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.

Read: Uploaded notes, [**?**, Pommersheim-Marks-Flapan, Chapter 10]

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 $\operatorname{ord}_m r = \phi(r)$.

We saw in the reading that primitive roots always exist modulo a prime.

Theorem 1 (Primitive Root Theorem)**.** Let p be prime. Then there exists a primitive root modulo p.

What about composites?

Example 1.
- Since $\phi(6) = \phi(3)\phi(2) = 2$ and $\operatorname{ord}_6 5 = 2$, 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, $\operatorname{ord}_8 1 = 1$ and $\operatorname{ord}_8 3 = \operatorname{ord}_8 5 = \operatorname{ord}_8 7 = 2$.
- Since $\phi(9) = 3^1(3-1) = 6$ by **??**, we check:

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

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

$$4^1 = 4, \qquad 4^2 = 2^4 \equiv 7 \pmod 9, \qquad 4^3 = 2^6 \equiv 1 \pmod 9$$

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

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

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

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

Learning outcomes:

Author(s): Claire Merriman

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

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

is a set of reduced residues modulo m.

This is the general version of Reading Proposition 10.3.2, using exponents $1, 2, \ldots, \phi(m)$ instead of $0, 1, \ldots, \phi(m) - 1$. 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

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

In-class Problem 1 Use only the results through Proposition 1/Reading Lemma 10.3.5 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

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

Proof Let $i, r, m \in \mathbb{Z}$ with $i, m > 0$ and r a primitive root modulo m. Then $\operatorname{ord}_m r = \phi(m)$ 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 proceding 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 $\operatorname{ord}_p(a^i) \mid j$.

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

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

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

$\blacksquare$

Exercises cited in the reading, also on Homework 6:

In-class Problem 2 Prove the following statement, which is the converse of Reading Proposition 10.3.2:

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 Reading Lemma 10.3.5

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

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