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* $\mathrm{ord}_m\, a$*, 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	$\text{ord}_7 a$
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 $\text{ord}_m a \mid \phi(m)$.

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 $\text{ord}_m a \mid n$. 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 Division Algorithm, 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 (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 $i \equiv j \pmod{\text{ord}_m a}$.*

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 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, $\text{ord}_m a \mid i - j$. 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* $\operatorname{ord}_7 2 = 3$, *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.

($\Rightarrow$) 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 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.

($\Leftarrow$) 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 $a^i \equiv a^j \pmod m$.

■

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 2 (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 2.
- *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* $5i \equiv j \pmod 6$.

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

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

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

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*

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

In-class Problem 2 *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*

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

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 3 *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 4 *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

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

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 $f(x) \equiv a_1 x + a_0 \pmod p$. 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.

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 3 (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.