Order, Primitive Roots and Quadratic Residue

BdMO National Camp 2021

Atonu Roy Chowdhury
atonuroychowdhury@gmail.com

April 29, 2021

§1 Order!

Let's recall two of the theorems that we've seen before.

Theorem 1.1 (Fermat's Little Theorem and Euler's Theoem)
Let p be a prime number and a be an integer coprime with p. Then

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

More generally, if m and a are positive integers with $\gcd(a, m) = 1$, then

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

That is, if you take the sequence $a^1, a^2, a^3, \ldots$ in mod m, then the sequence eventually reaches 1 at $a^{\varphi(m)}$, and thus it becomes periodic. But, does the sequence reach 1 before $\varphi(m)$?
The answer is yes. You can easily find examples. One simple example is: taking $a = 2$ and $m = 7$. Then $\varphi(m) = \varphi(7) = 6$, but $2^3 \equiv 1 \pmod{7}$. So 6 is not the smallest n such that $2^n \equiv 1 \pmod{7}$. We shall call this smallest such n "order".

Definition 1.1 (Order modulo m)**.** Let a and m be coprime positive integers. Then the order of a modulo m, denoted by $\mathrm{ord}_m(a)$ is defined as follows:

$$\mathrm{ord}_m(a) := \min\{n \in \mathbb{N} : a^n \equiv 1 \pmod{m}\}$$

That means, if $\mathrm{ord}_m(a) = d$, then $a^d \equiv 1 \pmod{m}$ and for every positive integer k smaller than d, we have $a^k \not\equiv 1 \pmod{m}$.

Now a natural question arises: is there some formula using which we can calculate order? Sadly, the answer is no. But hey, don't get frustrated. You don't really have to check every integer from 1 to $\varphi(m)$. To reduce your hardwork, there comes our next theorem. Evan Chen named it "Fundamental Theorem of Orders", so I'm keeping the name.

Theorem 1.2 (Fundamental Theorem of Orders)
$a^N \equiv 1 \pmod{m}$ if and only if $\mathrm{ord}_m(a) \mid N$.

Proof. Let $\text{ord}_m(a) = d$. The if direction is trivial. If

$$d \mid N \implies N = dq \implies a^N \equiv a^{dq} \equiv \left(a^d\right)^q \equiv 1^q \equiv 1 \pmod{m}$$

For the other direction, we just need to use the division algorithm to arrive at contradiction. Assume for the sake of contradiction that $d \nmid N$. That means, N leaves some non-zero remainder upon division by d. So $N = dq + r$, where $0 < r < d$. Now,

$$1 \equiv a^N \equiv a^{dq+r} \equiv \left(a^d\right)^q a^r \equiv 1^q a^r \equiv a^r \pmod{m} \implies \boxed{a^r \equiv 1 \pmod{m}}$$

By definition of order, for every positive integer k smaller than d, we have $a^k \not\equiv 1 \pmod{m}$. Here, r is a positive integer smaller than d, but $a^r \equiv 1 \pmod{m}$. Thus we arrive at a contradiction. Hence d must divide N. □

This theorem immediately gives us a corollary.

Corollary 1.3

If $\gcd(a, m) = 1$, then $\text{ord}_m(a) \mid \varphi(m)$

Now we shall see an application of the *Fundamental Theorem of Orders*.

Lemma 1.4

Let $d = \text{ord}_m(a)$. Then $a^x \equiv a^y \pmod{m}$ if and only if $x \equiv y \pmod{d}$.

Proof. WLOG, we can assume that $x \geq y$. Order is defined only when $\gcd(a, m) = 1$. Therefore, we can actually divide both sides of the modular equation by a^y.

$$a^x \equiv a^y \pmod{m} \iff a^{x-y} \equiv 1 \pmod{m} \iff d \mid x - y \iff x \equiv y \pmod{d}$$

Thus, we are done. □

Alright, time for a fun exercise.

Exercise 1.1

Let a and n be coprime integers. Show that $n \mid \varphi(a^n - 1)$

Solution. Let $N = a^n - 1$. Obviously $\gcd(a, N) = \gcd(a, a^n - 1) = 1$. Then by *Corollary 1.3*,

$$\text{ord}_N(a) \mid \varphi(N)$$

If we can show that $\text{ord}_N(a) = n$, then we are basically done. It's actually not hard at all to show. Obviously, $a^n \equiv 1 \pmod{N}$. Now,

$$0 < k < n \implies a^k - 1 < a^n - 1 \implies N \nmid a^k - 1 \implies a^k \not\equiv 1 \pmod{N}$$

Therefore, $\text{ord}_N(a) = n$ and we are done. ■

§2 Primitive Roots

We've seen a few example in the Orders section that $\phi(m)$ may not be the smallest positive integer to raise power such that it becomes 1 modulo m. But occasionally it is the smallest such positive integer. That's when things start getting interesting.

Definition 2.1 (Primitive Root)**.** An integer g is said to be a primitive root modulo n if $\gcd(g, n) = 1$ and

$$\text{ord}_n(g) = \varphi(n)$$

Notice that primitive roots might not always exist. Also, even if they do, they need not be unique. So, what's interesting about primitive roots? Well, they exist when we need them the most.

Theorem 2.1

Let p be a prime number. Then there exists a primitive root modulo p.

This theorem has a stronger generalization. We don't need it now.

Proof. Before jumping into the proof, we need a lemma. I'll leave the proof of the lemma as an exercise for the reader.

Lemma 2.2

For every positive integer n,

$$\sum_{d|n} \varphi(d) = n$$

That is, a number is exactly equal to the sum of its divisor's φ.

We know that $a^{p-1} \equiv 1 \pmod{p}$, and hence $\text{ord}_p(a)$ is a divisor of $p-1$ for every a with $1 \leq a \leq p-1$. Let $d \mid p-1$. For every such d, we shall consider this set

$$S_d = \{a \ : \ 1 \leq a \leq p-1 \text{ and } \text{ord}_p(a) = d\}$$

Notice that, if we take union of S_d over all the divisors of $p-1$, we shall get the whole reduced residue system of p. Furthermore, all these S_d's are disjoint. Therefore,

$$\bigcup_{d|p-1} S_d = RRS(p) \implies \boxed{\sum_{d|p-1} |S_d| = p-1}$$

We shall prove in the next class that, the number of solutions (modulo p) to $x^d \equiv 1 \pmod{p}$ is at most d. The elements of the set $X = \left\{a, a^2, a^3, \ldots, a^d\right\}$ satisfies this modular equation and there are d different elements in X. Therefore, S_d must be a subset of this X.
Now we claim that, if $a \in S_d$, then $a^i \in S_d$ if and only if $\gcd(i, d) = 1$. To prove our claim, let $\gcd(i, d) = g > 1$ and $d = gx, i = gy$ where x and y are coprime.

$$b = a^i = a^{gy} \implies b^x = a^{gxy} = \left(a^d\right)^y \equiv 1 \pmod{p}$$

Obviously x is smaller than d because $g > 1$. Thus $b = a^i$ does not have order d. It can be shown easily that, if $\gcd(i, d) = 1$, then a^i has order d, in other words $a^i \in S_d$.

From this, we can conclude that, $S_d = \{a^i : \gcd(i,d) = 1\}$, and there are at most $\varphi(d)$ such elements. Therefore, $|S_d| \leq \varphi(d)$. Putting all the pieces of the puzzle together,

$$p - 1 = \sum_{d|p-1} \varphi(d) \geq \sum_{d|p-1} |S_d| = p - 1$$

Therefore, we must have $|S_d| = \varphi(d)$ for every d. Hence, $S_{p-1} = \varphi(p-1) > 0$. So such element with order $p-1$ exists. □

Not only have we showed that element with order $p-1$ exists, we've also showed that there are $\varphi(p-1)$ such elements with order $p-1$.

Lemma 2.3

If g is a primitive root modulo m and $\varphi(m)$ is even, then

$$g^{\frac{\varphi(m)}{2}} \equiv -1 \pmod{m}$$

Proof. We shall prove the case of m being prime here. The composite case can be shown using the stronger generalization of Theorem 2.1.
When m is prime, $\varphi(m) = m-1 = 2n$. g is a primitive root modulo m, so definitely $\gcd(g,m) = 1$. So

$$g^{2n} \equiv 1 \pmod{m} \implies m \mid g^{2n} - 1 = (g^n + 1)(g^n - 1) \implies g^n \equiv \pm 1 \pmod{m}$$

If $g^n \equiv 1 \pmod{m}$, then we get $\text{ord}_m(g) < \varphi(m)$. Thus we arrive at a contradiction. Therefore, $g^n \equiv 1 \pmod{m}$ □

Lemma 2.4

If g is a primitive root modulo m, then the set $S = \{g, g^2, g^3, \ldots, g^{\varphi(m)}\}$ is a reduced residue system modulo m.

Proof. $\gcd(g,m) = 1 \implies \gcd(g^i, m) = 1$. Therefore, every element of S is coprime to m. So all we need to show is every element of S is distinct modulo m.
Assume for the sake of contradiction that there exists some a, b with $g^a \equiv g^b \pmod{m}$. WLOG, $a > b$. Since g is coprime with m, we can actually divide both sides by g^b. Then we get,

$$g^{a-b} \equiv 1 \pmod{m}$$

a and b lie between 1 and $\varphi(m)$. So their difference should be strictly smaller than $\varphi(m)$. Thus we get g has order smaller than $\varphi(m)$, which contradicts with the fact that g is a primitive root modulo m. □

Now we shall prove Wilson's theorem, but not the proof you usually see in textbooks. We shall prove it using primitive roots.

Theorem 2.5 (Wilson's Theorem)

If p is a prime number, then

$$(p-1)! \equiv -1 \pmod{p}$$

Proof. $p = 2$ is trivial, so we shall consider the case of p being odd prime.
p is a prime, so it has a primitive root, namely g. By Lemma 2.4,

$$\left\{g, g^2, g^3, \ldots, g^{p-1}\right\} \equiv \{1, 2, 3, \ldots, p-1\} \pmod{p}$$

If we multiply all these, we shall get,

$$\begin{aligned}(p-1)! &\equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \\ &\equiv g \cdot g^2 \cdot g^3 \cdots g^{p-1} \\ &\equiv g^{1+2+3+\cdots+(p-1)} \\ &\equiv g^{\frac{(p-1)p}{2}} \\ &\equiv \left(g^{\frac{p-1}{2}}\right)^p \\ &\equiv (-1)^p \equiv -1 \pmod{p}\end{aligned}$$

Thus, we are done. □

Theorem 2.6 (Generalization of Theorem 2.1)
Let n be a positive integer. A primitive root modulo n exists if and only if

$$n \in \left\{2, 4, p^k, 2p^k\right\}$$

where p is an odd prime number.

I'm not stating the proof here. I'm gonna added it as an exercise problem.

§3 Quadratic Residue

The word "Quadratic" suggests that it has something to do with squares, and from the word "Residue" you're probably guessing that we will probably work with remainders. Yes, it is what it sounds like. Basically "Quadratic residue" deals with the remainders of square numbers. Let's jump into definition.

Definition 3.1 (Quadratic Residue)**.** Let m be a positive integer. An integer n is called a **quadratic residue modulo** m if there exists some x such that $x^2 \equiv n \pmod{m}$.

For example, 4 is a quadratic residue modulo 5, because $7^2 \equiv 4 \pmod{5}$. But 3 is not a quadratic residue modulo 5, because there does not exist any integer x such that $x^2 \equiv 3 \pmod{5}$.

Definition 3.2 (Quadratic Residue Class)**.** Let m be a positive integer. The Quadratic Residue Class of m, denoted by $\text{qr}(m)$, is defined as follows:

$$\text{qr}(m) = \{n : n \text{ is a quadratic reisude modulo } m\}$$

There is an equivalent definition:

$$\text{qr}(m) = \left\{x^2 \bmod m \ : \ 0 \leq x \leq m-1\right\}$$

It's not that hard to see that $x^2 \equiv (m-x)^2 \pmod{m}$. As a result, the set $\text{qr}(m)$ will have at most $\frac{m}{2} + 1$ elements. Because two elements contribute to the same quadratic residue.
Now, let's talk about a fundamental result about quadratic residue and primes.

Proposition 3.1

Let p be an odd prime. If -1 is a quadratic residue modulo p, then $p \equiv 1 \pmod{4}$

Proof. Assume for the sake of contradiction that $p \equiv 3 \pmod{4}$, and -1 is a quadratic residue modulo p. That is, there exists some positive integer x such that $x^2 \equiv -1 \pmod{p}$.
As $p \equiv 3 \pmod{4}$, we can express p as $4k+3$ form. Also, $p \mid x^2+1$ gives us $\gcd(x,p) = 1$. Therefore, by *Fermat's Little Theorem*,

$$x^{p-1} \equiv 1 \pmod{p} \implies 1 \equiv x^{4k+2} \equiv \left(x^2\right)^{2k+1} \equiv (-1)^{2k+1} \equiv -1 \pmod{p}$$

which leads to a contradiction. Therefore, $p \equiv 1 \pmod{4}$. □

However, this proposition does not necessarily imply that -1 is a quadratic residue for every prime of the form $4k+1$. But it can be shown easily that for every prime of such form, you can find a positive integer x with $x^2 \equiv -1 \pmod{p}$.

Lemma 3.2

If $p \equiv 1 \pmod{4}$ is a prime, then there exists a positive integer x with $x^2 \equiv -1 \pmod{p}$.

Proof. We shall prove it by constructing such x. The construction is motivated by *Wilson's Theorem*. Wilson's theorem says that, if p is a prime, then $(p-1)! \equiv -1 \pmod{p}$. We are given that p is a prime of the form $4k+1$. Substituting this into Wilson's theorem, we get that

$$1 \cdot 2 \cdot 3 \cdots (2k) \cdot (2k+1) \cdots (4k-1) \cdot 4k \equiv -1 \pmod{p}$$

Our main idea is to express the LHS as a square. How can we do it? Notice that,

$$\begin{aligned} 4k &\equiv -1 \pmod{p} \\ 4k-1 &\equiv -2 \pmod{p} \\ 4k-2 &\equiv -3 \pmod{p} \\ &\cdots \\ 2k+2 &\equiv -(2k-1) \pmod{p} \\ 2k+1 &\equiv -2k \pmod{p} \end{aligned}$$

If we multiply all these, we would get,

$$(2k+1)(2k+2)\cdots(4k-2)(4k-1)4k \equiv 1\cdot 2\cdot 3\cdots(2k-1)\cdot 2k \pmod{p}$$

The negative signs got canceled out because an even number of negative numbers are multiplied. Now, if we substitute this into Wilson's theorem, we get

$$(1\cdot 2\cdot 3\cdots(2k-1)\cdot 2k)\,(1\cdot 2\cdot 3\cdots(2k-1)\cdot 2k) \equiv -1 \pmod{p} \implies ((2k)!)^2 \equiv -1 \pmod{p}$$

Thus we have successfully constructed such x. So we are done. □

I intend to discuss about quadratic residues more in the diophantine equations note. In this note, I wanna introduce about Legendre Symbol.

Definition 3.3 (Legendre Symbol)**.** The Legendre symbol for a positive integer n and a prime p is denoted by $\left(\frac{n}{p}\right)$ and defined as:

$$\left(\frac{n}{p}\right) = \begin{cases} 0 & \text{if } p \mid n \\ 1 & \text{if } n \in \operatorname{qr}(p) \\ -1 & \text{if } n \notin \operatorname{qr}(p) \end{cases}$$

The definition is basically saying that, if $p \mid n$, then $\left(\frac{n}{p}\right)$ is 0. When $p \nmid a$, we have two cases. If n is a quadratic residue modulo p, then $\left(\frac{n}{p}\right)$ is 1, otherwise it's -1.
Now you may ask, "0 is always a quadratic residue modulo p. $p \mid n$ means $n \equiv 0 \pmod{p}$, so n is a quadratic residue modulo p. Why didn't we put 1 as the value of $\left(\frac{n}{p}\right)$? Doesn't it make more sense to have 1 for **all** quadratic residues?" Well, the definition is of Legendre Symbol has a greater purpose to serve other than denoting quadratic residue. That greater purpose is our next theorem.

Theorem 3.3 (Euler's Criterion)

$$\left(\frac{n}{p}\right) = n^{\frac{p-1}{2}} \mod p$$

Proof. If $p \mid n$, then the result is trivial. So let's assume $p \nmid n$.
If n is a quadratic residue, then $n \equiv x^2 \pmod{p}$. By Fermat's Little Theorem,

$$x^{p-1} \equiv 1 \pmod{p} \implies \left(\frac{n}{p}\right) = 1 \equiv \left(x^2\right)^{\frac{p-1}{2}} \equiv n^{\frac{p-1}{2}} \pmod{p}$$

Now, all we are left with is, whenever n is not a quadratic residue, $n^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. We shall need Wilson's theorem for this.
Take any integer x with $1 \leq x \leq p-1$. Take $y = nx^{-1}$, where x^{-1} denotes the multiplicative inverse of x modulo p[1]. Therefore, we have

$$xy \equiv x \pmod{p}$$

Notice that, x and y can't be equal. Because if x and y are equal, then n becomes a quadratic residue modulo p.
If we choose a different x, we shall get a different y. Thus, we can divide all the integers from 1 to $p-1$ in $\frac{p-1}{2}$ pairs of (x, y). Let the pairs are $(x_1, y_1), (x_2, y_2), \ldots, (x_{\frac{p-1}{2}}, y_{\frac{p-1}{2}})$. Using Wilson's theorem,

$$\begin{aligned} -1 &\equiv (p-1)! \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \\ &\equiv (x_1 y_1) \cdot (x_2 y_2) \cdots (x_{\frac{p-1}{2}} y_{\frac{p-1}{2}}) \\ &\equiv n \cdot n \cdots n \\ &\equiv n^{\frac{p-1}{2}} \pmod{p} \end{aligned}$$

Thus, we are done. □

Legendre Symbol has some very nice properties. I'm not proving these, you should try to prove them yourself.

Lemma 3.4

The Legendre Symbol $\left(\frac{n}{p}\right)$ has the following properties:

i. If $p \nmid ab$, then $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

ii. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

iii. If p and q are distinct odd primes, then $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$

The last one is known as "The Law of Quadratic Reciprocity".

[1] This basically means that $xx^{-1} \equiv 1 \pmod{p}$

§4 Exercise Problems

Problem 4.1. Find all positive integers n such that $n \mid 2^n - 1$.

Problem 4.2. Find all pairs of prime numbers p, q such that $pq \mid (5^p - 2^p)(5^q - 2^q)$.

Problem 4.3. Find all triplets of prime numbers p, q, r such that

$$p \mid q^r + 1, \quad q \mid r^p + 1, \quad r \mid p^q + 1$$

Problem 4.4. Let $p \geq 2$ be a prime number. Find all positive integer k such that p divides

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

Problem 4.5. Let g be a primitive root modulo n. Then g^m is also a primitive root modulo n if and only if m is relatively prime to $\varphi(n)$.

Problem 4.6. Let n be an odd positive integer. Show that there exists a primitive root modulo n if and only if there exists a primitive root modulo $2n$

Problem 4.7. Let p be an odd prime and g be a primitive root modulo p. Then either g or $g + p$ is a primitive root modulo p^k for every $k \geq 1$.

Problem 4.8. If any exists, there are exactly $\varphi(\varphi(n))$ primitive roots modulo n.

Problem 4.9. For each non-negative integer m, let $n_m = 101m - 100 \cdot 2^m$. Let a, b, c, d be integers with $0 \leq a, b, c, d \leq 99$ such that

$$n_a + n_b \equiv n_c + n_d \pmod{10100}$$

Problem 4.10. Find all pairs of positive integers (a, b) such that $ab(a + b)$ is not divisible by 7 , but $(a + b)^7 - a^7 - b^7$ is divisible by 7^7.

Problem 4.11. Find all pairs of positive integers x, y such that $4xy - x - y$ is a perfect square.

Problem 4.12. a, b are coprime positive integers and p is an odd prime number. If $p \mid a^2 + b^2$, show that $p \equiv 1 \pmod 4$

Problem 4.13. Find all triplets of positive integers a, b, c such that $a^2 + 1 = b(2^c - 1)$

Problem 4.14. Prove Lemma 3.4

Problem 4.15. Prove Theorem 2.6