PRIMITIVE ROOTS

**THM (Euler):**

Let \( a, m \in \mathbb{Z} \) with \( m > 0 \), \( (a, m) = 1 \).

Then \( a^\phi(m) \equiv 1 \pmod{m} \)

**Question:** Can a smaller exponent \( N \) satisfy \( a^N \equiv 1 \pmod{m} \) \( \forall a \in \mathbb{Z} \) coprime to \( m \)?

In other words, given \( m \), when is there an integer \( a \) s.t. \( a \not\equiv 1 \pmod{m} \) \( \forall i < \phi(n) \)?

The answer to the second question is "when a primitive root exists". Understanding this is the objective of the next few lectures.

We start by defining the order of \( a \mod m \).

**Def:** Let \( a, m \in \mathbb{Z} \) with \( m > 0 \), \( (a, m) = 1 \).

The order of \( a \) modulo \( m \), denoted \( \text{ord}_m a \), is the least positive integer \( N \) s.t. \( a^N \equiv 1 \pmod{m} \).
**LEM:** Euler's Theorem \( \Rightarrow \text{ORD}_M a \leq \phi(M) \\

**Ex:** Take \( M = 7 \), \( a = 3 \)

\[
3^1 \equiv 1, \quad 3^2 \equiv 2, \quad 3^3 \equiv 2 \times 2 - 1 \equiv 6 \pmod{7} \\
3^4 \equiv 4, \quad 3^5 \equiv 5, \quad 3^6 \equiv 1
\]

So \( \text{ORD}_7 3 = 6 = \phi(7) \)

With similar calculations for the other \( a \) we get

\[
\begin{array}{ccccccc}
(a, 7) & 1 & 2 & 3 & 4 & 5 & 6 \\
\hline
\text{ORD}_7 a & 1 & 3 & 6 & 3 & 6 & 2 \\
\end{array}
\]

**Ex:** \( M = 8 \)

\[
\begin{array}{cccc}
(a, 8) & 1 & 3 & 5 & 7 \\
\hline
\text{ORD}_8 a & 1 & 2 & 2 & 2 \\
\end{array}
\]

* Note that \( \text{ORD}_8 a \leq \phi(8) \) \( \forall a \) continue to 9

* Note that \( \text{ORD}_M a \) is always a divisor of \( \phi(M) \)
Prop: Let \( a, m \in \mathbb{Z}, \, m \geq 0, \, (a, m) = 1 \)
then \( a^N \equiv 1 \pmod{m} \) for some \( N > 0 \)
if and only if \( \text{ord}_m a \mid N \)

Proof: \( \Rightarrow \) Suppose \( a^N \equiv 1 \pmod{m} \) for \( N > 0 \)
Div. Alg. gives
\[
N = \text{ord}_m a \cdot q + r, \quad 0 \leq r < \text{ord}_m a
\]
Then,
\[
a^N = (a^{\text{ord}_m a})^q \cdot a^r \equiv 1^q \cdot a^r \equiv 1 \pmod{m}
\]
since \( \text{ord}_m a \) is minimal \( \Rightarrow r = 0 \)
that is, \( \text{ord}_m a \mid N \)

\( \Leftarrow \) Suppose \( \text{ord}_m a \mid N \), i.e. \( N = \text{ord}_m a \cdot k \)
thus
\[
a^N = (a^{\text{ord}_m a})^k \equiv 1^k \equiv 1 \pmod{m}
\]

Corollary: Let \( a, m \in \mathbb{Z}, \, m \geq 0, \, (a, m) = 1 \).
then, \( \text{ord}_m a \mid \phi(m) \)

Proof: By \( \phi \) \( a \equiv 1 \pmod{m} \)
then \( \text{ord}_m a \mid \phi(m) \) by the proposition
Example: \( M = 11 \Rightarrow \phi(11) = 10; \ \alpha = 2 \).

Then the possible orders mod 11 are \( \{1, 2, 5, 10\} \).

We have \( 2^1 \equiv 2 \), \( 2^2 \equiv 4 \), \( 2^5 \equiv 32 \equiv 10 \pmod{11} \).

Thus \( 2^{10} \equiv 1 \pmod{11} \) and \( \text{ord}_{11} 2 = 10 \).

Note that we have avoided computing \( 2, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9 \pmod{11} \).

Example:

Def: An integer \( \alpha \) is called a primitive root modulo \( M \) if \( \text{ord}_M \alpha \) is as large as possible, that is \( \text{ord}_M \alpha = \phi(M) \).

Example:

- \( \alpha = 3 \) or \( \alpha = 5 \) are primitive roots mod 7.
- \( \alpha = 2 \) is a primitive root mod 11.
- There are no primitive roots mod 8.

Main Question:

What integers have primitive roots?
Proposition: Let \( a, M \in \mathbb{Z}^+ \), \( a > 0 \), \( (a, M) = 1 \).

(i) \( a^i \equiv a^j \pmod{M} \) \( \iff \) \( i \equiv j \pmod{\text{ORD}_M a} \)

(ii) Let \( i > 0 \), then, \( \text{ORD}_M a^i = \frac{\text{ORD}_M a}{(\text{ORD}_M a, i)} \)

Proof: Let \( (a, M) = 1 \).

(i) \( a^i \equiv a^j \pmod{M} \) \( \iff \) \( a^i \equiv a^j \pmod{\text{ORD}_M a} \)

\[ a^i \equiv a^j \pmod{\text{ORD}_M a} \]

Thus \( a^{i-j} \equiv 1 \pmod{M} \) \( \iff \) \( \text{ORD}_M a^i \mid i-j \) (Proposition)

\[ \iff i \equiv j \pmod{\text{ORD}_M a} \]

(ii) We have \( (a^i)^{\text{ORD}_M a^i} = a^{i \cdot \text{ORD}_M a^i} \equiv 1 \pmod{M} \)

Proposition

\[ \implies \text{ORD}_M a^i \mid i \cdot \text{ORD}_M a^i \text{ and } \text{ORD}_M a^i \]

is minimal with this property. Indeed, if

\[ \text{ORD}_M a^i \mid i \cdot k \implies a^i = (a^i)^{\text{ORD}_M a^i} \equiv 1 \implies \text{ORD}_M a^i \mid k \]

Thus \( i \cdot \text{ORD}_M a^i = \text{LCM} (\text{ORD}_M a^i, i) = \frac{i \cdot \text{ORD}_M a}{(\text{ORD}_M a^i, i)} \)

\[ \implies \text{ORD}_M a^i = \frac{\text{ORD}_M a}{(\text{ORD}_M a, i)} \]

\[ \blacksquare \]
Prop: Let \( a, M \in \mathbb{Z}^+, M > 0, \ (a, M) = 1 \)

(i) \( a^i = a^j \ (\text{mod } M) \iff i \equiv j \ (\text{mod } \text{ord}_M a) \)

(ii) Let \( i > 0 \). Then, \( \text{ord}_M a^i = \frac{\text{ord}_M a}{\text{gcd}(M, a_i)} \)

Def: An integer \( a \) coprime to \( M > 0 \) is a \( \text{PR} \) \( \text{mod } M \)

\[ \text{if } \text{ord}_M a = \phi(M) \]

Co12: If \( a \) is a \( \text{PR} \) \( \text{mod } M \), then \( \{ 1, a, a^2, \ldots, a^{\phi(M)-1} \} \) is a reduced system \( \text{mod } M \).

Proof: Since \((a, M) = 1\) because \( a \) is \( \text{PR} \) we have that all the integers in the set are coprime to \( M \).

There are \( \phi(M) \) integers in the set so we have to show no two of them are congruent.

Suppose \( a^i \equiv a^j \ (\text{mod } M) \) \( \implies \text{ord}_M a^i \mid i-j \implies i \equiv j \ (\text{mod } \text{ord}_M a) \implies i \equiv j \ (\text{mod } \phi(M)) \)

\( \implies i = j \) since \( 0 \leq i, j \leq \phi(M) - 1 \)
Example: Let \( M = 7 \), \( \alpha = 3 \) is a PR.

\[
\begin{array}{cccccc}
1 & 2 & 3 & 4 & 5 & 6 \\
3 & 3 & 2 & 6 & 4 & 5 \\
6 & 3 & 2 & 3 & 6 & 1 \\
\end{array}
\]

The corollary predicts we would get a RRS. We can use the formula:

\[
\text{ORD}_7 3^2 = \frac{\text{ORD}_7 3}{\text{ORD}_7 3^2, 2} = \frac{6}{(6, 2)} = \frac{6}{2} = 3
\]

Corollary: If a PR \( \text{mod} \ M \) exists then there are exactly \( \phi(\phi(M)) \) non-congruent PR \( \text{mod} \ M \).

Proof: Let \( n \) be a PR \( \text{mod} \ M \). Thus \( \text{ORD}_M n = \phi(M) \). Any other PR is congruent to \( 12^i \) for \( 1 \leq i \leq \phi(M) \). By the previous corollary, so \( \text{ORD}_M n^i = \phi(n) \) for that \( i \).

Moreover,

\[
\text{ORD}_M n^i = \frac{\text{ORD}_M n}{\text{ORD}_M n^i, i} \iff \phi(n) = \frac{\phi(n)}{(\phi(n), i)}
\]

\( \iff (\phi(n), i) = 1 \) with \( 1 \leq i \leq \phi(M) \)

There are exactly \( \phi(\phi(M)) \) such \( i \). \( \Box \)
Recall that we aim to understand which integers have primitive roots.

Here are two examples of integers that do not have PR:

\[
\text{Ex 1: } M = 15, \quad \phi(15) = \phi(3) \cdot \phi(5) = 2 \cdot 4 = 8
\]

\[
\begin{array}{cccccccc}
\alpha & 1 & 2 & 4 & 7 & 8 & 11 & 13 & 14 \\
(\alpha, 15) = 1 & & & & & & & \\
\text{ord}_{15} \alpha & 1 & 4 & 2 & 4 & 4 & 4 & 2
\end{array}
\]

\[
\text{Ex 2: } M = 16, \quad \phi(16) = 8
\]

\[
\begin{array}{cccccccc}
\alpha & 1 & 3 & 5 & 7 & 9 & 11 & 13 & 15 \\
(\alpha, 16) = 1 & & & & & & & & \\
\text{ord}_{16} \alpha & 1 & 4 & 4 & 2 & 2 & 4 & 4 & 2
\end{array}
\]

\[
\text{Ex 3: There are no PR } \mod 8
\]

What is the issue in this cases?

Note that \( a \equiv 1 \pmod{15} \Rightarrow \begin{cases} a^8 \equiv 1 \pmod{3} \\ a^8 \equiv 1 \pmod{5} \end{cases} \)
However, from FLT
\[
\begin{align*}
\alpha^2 &\equiv 1 \pmod{3} \\
\alpha^4 &\equiv 1 \pmod{5}
\end{align*}
\Rightarrow \alpha^4 \equiv 1 \pmod{15}
\]

This is a general phenomenon:

**THM:** Let \( n \in \mathbb{Z}^+ \). Suppose \( M \) satisfies

\[M = kN, \quad (k, N) = 1, \quad \phi(k), \phi(N) \text{ are even}.
\]

Then, for all \( a \in \mathbb{Z} \) coprime to \( M \) we have

\[a^{\phi(M)} \equiv 1 \pmod{M}.
\]

In particular, there is no \( PR \mod M \).

**Proof:** By Euler's THM
\[
\begin{align*}
\alpha^\phi(k) &\equiv 1 \pmod{k} \\
\alpha^\phi(N) &\equiv 1 \pmod{N}
\end{align*}
\]

Let \( \ell = \text{LCM} \left( \phi(k), \phi(N) \right) = \frac{\phi(k) \cdot \phi(N)}{(\phi(k), \phi(N))} \)

Then \( \ell = \phi(k)k' = \phi(M)M' \Rightarrow \alpha^\ell \equiv 1 \pmod{k} \Rightarrow \alpha^\ell \equiv 1 \pmod{N} \)

Since \( \phi(k), \phi(N) \) are even \( \ell | \frac{\phi(k) \cdot \phi(N)}{2} = \frac{\phi(N)}{2} \)

\[\Rightarrow \alpha^{\ell/2} \equiv 1 \pmod{M} \]

\[\square\]
Corollary: If \( n \in \mathbb{Z}_{>0} \) is divisible by two different primes, then there are no primitive roots \( \text{Mod} \ M \).

Proof: Write \( M = p \cdot q \cdot r \cdot d \) with \( (p, p) = (r, q) = 1 \). Set \( k = p^d \) and \( N = q^e \cdot r \).

Thus \( M = k \cdot N \) and \( (k, N) = 1 \).

Moreover,

\[
\phi(k) = (p-1)^{d-1}, \quad \phi(N) = (q-1)^{e-1} \cdot \phi(r)
\]

are even, so we can apply the THM.

Corollary: If \( n \in \mathbb{Z}_{>0} \) is divisible by \( 4 \cdot p \) where \( p \) is an odd prime, then there are no primitive roots \( \text{Mod} \ M \).

Proof: Write \( M = 2^d \cdot p \cdot r \cdot d \cdot z \), \( (zp, r) = 1 \).

Set \( k = z^d \) and \( N = p^e \cdot r \).

Then \( M = k \cdot N \), \( (k, N) = 1 \) and

\[
\phi(k) = 2^{d-1} \cdot 1, \quad \phi(N) = (p-1)^{e-1} \cdot \phi(r)
\]

are even, so we apply the THM.
Lecture 26

THM: Suppose \( M = 2^d, \ d \geq 3 \). Then,

(A) \( a^{d-2} \equiv 1 \pmod{M} \) \( \forall a \text{ odd} \)

(B) THERE IS NO PR \( a \pmod{M} \)

PROOF: (B) We have \( \phi(M) = \phi(2^d) = 2^{d-1} \).

Since \( 2 < 2^{d-1} \) it follows from (A) there is no odd \( a \) with maximal order, i.e., APR.

(A) We use induction on \( d \geq 3 \).

\[ \text{Base: } d = 3 \implies \phi(M) = 8 \text{ and } 2^{d-2} = 2 \]

We check \( 1^2 = 1, \ 3^2 = 9 \equiv 1, \ 5^2 = 25 \equiv 1, \ 7^2 \equiv 1 \pmod{8} \).

Hypothesis: Suppose the result is valid for \( d-1 \); that is

\[ a^{d-3} \equiv 1 \pmod{2^{d-1}} \] (A)

\[ a^{d-3} = 1 + k \cdot 2^{d-1}, \ k \in \mathbb{Z} \]

STEP: (A) \( \implies a^2 = 1 + k \cdot 2^{d-1} \), \( k \in \mathbb{Z} \).

Squaring both sides gives

\[ a^2 = (1 + k \cdot 2^{d-1})^2 = 1 + k \cdot 2^d + k^2 \cdot 2^{2d-2} \]

\[ \implies a^2 \equiv 1 \pmod{2^d} \] since \( 2d-2 \geq d \).
From all the previous results we conclude that primitive roots may exist for integers of the form
\[
\begin{align*}
N &= 2^d, \ d \leq 2 \\
N &= p^d, \ p \text{ an odd prime }, \ d \geq 1 \\
N &= 2p^d, \ p \text{ an odd prime }, \ d \geq 1
\end{align*}
\]

Indeed, we have

\underline{Thm (Primitive Root Theorem)}

Let \( N \in \mathbb{Z} \). Then, a primitive root mod \( N \) exists if and only if \( N \)
is of the form
\[
N = 1, 2, 4, p^d \text{ or } 2p^d, \ \text{where } d \geq 1
\]
and \( p \) is an odd prime.
**Theorem (Legendre):**

Let \( p \) be a prime. Then, there exists a primitive root \( \mod p \).

The proof relies on 2 ingredients:

1. \( N = \sum_{d | N} \phi(d) \)

2. The following lemma:

**Lemma (Legendre):**

Let \( f(x) = x^N + a_{N-1}x^{N-1} + \ldots + a_1x + a_0 \)

be a polynomial with integer coefficients and degree \( N \geq 1 \).

Then, \( f \) has at most \( N \) roots \( \mod p \).
**Proof:** Induction + Contradiction

**Base:** \( N = 1 \).

\[ f(x) = x + a_0 \text{ has one root } x \equiv -a_0 \pmod{p} \]

**Hypothesis:** Suppose the statement holds for polynomials of degree \( n - 1 \).

**Step:** Let \( f \) be of degree \( n \).

We assume \( f \) has \( n + 1 \) roots \( \pmod{p} \) to get a contradiction.

Let \( c_0, c_1, \ldots, c_n \) denote the \( n + 1 \) roots \( \pmod{p} \).

That is, \( f(c_k) \equiv 0 \pmod{p} \) and \( c_i \not\equiv c_j \pmod{p} \)

\( \forall i \neq j \)

We compute,

\[ f(x) - f(c_0) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 - (c_0^n + a_{n-1}c_0^{n-1} + \ldots + a_1c_0 + a_0) \]

\[ = x^n - c_0^n + a_{n-1}(x^{n-1} - c_0^{n-1}) + \ldots + a_1(x - c_0) \quad (*) \]

Note that \( x - c_0 \equiv (x - c_0)h_{N-1}(x) \)

Where \( h_{N-1}(x) \) is a polynomial of degree \( n - 1 \).

Then,

\[ (*) = (x - c_0)h_{N-1}(x) + a_{n-1}(x - c_0)h_{n-2}(x) + \ldots + a_2(x - c_0)h_1(x) + a_1(x - c_0) = \]
\( \cos(x) = (x - c_0)g(x) \) where \( g(x) \) is a polynomial of degree \( N-1 \).

So \( f(x) - f(c_0) = (x - c_0)g(x) \).

Let \( C_k \neq c_0 \), that is \( k \geq L \). Then,

\[
\begin{align*}
    f(C_k) - f(c_0) &\equiv (C_k - c_0)g(C_k) \pmod{p} \\
                   &\implies f(C_k) \equiv f(c_0) \equiv 0 \pmod{p}
\end{align*}
\]

Since \( p \) is a prime and \( C_k - c_0 \neq 0 \pmod{p} \), then \( g(C_k) \equiv 0 \pmod{p} \) \( \forall k = 1, \ldots, N \).

So \( g \) has \( N \) roots \( \pmod{p} \) and degree \( N-1 \), a contradiction with induction hypothesis.
Theorem 1. If \( F(d) = \emptyset \), then \( x \in a \) or \( a \in x \).

1. \( \iff \) \( E \) or \( a \in \emptyset \) A and \( d \) when \( d \parallel x \).

2. Show that all elements of \( a \) and \( d \) exists.

We show that either \( F(d) = 0 \) or \( F(d) = \emptyset \).

Let \( F(d) \) denote the number of

Proof: Let \( F(d) \) denote the number of

In particular, the une \( \emptyset \) \( \emptyset \) or \( \emptyset \).

Thus the result exactly \( \phi(d) \), we receive a.

Then \( \emptyset \) or \( \emptyset \) is a prime. Let \( \emptyset \) be a prime.

which implies the theorem we seek.

We will prove the following result.

Note 2
We will first prove 2 assuming 1.

2) We will show \( F(d) = \phi(d) \) \( \forall d \mid p-1 \). In particular, an element (actually \( \hat{\phi}(d) \)) exists with order \( d \).

Recall: 1) \( \sum_{d \mid n \atop d > 1} \phi(d) = N \)

Since every integer \( a \) in \( \mathbb{Z}_p \) has an order and \( \text{ord}_p a \mid \phi(p) = p-1 \) we have

\[
\sum_{d \mid p-1 \atop d > 1} F(d) = p-1 \quad \overset{\bullet}{=} \quad \sum_{d \mid p-1 \atop d > 1} \phi(d)
\]

We partition the elements by orders.

From 1) we know that if \( F(d) \neq 0 \) then \( F(d) = \phi(d) \)

So we can subtract \( F(d) = \phi(d) \) at both sums every time.

We have a divisor \( d \) s.t. \( F(d) \neq 0 \) to get

\[
\sum_{d \mid p-1 \atop F(d) = 0} F(d) = 0 = \sum_{d \mid p-1 \atop F(d) = 0} \phi(d)
\]

Since \( \phi(d) \geq 1 \) there is nothing left on the sum.

And we conclude \( F(d) = \phi(d) \) \( \forall d \mid p-1 \), as desired.
Lecture 27

**Theorem:** Let \( p \) be a prime. Let \( d \) divide \( p-1 \).

Then, there are exactly \( \phi(d) \) integers \( a \) such that \( 1 \leq a \leq p-1 \) and \( \text{ord}_p a = d \).

In particular, there are \( \phi(p-1) \) PR \( \text{mod} \) \( p \).

**Proof:** Let \( F(d) \) denote the number of integers \( a \) such that \( 1 \leq a \leq p-1 \) and \( \text{ord}_p a = d \).

\( i \) We will show that either \( F(d) = 0 \) or \( F(d) = \phi(d) \).

\( \rightarrow \) If \( F(d) = 0 \) there are no integers of order \( d \).

\( \rightarrow \) Suppose there is an integer of order \( d \). Denote it by \( a \).

- Note that any integer of order \( d \) is a root of \( f(x) = x^d - 1 \); since \( f(y) \equiv y^d - 1 \equiv 0 \) \( \implies y \equiv 1 \) \( \text{mod} \) \( p \).

Moreover, \( f(a^i) \equiv (a^i)^d - 1 = (a^d)^i - 1 \equiv 1^i - 1 \equiv 0 \) \( \text{mod} \) \( p \)

and \( a, a^i, ..., a^{d-1} \) \( \text{mod} \) \( p \) are distinct because \( d = \text{ord}_p a \).

Then, by Lagrange's Lemma, we conclude that the \( a^i \) are all the roots of \( f \) \( \text{mod} \) \( p \).

\( \rightarrow \) Then, all the elements of order \( d \) are among the \( a^i \).
So, we need to count how many of the $a_i$ have order $d$. We know that:

\[
\text{ord}_p a_i = \text{ord}_p a \iff d = \frac{d}{(d, i)} \iff (d, i) = 1
\]

which occurs exactly for $\phi(d)$ values of $i$, i.e. $d_i$.

1. Show that an element of order $d$ exists if $d \mid p-1$.

Recall: \[\sum_{d \mid n} \phi(d) = n\]  \hspace{1cm} (\star)

Since every $a_i$ in $\mathbb{Z}_p$ has an order and $\text{ord}_p a_i \mid \phi(p)$,

we have:

\[\sum_{d \mid p-1} F(d) = p-1 = \sum_{d \mid p-1} \sum_{d > 1} \phi(d)\]

From (\star) we know that if $F(d) \neq 0$ then $F(d) = \phi(d)$.

So we can subtract $F(d)$ to both sums at divisors $d$ for which $F(d) \neq 0$, to get:

\[\sum_{d \mid p-1} F(d) = 0 = \sum_{d \mid p-1} \phi(d) \Rightarrow \phi(d) = 0 = F(d)\]  \hspace{1cm} (\text{only when } F(d) = 0)

so $F(d) = \phi(d)$ for all $d \mid p-1$.
Let: There is no formula to produce \( P_N \).

- The probability of finding one at random is \( \frac{\phi(p-1)}{p-1} \).

Ex: Find all integers of order 6 modulo 19, knowing that 2 is a primitive root mod 19.

We have \( \phi(6) = 2 \) so there are 2 integers of order 6 in \( 1 \leq x \leq \phi(19) = 18 \). We know that \( 2^1 \equiv 1 \equiv 18 \) generates all the residues mod 19 which are \( \neq 0 \) those of order 6 correspond to the values of \( i \) satisfying

\[
\text{ord}_{19} 2 = \frac{\text{ord}_{19} 2}{(\text{ord}_{19} 2, 1, i)} = 6
\]

\( (18, i) = 3 \) because \( \text{ord}_{19} 2 = 18 \).

\( \Rightarrow i = 3 \) \( \text{ord}_{19} 1 = 15 \)

Then, \( 2^3 \equiv 8 \pmod{19} \)

\[
2^{15} \equiv (2^4)^3 \cdot 2^3 \equiv (-3)^3 \cdot 8 \equiv -64 \equiv 12 \pmod{19}
\]

Are the two residues of order 6.
**THM (Primitive Root Theorem):** Let \( N \in \mathbb{Z}/p \). Then, there is a \( \text{PR} \ mod \ N \) \( \Rightarrow N = 1, 2, 4, p, 2p \) where \( p \) is an odd prime, \( d \geq 1 \).

**THM:** Let \( N = 2p^d \), \( p \) an odd prime, \( d \geq 1 \). Then, there exists a \( \text{PR} \ mod \ N \).

**REM:** We will assume there is a \( \text{PR} \ mod \ p^d \) which is proved in the book.

**Proof:** Let \( \alpha \) be a primitive root \( \mod p^d \)

- We can assume \( \alpha \) is odd, otherwise replace it with \( 12 + p^d \) which is also a \( \text{PR} \ mod \ p^d \) since \( 12 + p^d \equiv 1 \pmod{p^d} \).

So, \( (2p^d, 12) = 1 \). We will show that \( 12 \) is also \( \text{PR} \ mod \ N = 2p^d \).

Note \( \phi(2p^d) = \phi(2) \phi(p^d) = \phi(p^d) \Rightarrow \text{ORD}_N 12 | \phi(2p^d) = \phi(p^d) \)

Now \( \text{ORD}_N R^2 \equiv 1 \pmod{2p^d} \Rightarrow \text{ORD}_N R^2 \equiv 1 \pmod{p^d} \)

\( \Rightarrow \text{ORD}_p 12 | \text{ORD}_N 12 \Rightarrow \phi(p^d) | \text{ORD}_N 12 \)

Since \( \text{ORD}_N R \), \( \phi(p^d) \) are positive and we have shown \( \text{ORD}_N R | \phi(p^d) \) and \( \phi(p^d) | \text{ORD}_N 12 \) we conclude \( \text{ORD}_N 12 = \phi(p^d) = \phi(2p^d) \), that is, \( 12 \) is \( \text{PR} \ mod \ N = 2p^d \).
Index Arithmetic (Discrete Logarithms)

Let \( p \) be a PR \( \bmod N \).
Recall that \( \{1, 2, 3, \ldots, \phi(N)-1\} \) is a residue system \( \bmod N \), so \( \forall a \in \mathbb{Z} \) s.t. \( (a, N) = 1 \) we have
\[
1^i \equiv a \pmod{N}
\]
for some \( i \), \( 1 \leq i \leq \phi(N)-1 \).

Definition: Fix \( p \) a PR \( \bmod N \). For \( a \in \mathbb{Z} \), \( (a, N) = 1 \), the index of \( a \) relative to \( p \) is the least positive integer \( i \) s.t. \( 1^i \equiv a \pmod{N} \). We denote it by \( \text{IND}_p a \).

Example: \( N = 7 \), \( p = 3 \)

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>3</td>
<td>2</td>
<td>6</td>
<td>4</td>
<td>5</td>
<td>1</td>
</tr>
</tbody>
</table>

\[ \text{IND}_3 1 = 6, \quad \text{IND}_3 2 = 1, \quad \text{IND}_3 3 = 4, \quad \text{IND}_3 4 = 5, \quad \text{IND}_3 5 = 3 \]

The reason why indices are called "discrete logs" is that they "share" properties with usual logs in real numbers.
Proposition: Let $R$ be a PR mod $N$.

Let $a, b \in \mathbb{Z}$ coprime to $N$.

(a) $\text{IND}_R 1 \equiv 0 \pmod{\phi(n)}$

(b) $\text{IND}_R 1 \equiv 1 \pmod{\phi(n)}$

(c) $\text{IND}_R (a \cdot b) \equiv \text{IND}_R a + \text{IND}_R b \pmod{\phi(n)}$

(d) $\text{IND}_R a^d \equiv d \cdot \text{IND}_R a \pmod{\phi(n)}$, $d \in \mathbb{Z}_{\geq 0}$

Proof: (a) By FT $1^2 \equiv 1 \pmod{N}$ and since $N$ is PR no smaller positive exponent has this property so $\text{IND}_R 1 = \phi(n) \equiv 0 \pmod{\phi(n)}$

(b) Since 1 is the smallest positive exponent such that $1^2 \equiv 1 \pmod{N}$ we have $\text{IND}_R 1 = 1^2 \equiv 1 \pmod{\phi(n)}$

(c) By definition of IND we have

\[
\begin{align*}
\text{IND}_R (a \cdot b) & \equiv a \cdot b^\ast \mod N \\
\text{IND}_R a \cdot b & \equiv \text{IND}_R a + \text{IND}_R b \mod N
\end{align*}
\]

\[
\Rightarrow \text{IND}_R (a \cdot b) \equiv \text{IND}_R a + \text{IND}_R b \pmod{\phi(n)}
\]

(d) Exercise
Lecture 28

**Proposition:** Let $L$ be a PR mod $N$.

Let $a, b \in \mathbb{Z}$ coprime $N$.

(a) $\text{IND}_L a \equiv 0 \pmod{\phi(N)}$

(b) $\text{IND}_L a \equiv 1 \pmod{\phi(N)}$

(c) $\text{IND}_L (ab) \equiv \text{IND}_L a \cdot \text{IND}_L b \pmod{\phi(N)}$

**Proof:**

(a) By Euler's Theorem $L^\phi(N) \equiv 1 \pmod{N}$

And since $L$ is PR no positive scalar exponent has this property, so $\text{IND}_L 1 \equiv \phi(N) \equiv 0 \pmod{\phi(N)}$

(b) Since $1$ is the smallest positive exponent such that $L^1 \equiv 1 \pmod{N}$ we have $\text{IND}_L 1 \equiv 1 \equiv 1 \pmod{\phi(N)}$

(c) By definition of index we have $\text{IND}_L a \cdot b \equiv \text{IND}_L a \cdot \text{IND}_L b \equiv \text{IND}_L (ab) \equiv \text{IND}_L a \cdot \text{IND}_L b \pmod{\phi(N)}$

(c) Similar to (c), exercise
We can use indices to solve certain equations in congruences.

Let \( \ell \) be a PL mod \( N \). Consider the equation

\[
ax^d \equiv \ell \pmod{N}
\]

Rewrite it as

\[
\text{ind}_R ax^d \equiv \text{ind}_R \ell \pmod{N}
\]

\[\iff \text{ind}_R ax^d \equiv \text{ind}_R \ell \pmod{\phi(N)}\]

\[\iff \text{ind}_R a + d \text{ind}_R x \equiv \text{ind}_R \ell \pmod{\phi(N)}\]

\[\iff d \text{ ind}_R x \equiv \text{ind}_R \ell - \text{ind}_R a \pmod{\phi(N)} \quad (\star)\]

Relabeling \( y = \text{ind}_R x \), \( a' = d \), \( \ell' = \text{ind}_R \ell - \text{ind}_R a \)

The congruence \((\star)\) becomes

\[a' y \equiv \ell' \pmod{\phi(N)}\]

which is a linear congruence in one variable, so we know how to solve it.

REM: To do practical computations it is important to compile tables of indices:

\begin{align*}
\text{Ex: } N = 17, \ 12 \equiv 3 \text{ is a primitive root } \\
\begin{array}{cccccccccccccccc}
\alpha & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\
\text{ind}_8 \alpha & 1 & 14 & 11 & 12 & 5 & 15 & 11 & 10 & 2 & 3 & 7 & 13 & 4 & 9 & 6 & 8
\end{array}
\end{align*}
Ex: Solve \( 6^x \equiv 1 \pmod{17} \)

We have \( \phi(17) = 16 \) and taking indices in both sides gives \( \text{IND}_3 (6^x) \equiv \text{IND}_3 1 \pmod{16} \)

\[ \Rightarrow \text{IND}_3 6 + 12 \text{IND}_3 x \equiv \text{IND}_3 1 \pmod{16} \]

\[ \Rightarrow 15 + 12 \text{IND}_3 x \equiv 7 \pmod{16} \]

\[ \Rightarrow 12 \text{IND}_3 x \equiv 8 \pmod{16} \quad \overset{(*)}{\iff} \quad 3 \text{IND}_3 x \equiv 2 \pmod{4} \]

\[ \Rightarrow \text{IND}_3 x \equiv 2, 6, 10, 14 \pmod{16} \]

\[ \Rightarrow 3^x \equiv 3, 3, 3, 3 \pmod{17} \]

\[ \Rightarrow x \equiv 9, 15, 8, 2 \pmod{17} \]

Ex: Solve \( 7^x \equiv 6 \pmod{17} \)

Taking indices \( \Rightarrow \text{IND}_3 7^x \equiv \text{IND}_3 6 \pmod{16} \)

\[ \Rightarrow x \cdot \text{IND}_3 7 \equiv \text{IND}_3 6 \quad \overset{(*)}{\iff} \quad 11 x \equiv 15 \pmod{16} \]

\[ \Rightarrow 3 \cdot 11 x \equiv 45 \pmod{16} \quad \overset{(*)}{\iff} \quad x \equiv 13 \pmod{16} \]
We have used indices to solve particular congruence equations.

We also have the following general result:

**Theorem:** Let \( N \) be an integer admitting a primitive root. Let \( a \in \mathbb{Z} \), \((a,N)=1\). Consider the congruence equation

\[
    x^k \equiv a \pmod{N}
\]

(A) If \( a \not\equiv 1 \pmod{N} \), where \( d = (k, \phi(N)) \), then \((*)\) has no solutions.

(B) If \( a^d \equiv 1 \pmod{N} \), then there are exactly \( d \) solutions \( \pmod{N} \).

**Proof:** Let \( R \) be a primitive root \( \pmod{N} \).

\[
    x^k \equiv a \pmod{N} \Leftrightarrow \text{ind}_R x^k \equiv \text{ind}_R a \pmod{\phi(N)}
\]

\[\Leftrightarrow k \text{ind}_R x \equiv \text{ind}_R a \pmod{\phi(N)} \Leftrightarrow ky \equiv \text{ind}_R a \pmod{\phi(N)} \]

This is a linear congruence in \( y \) that has no solutions if \( d = (k, \phi(N)) \nmid \text{ind}_R a \) and has exactly \( d \) solutions if \( d \mid \text{ind}_R a \).
Finally, note \( A \equiv 1 \pmod{N} \iff \)

\[
\text{IND}_R A^{\phi(n)/d} \equiv \text{IND}_R 1 \equiv 0 \pmod{\phi(n)}
\]

\[
\Leftrightarrow \left( \frac{\phi(n)}{d} \right), \text{IND}_R A \equiv 0 \pmod{\phi(n)}
\]

\[
\Leftrightarrow d \mid \text{IND}_R A, \text{ proving (A) and (B)} \ 
\]

Example: Solve \( x^3 \equiv 6 \pmod{7} \)

In this notation

\( a = 6, \ N = 7, \ k = 3 \)

\( d = (3, \phi(7)) = (3, 6) = 3 \)

Compute \( \frac{\phi(n)}{d} \)

\( 2 = 6 \equiv 36 \equiv 1 \pmod{7} \)

Thus \( x^3 \equiv 6 \pmod{7} \) has exactly \( d = 3 \) non-congruent solutions