Orders and Primitive Roots

Minseok Eli Park

August 2020

§1 Orders

Before we begin, what are orders?

Definition 1.1. For relatively prime integers a and m, the *order* of an integer $a \mod m$ is the smallest positive integer x such that
$$a^x \equiv 1 \mod m$$

This is denoted as $x = \text{ord}_m a$

Most times, we use orders with m replaced with a prime p, but it is still important to know its general form.

Let's take a look at a quick example, to familiarize ourselves with orders.

Problem 1.2 — What is the order of $3 \mod 11$?

Solution. We make a table comparing x and $3^x \mod 11$.

x	1	2	3	4	5
$3^x \mod 11$	3	9	5	4	1

So we see that 5 is the smallest value of x such that $3^x \equiv 1 \mod 11$, meaning $\text{ord}_{11}3 = \boxed{5}$

□

§2 Main Theorem of Orders

This theorem is at the heart of most problems involving orders.

Theorem 2.1
For relatively prime integers a and m and integer n, $a^n \equiv 1 \mod m$ if and only if $\text{ord}_m a \mid n$

Proof. First, if $\text{ord}_m a | n$, then we let $n = k\text{ord}_m a$ for some positive integer k. Then, we have as follows.

$$a^{\text{ord}_m a} \equiv 1 \mod m$$
$$(a^{\text{ord}_m a})^k \equiv 1^k \mod m$$
$$a^{k\text{ord}_m a} \equiv 1 \mod m$$
$$a^n \equiv 1 \mod m$$

Now, we prove the other direction, which assumes $a^n \equiv 1 \mod m$.

Let $n = k \cdot \text{ord}_m a + r$ where r is the remainder after dividing n by $\text{ord}_m a$. We want to prove $r = 0$.

$$a^n \equiv 1 \mod m$$
$$a^{k\text{ord}_m a + r} \equiv 1 \mod m$$
$$(a^{\text{ord}_m a})^k * a^r \equiv 1 \mod m$$
$$1 * a^r \equiv 1 \mod m$$
$$a^r \equiv 1 \mod m$$

If r is positive, this contradicts the fact that $x = \text{ord}_m a$ is the smallest positive integer x such that $a^x \equiv 1 \mod m$. So, r must be 0, and we are done. □

Although the above is our main theorem, the really commonly used corollary is stated below. To be even more specific, the form replacing m with a prime p is most relevant.

Corollary 2.2
For relatively prime integers a and m, $\text{ord}_m a \mid \phi(m)$.

Proof. By Fermat's Little Theorem, we have

$$a^{\phi(m)} \equiv 1 \mod m$$

So, replacing n with $\phi(m)$ in the above theorem completes the corollary. □

§3 Examples

As with the rest of contest math, the best way to learn is to do some examples. Let's look at a few.

Problem 3.1 (2019 AIME I #14) — Find the least odd prime factor of $2019^8 + 1$

Solution. Let $2019^8 \equiv -1 \mod p$ for some odd prime p. We want to find the smallest possible value of p.

Squaring both sides give $2019^{16} \equiv 1 \mod p$, so $\text{ord}_p 2019 \mid 16$.

But, by given, $2019^8 \equiv -1 \mod p$ and $p \neq 2$, so $\text{ord}_p 2019 \neq 8$. This must mean $\text{ord}_p 2019 = 16$.

By Theorem 2.1, we have that $\text{ord}_p 2019 = 16 \mid \phi(p) = p - 1$, so $p \equiv 1 \mod 16$.

We first test $p = 17$, as it is the smallest prime such that $p \equiv 1 \mod 16$.

$$2019^8 + 1 \equiv 13^8 + 1 \equiv 169^4 + 1 \equiv (-1)^4 + 1 \equiv 2 \mod 17$$

So 17 is not a factor.

We now test the next biggest prime p such that $p \equiv 1 \mod 16$, which is 97.

$$2019^8 + 1 \equiv (-18)^8 + 1 \equiv 33^4 + 1 \equiv 22^2 + 1 \equiv 485 \equiv 0 \mod 97$$

So $\boxed{97}$ is a factor, and we have verified that it is the smallest. □

Problem 3.2 (Classic) — Prove for all integers $n \geq 2$ that n does not divide $2^n - 1$.

Solution. Let p be the smallest prime factor of n, which must exist because $n \geq 2$. For the sake of contradiction, assume $n \mid 2^n - 1$.

We know that $p \mid 2^n - 1$, so $2^n \equiv 1 \mod p$. By Theorem 2.1, we have $\text{ord}_p 2 \mid n$ and $\text{ord}_p 2 \mid \phi(p) = p - 1$.

The first statement implies that $\text{ord}_p 2$ is a factor of n. The second statement implies $\text{ord}_p 2 \leq p-1$. This is a contradiction, because we assumed that p was the smallest prime factor of n. So, we are done. □

Problem 3.3 (Bulgaria 1996/4/1) — Find all pairs of primes p, q such that $pq \mid (5^p - 2^p)(5^q - 2^q)$

Solution. We can divide this problem into cases. Either $p \mid 5^p - 2^p$ is true, or it isn't (implying $p \mid 5^q - 2^q$. Similarly, we have that either $q \mid 5^q - 2^q$ is true, or it isn't (implying $q \mid 5^p - 2^p$). This gives us 4 cases.

We assume both statements are true.

$$p \mid (5^p - 2^p)$$
$$5^p - 2^p \equiv 0 \mod p$$
$$5 - 2 \equiv 0 \mod p$$
$$3 \equiv 0 \mod p$$

So we determine that $p = 3$. Using the same logic, we have $q = 3$, giving us the pair $(3, 3)$.

Now assume the first statement about p is still true, but the statement about q is false. From our earlier work, we still have $p = 3$. Now, since the statement about q is false, we have as follows.

$$q \mid 5^p - 2^p$$
$$5^p - 2^p \equiv 0 \mod q$$
$$5^3 - 2^3 \equiv 0 \mod q$$
$$117 \equiv 0 \mod q$$

So, the possibilities of q are 3 and 13, producing a new distinct pair $(3, 13)$.

Now, we assume the first statement isn't true, giving us $p \mid 5^q - 2^q$. Assuming $q \mid 5^q - 2^q$ gives us $(13, 3)$ by symmetry on the last case, so we now assume $q \mid 5^p - 2^p$.

$$p \mid 5^q - 2^q$$
$$5^q \equiv 2^q \mod p$$
$$(5 \cdot 2^{-1})^q \equiv 1 \mod p$$
$$\text{ord}_p(5 \cdot 2^{-1} \mid q)$$

Sinc q is a prime, there are only two possibilities for $\text{ord}_p(5 \cdot 2^{-1}$: 1 and q.

Assume that $\text{ord}_p(5 \cdot 2^{-1} = 1$. Then, we must have as follows.

$$(5 \cdot 2^{-1})^1 \equiv 1 \mod p$$
$$5 \equiv 2 \mod p$$

The above statement is only true for $p = 3$, which we have already covered. So now, we have $\text{ord}_p(5 \cdot 2^{-1}) = q$.

We also know by Corollary 2.2 that $\text{ord}_p(5 \cdot 2^{-1}) \mid \phi(p) = p - 1$, so $q \mid p - 1$, which means $q < p$.

Using a similar argument switching p and q, we get $p < q$. But this contradicts our previous result, $q \leq p$, so there are no pairs in this case.

So, our only pairs are $\boxed{(3, 3), (3, 13), (13, 3)}$ □

§4 Primitive Roots

We will very briefly discuss primitive roots.

Definition 4.1. Let g, m be positive integers. We say that g is a primitive root $\mod m$ if $\text{ord}_m g = \phi(m)$.

Theorem 4.2

There exists a primitive root $\mod m$ if and only if $m = 1, 2, 4, p^k$ or $2p^k$ for some positive integer k.

We will not prove this theorem. The useful part of primitive roots is that there must exist a primitive root $\mod p$ for a prime p.

Let's investigate another quick example, for the sake of familiarization.

Problem 4.3 — Find the primitive roots $\mod 5$.

Solution. We find the order of 1, 2, 3, and 4 $\mod 5$. We disclude 0 because it is not relatively prime to 5.

- The powers of 1 are 1, ... so the order is 1.
- The powers of 2 are 2, 4, 3, 1, ... so the order is 4.
- The powers of 3 are 3, 4, 2, 1, ... so the order is 4.
- The powers of 4 are 4, 1, ... so the order is 2.

So, the primitive roots are the terms with order $\phi(5) = 4$, which are $\boxed{2 \text{ and } 3}$ □

Let's finish with a cute example.

Problem 4.4 — Prove that if p is a prime such that $p \equiv 1 \mod 4$, then there exists a positive integer a such that $a^2 \equiv -1 \mod p$.

Solution. The statement $a^2 \equiv -1 \mod p$ implies that $a^4 \equiv 1 \mod p$. We recall our definition of primitive roots, which is $g^{p-1} \equiv 1 \mod p$, and are motivated to plug in $a = g^{\frac{p-1}{4}}$. We can only plug this in because $\frac{p-1}{4}$ is an integer.

Clearly, $a^4 \equiv (g^{\frac{p-1}{4}})^4 \equiv g^{p-1} \equiv 1 \mod p$, so we verified that $\text{ord}_p(g^{\frac{p-1}{4}}) \mid 4$. We now need to verify that $a^2 \not\equiv 1 \mod p$.

$$a^2 \equiv (g^{\frac{p-1}{4}})^2 \equiv g^{\frac{p-1}{2}} \not\equiv 1 \mod p$$

If the above were congruent to $1 \mod p$, then we would have a contradiction because by definition of primitive roots, $\text{ord}_p g = p - 1$, not $\frac{p-1}{2}$. So, we have verified that $a^2 \not\equiv 1 \mod p$, which implies $a^2 \equiv -1 \mod p$. □