Lecture 6: Primitive Roots and The Quadratic Reciprocity Law

Lecture 6

Objectives

By the end of this lecture you should be able to understand

1. Primitive Roots
2. The Quadratic Reciprocity Law
3. How to compute the the Legendre and Jacobi symbols

Outline

Order of a Modulo n

- Recall Euler's theorem:

Theorem

Let $n \geq 1$ *and* $\gcd(a, n) = 1$, *then* $a^{\phi(n)} \equiv 1 \pmod{n}$

- Actually, an exponent $e < \Phi(n)$ might exist that can also give 1!

Definition (Order Modulo n)

Let $n \geq 1$ and $\gcd(a, n) = 1$, then the order of a modulo n, denoted by $\mathrm{Ord}_n(a)$, is the smallest integer k such that $a^k \equiv 1 \pmod{n}$

Definition (Primitive Root Modulo n)

When $\mathrm{Ord}_n(a) = \Phi(n)$, we call a as a primitive root modulo n

- Primitive roots are important tool in number theory analysis and they exist for any prime modulus.

Example – Order of a Modulo 7

For $n = 7$, we can create a table for all combinations of a and e for the modular exponentitation $a^e \pmod 7$

a/e	1	2	3	4	5	6	$\mathrm{Ord}_7(a)$
1	1	1	1	1	1	1	1
2	2	4	1	2	4	1	3
3	3	2	6	4	5	1	6
4	4	2	1	4	2	1	3
5	5	4	6	2	3	1	6
6	6	1	6	1	6	1	2

In modulo 7, primitive roots are 3 and 5.

Example – Order of a Modulo 13

a/e	1	2	3	4	5	6	7	8	9	10	11	12	$\mathrm{Ord}_{13}(a)$
1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	3	6	12	11	9	5	10	7	1	12
3	3	9	1	3	9	1	3	9	1	3	9	1	3
4	4	3	12	9	10	1	4	3	12	9	10	1	6
5	5	12	8	1	5	12	8	1	5	12	8	1	4
6	6	10	8	9	2	12	7	3	5	4	11	1	12
7	7	10	5	9	11	12	6	3	8	4	2	1	12
8	8	12	5	1	8	12	5	1	8	12	5	1	4
9	9	3	1	9	3	1	9	3	1	9	3	1	3
10	10	9	12	3	4	1	10	9	12	3	4	1	6
11	11	4	5	3	7	12	2	9	8	10	6	1	12
12	12	1	12	1	12	1	12	1	12	1	12	1	2

In modulo 13, primitive roots are 2, 6, 7 and 11.

Example – Order of a Modulo 9

For $n = 9$, we can create a table for all combinations of a and e for the modular exponentitation $a^e \pmod 9$. Note that here $\Phi(9) = 6$, so the column that should give 1's like before is at $e = \Phi(9) = 6$

a/e	1	2	3	4	5	6	7	8	$\text{Ord}_9(a)$
1	1	1	1	1	1	1	1	1	1
2	2	4	8	7	5	1	2	4	6
3	3	0	0	0	0	0	0	0	undef
4	4	7	1	4	7	1	4	7	3
5	5	7	8	4	2	1	5	7	6
6	6	0	0	0	0	0	0	0	undef
7	7	4	1	7	4	1	7	4	3
8	8	1	8	1	8	1	8	1	2

In modulo 9, primitive roots are 2 and 5. For $a = 3, 6$, order is undefined because $\gcd(9, 3) \neq 1$ and $\gcd(9, 6) \neq 1$

Relation between Order and Exponents

Theorem

Let $\mathrm{Ord}_n(a) = k$*, then* $a^h \equiv 1 \pmod{n}$ *iff* $k \mid h$

Proof.

$\Leftarrow$ Assume $k \mid h$, then $h = jk$, then $a^h \equiv a^{jk} \equiv \left(a^k\right)^j \equiv 1 \pmod{n}$
$\Rightarrow$ Assume $a^h \equiv 1 \pmod{n}$, with $h = jk + r, r \in \{0, \ldots, k-1\}$

- Then $\cancel{a^h} \equiv \cancel{a^{kj}} a^r \Rightarrow a^r \equiv 1 \pmod{n}$
- But since r is less than k, we end up with $r = 0$
- Therefore, $h = jk$ or $k \mid h$

$\square$

- Since $a^{\phi(n)} \equiv 1 \pmod{n}$, then $\mathrm{Ord}_n(a) = k \mid \Phi(n)$.
- Therefore, we compute $\mathrm{Ord}_n(a)$ by searching in all divisors of $\Phi(n)$.

Equivalence of Exponents

Theorem

Let $\mathrm{Ord}_n(a) = k$*, then* $a^i \equiv a^j \pmod{n}$ *iff* $i \equiv j \pmod{k}$

Proof.

$\Leftarrow$ Assume $a^i \equiv a^j \pmod{n}$, $i \geq j$.

- Since $\gcd(a, n) = 1$, then divide by a^j to get $a^{i-j} \equiv 1 \pmod{n}$
- Then $k \mid i - j$ or $i \equiv j \pmod{k}$

$\Rightarrow$ Assume $i \equiv j \pmod{k}$

- Then $i = j + qk$ for $q \in \mathbb{Z}$
- But $a^k \equiv 1 \pmod{n}$
- Then, $a^i \equiv a^j \cancel{a^{qk}} \pmod{n} \Rightarrow a^i \equiv a^j \pmod{n}$

$\square$

Equivalence of Exponents – Corollary

Corollary

Let $\mathrm{Ord}_n(a) = k$*, then the integers* $a, a^2, a^3, \ldots, a^k$ *are incongruent modulo* n *(i.e., every two number are not congruent to each other)*

Proof.

- If $a^i \equiv a^j \pmod{n}$ for $1 \leq i \leq j \leq k$, then the previous theorem ensures that $i \equiv j \pmod{k}$.
- However, both i and j are less than k!
- Therefore, the congruence $i \equiv j \pmod{k}$ becomes equivalent to the equality $i = j$
- Then, within this set, $a^i \equiv a^j \pmod{n}$ only when $i = j$, or

$$a^i \not\equiv a^j \pmod{n} \ \forall\, i \neq j \text{ and } i, j \in \{1, \ldots, k\}$$

$\square$

Reduced Residue Systems Based on Primitive Roots

Theorem

Let $\gcd(a, n) = 1$, *and let the reduced residue system*

$$\{a_1, a_2, \ldots, a_{\Phi(n)}\} \tag{1}$$

be the set of $\Phi(n)$ *positive integers less than n and are co-primes with n. If a is a primitive root of n, then the set*

$$\{a^1, a^2, \ldots, a^{\Phi(n)}\} \tag{2}$$

is also a reduced residue system equivalent to (1) in some order.

Example

- $a = 2$ is a primitive root in modulo $n = 9$ with $\Phi(9) = 6$
- Therefore, the set $\{2^1, \ldots, 2^6\}$ is equivalent to the set {1,2,4,5,7,8} of residues that are co-primes with the modulo $n = 9$.

Motivation for Solving $x^2 \equiv a \pmod{p}$

Square Root Binary Tests

- Test if a large integer a is a perfect square or not in modulo p, i.e, does it have a square root or not? By solving $x^2 \equiv a \pmod{p}$.
- Explicitly calculating the square root using floating-point precision won't work because large integers cannot fit in single (32-bit) or double (64-bit) precision. The square root itself might not be important, what we need is the binary test.

Quadratic Congruence

- Study the solvability of quadratic congruences

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

where p is an odd prime and $a \not\equiv 0 \pmod{p}$ or $\gcd(a, p) = 1$

- For consistency, we study the standard form $x^2 \equiv a \pmod{p}$ and map any quadratic congruence to it.

Quadratic Residues

Definition

Let p be an odd prime and $\gcd(a, p) = 1$. If the quadratic congruence $x^2 \equiv a \pmod{p}$ has a solution, then a is called a quadratic residue of p. Otherwise, it is called a quadratic nonresidue of p.

Example

In modulo 13, we can find all quadratic residues by exhaustive search:

$$1^2 \equiv 12^2 \equiv 1 \pmod{13}, \quad 2^2 \equiv 11^2 \equiv 4 \pmod{13}$$
$$3^2 \equiv 10^2 \equiv 9 \pmod{13}, \quad 4^2 \equiv 9^2 \equiv 3 \pmod{13}$$
$$5^2 \equiv 8^2 \equiv 12 \pmod{13}, \quad 6^2 \equiv 7^2 \equiv 10 \pmod{13}$$

- The quadratic residues of 13 are 1, 3, 4, 9, 10, 12.
- The quadratic nonresidues of 13 are 2, 5, 6, 7, 8, 11.

Euler's Criterion

Theorem

Let p be an odd prime and $\gcd(a,p)=1$. *Then a is a quadratic residue of p iff*

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

Lemma

Let p be an odd prime and $\gcd(a,p)=1$, *then*

$$\left(a^{(p-1)/2}-1\right)\left(a^{(p-1)/2}+1\right) = a^{p-1}-1 \equiv 0 \, \textit{(By Fermat's)}$$

Then, either $a^{(p-1)/2} \equiv 1 \pmod{p}$ *or* $a^{(p-1)/2} \equiv -1 \pmod{p}$

- Therefore, Euler's criterion is binary: It either gives 1 or -1

Legendre Symbol

Quadratic congruence analysis is simplified by the Legendre symbol

Definition

Let p be an odd prime and $\gcd(a,p)=1$. The Legendre symbol (a/p) is defined by

$$(a/p)=\begin{cases}1, & \text{if } a \text{ is a quadratic residue of } p\\ -1, & \text{if } a \text{ is a quadratic nonresidue of } p\end{cases}$$

Example

In module 13, the results of slide 15 are summarized as:
$(1/13)=(3/13)=(4/13)=(9/13)=(10/13)=(12/13)=1$
and
$(2/13)=(5/13)=(6/13)=(7/13)=(8/13)=(11/13)=-1$

Properties of Legendre Symbol

Let p be an odd prime and let a and b be integers co-primes to p

- If $a \equiv b \pmod{p}$, then $(a/p) = (b/p)$
- $(a^2/p) = 1$
- $(a/p) \equiv a^{(p-1)/2} \pmod{p}$
- $(ab/p) = (a/p)(b/p)$
- $(1/p) = 1$ and $(-1/p) = (-1)^{(p-1)/2}$

For the proof of these properties, please check Theorem 9.2 in Burton's textbook.

Quadratic Reciprocity Law

Theorem

If p and q are distinct odd primes, then

$$(p/q)(q/p) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$
$$= \begin{cases} 1, & \textit{if } p \equiv 1 \pmod 4 \ \textit{or } q \equiv 1 \pmod 4 \\ -1, & \textit{if } p \equiv q \equiv 3 \pmod 4 \end{cases}$$

Multiplying both sides by (q/p) and noting that $(q/p)^2 = 1$, we have

Corollary

$$(p/q) = \begin{cases} (q/p), & \textit{if } p \equiv 1 \pmod 4 \ \textit{or } q \equiv 1 \pmod 4 \\ -(q/p), & \textit{if } p \equiv q \equiv 3 \pmod 4 \end{cases}$$

Application of Quadratic Reciprocity Law

Corollary

$$(p/q) = \begin{cases} (q/p), & \textit{if } p \equiv 1 \pmod 4 \textit{ or } q \equiv 1 \pmod 4 \\ -(q/p), & \textit{if } p \equiv q \equiv 3 \pmod 4 \end{cases}$$

Assume the canonical factorization of

$$a = \pm 2^{k_0} p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r},$$

then we can use the multiplicative property to get

$$(a/p) = (\pm 1/p)(2^{k_0}/p)(p_1^{k_1}/p)(p_2^{k_2}/p)\ldots(p_r^{k_r}/p)$$

- Recursively replace (p_i/p) by a new Legendre symbol having smaller denominator, i.e., invert and divide by the new modulo
- By successive inversion and division, the computation can be reduced to simple binary tests $(-1/p)$, $(2/p)$ and $(3/p)$.

Basic Square Root Binary Tests

To develop an efficient square-root binary test, a divide-and-conquer algorithm can be developed to reduce an arbitrarily large integer into one of the following 3 cases which can be easily calculated.

$$(-1/p) = \begin{cases} 1, & p \equiv 1 \pmod 4 \\ -1, & p \equiv 3 \pmod 4 \end{cases}$$

$$(2/p) = \begin{cases} 1, & p \equiv \pm 1 \pmod 8 \\ -1, & p \equiv \pm 3 \pmod 8 \end{cases} = (-1)^{(p^2-1)/8}$$

$$(3/p) = \begin{cases} 1, & p \equiv \pm 1 \pmod{12} \\ -1, & p \equiv \pm 5 \pmod{12} \end{cases}$$

The Jacobi Symbol

Definition

Let n be an odd integer where $n = q_1 \dots q_k$ and $q_i's$ are odd primes, not necessarily distinct. Let a is an integer co-prime with n, i.e., $\gcd(a, p) = 1$. The Legendre symbol $(a|n)$ is defined by

$$(a|n) = (a/q_1)(a/q_2)\dots(a/q_k)$$

where (a/q_i) is the Legendre symbol.

- By definition, $(a|1) = 1$ for all $a \in \mathbb{Z}$.
- The Jacobi symbol extends the domain of definition of the Legendre symbol by extending the denominator into composites.
- The Jacobi symbol has better properties from a computational point of view where we can efficiently compute it without knowing the canonical factorization of either a or n.

Properties of Jacobi Symbol

Let m, n be odd positive integers and let $a, b \in \mathbb{Z}$, then

- If $a \equiv b \pmod{n}$, then $(a|n) = (b|n)$
- $(ab|n) = (a|n)(b|n)$
- $(a|mn) = (a|m)(a|n)$
- $(1|n) = 1$ and $(-1|n) = (-1)^{(n-1)/2}$
- $(2|n) = (-1)^{(n^2-1)/8}$
- $(m|n) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}(n|m)$

For the proof of these properties, please check Section 12.2 in 9.2 in Victor Shoup's textbook.

Computing the Jacobi Symbol

Given: odd positive integer n and integer a
Required: Compute the Jacobi symbol $(a|n)$

$\sigma \leftarrow 1$
repeat
    // loop invariant: n is odd and positive
    $a \leftarrow a \bmod n$
    if $a = 0$ then
        if $n = 1$ then return σ else return 0
    compute a', h such that $a = 2^h a'$ and a' is odd
    if $h \not\equiv 0 \pmod 2$ and $n \not\equiv \pm 1 \pmod 8$ then $\sigma \leftarrow -\sigma$
    if $a' \not\equiv 1 \pmod 4$ and $n \not\equiv 1 \pmod 4$ then $\sigma \leftarrow -\sigma$
    $(a, n) \leftarrow (n, a')$
forever