Monday, March 11: 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 .

Reading None

Review of ϕ-function (15 minutes)

Remark 1. *From before break, Theorem 3.2 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 *Chapter 2, Exercise 71, using Euler's Generalization of Fermat's Little Theorem and the Chinese Remainder Theorem*

(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 Chinese Remainder Theorem,*

$$x \equiv n^7 \pmod 7$$
$$x \equiv n^7 \pmod 9$$

has a unique solution modulo 63. By Corollary 2.15, $n^7 \equiv n \pmod 7$.

Since $(n, 9) = 1$ and $\phi(9) = 6$, Euler's Generalization of Fermat's Little Theorem 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): Corollary 2.15 only requires the modulus is prime. Euler's Generalization of Fermat's Little Theorem does require $(n, m) = 1$, so you cannot use it for this problem, but $n \equiv 0 \pmod 9$.*

Order of a modulo m (35 minutes)

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* $\text{ord}_m\, a$*, 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	$\operatorname{ord}_7 a$
1	1	1	1	1	1	1
2	4	1	2	4	1	3
3	2	6	4	5	1	6
4	2	1	4	2	1	3
5	4	6	2	3	1	6
6	1	6	1	6	1	2

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 $\operatorname{ord}_m a \mid \phi(m)$.

Proposition (Proposition 5.1)**.** *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 $\operatorname{ord}_m a \mid n$. In particular, $\operatorname{ord}_m a \mid \phi(m)$.*

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 $\operatorname{ord}_m a \mid n$.

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

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

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

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

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

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

by definition of order of a modulo m.

■

Proposition (Proposition 5.2)**.** *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 $i \equiv j \pmod{\operatorname{ord}_m a}$.*

Example 1. *Let $a = 2$ and $m = 7$. Since $\operatorname{ord}_7 2 = 3$, $2^i \equiv 2^j \pmod{7}$ 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 Corollary 2.8, 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 Proposition 5.1, $\operatorname{ord}_m a \mid i - j$. Thus, $i \equiv j \pmod{\operatorname{ord}_m a}$ by definition.

(⇐) *Assume that* $i \equiv j \pmod{3}$. *Then* $3 \mid i-j$ *by definition. Since* $\operatorname{ord}_7 2 = 3$, *Proposition 5.1 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 5.2 Let $a, m \in \mathbb{Z}$ with $m > 0$ and $(a, m) = 1$. Without loss of generality, assume that $i \geq j$ for nonnegative integers i and j.

(⇒) 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 Corollary 2.8, 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 Proposition 5.1, $\operatorname{ord}_m a \mid i-j$. Thus, $i \equiv j \pmod{\operatorname{ord}_m a}$ by definition.

(⇐) Assume that $i \equiv j \pmod{\operatorname{ord}_m a}$. Then $\operatorname{ord}_m a \mid i-j$ by definition, and Proposition 5.1 states that $a^{i-j} \equiv 1 \pmod{m}$. Multiplying both sides of the congruence by a^j gives $a^i \equiv a^j \pmod{m}$.

■

Reading for March 13: Primitive roots modulo p

The original scan on Moodle is a bit hard to read, especially as some parts are annotated and some parts are covered up–since I have not receieved the book from interlibrary loan to re-scan, I will transcribe (incorporating the annotations/references to our textbook and examples.)

Turn in: For each result in the typed or 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 $d = qs$), also note this

Definition of primitive root

If a is a nonzero element of $\mathbb{Z}_7$ (ie, $a \not\equiv 0 \pmod{7}$), then Fermat's Little Theorem tells us that $a^6 \equiv 1 \pmod{7}$. This implies that the order of every element of $\mathbb{Z}_7$ is at most 6. At the beginning of this chapter (Table of exponents modulo 7) we saw that $\operatorname{ord}_7 3 = 6$. We can also say that the element $3 \in \mathbb{Z}_7$ has order 6.

Annotation. The notation $\overline{a} \in \mathbb{Z}_m$ is a more group theory way of writing $a \pmod{m}$, where $\overline{a}$ referes to the congruence class of a modulo m. See Strayer Chapter 2, Example 4.

Definition 2 (Definition 10.3.1)**.** *Let* p *be prime and let* $\overline{a} \in \mathbb{Z}_p$ *with* $a \not\equiv 0 \pmod{p}$. *Then* $\overline{a}$ *is said to be a* primitive root in $\mathbb{Z}_p$ *or* primitive root modulo p *if* $\operatorname{ord}_p a = p - 1$.

Annotation. See also to Strayer Chapter 5, Definition 2.

Remark 3. *Primitive roots may also be defined for* $\mathbb{Z}_n$ *when* n *is composite. (See Paper 3 topics)*

Example 1. (a) *Is* $\overline{2} \in \mathbb{Z}_7$ *a primitive root?*

(b) *Is* $\overline{5} \in \mathbb{Z}_7$ *a primitive root?*

Solution: *Computing powers of* 2 *and* 5 *modulo* 7, *we find*

$$\begin{aligned} 2^1 &\equiv 2 \pmod 7 \\ 2^2 &\equiv 4 \pmod 7 \\ 2^3 &\equiv 1 \pmod 7 \end{aligned} \qquad\qquad \begin{aligned} 5^1 &\equiv 5 \pmod 7 \\ 5^2 &\equiv 4 \pmod 7 \\ 5^3 &\equiv 6 \pmod 7 \\ 5^4 &\equiv 2 \pmod 7 \\ 5^5 &\equiv 3 \pmod 7 \\ 5^6 &\equiv 1 \pmod 7 \end{aligned}$$

(a) *Thus, the order of* $\overline{2}$ *is* 3, *so* $\overline{2}$ *is not a primitive root (in* $\mathbb{Z}_7$*)*

(b) *We see that the order of* $\overline{5}$ *is* 6; *hence,* $\overline{5}$ *is a primitive root (in* $\mathbb{Z}_7$*)*

Example 2. *Determine which elements of* Z_{11} *are primitive roots.*

Annotation. We have not determined the order of elements modulo 11, so here is a chart:

a^1	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	$\operatorname{ord}_{11} a$
1	1	1	1	1	1	1	1	1	1	1
2	4	8	5	10	9	7	3	6	1	10
3	9	5	4	1	3	9	5	4	1	5
4	5	9	3	1	4	5	9	3	1	5
5	3	4	9	1	5	3	4	9	1	5
6	3	7	10	5	8	7	9	2	1	10
7	5	2	3	10	4	6	9	8	1	10
8	9	6	4	10	3	2	5	7	1	10
9	4	3	5	1	9	4	3	5	1	10
10	1	10	1	10	1	10	1	10	1	2

Table 2: Table of exponents modulo 11

Solution: *From Table of exponents modulo* 11, *we determined the orders of all of the nonzero elements of* $\mathbb{Z}_{11}$:

$$\begin{aligned} \operatorname{ord}_{11} 1 &= 1 \\ \operatorname{ord}_{11} 10 &= 2 \\ \operatorname{ord}_{11} 3 &= \operatorname{ord}_{11} 4 = \operatorname{ord}_{11} 5 = \operatorname{ord}_{11} 9 = 5 \\ \operatorname{ord}_{11} 2 &= \operatorname{ord}_{11} 6 = \operatorname{ord}_{11} 7 = \operatorname{ord}_{11} 8 = 10. \end{aligned}$$

Hence, the primitive roots in $\mathbb{Z}_{11}$ *(ie, the primitive roots modulo* 11*) are* $\overline{2}, \overline{6}, \overline{7},$ *and* $\overline{8}$.

Example 3. *Find a primitive root in* $\mathbb{Z}_{17}$*, if one exists.*

Solution: *For want of a better strategy, we will check the orders of the elements* $\overline{1}, \overline{2}, \overline{3}, \ldots,$ *until we find an element of order 16.*

$$\begin{array}{lll}
1^1 \equiv 1 \pmod{17} & 2^1 \equiv 2 \pmod{17} & 3^1 \equiv 3 \pmod{17} \\
 & 2^2 \equiv 4 \pmod{17} & 3^2 \equiv 9 \pmod{17} \\
 & 2^3 \equiv 8 \pmod{17} & 3^3 \equiv 10 \pmod{17} \\
 & 2^4 \equiv 16 \pmod{17} & 3^4 \equiv 13 \pmod{17} \\
 & 2^5 \equiv 15 \pmod{17} & 3^5 \equiv 5 \pmod{17} \\
 & 2^6 \equiv 13 \pmod{17} & 3^6 \equiv 15 \pmod{17} \\
 & 2^7 \equiv 9 \pmod{17} & 3^7 \equiv 11 \pmod{17} \\
 & 2^8 \equiv 1 \pmod{17} & 3^8 \equiv 16 \pmod{17} \\
 & & 3^9 \equiv 14 \pmod{17} \\
 & & 3^{10} \equiv 8 \pmod{17} \\
 & & 3^{11} \equiv 7 \pmod{17} \\
 & & 3^{12} \equiv 4 \pmod{17} \\
 & & 3^{13} \equiv 12 \pmod{17} \\
 & & 3^{14} \equiv 2 \pmod{17} \\
 & & 3^{15} \equiv 6 \pmod{17} \\
 & & 3^{16} \equiv 1 \pmod{17}
\end{array}$$

From the left column, we see that 1 *has order* 1.

From the center column, we see that 2 *has order* 8.

From the right column, we see that the order of 3 *equals* 16, *and we conclude that* 3 *is a primitive root modulo* 17.

We did not actually need to compute all of those powers of 3 *to determine that* 3 *is a primitive root. We know that* $\operatorname{ord}_{17} 3$ *must be a divisor of* $17 - 1 = 16$, *by Proposition 5.1. Once we have computed from* 3^1 *to* 3^8 *and not yet obtained an answer of* 1, *we know* $\operatorname{ord} -173 > 8$. *Since the only divisor of* 16 *that is greater than* 8 *is 16 itself, we can then conclude that* $\operatorname{ord}_{17} 3 = 16$. *(This observation is generalized in Exercise 7.)*

In Exercise 3, we found $\overline{3}$ is a primitive root of $\mathbb{Z}_{17}$ (ie, 3 is a primitive root modulo 17.) Looking again at the column of powers of $\overline{3}$ from the example, observe that these powers cycle through all of the nonzero elements of $\mathbb{Z}_{17}$. That is, every nonzero element is equivalent to $\overline{3}$ raised to some power. This is a general fact about primite roots, which we will now prove.

Proposition (Proposition 10.3.2)**.** *Let* p *be a prime and let* $a \in \mathbb{Z}_p$ *be a primitive root. Then every nonzero* *element of $\mathbb{Z}_p$ appears exactly once on the list*

$$\overline{a}^0, \overline{a}^1, \ldots, \overline{a}^{p-2} \pmod{p}.$$

Annotation. Let p be a prime and let $a \in \mathbb{Z}$ be a primitive root modulo p. Then every integer n where $p \nmid n$ is conguent to exactly one of

$$a^0, a^1, \ldots, a^{p-2} \pmod{p}. \tag{1}$$

Proof First, we show that the elements in the list (1) are distinct. Suppose that

$$a^j \equiv a^k \pmod{p}$$

with j and k in the range $0, \ldots, p-2$. Since $\operatorname{ord}_p a = p - 1$, we know that the two powers of a are equal if and only if the exponents are congruent modulo $p - 1$, by Proposition 5.2. Hence,

$$j \equiv k \pmod{p-1}.$$

But since j and k are restricted to the range $0, \ldots, p-2$, it follows that $j = k$. THus, we have show the elements in list (1) are all distinct.

Note that since $a \not\equiv 0 \pmod{p}$, each element in the like (1) is a nonzero element modulo p. There are $p - 1$ elements in list (1), and we have just shown that these elements are distinct. Since there are exactly $p - 1$ nonzero residues modulo p, list (1) must include every nonzero residue modulo p. ■

Question 2 *In $\mathbb{Z}_{11}$, $\overline{2}$ is a primitive root. Express each of the following elements as $\overline{2}^k$, where k is in the range* $0, \ldots, 9$

(a) $\overline{5}$

(b) $\overline{9}$

The converse of Proposition 10.3.2 is also true. More precisely, if $\overline{a} \in \mathbb{Z}_p$, and if every nonzero element if $\mathbb{Z}_p$ can be expressed as a power of $\overline{a}$, then $\overline{a}$ must be a primitive root. (See Exercise 11.)

Existence of primitive roots in a prime modulus

In Example 3, we asked whether there exists a primitive root in $\mathbb{Z}_{17}$. To solve this, we did not have to search very vary. Although $\overline{1}$ and $\overline{2}$ are not primitive roots we found that $\overline{3}$ is a primitive roots. If we looke for primitive roots modulo other primes, we find a similar situation. For example, modulo 47, we find that 5 is a primitive root, and modulo 293, we find that 2 is a primitive toot, In fact, every prime less that 100 has a primitive root that is less than or equal to 7. Every prime less that 1,000,000 has a primitive root that is less than or equal to 73.

The main result of this chapter is the Primitive Root Theorem, which states that for every prime p, there exists a primitive root modulo p. Although this is easy to state, priving it is quite tricky. So tricky, in fact, that the proof given by the great Leonhard Euler was incorrect. It was Lagrange who gave the first correct proof of the Primitive Root Theorem.

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

To prove the Primitive Root Theorem, we must first prove that in $\mathbb{Z}_{,}$ there exists an element of order $p-1$. Our first step is to prove that there exists an element of order q^s, where q is prime and q^s divides $p-1$. (Numbers of the form q^s where q is prime and $s \in \mathbb{N}$ are called *prime powers.*)

Lemma (Lemma 10.3.4)**.** *Let p be a prime and let q^s be a prime power (where q is prime and $s \geq 1$). If $q^s \mid p-1$, then there exits an element of order q^s modulo p.*

Before proving this lemma, let's see a quick example.

Example 4. *Suppose that $p = 101$. Then $p - 1 = 100 = 2^2(5^2)$, which is divisible by the following prime powers:*

$$2^1 = 2, 2^2 = 4, 5^1 = 5, 5^2 = 25.$$

Thus, Lemma 10.3.4 guarentees that we will find elements of orders $2, 4, 5,$ and 25 modulo 101.

Proof of Lemma 10.3.4 Let p be a prime. Let q be prime and $s \in \mathbb{N}$ such that $q^s \mid p-1$. Consider the following congruences:

$$x^{q^s} \equiv 1 \pmod{p} \tag{2a}$$

$$\text{and } x^{q^{s-1}} \equiv 1 \pmod{p}. \tag{2b}$$

By Proposition 5.8, equation (2a) has q^s solutions and equation (2b) has q^{s-1} solutions. Since $q^s > q^{s-1}$, there must be at least one $a \in \mathbb{Z}$ that is a solution to (2a) and not (2b). That is,

$$a^{q^s} \equiv 1 \pmod{p} \tag{3a}$$

$$\text{but } a^{q^{s-1}} \not\equiv 1 \pmod{p}. \tag{3b}$$

Claim 1. *a has order q^s.*

Proof of Claim 1 By equation (3a), it follows (using Proposition 5.1) that $\operatorname{ord}_p a$ divides q^s. Thus, the order of a modulo p is one of the numbers in the list

$$1, q, q^2, \ldots, q^{s-1}, q^s. \tag{4}$$

However, from (3b), it follows (again using Proposition 5.1) that $\operatorname{ord}_p a$ does not divide q^{s-1}. Since the only number in list (4) that does not divide q^{s-1} is q^s, we conclude that the order of a modulo p is q^s.

Thus, we have found an integer a with order q^s modulo p. ■

Suppose we want to know whether $\mathbb{Z}_{101}$ has primitive root–that is, an element of order 100. Lemma 10.3.4 tells us that there is an element $\overline{a}$ of order 4, and element b of order 25 (see Example 4). It turns out that the product $\overline{ab}$ will have order $4 \cdot 25 = 100$ and hence, $\overline{ab}$ is the primitive root we seek. This is guarenteed by the following lemma.

Lemma (Lemma 10.3.5)**.** *Let $n \in \mathbb{N}$, and let $\overline{a}, \overline{b} \in \mathbb{Z}_n$ be reduced residues (see: reduced residue system modulo m). If $\operatorname{ord}_n a$ and $\operatorname{ord}_n b$ are relatively prime, then*

$$\operatorname{ord}_n(ab) = (\operatorname{ord}_n a)(\operatorname{ord}_n b).$$

Proof On Homework 6–Strayer Chapter 5, Exercise 5a. ■

In Example 4, we used Lemma 10.3.4 to determine that $\mathbb{Z}_{101}$ has orders 4 and 25. By Lemma 10.3.5, the product of these elements has order 100, os it is a primitive root. We will use this same argument, which combines Lemma 10.3.4 and Lemma 10.3.5 to give a general proof of the Primitive Root Theorem.

Proof of Primitive Root Theorem Let p be prime.

If $p = 2$, then 1 is a primitive root modulo p. Thus, we may assume $p > 2$.

Factor $p - 1$ into primes:

$$p - 1 = q_1^{a^1} q_1^{a_2} \cdots q_m^{a_m}.$$

By Lemma 10.3.4, for each $k = 1, 2, \ldots, m$, there exists an integer x_k of order $q_k^{a_k}$ modulo p. Let

$$x \equiv x_1 x_2 \cdots x_m \pmod{p}.$$

Applying Lemma 10.3.5 repeatedly (see Exercise 14), we find

$$\begin{aligned}\operatorname{ord}_p x &= (\operatorname{ord}_p x_1)(\operatorname{ord}_p x_2) \cdots (\operatorname{ord}_p x_m)\\ &= q_1^{a^1} q_1^{a_2} \cdots q_m^{a_m}\\ &= p - 1\end{aligned}$$

Hence, x is a primitive root modulo p. ■

We have now proved that $\mathbb{Z}_p$ always has at least one primitive root, but as we have seen, $\mathbb{Z}_p$ often has more than one primitive root. It turns out that once we know *one* primitive root in $\mathbb{Z}_p$, it is easy to find all primitive roots in $\mathbb{Z}_p$. The following lemma tells us how to do this.

Lemma (Lemma 10.3.6)**.** *Let p be prime, and let $a \in \mathbb{Z}$ be a primitive root modulo p. Then for any $j \in \mathbb{Z}$, a^j is a primitive root modulo p if and only if* $\gcd(j, p-1) = 1$.

Proof Let p be prime, and let $a \in \mathbb{Z}$ be a primitive root modulo p.

By Proposition 5.4,

$$\operatorname{ord}_p(a^j) = \frac{p-1}{\gcd(j, p-1)}.$$

Thus, $\operatorname{ord}_p(a^j) = p - 1$ if and only if $\gcd(j, p-1) = 1$. ■

Naomi's Numerical Proof Preview: Theorem 10.3.7

Let's see whether we can use this llemma to determine how many primitive roots there are modulo 19. Let $\overline{a} \in \mathbb{Z}_{19}$ be a primitive root (modulo 19). Then the nonzero elements of $\mathbb{Z}_{19}$ are

$$\overline{a}^0, \overline{a}^1, \overline{a}^2, \ldots, \overline{a}^{17}.$$

Lemma 10.3.6 tells us which of these elements are primitive roots modulo 19: precisely those in which the exponent is relatively prime to 18. Thus, the primitive roots modulo 19 are

$$\overline{a}^1, \overline{a}^5, \overline{a}^7, \overline{a}^{11}, \overline{a}^{13}, \overline{a}^{17}.$$

We see then that the primitive roots modulo 19 correspond to the exponents $1, 5, 7, 11, 13$ and 17, which are the positive integers less than 18 which are relatively prime to 18. The nunber of such integers is exactly $\phi(18) = 6$. In general, we have the following theorem.

Theorem (Theorem 10.3.7)**.** *Let p be prime. Then there are exactly $\phi(p-1)$ primitive roots modulo p.*

Proof Let $a \in \mathbb{Z}$ be a primitive root modulo p. Then by Proposition 10.3.2, we know that the list of reduced residues modulo p comprises the elements

$$a^0, a^1, a^2, \ldots, a^{p-2}$$

By Lemma 10.3.6, an integers a^j is a primitive root modulo p if and only if $\gcd(j, p-1) = 1$. Thus, the number of primitive roots equals the number of positive integers j that are less than $p-1$ and relatively prime to $p-1$. By definition, this is exactly $\phi(p-1)$. ■

Referenced Exercises

Exercise 3 *(Exercise 11) Prove the following statement, which is the converse of Proposition 10.3.2:*

Let p be prime, and let $\overline{a} \in \mathbb{Z}_p$. If every nonzero element of $\mathbb{Z}_p$ is a power of $\overline{a}$, then $\overline{a}$ is a primitive root (modulo p).

Exercise 4 *(Exercise 14) Prove the following generalization of Lemma 10.3.5*

Lemma. *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*

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

Wednesday, March 13: 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 .

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.

Primitive roots and comparing Strayer to the reading

Definition 3 (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. What about composites?

Example 5.

- *Since $\phi(4) = 2$, and $\operatorname{ord}_4 3 = 2$, 3 is a primite 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* $\operatorname{ord}_6 5 = 2$, 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 Theorem 3.3,* $\phi(8) = 4$. *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 Theorem 3.3, 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 Proposition 5.2 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* $5i \equiv j \pmod 6$.

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

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

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

Proposition (Proposition 5.3). *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 Proposition 10.3.2, using exponents $1, 2, \ldots, \phi(m)$ instead of $0, 1, \ldots, \phi(m)-1$. Since Strayer's statement of Proposition 5.2 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 (Proposition 5.4). *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 5 *Use only the results through Proposition 5.3/Lemma 10.3.5 to prove the primitive root version:*

Proposition. *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 Proposition 1.10. 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. Proposition 5.1 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, Proposition 5.1 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

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

■

Exercises cited in the reading, also on Homework 6:

In-class Problem 6 *Prove the following statement, which is the converse of 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 7 *Prove the following generalization of Lemma 10.3.5*

Lemma. *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*

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

Friday, March 15: Lagrange's Theorem

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

- Prove Lagrange's Theorem .

Reading Strayer Section 5.2

Turn in: (a) Exercise 10a: Determine the number of incongruent primitive roots modulo 41

Solution: Since 41 is prime, Theorem 10.3.7 says there are $\phi(41) = 40$ primitive roots modulo 41.

(b) Exercise 11a: Find all incongruent integers having order 6 modulo 31.

Solution: From Appendix E, Table 3, 3 is a primitive root modulo 31. By Proposition 5.4, the elements of order 6 modulo 31 are those where

$$6 = \operatorname{ord}_{31}(3^i) = \frac{\phi(31)}{(\phi(31), i)} = \frac{30}{5}.$$

The positive integers less than 31 where $(30, i) = 5$ are $i = 5, 25$. So the elements of order 6 are $3^5, 3^{25}$.

The problem does not ask for the least nonnegative residues. However, we can also find those:

$$3^5 \equiv (-4)(9) \equiv -5 \equiv 26 \pmod{31}$$

$$3^{25} \equiv (-5)^5 \equiv (-6)^2(-5) \equiv -25 \equiv 6 \pmod{31}$$

Quiz (10 minutes)

Lagrange's Theorem

The goal is to finish proving the Primitive Root Theorem with a look at polynomials.

Theorem (Theorem 5.7 (Lagrange))**.** *Let p be a prime number and let*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

for integers $a_0, a_1, \ldots, a_n$. Let d be the greatest integer such that $a_d \not\equiv 0 \pmod{p}$t then d is the degree of $f(x)$ modulo p. *Then the congruence*

$$f(x) \equiv 0 \pmod{p}$$

has at most d incongruent solutions. We call these solutions roots of $f(x)$ modulo p.

Proof from class We proceed by induction on the degree d.

First, for degree $d = 0$, note that $f(x) \equiv a_0 \not\equiv 0 \pmod{p}$ by assumption, so $f(x) \equiv 0 \pmod{p}$ for 0 integers.

Base Case: $d = 1$**.** Then $f(x) \equiv a_1 x + a_0 \pmod{p}$. Since $a_1 \not\equiv 0 \pmod{p}$ by assumption, $p \nmid a_1$. Since p is prime, $(a_1, p) = 1$. Thus, by Corollary 2.8, there is a unique solution modulo p to $a_1 \not\equiv 0 \pmod{p}$.

Induction Hypothesis: Assume that for all $k < d$, if $f(x)$ has degree k modulo p, then

$$f(x) \equiv a_k x^k + a_{k-1}x^{k-1} + \cdots + a_1 x + a_0 \equiv 0 \pmod{p}$$

has at most k incongruent solutions.

We will proceed by contradiction. That is, assume that there exists $f(x)$ with degree d modulo p and at least $d+1$ roots modulo p. Call these roots $r_1, r_2, \ldots, r_d, r_{d+1}$. Consider the polynomial

$$g(x) = a_d(x - r_1)(x - r_2)\cdots(x - r_d).$$

Then $f(x)$ and $g(x)$ have the same leading term modulo p. The polynomial $h(x) = f(x) - g(x)$ is either the 0 polynomial or it has degree less than d modulo p.

If $h(x)$ is the 0 polynomial, then

$$h(r_1) \equiv h(r_2) \equiv \cdots \equiv h(r_{d+1}) \equiv 0 \pmod{p}$$

and

$$f(r_1) \equiv f(r_2) \equiv \cdots \equiv f(r_{d+1}) \equiv 0 \pmod{p}$$

implies

$$g(r_1) \equiv g(r_2) \equiv \cdots \equiv g(r_{d+1}) \equiv 0 \pmod{p}.$$

That is,

$$a_d(r_{d+1} - r_1)(r_{d+1} - r_2)\cdots(r_{d+1} - r_d) \equiv 0 \pmod{p}.$$

Since p is prime, repeated applications of Homework 4, Problem 9a gives that one of $a_d, r_{d+1} - r_1, r_{d+1} - r_2, \ldots, r_{d+1} - r_d$ is 0 modulo p. Now, $a_d \not\equiv 0 \pmod{p}$ by assumption, and the r_i are distinct modulo p, so we have a contradiction. Thus, $h(x)$ is not the 0 polynomial.

Since $r_1, r_2, \ldots, r_d$ are roots of both $f(x)$ and $g(x)$, they are also roots of $h(x)$. This contradicts the induction hypothesis, since $h(x)$ has degree less than d by construction.

Thus, $f(x)$ has at most d incongruent solution modulo p. ■

Modified proof from Strayer We proceed by induction on the degree d.

First, for degree $d = 0$, note that $f(x) \equiv a_0 \not\equiv 0 \pmod{p}$ by assumption, so $f(x) \equiv 0 \pmod{p}$ for 0 integers.

Base Case: $d = 1$. Then $f(x) \equiv a_1x + a_0 \pmod{p}$. Since $a_1 \not\equiv 0 \pmod{p}$ by assumption, $p \nmid a_1$. Since p is prime, $(a_1, p) = 1$. Thus, by Corollary 2.8, there is a unique solution modulo p to $a_1 \not\equiv 0 \pmod{p}$.

Induction Hypothesis: Assume that for all $k < d$, if $f(x)$ has degree k modulo p, then

$$f(x) \equiv a_kx^k + a_{k-1}x^{k-1} + \cdots + a_1x + a_0 \equiv 0 \pmod{p}$$

has at most k incongruent solutions.

If the congruence $f(x) \equiv 0 \pmod{p}$ has no solutions we are done. Otherwise, assume that there exists at least one solution, say a. Dividing $f(x)$ by $(x - a)$ gives

$$f(x) \equiv (x - a)q(x) \pmod{p}$$

where $q(x)$ is a polynomial of degree $d - 1$ modulo p. Since $q(x)$ has at most $d - 1$ roots modulo p by the induction hypothesis, there are at most $d - 1$ incongruent additional roots of $f(x)$ modulo p. Thus, there are a total of at most d incongruent roots modulo p. ■

Proposition (Proposition 5.8)**.** *Let p be prime and m a positive integer where $m \mid p-1$. Then*

$$x^m \equiv 1 \pmod{p}$$

has m incongruent solutions modulo p.

Proof Let p be prime and m a positive integer where $m \mid p-1$. Then there exists $k \in \mathbb{Z}$ such that $mk = p-1$. Then

$$x^{p-1} - 1 = (x^m - 1)(x^{(k-1)m} + x^{(k-2)m} + \cdots + x^{2m} + x^m + 1)$$

By Fermat's Little Theorem, there are $p-1$ incongruent solutions to $x^{p-1} - 1 \equiv 0 \pmod{p}$, namely $1, 2, \ldots, p-1$. We will show that m of these are solutions to $x^m - 1 \equiv 0 \pmod{p}$ and the rest are solutions to $x^{(k-1)m} + x^{(k-2)m} + \cdots + x^{2m} + x^m + 1 \equiv 0 \pmod{p}$.

By Theorem 5.7 (Lagrange), there are at most $(k-1)m$ solutions to $x^{(k-1)m} + x^{(k-2)m} + \cdots + x^{2m} + x^m + 1 \equiv 0 \pmod{p}$. Thus, there are at least $p - 1 - (k-1)m = m$ incongruent solutions to $x^m - 1 \equiv 0 \pmod{p}$. Since there are also at least m incongruent solutions to $x^m - 1 \equiv 0 \pmod{p}$ by Theorem 5.7 (Lagrange), there are exactly m incongruent solutions to $x^m - 1 \equiv 0 \pmod{p}$ and thus $x^m \equiv 1 \pmod{p}$. ■

Definition 4 (Roots of unity)**.** *Let p be prime and m a positive integer. We call the solutions to*

$$x^m \equiv 1 \pmod{p}$$

the m^{th} roots of unity modulo p*.*