6.S096: Number Theory January 17, 2024

Lecture 1— Primitive Roots and Quadratic Reciprocity

A. Anas Chentouf, M. Wacyl Meddour, M.A.O. *Scribe:*

1 Primitive Roots

We have proven that the order of x modulo n is a divisor of $\phi(n)$. One may wonder what the extreme cases are. The first occurs when $\text{ord}_n(x) = 1$, and this implies $x \equiv 1 \bmod n$, which is not that interesting. The other extreme case occurs when $\text{ord}_n(x) = \varphi(n)$, and is much more interesting.

Definition 1.1: Primitive Roots

If $\text{ord}_n(g) = \varphi(n)$, then g (and its residue class) are said to be *primitive roots* modulo n.

Naturally, there are some questions to ask here.

1. For which moduli are there primitive roots?

2. How many primitive roots are there?

1.1 Existence of Primitive Roots

We answer the first question, but without providing an entire proof.

Theorem 1.2: Existence of Primitive Roots

A primitive root exists modulo n if and only if $n = 2, 4, p^k$ or $2p^k$ where p is an odd prime and $k \geq 1$.

Now we'll discuss the reason why primitive roots don't exist for positive integers not in the form described above.

Lemma 1.3: Stronger version of Euler's theorem

Let $n = p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m}$ denote the prime factorization of n and let

$$M = \text{lcm}(\varphi(p_1^{a_1}), \varphi(p_2^{a_2}), \cdots, \varphi(p_m^{a_m}))$$

Then $x^M \equiv 1 \bmod n$ whenever $\gcd(x, n) = 1$

,

Proof. □

It's clear that $M|\varphi(p_1^{a_1})\varphi(p_2^{a_2})\cdots\varphi(p_m^{a_m}) = \varphi(n)$ So in order for a primitive root to exist $\bmod n$, it must be the case that $M = \varphi(n)$, for otherwise all integers x with $\gcd(x, n) = 1$ would have orders less than $\varphi(n)$. But for the equation $M = \varphi(n)$ or

$$\mathrm{lcm}(\varphi(p_1^{a_1}), \varphi(p_2^{a_2}), \cdots, \varphi(p_m^{a_m})) = \varphi(p_1^{a_1})\varphi(p_2^{a_2})\cdots\varphi(p_m^{a_m})$$

to hold, the numbers $\varphi(p_j^{a_j})$ must be pairwise co-prime! (To see this, look at the p-adic valuation of both sides for each prime q). However $\varphi(k)$ is even for all $k > 2$, thus the equality above can only be true in very specific cases.

To see this more concretely, Let's look at the following example:

1.2 Number of Primitive Roots

We now answer the second question, this time with proof!

Proposition 1.4: Primitive Roots are Generators

If g is a primitive root modulo n, then $\{g^0, g^1, \cdots, g^{\phi(n)-1}\}$ is the complete set of invertible residues modulo n.

Proof. There are $\varphi(n)$ invertible residues, and so it suffices to prove that the elements in the set $\{g^0, g^1, \cdots, g^{\phi(n)-1}\}$ are pairwise distinct modulo n. In fact, assume that $g^i \equiv g^j \bmod n$, for some $i \geq j$. then $g^{i-j} \equiv 1 \bmod n$, but note that $i - j < \varphi(n)$, and so $i - j = 0$ by the definition of primitive roots. □

Theorem 1.5: Number of Primitive Roots

If there exists a primitive root modulo n, then there are exactly $\varphi(\varphi(n))$ of them.

Proof. Consider a primitive root g. Note that by Proposition 1.4, the set $\{g^i\}_{i=0}^{\varphi(n)-1}$ contains all invertible residues, and hence all primitive roots. Note that g^i is a primitive root if and only if the smallest positive k such that $g^i k \equiv 1 \bmod n$ is $k = \phi(n)$. Alternatively, the smallest k such that $ik \equiv 0 \bmod \varphi(n)$ is $\varphi(n)$. In other words, i must be coprime to $\varphi(n)$, and there are exactly $\varphi(\varphi(n))$ such residues. □

In fact, we just proved the following result.

Lemma 1.6

If g is a primitive root modulo n, then g^i is a primitive root modulo n if and only if i is coprime to $\varphi(n)$.

In general, if there is a primitive root mod n and d is a divisor of $\varphi(n)$, then there are exactly $\varphi(d)$ elements of order equal to d.

1.3 Applications of Primitive Roots

We first apply the concept of primitive roots to prove two beautiful results.

Theorem 1.7

Let p be a prime number. Then

$$\sum_{m=1}^{p-1} m^k \pmod{p} = \begin{cases} p-1 & \text{if } p-1|k, \\ 0 & \text{if } p-1 \nmid k. \end{cases}$$

Proof. If $p-1|k$, then by Fermat's Little Theorem,

$$\sum_{m=1}^{p-1} m^k \equiv \sum_{m-1}^{p} 1 \equiv p-1 \pmod{p}.$$

Otherwise, let g be a primitive root modulo p. Note that the sum ranges over the invertible residues modulo p, which are exactly generated by g^i as i ranges from 1 to $p-1$, and so

$$\sum_{m=1}^{p-1} m^k = \sum_{i=1}^{p-1} g^{ik} = g^k \sum_{i=0}^{p-2} g^{ik}.$$

We can evaluate this as a geometric sum to be

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

noting that g^k-1 is nonzero modulo p since $p-1 \nmid k$. The numerator however is equal to 0, and this concludes the proof. □

Another application of quadratic residues allows us to segway into our next topic: quadratic residues.

Theorem 1.8: Fermat's Christmas Theorem

Let p be an odd prime. Then there exists x such that $x^2 \equiv -1 \bmod p$ if and only if $p \equiv 1 \bmod 4$.

Proof. We first prove that $p \equiv 1 \bmod 4$ is a necessary condition. Assume that $x^2 \equiv -1 \bmod 4$. Then $x^{p-1} \equiv (x^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \bmod 4$. By Fermat's Little Theorem, $\frac{p-1}{2}$ must be even and so $p \equiv 1 \bmod 4$.

To prove it is sufficient, consider a primitive root g modulo p. Since $p \equiv 1 \bmod 4$, we can consider $x = g^{\frac{p-1}{4}}$. This element satisfies $x^2 \equiv g^{\frac{p-1}{2}} \pmod p$. Note that $x^4 \equiv 1 \pmod p$ by Fermat, and so $(x^2-1)(x^2+1) \equiv 0 \pmod p$. However, since g is a primitive root, it has order exactly $p-1$ and so $x^2 \equiv g^{\frac{p-1}{2}} \not\equiv 1 \pmod p$, and so $x^2 \equiv -1 \pmod p$, as desired. □

2 Quadratic Reciprocity

The previous result can be expressed in terms of the language of quadratic residues.

Definition 2.1: Quadratic Residues

Let p be an odd prime number, and a an integer such that $p \nmid a$. We say that a is a *quadratic residue* modulo p if there exists x such that $x^2 \equiv a \bmod p$. Otherwise, we say that a is a *quadratic nonresidue*.

We see that $\{1^2, 2^2, \cdots, (p-1)^2\}$ are all the quadratic residues $\bmod p$ but since $x^2 \equiv (p-x)^2 \bmod p$, we can consider only the first half

$$\{1^2, 2^2, \cdots, \frac{(p-1)}{2}^2\}.$$

To show that these elements are distinct , suppose that $i^2 \equiv j^2 \bmod p$ where $1 \leq i, j \leq \frac{p-1}{2}$ and $i \not\equiv j \bmod p$, then $p|(i-j)(i+j)$.
Since $i \not\equiv j \bmod p$, then $p|i+j$ but $i+j < p/2 + p/2 = p$ which is impossible.

Therefore we can conclude that :

Lemma 2.2: Number of Quadratic Residues

For any odd prime p, there are exactly $\frac{p-1}{2}$ quadratic residues. Furthermore they are equal to the set:

$$\{1^2, 2^2, \cdots, \frac{p-1}{2}^2\}$$

This also tells us that there are $\frac{p-1}{2}$ quadratic nonresidues.

Now we'll look at quadratic residues by using primitive roots.

Lemma 2.3: Writing quadratic residues using primitive roots

Let g denote a primitive root mod$p$ then the set of all quadratic residues mod$p$ is equal to

$$\{g^k : k \text{ is even}\} = \{g^2, g^4 \cdots, g^{p-1}\}$$

And the set of quadratic nonresidues is equal to:

$$\{g^k : k \text{ is odd}\} = \{g^1, g^3 \cdots, g^{p-2}\}$$

Proof. Any quadratic residue a is the square of some element x in $\{1, 2, \cdots, p-1\}$ but we also know that there exists some number k such that $x \equiv g^k \bmod p$ which implies that $a \equiv g^{2k} \equiv g^{\text{even number}} \bmod p$. This implies that the rest of the elements $\{g^k : k \text{ is odd}\}$ must be the set of all quadratic nonresidues. □

Now let's express the result of Theorem 1.8 in terms of the language of quadratic residues.

Theorem 2.4: Fermat's Christmas Theorem, v2.0

Let p be a prime number. Then -1 is a quadratic residue modulo p if and only if $p \not\equiv 3 \bmod 4$.

Proposition 2.5: Euler's Criterion

Let p be a prime number and a an integer. Then

$$a^{\frac{p-1}{2}} \equiv \begin{cases} 1 \pmod p & \text{if } a \text{ is a quadratic residue modulo } p, \\ -1 \pmod p & \text{if } a \text{ is a quadratic residue modulo } p, \\ 0 & \text{if } p|a. \end{cases}$$

Proof. First of all let's calculate $x = g^{\frac{p-1}{2}}$ for a primitive root g. Since $x^2 \equiv g^{p-1} \equiv 1 \bmod p$. This tells us that $x \equiv \pm 1 \bmod p$. However it can't be possible that $g^{\frac{p-1}{2}} \equiv 1 \bmod p$ since g is a primitive root, so we must have $g^{\frac{p-1}{2}} \equiv -1 \bmod p$. Now a be an arbitrary element of $\{1, 2, \cdots, p-1\}$. Write $a \equiv g^m \bmod p$ for some integer m. Then $a^{\frac{p-1}{2}} \equiv g^{m\frac{p-1}{2}} \equiv (-1)^m$ which by Lemma 2.3 is equal to 1 if a is a quadratic residue(i.e. m even) and -1 if a is a quadratic nonresidue (when m is odd). The case $p|a$ is trivial.

□

Definition 2.6: Legendre Symbol

The Legendre symbol $\left(\frac{a}{p}\right)$ is defined as

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p, \\ -1 & \text{if } a \text{ is a quadratic residue modulo } p. \end{cases}$$

The following result follows directly from Proposition 2.5.

Proposition 2.7: Legendre Symbol is Multiplicative

For all integers a and b coprime to p, we have that

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

This tells us 3 three things: The product of two quadratic residues is a quadratic residue ($1 \times 1 = 1$), the product of two quadratic nonresidues is a quadratic residue($-1 \times -1 = 1$), and the product of a quadratic residue and quadratic non-residue is a quadratic nonresidue($1 \times -1 = -1$).

Notice that if we write each element as a power of primitive root g. Then this result is really just telling us the very familiar laws of parity (even+even=even , odd+odd=even, odd+even=odd)

Now we'll get to the main theorem concerning quadratic residues .

Theorem 2.8: The Law of Quadratic Reciprocity

Let p, q denote distinct odd primes, then:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \times \frac{q-1}{2}}$$

This can be equivalently stated as :

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) & \text{if at least one of } p \text{ or } q \text{ is } 1 \bmod 4, \\ -\left(\frac{q}{p}\right) & \text{if both } p \text{ and } q \text{ are } 3 \bmod 4 \end{cases}$$

This theorem allows us to calculate $\left(\frac{p}{q}\right)$ directly from $\left(\frac{q}{p}\right)$

Theorem 2.9: Criterion for 2 and -1

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

and

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

Theorem 2.8 and 2.9 allow us to compute Legendre symbol for all integers in an efficient manner.

Example.

We'll determine whether 21 is a quadratic residue mod61 We see that:

$$\left(\frac{21}{61}\right) = \left(\frac{3}{61}\right)\left(\frac{7}{61}\right) = \left(\frac{61}{3}\right)\left(\frac{61}{7}\right) = \left(\frac{1}{3}\right)\left(\frac{5}{7}\right) = 1\cdot\left(\frac{7}{5}\right) = \left(\frac{2}{5}\right) = (-1)^{\frac{5^2-1}{8}} = -1$$

Now let's ask the same question for 51 mod 103

$$\left(\frac{51}{103}\right) = \left(\frac{3}{103}\right)\left(\frac{17}{103}\right) = -\left(\frac{103}{3}\right)\left(\frac{103}{17}\right) = -\left(\frac{1}{3}\right)\left(\frac{1}{17}\right) = -1$$

Example.

Let's find all odd primes p such that the equation $x^2 \equiv 3 \bmod p$ has a solution.

This condition tells us that

$$1 = \left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) \cdot (-1)^{\frac{p-1}{2}}$$

So we have 2 cases to consider:

Case 1:

$$\left(\frac{p}{3}\right) = 1 \text{ and } (-1)^{\frac{p-1}{2}} = 1$$

The first equation implies that $p \equiv 1 \bmod 3$ (because 1 is the only quadratic residue mod3) and the second says that $p \equiv 1 \bmod 4$. Combining these 2 equations gives $p \equiv 1 \bmod 12$

Case 2:

$$\left(\frac{p}{3}\right) = -1 \text{ and } (-1)^{\frac{p-1}{2}} = -1$$

The first equation implies that $p \equiv 2 \bmod 3$ (Since 2 is the only quadratic nonresidue mod3) and the second says that $p \equiv 3 \bmod 4$. Combining these 2 equations gives $p \equiv 11 \bmod 12$

So we can conclude that the only primes p for which 3 is a quadratic residue are exactly those that leave a remainder of 1 or 11 when divided by 12.