An Introduction to Orders and Primitive Roots

27 January 2025

This handout will cover the basics of orders and primitive roots. The sections are brief with a handful of nice exercises. You should do all the exercises or at least read the solutions since there are solutions to all of them. Exercises and Problems marked with a * are extremely difficult and almost definitely require the reader to read the solution.

§1 The Order of an Integer

Definition 1.1. Letting n be a positive integer such that $n > 1$ and the $gcd(a, n) = 1$, we define the order of $a \pmod n$ to be the smallest positive integer k such that

$$a^k \equiv 1 \pmod n$$

The largest possible value of the order of $a \pmod n$ is $\phi(n)$ because by Euler's Totient Theorem, we always have

$$a^{\phi(n)} \equiv 1 \pmod n$$

Currently, we don't have any tools to find the order of any integer $a \pmod n$ and we need to brute force the integers $2, 3, \ldots, n-2$ to find the order. The first theorem can help us find them easier and is of great importance.

Theorem 1.2

If the order of $a \pmod n$ is k then $a^m \equiv 1 \pmod n$ if and only if $k \mid m$. In other words, the order of $a \pmod n$ must divide m.

Proof. We need to show both that if $k \mid m$, $a^m \equiv 1 \pmod n$ and if $a^m \equiv 1 \pmod n$ then $k \mid m$.

If $k \mid m$, then for some integer j,

$$a^k \equiv a^{hj} \equiv 1^j \equiv 1 \pmod n$$

If $a^m \equiv 1 \pmod n$, by the division algorithm, $m = qk + r$ and

$$a^m \equiv a^{qk+r} \equiv (a^q)^k a^r \equiv a^r \equiv 1$$

Since r is less than k, and k is the order, r cannot be the order of $a \pmod n$, $r = 0$. As a result $k \mid m$.

□

From this we know that the order of $a \pmod n$ always divide $\phi(n)$ since $m = \phi(n)$ always work. This is very important!

Example 1.3
Find the order of 3 (mod 14).

Solution. By Theorem 1.2, we know that the order divides $\phi(14) = 6$. Testing the divisors which are 1, 2, 3, 6, we get

$$3^1 \equiv 3 \pmod{14}$$
$$3^2 \equiv 9 \pmod{14}$$
$$3^3 \equiv -1 \pmod{14}$$
$$3^6 \equiv 1 \pmod{14}$$

As a result, the order of 3 (mod 14) is 6; □

Theorem 1.4
If the order of $a \pmod{n}$ is k, then $a^x \equiv a^y \pmod{n}$ if and only if $x \equiv y \pmod{k}$.

Proof. If $a^x \equiv a^y \pmod{n}$,

$$a^{x-y} \equiv 1 \pmod{n}$$

By Theorem 1.2, $k \mid x - y$ and $x \equiv y \pmod{k}$.

If $x \equiv y \pmod{k}$, we can use the division algorithm to get

$$a^x \equiv a^{y+qk} \equiv a^y \pmod{n}$$

since a^k is congruent to 1.

□

For example, since 3 (mod 14) is 6, 3^1 and 3^7 have the same remainder modulo 14.

Below are a few exercises that you should do! There are solutions to all of the exercises and problems in the back of the handout!

Exercise 1.5. Prove that for positive integers $a > 1$ and for any positive integers n

$$n \mid \phi(a^n - 1)$$

Exercise 1.6. Show that the odd prime divisors of an integer n^2+1 are always congruent to 1 (mod 4).

Exercise 1.7. Show that if an integer a has order k mod n, then a^h will have order of $\frac{k}{gcd(h,k)}$ mod n.

Exercise 1.8. Show that if a has order h mod n and b has order k mod n such that $gcd(h, k) = 0$, then that the order of ab is hk mod n.

Exercise 1.9. Prove that given odd primes q and p such that $q \mid a^p - 1$, then for some integer a and k, either $q \mid (a - 1)$ or $q = 2kp + 1$.

§2 Primitive Roots

Definition 2.1. If the order of $a \pmod n$ is $\phi(n)$, then a is a primitive root mod n.

Example 2.2
What is one primitive root modulo 5?

Solution. We can see that 2 is a primitive root modulo 5 as we can see because 2 has order 4.

$$2^1 \equiv 2 \pmod 5$$
$$2^2 \equiv 4 \pmod 5$$
$$2^3 \equiv 3 \pmod 5$$
$$2^4 \equiv 1 \pmod 5$$

□

There are quite a a few important and interesting theorems regarding primitive roots and in this section we will introduce a few of them.

Theorem 2.3
If g is a primitive root mod n, then the set $\{g^1, g^2, \ldots, g^{\phi n-1}\}$ contains the positive integers that are relatively prime to n and less than n.

Proof. Lets assume that there are some i and j such that

$$g^i \equiv g^j \pmod n$$

Let k be the order of $g \pmod n$. By Theorem 1.4, we know that

$$i \equiv j \pmod k$$

Since g by definition is a primitive root, $k = \phi(n)$. Since both i and j is less than $\phi(n)$, for them to be congruent they need to be equal. As a result they are the same number. □

Theorem 2.4
If there exists a primitive root mod n, then there are exactly $\phi(\phi(n))$ primitive roots mod n.

Proof. From Theorem 2.3, once we know that there is a primitive root g mod n, we can find all the other primitive roots in the set $\{g^1, g^2, \ldots, g^{\phi n-1}\}$.

By Exercise 1.7, for g^h for some h to be also a primitive root, $\frac{\phi(n)}{gcd(\phi(n),h)} = \phi(n)$. As a result, we need to find the number of integers so that $\phi(n)$ and h are relatively prime and also less than $\phi(n)$. The answer is therefore just $\phi(\phi(n))$. □

Theorem 2.5

2, 4, p, p^k and $2p^k$ are the only numbers with primitive roots for a some odd prime p and some positive integer k.

We will exclude the proof for this as it is quite long and tedious.

Corollary 2.6

There are exactly $\phi(n-1)$ incongruent primitive roots of a prime p.

Proof. Follows directly from Theorem 2.4 and 2.5, □

Now we generally know how many primitive roots are there modulo n and an interesting property about them but how do we actually find them? Well, you'll learn how to find them in the exercises!

Exercise 2.7. How many primitive roots does 12 have? How many primitive roots does 7 have?

Exercise 2.8. Prove that for $k \geq 3$, 2^k has no primitive roots.

(a) Try to find integers that are primitive roots of 2^3 and 2^4. See anything interesting?

(b) Look at the powers, for what powers x does $a^x \equiv 1 \pmod{2^k}$?

(c) Prove that for $k \geq 3$, 2^k has no primitive roots. (Don't use Theorem 2.5)

Exercise 2.9. Show that if p is an odd prime then p^k and $2p^k$ has the same number of primitive roots.

Exercise 2.10. Which of the following integers have primitive roots? 33, 338, 289, 64

Exercise 2.11. Prove that $x^2 \equiv 1 \pmod{p}$ only have the incongruent positive solutions 1 and -1 for some prime p.

Exercise 2.12. Show that if p is prime and for some primitive root g that

$$g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

Exercise 2.13. For any positive integer k and prime number p, find the value of

$$1^k + 2^k + 3^k + \cdots + (p-1)^k \pmod{p}$$

Exercise 2.14. If a is a perfect square, can it be a primitive root mod p? Prove or disprove it.

§3 Some Extra Problems

Problem 3.1. Show that $n \nmid 2^n - 1$ for $n > 1$.

Problem 3.2 (AIME I 2019)**.** Find the least odd prime factor of $2019^8 + 1$.

Problem 3.3. Prove that the inverse of a primitive root g modulo n is also a primitive root.

Problem 3.4. Show that any prime factors of $2^{2^n} + 1$ minus one divides 2^{n+1}.

§4 Solutions

1.5 Prove that for positive integers $a > 1$ and for any positive integers n

$$n \mid \phi(a^n - 1)$$

Solution. The order of $a \pmod{a^n - 1}$ is n because n is the first power for which a is greater than $a^n - 1$ and coincidentally, it is congruent to 1 modulo $a^n - 1$. By Theorem 1.2, n divides $a^n - 1$. □

1.6 Show that the odd prime divisors of an integer $n^2 + 1$ are always congruent to 1 (mod 4).

Solution. Once again, Theorem 1.2 will be our friend here. We have that

$$n^2 \equiv -1 \pmod{p}$$

$$n^4 \equiv 1 \pmod{p}$$

Therefore, 4 is the order of $n \pmod{p}$. Now by Theorem 1.2, $4 \mid \phi(p) \implies 4 \mid (p-1) \implies p \equiv 1 \pmod{4}$ □

1.7 Show that if an integer a has order k mod n, then a^h will have order of $\frac{k}{gcd(h,k)}$ mod n.

Solution. Let $h_0 = \frac{h}{gcd(h,k)}$ and $k_0 = \frac{k}{gcd(h,k)}$.

We have that,

$$(a^h)^{k_0} \equiv (a^k)^{h_0} \equiv 1^{h_0} \equiv 1 \pmod{n}$$

If the order of a^h mod n is x, the above equation shows that $x \mid k_0$.

Since $k \mid hx$, we should have $k_0 \mid h_0 x$ but since k_0 and h_0 share no common factors, $k_0 \mid x$.

As we have both $k_0 \mid x.$ and $x \mid k_0$, $x = k_0 = \frac{k}{gcd(h,k)}$ □

1.8 Show that if a has order h mod n and b has order k mod n such that $gcd(h,k) = 0$, then that the order of ab is hk mod n.

Solution. It is easy to see that $ab^{hk} \equiv 1 \pmod{n}$. We therefore have that if ab modulo n has order x, then $x \mid hk$.

We can also see that

$$1 \equiv ab^{kx} \equiv a^{kx}(b^k)^x \equiv (a^k)^x \pmod{n}$$

$$1 \equiv ab^{hx} \equiv (a^h)^x b^{hx} \equiv (b^h)^x \pmod{n}$$

From Exercise 1.7, we know that the order of a^k is h we know that the order of b^h is k. From Theorem 1.2, that $h \mid x$ and $k \mid x$.

The smallest possible value of x that satisfy those conditions is $lcm(h,k)$ and since $gcd(h,k) = 1$, $x = hk$.

□

1.9 Prove that given odd primes q and p such that $q \mid a^p - 1$, then for some integer a and k, either $q \mid (a-1)$ or $q = 2kp + 1$.

Solution.

$$q \mid a^p - 1 \implies a^p \equiv 1 \pmod{q}$$

Since p is prime, p should be a multiple of the order. Therefore the order is either 1 or p. In the first case we have

$$a \equiv 1 \pmod{q} \implies q \mid (a-1)$$

In the second case,

$$p \mid \phi(q)$$
$$p \mid (q-1)$$

$q-1$ is even so $2p \mid (q-1)$. Therefore, $q - 1 = 2kp \implies q = 2kp + 1$ □

2.7 How many primitive roots does 12 have? How many primitive roots does 7 have?

Solution. $\phi(12) = 4$ so we can just check powers of 2 of $5, 7, 11$.

$$5^2 \equiv 1 \pmod{12}$$
$$7^2 \equiv 1 \pmod{12}$$
$$11^2 \equiv 1 \pmod{2}$$

As a result 12 do not have any primitive roots. □

2.8 Prove that for $k \geq 3$, 2^k has no primitive roots.

Solution. After playing with the powers of 2, we noticed that for $a^2 \equiv 1 \pmod 8$ and $a^4 \equiv 1 \pmod{16}$ where a is an odd integer. (The numbers relatively prime to the powers of 2 are all the odd integers).

This might us to think that $a^{2^{k-2}} \equiv 1 \pmod{2^k}$ for all $k \geq 3$.

Lets prove this by induction. When $k = 3$, we can brute force to see that $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod{2^3}$.

Lets now show that it is true for all k.

$$2^{2^{k-2}} \equiv 1 \pmod{2^k}$$
$$2^{2^{k-2}} = 1 + m2^k$$
$$2^{2^{k-1}} = (1 + m2^k)^2$$
$$2^{2^{k-1}} = 1 + m2^{k+1} + m^2 2^{2k}$$
$$2^{2^{k-1}} = 1 + 2^{k+1}(m + m^2 2^{k-1})$$
$$2^{2^{k-1}} \equiv 1 \pmod{2^{k+1}}$$

□

2.9 *Solution.* Theorem 2.4 tell us that p^k has $\phi(\phi(p^k)) = \phi(p^k - p^{k-1})$ primitive roots and $2p^k$ has $\phi(\phi(2p^k))$ primitive roots. Since p is an odd prime $\phi(\phi(2p^k)) = \phi(p^k - p^{k-1}) = \phi(\phi(p^k))$ □

2.10 Which of the following integers have primitive roots? 33, 338, 289, 64.

Solution. $33 = 11 * 3$, $338 = 2 * 13^2$, $289 = 17^2$, $64 = 2^6$. Theorem 2.5 now tell us that 33, 338 and 289 have primitive roots. □

2.11 Prove that $x^2 \equiv 1 \pmod{p}$ only have the incongruent solutions 1 and -1 for some prime p.

Solution.

$$x^2 - 1 \equiv 0 \pmod{p}$$
$$(x-1)(x+1) \equiv 0 \pmod{p}$$
$$p \mid (x-1) \text{ or } p \mid (x+1)$$
$$x = 1, -1$$

□

2.12 Show that if p is prime and for some primitive root g that

$$g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

Solution. We will use the previous exercise to solve this. Let $x = g^{(p-1)/2}$. We then have

$$x^2 \equiv 1 \pmod{p}$$

We know that $x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$ and that $g^{(p-1)/2}$ is either 1 or -1. The former case will contradict the fact that g is a primitive root so we then have that its equal to -1. □

2.13 For any positive integer k and prime number p, find the value of

$$1^k + 2^k + 3^k + \cdots + (p-1)^k \pmod{p}$$

Solution. Recall Theorem 2.3. We can rewrite the congruence as

$$g^k + g^{2k} + g^{3k} + \cdots + g^{(p-1)k} \pmod{p}$$

This is merely a geometric series so we can write it as

$$\frac{g(1-g^{p-1})}{1-g}$$

$g^{p-1} = 1$ so the entire term equals 0. Be careful though as if $g \equiv 1 \pmod{p}$, it is undefined. The only time when this happen $(p-1) \mid k$.

Therefore, $1^k + 2^k + 3^k + \cdots + (p-1)^k \equiv 0 \pmod{p}$ when $(p-1) \not\equiv k$ and -1 otherwise since the terms are equal 1 and there are $p-1$ of them. □

2.14 If a is a perfect square, can it be a primitive root mod p? Prove or disprove it.

Solution. $a = b^2$ for some b. Using Exercise 2.12 $a^{(p-1)/2}$ should be congruent to -1 mod p but

$$a^{(p-1)/2} \equiv b^{p-1} \equiv 1 \pmod{p}$$

□

3.1 Show that $n \nmid 2^n - 1$ for $n > 1$.

Solution. Suppose that there are some n such that $n \mid 2^n - 1$. Then for a prime divisor of p or n, $p \mid n \mid 2^n - 1$. We then have the following congruences:

$$2^n \equiv 1 \pmod{n} \implies 2^n \equiv 1 \pmod{p}$$

$$2^{p-1} \equiv 1 \pmod{p}$$

We need the order of 2 modulo p to divide both n and $p-1$. But $p-1$ is relatively prime to p and therefore is also relatively prime to n. Consequently, $n \nmid 2^n - 1$. □

3.2 Find the least odd prime factor of $2019^8 + 1$.

Solution. Let the prime factor be p.

$$2019^8 + 1 \equiv 0 \pmod{p}$$

$$2019^8 \equiv -1 \pmod{p}$$

$$2019^{16} \equiv 1 \pmod{p}$$

The order of 2019 mod p is 16 because the other possible $1, 2, 4, 8$ that divides 16 results in $2019^8 \equiv 1 \pmod{p}$ because they are divisors of 8.

Now, the order divides $\phi(p) = p - 1$. Checking for primes such that $p \equiv 1 \pmod{16}$. The first prime we found is 17. Be careful though as we have only show that 17 is possible.

$$2019^8 \equiv 13^8 \equiv -4^8 \equiv -2^{16} \equiv 1 \pmod{17}$$

which does not work.

The next prime we found thatch congruent to 1 mod 16 is 97. Testing for it again,

$$2019^8 \equiv 79^8 \equiv -18^8 \equiv 324^4 \equiv 33^4 \equiv 1089^2 \equiv 22^2 \equiv -1 \pmod{97}$$

We have found 97 to be the smallest prime factor of $2019^8 + 1$. □

3.3 Prove that the inverse of a primitive root g modulo n is also a primitive root.

Solution. It is easy to see that if the order of g^-1 is k, then k divides $\phi(n)$ but if $k < \phi(n)$ it implies that g^k is congruent to 1 modulo n, contradicting the statement that it is a primitive root. □

3.4 Show that any prime factors of $2^{2^n} + 1$ minus one divides 2^{n+1}.

Solution. Let any prime factor of be p and the order of 2 mod p be k. Then,

$$2^{2^n} \equiv -1 \pmod{p}$$

$$2^{2^{n+1}} \equiv 1 \pmod{p}$$

$$k \mid 2^{n+1}$$

The possible orders are $2^0, 2^1, \ldots, 2^{n+1}$. If $k < 2^0, 2^1, \ldots, 2^n$, it implies that $2^{2^n} \equiv 1 \pmod{p}$ which contradicts our first congruence so the $k = 2^{n-1}$ and we have $2^{n+1} \mid p$. □