv 7 \pmod{9}, \quad 7^2 \equiv (-2)^2 \equiv 4 \pmod{9}, \quad 7^3 \equiv (-2)^3 \equiv -8 \equiv 1 \pmod{9}$$

$$\begin{aligned} \text{ord}_9(1) &= 1 \\ \text{ord}_9(2) &= \text{ord}_9(5) = 6 \\ \text{ord}_9(4) &= \text{ord}_9(7) = 3 \\ \text{ord}_9(8) &= 2 \end{aligned}$$

Proposition 1. Let r be a primitive root modulo m . Then

$$\{r, r^2, \dots, r^{\phi(m)}\}$$

is a set of reduced residues modulo m .

This is the general version of ??, using exponents $1, 2, \dots, \phi(m)$ instead of $0, 1, \dots, \phi(m) - 1$. Since Strayer's statement of ?? is already stated and proved for composites, and both lists have the same number of elements, the only changes to the proof is replacing $p - 1$ with $\phi(m)$. Note $a^0 \equiv a^{\phi(m)} \equiv 1 \pmod{m}$ when $(a, m) = 1$.

Proposition 2. Let $a, m \in \mathbb{Z}$ with $m > 0$ and $(a, m) = 1$. If i is a positive integer, then

$$\text{ord}_m(a^i) = \frac{\text{ord}_m a}{\gcd(\text{ord}_m a, i)}.$$

In-class Problem 1 Use only the results through /?? to prove the primitive root version:

Proposition 3. Let $r, m \in \mathbb{Z}$ with $m > 0$ and r a primitive root modulo m . If i is a positive integer, then

$$\text{ord}_m(r^i) = \frac{\phi(m)}{\gcd(\phi(m), i)}.$$

Proof Let $i, r, m \in \mathbb{Z}$ with $i, m > 0$ and r a primitive root modulo m . Then $\text{ord}_m r = \phi(m)$ by definition. Let $d = (\phi(m), i)$. Then there exists positive integers j, k such that $\phi(m) = dj, i = dk$ and $(j, k) = 1$ by ??. Then using the preceding equations and exponent rules, we find

$$(a^i)^j = (a^{dk})^{\phi(m)/d} = (a^{\phi(m)})^k \equiv 1 \pmod{m}$$

since $a^{\phi(m)} \equiv 1 \pmod{p}$ by definition. ?? says that $\text{ord}_p(a^i) \mid j$.

Since $a^{i \text{ord}_p(a^i)} \equiv (a^i)^{\text{ord}_p(a^i)} \equiv 1 \pmod{p}$ by definition of order, ?? says that $\text{ord}_p a \mid i \text{ord}_p(a^i)$. Since $\text{ord}_p a = \phi(m) = dj$ and $i = dk$, we have $dj \mid dk \text{ord}_p(a^i)$ which simplifies to $j \mid k \text{ord}_p(a^i)$. Since $(j, k) = 1$, we can conclude $j \mid \text{ord}_p(a^i)$.

Since $\text{ord}_p(a^i) \mid j, j \mid \text{ord}_p(a^i)$ and both values are positive, we can conclude that $\text{ord}_p(a^i) = j$. Finally, we have

$$\text{ord}_p(a^i) = j = \frac{\phi(m)}{d} = \frac{\phi(m)}{(\phi(m), i)}.$$

■

Exercises cited in the reading, also on Homework 6:

In-class Problem 2 Prove the following statement, which is the converse of ??:

Let p be prime, and let $a \in \mathbb{Z}$. If every $b \in \mathbb{Z}$ such that $p \nmid b$ is congruent to a power of a modulo p , then a is a primitive root modulo p .

In-class Problem 3 Prove the following generalization of ??

Lemma 1. Let $n \in \mathbb{Z}$ and let x_1, x_2, \dots, x_m be reduced residues modulo n . Suppose that for all $i \neq j$, $\text{ord}_n(x_i)$ and $\text{ord}_n(x_j)$ are relatively prime. Then

$$\text{ord}_n(x_1 x_2 \cdots x_m) = (\text{ord}_n x_1)(\text{ord}_n x_2) \cdots (\text{ord}_n x_m).$$