Chapter 9
Primitive Roots

邱錫彥 老師

Contents

9.1 The order of an integer and primitive root

- If $(a, m) = 1$, then $\exists\ \phi(m) \ni a^{\phi(m)} = 1 \bmod m$, $\phi(m) \in Z^+$. Thus by the well-order property, $\exists$ a least positive integer $x \ni a^x = 1 \bmod m$.

> *Def:*
>
> Let $(a, m) = 1$,
> the least positive integer $x \ni a^x = 1 \bmod m$
> is called the order of a modulo m,
> denoted by $\text{ord}_m a$.

Thm:

If$(a, n)=1$, then $a^x = 1 \bmod n$, iff $(ord_n a) | x$.

Proof:

$\rightarrow$ If $ord_n\, a | x$, then $\exists\, k \in z \ni x = k \cdot ord_n a$

$\therefore\ a^x = (a^{ord_n a})^k = 1 \bmod n$

$\leftarrow$ If $a^x = 1 \bmod n$. Let $x = q\ ord_n\, a + r$,

$0 \leq r < ord_n a$.

Thus, $\therefore\ a^x = (\, a^{\,ord_n\, a}\,)^q \cdot a^r = 1 \bmod n$

$\because\ 0 \leq r < ord_n a$, and $ord_n a$ is the least

integer $\ni a^{ord_n a} = 1 \bmod n$

$\therefore r = 0 \Rightarrow ord_n a | x$

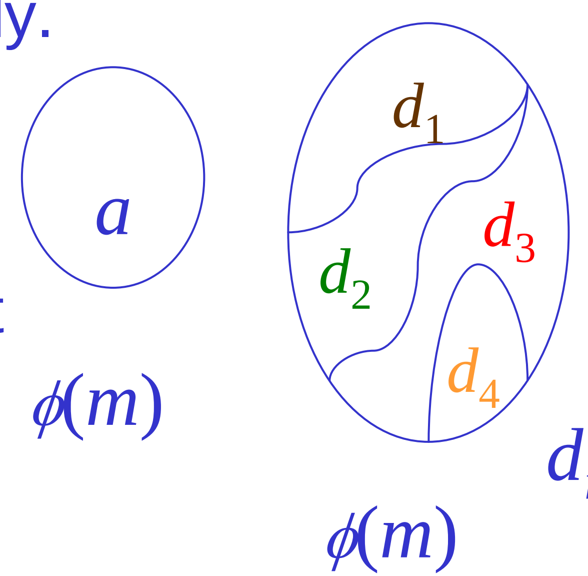
Corollary:

If $(a, m) = 1$, then $\mathrm{ord}_m a \mid \phi(m)$

Proof:

Following by Euler Theorem and above Theorem directly.

Reduced reside set



$d_i \mid \phi(m)$

$m = 11$

$\phi(m) = 10$

$1 \mid \phi(m)$, $2 \mid \phi(m)$

$5 \mid \phi(m)$, $10 \mid \phi(m)$

Thm:

If $(a, n) = 1$, then $a^i = a^j \bmod n$ iff $i = j \bmod (\mathrm{ord}_n a)$

Proof:

($\rightarrow$) If $i = j \bmod (\mathrm{ord}_n a)$,

then $a^i = a^{j+k\cdot \mathrm{ord}_n a} = a^j \bmod n$

($\leftarrow$) If $a^i = a^j \bmod n$.

$\because a^i = a^j \cdot a^{i-j} \bmod n \Rightarrow a^j \cdot a^{i-j} = a^j \bmod n$

$\because (a, n) = 1 \Rightarrow (a^j, n) = 1$.

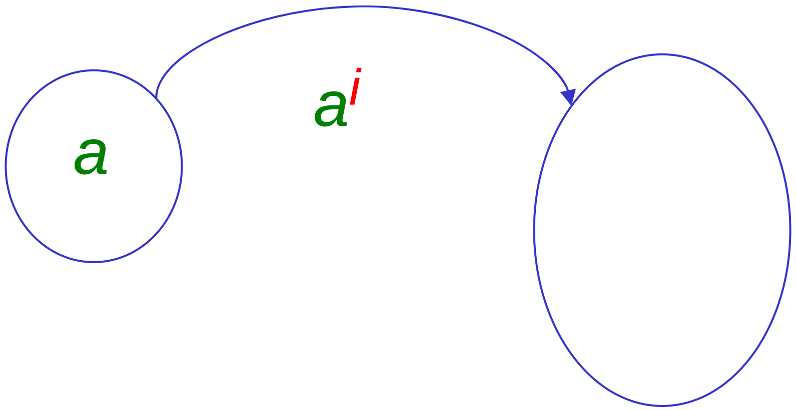
Thus, by Cancellation of a^j, we have $a^{i-j} = 1 \bmod n$

$\Rightarrow \mathrm{ord}_n a \mid (i - j)$, thus, $i = j \bmod (\mathrm{ord}_n a)$

Primitive roots

Def:

If $(r, n) = 1$ and if $\text{ord}_n r = \phi(n)$,
then r is called a primitive root modulo n.



Reduced reside set

$\phi(m)$

Question:

1. For any given n, does a primitive root modulo n exist?
2. If it exists, how to find one?
3. How to find all the primitive roots?

Thm:

If $(r, n) = 1$ and r is a primitive root modulo n, then the set of integers $S = \{r^1, r^2, \ldots, r^{\phi(n)}\}$ form a reduced residue set modulo n.

Proof:

We must show that

(1) $(r^i, n) = 1, \forall 1 \leq i \leq \phi(n)$

(2) $r^i \neq r^j \bmod n \; \forall\, i \neq j$ and $1 \leq i \leq \phi(n)$, $1 \leq j \leq \phi(n)$

(1) $\because$ $(r, n) = 1$, $\therefore$ $(r^i, n) = 1$ for any $i \in Z^+$

(2) Assume that $r^i = r^j \bmod n$, then $i = j \bmod \phi(n)$,

however, for $1 \le i \le \phi(n)$ and $1 \le j \le \phi(n)$, it

implied that $i = j$,

$\therefore S$ is a reduced residue set modulo n. ■

Thm:

If $\text{ord}_m a = t$ and if $u \in Z^+$, then $\text{ord}_m(a^u) = \dfrac{t}{(t, u)}$

Proof:

Let $s = \text{ord}_m(a^u)$, $v = (t, u)$, $t = t_1 v$ and $u = u_1 v$
then $(t_1, u_1) = 1$.

(1) $\because (a^u)^{t_1} = (a^{u_1 v})^{t/v} = (a^t)^{u_1} = (1)^{u_1} = 1 \bmod m$

$\therefore s = \text{ord}_m(a^u) | t_1$

(2) $\because (a^u)^s = a^{us} = 1 \bmod m$, $\therefore t = \text{ord}_m a | us$

$\Rightarrow t_1 v \,|\, u_1 v s \Rightarrow t_1 | u_1 s$

But $(t_1, u_1) = 1 \Rightarrow t_1 | s$

$\therefore s = \text{ord}_m(a^u) = t_1 = \dfrac{t}{v} = \dfrac{t}{(t, u)}$ ■

Corollary:

Let r be a primitive root modulo m. Then r^u is a primitive root modulo m iff $(u, \phi(m)) = 1$.

Proof:

$$\because \ \mathrm{ord}_m r^u = \frac{ord_m r}{(u, ord_m r)} = \frac{ord_m r}{(u, \phi(m))} = \phi(m)$$

$\therefore$ r^u is a primitive root modulo m iff $(u, \phi(m)) = 1$. ■

Thm:

If $m \in Z^+$ has a primitive root, then it has a total of $\phi(\phi(m))$ incongruent roots.

Proof:

Let r be a primitive root modulo m, then $r^1, r^2, \ldots, r^{\phi(m)}$ form a reduced residue system modulo m.

However, r^u is a primitive root iff $(u, \phi(m)) = 1$. Since there are exactly $\phi(\phi(m))$ such u, there are exactly $\phi(\phi(m))$ primitive roots modulo m. ■

- Thus, if we can find a primitive root r modulo m, then we can generate all the primitive root modulo m by calculating r^u mod m, where $(u, \phi(m)) = 1$.

- If $p = 2q + 1$, where p, q are primes.

  $\Rightarrow \phi(\phi(p)) = \phi(2q) = q - 1$

  $\Rightarrow$ rates of primitive root:

  $$\frac{q-1}{2q+1} \approx \frac{1}{2}, \text{ if } q >> 1.$$

9.2 Primitive roots for primes

- Every prime has a primitive roots.

Def:

Let $f(x)$ be a polynomial with integer coefficients. An integer c is said to be a root of $f(x)$ modulo m if $f(c) = 0 \bmod m$.

Remark:

1. If c is a root of $f(x)$ mod m, then u is also a root if $u = c \bmod m$.
2. $h(x) = x^{p-1}-1$ has exactly $p-1$ incongruent roots modulo p, where p is prime, (i.e., $x = 1, 2\ldots, p-1 \pmod p$)

Thm: Lagrange's Theorem

Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$ be a polynomial of degree n, $n \geq 1$, with $a_i \in Z$ and $p \nmid a_n$, then $f(x)$ has at most n incongruent roots modulo p.

Proof: By mathematical induction.

When $n = 1$, then $x = -\frac{a_0}{a_1}$ is the only root modulo p of $f(x)$. Thus it is true for $n = 1$.

Suppose it is true for polynomials of degree n-1.
Let $f(x)$ be such a polynomial of degree n.
Assume $f(x)$ has n+1 incongruent roots modulo p, say $c_0, c_1, \ldots c_n \ni f(c_k) = 0 \bmod p$ for $k = 0, 1, \ldots, n$.

We have $f(x) - f(c_0) = a_n(x^n - c_o^n) + \ldots + a_1(x - c_0)$

$$= (x - c_0)g(x)$$

Where $g(x)$ is a polynomial of degree n-1.

$\because f(c_k) - f(c_0) = (c_k - c_0)g(c_k) = 0 \bmod p$ and $c_k \neq c_0 \bmod p$

$\Rightarrow g(c_k) = 0$.

$\therefore c_k$ is a root of $g(x)$ mod p.

$\therefore g(x)$ has n incongruence roots modulo p.

This contradicts the induction hypothesis.

Hence $f(x)$ must have no more than n incongruent roots modulo p. ■

Thm:

Let p be prime and $d \mid p$-1. Then the polynomial x^d -1 has exactly d incongruent roots modulo p.

Proof:

Let p -1 = de, then

$x^{p-1} - 1 = (x^d - 1)(x^{d(e-1)} + x^{d(e-2)} + \ldots + x^d + 1) = (x^d - 1)g(x)$

$\because$ x^{p-1}-1 has p -1 incongruent roots modulo p and any root of x^p -1 modulo p is either a root of x^d -1 mod p or a root of $g(x)$ modulo p.

But $g(x)$ has at most $d(e-1) = de - d = p - d - 1$ roots modulo p.

$\therefore$ the polynomial $x^d - 1$ has at least $(p-1) - (p-d-1) = d$ incongruent roots. On the other hand, $x^d - 1$ has at most d incongruent roots modulo p.

$\therefore$ $x^d - 1$ has exactly d incongruent roots modulo p. ■

Thm 9.8:

Let p be a prime and let $d \in Z^{+}$ and $d \mid p - 1$.
Then the number of incongruent integers of order d modulo p is equal to $\phi(d)$.

Proof:

Let $F(d)$ denote the number of positive integers of order d modulo p that are less than p,

then $p-1 = \sum_{d \mid p-1} F(d)$

However, $p-1 = \sum_{d \mid p-1} \phi(d) \Rightarrow \sum_{d \mid p-1} \phi(d) = \sum_{d \mid p-1} F(d)$.

If we can prove that $F(d) \leq \phi(d)$.then we have $F(d) = \phi(d)$. Let $d \mid (p-1)$. If $F(d) = 0$, then $F(d) \leq \phi(d)$.

Otherwise, $\exists\ a \ni \text{ord}_p a = d$ satisfying $a^1, a^2, \ldots, a^d$ are incongruent modulo p.

And $(a^k)^d \bmod p = 1\ \forall k \in Z^+$.

$\because x^d - 1 \bmod p$ has exactly d incongruent roots modulo p, so every root modulo p is congruent to one of a^i, $1 \leq i \leq d$.

But the power of a with order d are those of the form a^k with $(k, d) = 1 \Rightarrow F(d) \leq \phi(d)$ ■

Ex:

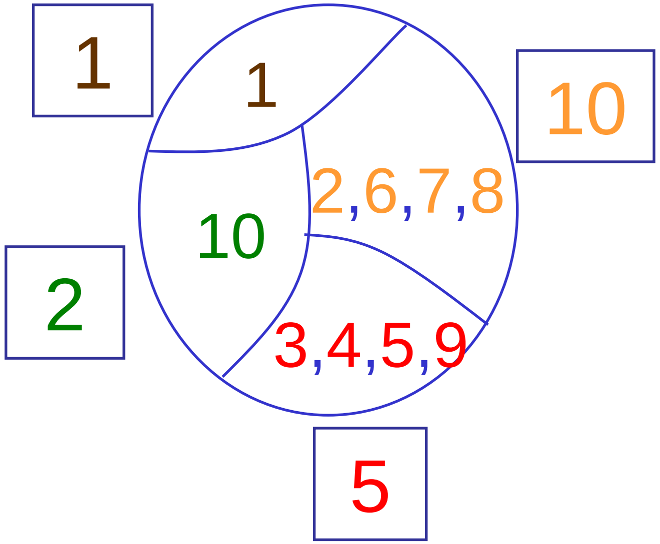
Let $p = 11$,

$1^1 = 1 \bmod p$, $2^{10} = 1$, $3^5 = 1$, $4^5 = 1$, $5^5 = 1$

$6^{10} = 1$, $7^{10} = 1$, $8^{10} = 1$, $9^5 = 1$, $10^2 = 1$

d	order d modulo p	$\phi(d)$
10	2, 6, 7, 8	4
5	3, 4, 5, 9	4
2	10	1
1	1	1

$\phi(p)=10$



Corollary :

Every prime of has a primitive root.

Proof:

Let p be prime. From above theorem, there are $\phi(p-1)$ incongruent integers of order $p-1$ mod p.

$\therefore$ p has $\phi(p-1)$ primitive roots.

- Let r be a primitive root modulo n and the factors of $\phi(n)$ be $d_1, d_2, \ldots, d_k$. Finding all primitive roots modulo n.

Sol: Find all integers s such that $(s, \phi(n)) = 1$.
Then all r^s mod n are also primitive roots modulo n.

- $r^{\frac{\phi(n)}{d_1}}$ mod n is an element whose order is d_1.

9.3 The existence of Primitive Roots

Object:

To find all positive integers having primitive roots.

Thm:

If p is an odd prime with primitive root r,
then either r or $r + p$ is a primitive root modulo p^2.

Proof:

Since r is a primitive root modulo $p \Rightarrow \text{ord}_p r = \phi(p) = p\text{-}1$

Let $n = \text{ord}_{p^2} r$, then $r^n = 1 \bmod p^2 \Rightarrow r^n = 1 \bmod p$.

$\therefore p - 1 | n$ and $n | \phi(p^2) = p(p - 1)$

$\Rightarrow n = p - 1$ or $n = p(p - 1)$ (1)

(1) If $n = p(p-1)$, then r is a primitive root modulo p^2.

(2) If $n = p-1 \Rightarrow r^{p-1} = 1 \bmod p^2$.

Let $s = r + p$. (Note s is also a primitive root mod p)

Then $s^{p-1} = (r+p)^{p-1}$

$$= r^{p-1} + (p-1)r^{p-2}p + \binom{p-1}{2} r^{p-3}p^2 + \ldots + p^{p-1}$$

$$= r^{p-1} + (p-1)r^{p-2}p \bmod p^2$$

$$= 1 + (p-1)pr^{p-2} \bmod p^2$$

$\because pr^{p-2} \neq 0 \bmod p^2 \Rightarrow s^{p-1} \neq 1 \bmod p^2 \Rightarrow \mathrm{ord}_{p^2} s \neq p-1$

$\therefore \mathrm{ord}_{p^2} s = p(p-1) = \phi(p^2)$

$\Rightarrow s = r + p$ is a primitive root mod p^2. ■

Ex:

The prime $p = 7$ has $r = 3$ as a primitive root.

From (1) $\Rightarrow$ either $\text{ord}_{49}3 = 6$ or $\text{ord}_{49}3 = 42$.

$\because 3^6 \neq 1 \bmod 49 \Rightarrow \text{ord}_{49}3 = 42\ (= 7\times 6)$,

$\Rightarrow$ 3 is a primitive root mod 49.

Note:

1. It is very seldom that a primitive root r modulo p is not also a primitive root modulo p^2.
2. If r is a primitive root modulo p^2, and $r < p$, then r is also a primitive root modulo p.

Thm:

Let p be an odd prime. Then p^k has a primitive root for all $k \in Z^+$. Moreover, if r is a primitive root modulo p^2, then r is a primitive root modulo p^k, for all positive integers k.

Ex:

3 is a primitive root modulo 7 and 7^2.

$\therefore$ 3 is also a primitive root modulo 7^k, $\forall k \in Z^+$.

Proof: Strategy: $\phi(p^k) = p^{k-1}(p-1)$

1. If r is a primitive root modulo p^2, i.e. $r^{p-1} \neq 1 \bmod p^2$.

   Show that $r^{p^{k-2}(p-1)} \neq 1 \bmod p^k$ (1)

   (By mathematical induction)

2. Using mathematical induction, show that

$$\mathrm{ord}_{p^k} r = p^{k-1}(p-1) = \phi(p^k)$$

(1)The case of $k = 2$ is true, since r is a primitive root modulo p^2. Assume that it is true for $k \geq 2$. Then

$$r^{p^{k-2}(p-1)} \neq 1 \bmod p^k.$$

$\because (r, p)=1 \Rightarrow (r, p^{k-1}) = 1$. $\therefore$ from Euler's Thm., we have $r^{p^{k-2}(p-1)} = r^{\phi(p^{k-1})} = 1 \bmod p^{k-1}$

$= 1 + dp^{k-1}$, where $p \nmid d$.

$$\therefore (r^{p^{k-2}(p-1)})^p = r^{p^{k-1}(p-1)} = (1+dp^{k-1})^p = 1 + p(dp^{k-1}) +$$

$$+ \binom{p}{2}(dp^{k-1})^2 + \ldots + (dp^{k-1})^p = 1 + dp^k \bmod p^{k+1}$$

$$\because p \nmid d, \therefore\ r^{p^{k-1}(p-1)} \neq 1 \bmod p^{k+1}$$

(2)Let $n = \text{ord}_{p^k} r$, then $n \mid \phi(p^k) = p^{k-1}(p-1)$. However, since $r^n = 1 \bmod p^k \Rightarrow r^n = 1 \bmod p \Rightarrow p-1 \mid n$.

$\therefore n = p^t(p-1)$, where $t \in z \ni 0 \le t \le k-1$.

If $0 \le t \le k-2$, then $r^{p^{k-2}(p-1)} = (r^{p^t(p-1)})^{p^{k-2-t}} = 1$ mod $p^k \Rightarrow r^{p^{k-2}(p-1)} = 1$ mod p^k, it would contradict (1)

$\therefore\ n = \text{ord}_{p^k} r = p^{k-1}(p-1) = \phi(p^k)$

$\Rightarrow$ r is also a primitive root modulo p^k ■

補充 ❖ How to find a primitive root modulo n?

Let $\phi(n) = p_1^{t_1} p_2^{t_2} \ldots p_k^{t_k}$ $t_1 \geq 1, \forall 1 \leq i \leq k$.

1. Randomly choose an integer r, $1 < r < n-1$.

   Check if $r^{\frac{\phi(n)}{p_i}} \neq 1 \mod n, \forall 1 \leq i \leq k$ (1)

2. If (1) holds for all i, then r must be a primitive root modulo n.

Ex. $n=37$, $\phi(n)=2^2 \times 3^2$, d=1,2,3,4,6,9,12,18.36

補充 n=37, $\phi(n)=2^2\times 3^2$, d=1,2,3,4,6,9,12,18.36

$$\frac{\phi(n)}{2}=18 \qquad \frac{\phi(n)}{3}=12 \qquad \frac{\phi(\phi(n))}{\phi(n)}=\frac{\phi(2p)}{2p}=\frac{p-1}{2p}\approx\frac{1}{2}$$

? If $n = 2p + 1$, $a(\bmod n_1) = a(\bmod n_2)$

If $n_2 \mid n_1$ and $(a \bmod n_1) < n_2$.

$A=kn_1 + b$, $7 \bmod 4 \neq 7 \bmod 2$

Thm: If *a* is an odd integer and if $k \in Z^+$, $k \geq 3$, then

$$a^{\frac{\phi(2^k)}{2}} = a^{2^{k-2}} \equiv 1 \mod 2^k$$

Proof:

By using mathematical induction.

If *a* is an odd integer, then $a = 2b + 1$, $b \in Z^+ \cup \{0\}$

$\therefore a^2 = (2b + 1)^2 = 4b^2 + 4b + 1 = 4b(b + 1) + 1$

Since either *b* or *b*+1 is even $\Rightarrow 8 \mid 4b(b + 1)$

$\Rightarrow a^2 = 1 \bmod 8 \quad \therefore$ It is true when $k = 3$.

Assume that $a^{2^{k-2}} = 1 \bmod 2^k$, then

$$\exists d \in z^{+} \ni a^{2^{k-2}} = 1 + d \cdot 2^{k}$$

$$\therefore a^{2^{k-1}} = (a^{2^{k-2}})^{2} = 1 + d \cdot 2^{k+1} + d^{2} \cdot 2^{2k}$$

$$\Rightarrow a^{2^{k-1}} = 1 \text{ mod } 2^{k+1}$$

■

Remark:

1. From this theorem we know that no power of 2, other than 2 and 4, has a primitive root.
2. The largest possible order modulo 2^k, $k \geq 3$, is

$$\frac{\phi(2^k)}{2} = 2^{k-2}.$$

Thm:

Let $k \geq 3$, then $\text{ord}_{2^k} 5 = \frac{\phi(2^k)}{2} = 2^{k-2}$.

Proof:

Since $5^{2^{k-2}} = 1 \bmod 2^k$ (from above theorem), if we can prove that $\text{ord}_{2^k} 5 \nmid 2^{k-3}$,

i.e, $5^{2^{k-3}} \neq 1 \bmod 2^k$, then $\text{ord}_{2^k} 5 = 2^{k-2}$.

By mathematical induction, for $k = 3$,

$5 = 1 + 4 \bmod 8$

$= 1 + 2^{k-1} \bmod 2^k \neq 1 \bmod 2^k$.

Assume that $5^{2^{k-3}} = 1 + 2^{k-1} \bmod 2^k$,

then $\exists\, d \in Z^+ \ni 5^{2^{k-3}} = 1 + 2^{k-1} + d \cdot 2^k$

$$\therefore 5^{2^{k-2}} = (1 + 2^{k-1})^2 + 2(1 + 2^{k-1})d \cdot 2^k + (d \cdot 2^k)^2$$

$$= (1 + 2^{k-1})^2 = 1 + 2^k + 2^{2k-2} = 1 + 2^k \neq 1 \bmod 2^{k+1}$$

$$\therefore \operatorname{ord}_{2^k} 5 = \frac{\phi(2^k)}{2} = 2^{k-2}$$

■

Thm:

If $n \in Z^+$ and $n \neq p^t$ or $n \neq 2p^t$, where p is an odd prime, then n does not have a primitive root.

Proof:

Let $n \in Z^+$ and $n = p_1^{t_1} p_2^{t_2} \cdots p_m^{t_m}$.

Assume that n has a primitive root r, then

$(r, n)=1$ and $\mathrm{ord}_n r = \phi(n)$.

$\because (r, n) = 1 \Rightarrow (r, p_i^{t_i}) = 1, \forall 1 \le i \le m$.

By Euler's theorem, we have $r^{\phi(p_i^{t_i})} = 1 \bmod p_i^{t_i}, \forall i$.

Let $u = \mathrm{lcm}(\phi(p_1^{t_1}), \phi(p_2^{t_2}), \cdots, \phi(p_m^{t_m}))$, then

$r^u = 1 \bmod p_i^{t_i}, \forall i = 1, 2, \cdots m$

$\therefore$ By CRT, we have $r^u = 1 \bmod n \Rightarrow \mathrm{ord}_n r = \phi(n) \le u$.

$\because \phi(n)$ is multiplicative $\Rightarrow \phi(n) = \phi(p_1^{t_1} p_2^{t_2} \cdots p_m^{t_m})$

$= \phi(p_1^{t_1}) \cdots \phi(p_m^{t_m})$

$$\Rightarrow \phi(p_1^{t_1})\phi(p_2^{t_2})\cdots\phi(p_m^{t_m}) \le \text{lcm}(\phi(p_1^{t_1}),\phi(p_2^{t_2})\cdots\phi(p_m^{t_m}))$$

However , it is only possible for that

$\phi(p_1^{t_1}),\phi(p_2^{t_2}),\cdots,\phi(p_m^{t_m})$ are pairwise relative prime.

$\because \phi(p_i^{t_i}) = p_i^{t_i}(p_i - 1)$ is even if p is odd,

or if $p_i = 2$ and $t_i \ge 2$.

$\therefore \phi(p_1^{t_1}),\phi(p_2^{t_2}),\cdots,\phi(p_m^{t_m})$ are not paitwise relatively prime unless $m = 1$ and $n = p^t$ or $m = 2$ and $n = 2p^t$, where p is an odd prime and t is positive integer. ■

Thm:

If p is an odd prime and $t \in Z^+$, then $2p^t$ possesses a primitive root. Let r be a primitive root modulo p^t.

(i) If r is odd, then r is also a primitive root modulo $2p^t$.

(ii) If r is even, then $r + p^t$ is a primitive root modulo $2p^t$.

Proof:

If r is a primitive root modulo p^t, then

$$r^{\phi(p^t)} = 1 \bmod p^t \Rightarrow \text{no } a < \phi(p^t) \ni r^a = 1 \bmod p^t$$

$$\therefore \phi(2p^t) = \phi(2)\,\phi(p^t) = \phi(p^t) \Rightarrow r^{\phi(2p^t)} = 1 \bmod p^t \qquad (1)$$

(i) If r is odd, then $r^{\phi(2p^t)} = 1 \bmod 2$ (2)

$\therefore r^{\phi(2p^t)} = 1 \bmod 2p^t \Rightarrow r$ is a primitive root modulo $2p^t$

(ii)If r is even , then $r + p^t$ is odd.

$$\left.\begin{aligned} &\because (r+p^t)^{\phi(2p^t)} = (r+p^t)^{\phi(p^t)} = 1 \bmod p^t \\ &\text{and } (r+p^t)^{\phi(2p^t)} = 1 \bmod 2 \end{aligned}\right\}$$

$\Rightarrow r + p^t$ is a primitive root modulo $2p^t$. ■

Thm:

The positive integer n, $n > 1$, possesses a primitive root iff $n = 2, 4, p^t$ or $2p^t$, where p is an odd prime and $t \in Z^+$.

9.4 Index Arithmetic

- Let r be a primitive root modulo m, $m \in Z^+$, then

$$S = \{r, r^2, \ldots, r^{\phi(m)}\}$$

is a reduced system of residues modulo m.

If $a \in S$, then $\exists$ a unique integer x with $1 \le x \le \phi(m) \ni$

$$r^x = a \bmod m.$$

Def:

Let m be a positive integer with primitive root r.

If $a \in Z^+$ with $(a, m) = 1$,

then the unique integer x with $1 \le x \le \phi(m)$ and $r^x = a \bmod m$ is called the *index* of a to the base r modulo m.

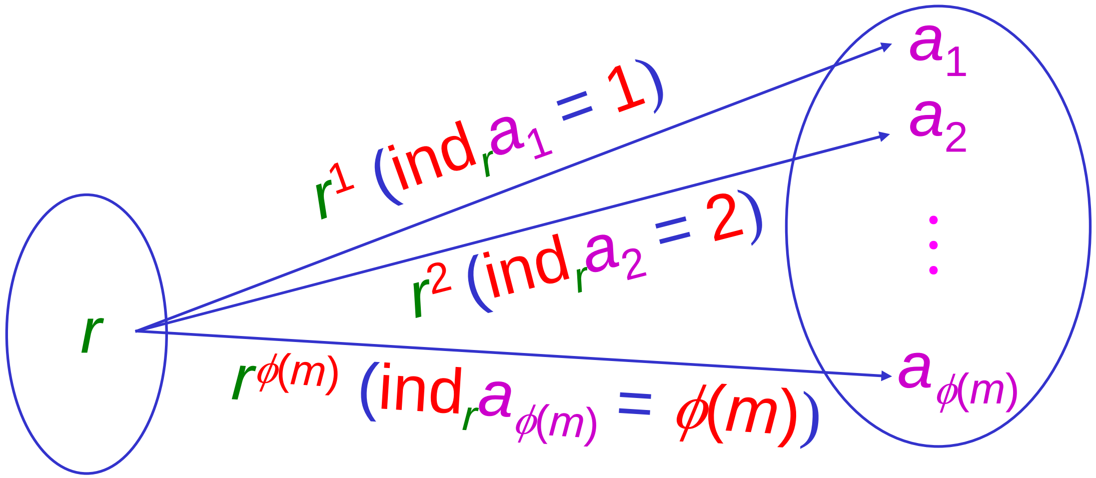
We write $x = \mathbf{ind}_r a$ (assume m is fixed) and

$$a = r^{\mathrm{ind}_r a} \bmod m$$

Property:

If $a = b \bmod m$ and $(a, m) = (b, m) = 1$,

then $\text{ind}_r a = \text{ind}_r b$



Thm:

Let $m \in Z^+$ with primitive root r, and a, b be integers relatively prime to m. Then

(i) $\text{ind}_r 1 = 0 \bmod \phi(m)$.

(ii) $\text{ind}_r(ab) = \text{ind}_r a + \text{ind}_r b \bmod \phi(m)$

(iii) $\text{ind}_r a^k = k \cdot \text{ind}_r a \bmod \phi(m)$ if $k \in Z^+$

Proof: (i) $\because r^{\phi(m)} = 1 \bmod m \Rightarrow \text{ind}_r 1 = \phi(m) = 0 \bmod \phi(m)$

(ii) $\because$ (1) $r^{\text{ind}_r(ab)} = ab \bmod m$ and

(2) $r^{\text{ind}_r a + \text{ind}_r b} = r^{\text{ind}_r a} \cdot r^{\text{ind}_r b} = ab \bmod m$

$\therefore \text{ind}_r(ab) = \text{ind}_r a + \text{ind}_r b \bmod \phi(m)$

(iii) $\because r^{\text{ind}_r a^k} = a^k \bmod m$ and $(r^{\text{ind}_r a})^k = a^k \bmod m$

$\therefore \text{ind}_r a^k = k \cdot \text{ind}_r a \bmod \phi(m)$

Ex: Solve $6x^{12} = 11 \bmod 17$

Sol:

(1)Find that 3 is a primitive root of 17. Form table 1, we have $\text{ind}_3(6x^{12}) = \text{ind}_3 11 = 7 \bmod 16$

Using (ii) and (iii), we have

$\text{ind}_3(6x^{12}) = \text{ind}_3 6 + 12\text{ind}_3 x \bmod 16$

$\Rightarrow 7 = 15 + 12\cdot\text{ind}_3 x \bmod 16$

$\Rightarrow 12\cdot\text{ind}_3 x = 8 \bmod 16$

$\Rightarrow \text{ind}_3 x = 2 \bmod 4$

$\Rightarrow \text{ind}_3 x = 2, 6, 10 \text{ or } 14 \bmod 16$

$\therefore x=3^2=9$, or $x=3^6=15$, or $x=3^{10}=8$, or $x=3^{14}=2$

Table 1.indices to the base 3 modulo 17

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\text{ind}_3 a$	16	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8

Ex:

Use table 1 to find all solutions of $7^x = 6 \bmod 17$

Sol:

$ind_3(7^x) = ind_3 6 = 15 \bmod 16$ From (iii), we have

$ind_3(7^x) = x \cdot ind_3 7 = 11x \bmod 16 = 15 \bmod 16$

$\because 11^{-1} = 3 \bmod 16 \quad \therefore x = 13 \bmod 16$

Def:

If m and $k \in Z^+$ and $(a, m) = 1$. We say that a is a <u>kth power residue of m</u> if

$$x^k = a \bmod m$$

has a solution.

Thm:

Let $m \in Z^+$ and r be a primitive root modulo m.
If $k \in Z^+$ and $(a, m) = 1$, then $x^k = a \bmod m$ has a solution iff

$$a^{\frac{\phi(m)}{d}} = 1 \bmod m$$

where $d = (k, \phi(m))$.

Furthermore, if there are solutions of $x^k = a \bmod m$, then there are exactly d incongruent solutions modulo m.

Proof:

$x^k = a \mod m$ has holds iff $k \cdot \text{ind}_r x = \text{ind}_r a \mod \phi(m)$ (1)

Let $d = (k, \phi(m))$ and $y = \text{ind}_r x \ni x = r^y \mod m$.

Then $ky = \text{ind}_r a \mod \phi(m)$ (2) has no solution if $d \nmid \text{ind}_r a$.

Hence there are no solutions of $x^k = a \mod m$ if $d \nmid \text{ind}_r a$.

If $d \mid \text{ind}_r a$, then there are exactly d solutions $\ni$ (1) holds.

Since $d \mid \text{ind}_r a$ iff $\dfrac{\phi(m)}{d}\text{ind}_r a = 0 \mod \phi(m)$

and this congruence holds iff $a^{\frac{\phi(m)}{d}} = 1 \mod m$. □

$(\dfrac{\phi(m)}{d}\text{ind}_r a = 0 \mod \phi(m) \Rightarrow \text{ind}_r a^{\frac{\phi(m)}{d}} = 0 \mod \phi(m) \Rightarrow a^{\frac{\phi(m)}{d}} = 1 \mod m.)$

Ex: Determine whether 5 is a sixth power residue of 17 (i.e., whether $x^6 = 5 \bmod 17$ has a solution.)

Sol: $\because (6, 16) = 2$ and $5^{\frac{16}{(6,16)}} = 5^8 = -1 \bmod 17 \neq 1 \bmod 17$

$\therefore$ 5 is not a sixth power residue of 17.

Thm*: If n is an odd compositive positive integer, then n passes Miller's test for at most $\frac{n-1}{4}$ bases b with $1 \leq b \leq n-1$.

Lemma:

Let p be an odd prime and let e, $q \in Z^+$. Then the number of incongruent solutions of

$$x^q = 1 \bmod p^e$$

is $(q, p^{e-1}(p-1))$.

Proof:

Let r be a primitive root of p^e, then $x^q = 1 \bmod p^e$ iff $qy = 0 \bmod \phi(p^e)$, where $y = \mathrm{ind}_r x$. $\because$ There are exactly $(q, \phi(p^e))$ incongruent solutions of $qy = 0 \bmod \phi(p^e) \Rightarrow$ there are $(q, \phi(p^e)) = (q, p^{e-1}(p-1))$ incongruent solutions of $x^q = 1 \bmod p^e$.

Proof of Thm*:

Let n -1 = $2^s t$, $s \in z^+$ and t is odd and $t \in z^+$.

For n to be a strong pseudo prime to be base b, either b^t = 1 mod n or $b^{2^j t} = -1 \bmod n$ for some $0 \le j \le s$-1. In either case, b^{n-1}=1 mod n.

If $p_j^{e_j} | n$, then $(n-1, \phi(p_j^{t_j})) = (n-1, p_j - 1)$. (page 195)

Let $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$.

$\because$ there are $(n-1, p_j^{e_j - 1}(p_j - 1)) = (n-1, p_j - 1)$

$p_j^{e_j}, j = 1, 2, \cdots, r.$ incongruent solutions of

x^{n-1} = 1 mod $\prod_{j=1}^{r}(n-1, p_j - 1)$

$\therefore$ By CRT, there are exactly

incongruent solutions of x^{n-1} = 1 mod n.

(1) For $p_k^{e_k}, e_k \geq 2, \because \frac{p_k - 1}{p_k^{e_k}} = \frac{1}{p_k^{e_{k-1}}} - \frac{1}{p_k^{e_k}} \leq \frac{2}{9}, (p_k = 3, e_k = 2)$

$$\therefore \prod_{j=1}^{r} (n-1, p_j - 1) \leq \prod_{j=1}^{r} (p_j - 1) \leq \prod_{j=1}^{r} p_j (\frac{2}{9} p_k^{e_k}) \leq \frac{2}{9} n$$

$\because \frac{2}{9} n \leq \frac{1}{4}(n-1)$ for $n \geq p. \therefore \prod_{j=1}^{r} p_j (\frac{2}{9} p_k^{e_k}) \leq \frac{1}{4}(n-1)$

$\therefore$ there are at most $\frac{n-1}{4}$ integers b, $1 \leq b \leq n$, for which n is a strong pseudo prime to be base b.

(2) For $n = p_1 p_2 \ldots p_r$, where $p_1, p_2, \ldots, p_r$ are distinct odd primes. Let $p_i - 1 = 2^{s_i} t_i$, $i = 1, 2, \ldots, r$, $s_i, t_i \in z^+$ and t_i is odd. Reorder the primes $p_1, p_2, \ldots p_r$ (if necessary) so that $s_1 \leq s_2 \leq \ldots \leq s_r$. Note that $(n-1, p_i-1) = 2^{\min(s, s_i)}(t, t_i)$

The number of solutions of $x^t = 1 \bmod p^i$ is $T_i = (t, t_i)$.

There are $2^j t_i$ solutions of $x^{2^j t} = -1 \bmod p_i$,

$0 \le j \le s_i - 1$, and no solutions otherwise. ∴ By CRT, there are $T_1 T_2 \ldots T_r$ solutions of $x^t = 1 \bmod n$, and $2^{jr} T_1 T_2 \ldots T_r$ solutions of $x^{2^j t} = -1 \bmod n$, $0 \le j \le s_i - 1$.

∴there are a total of $T_1 T_2 \cdots T_r \left[1 + \sum_{j=0}^{s_1 - 1} 2^{jr} \right] = T_1 T_2 \cdots T_r \left[1 + \frac{2^{s_1 r}}{2^{r-1}} \right]$

Integer b, $1 \le b \le n - 1$, for which n is a strong pseudo prime to the base b.

Note that $\phi(n) = (p_1 - 1)(p_2 - 1)\ldots(p_r - 1) = t_1 t_2 \cdots t_r 2^{s_1 + \cdots + s_r}$

We want to show that $T_1 T_2 \cdots T_r \left[1+\frac{2^{s_1 r}}{2^{r-1}}\right] \le \frac{\phi(n)}{4}$

$$\because \frac{1+\frac{2^{s_1 r}-1}{2^r-1}}{2^{s_1+s_2+\cdots+s_r}} \le \frac{1+\frac{2^{s_1 r}-1}{2^r-1}}{2^{s_1 r}} \le \frac{1}{2^r-1} \le \frac{1}{4} \quad \text{if } r \ge 3.$$

When $r = 2$, $n = p_1 p_2$ with $p_1 - 1 = 2^{s_1} t_1$

and $p_2 - 1 = 2^{s_2} t_2, s_1 \le s_2.$

If $s_1 = s_2$, then $\frac{\left[1+\frac{2^{s_1}-1}{3}\right]}{2^{s_1+s_2}} = \frac{1+\frac{2^{s_1}-1}{3}}{2^{s_1}\cdot 2^{s_2-s_1}} = \frac{\frac{1}{3}+\frac{1}{3\cdot 2^{2s_1}-1}}{2^{s_2-s_1}} \le \frac{1}{4}$

If $s_1 = s_2$, then $(n\text{-}1, p_1\text{-}1) = 2^s T_1$, and $(n\text{-}1, p_2\text{-}1) = 2^s T_2$.

Let note that $T_1 \neq t_1$, for if $T_1 = t_1$ then $(p_1\text{-}1) \mid (n\text{-}1)$, so that $n = p_1 p_2 = p_2 = 1 \bmod p_1\text{-}1$ which implies $p_2 > p_1$.

$\because T_1 \neq t_2$

$$\Rightarrow T_2 \leq \frac{t_2}{3}, \therefore T_1 T_2 \leq \frac{t_1 t_2}{3}.$$

$$\because \frac{\left[1 + \frac{2^{2s_1} - 1}{3}\right]}{2^{2s_1}} \leq \frac{1}{2} \Rightarrow T_1 T_2 \left[1 + \frac{2^{2s_1} - 1}{3}\right] \leq t_1 t_2 \frac{2^{2s_1}}{6} = \frac{\phi(n)}{6} \leq \frac{n-1}{6} \leq \frac{n-1}{4}$$

Remark:

The prob. that n is a strong pseudo prime to the random chosen base b, $1 \le b \le n-1$, is close to ¼ only for integers n with prime factor is of the form

$$n = p_1 p_2$$

with $p_1 = 1 + 2q_1$ and $p_2 = 1 + 4q_2$

where q_1, q_2 are odd primes, or

$$n = p_1 p_2 p_3$$

with $p_1 = 1 + 2q_1$, $p_2 = 1 + 2q_2$ and $p_3 = 1 + 2q_3$,

where q_1, q_2, q_3 are distinct odd primes.

9.5 Primary Test using primitive roots

From Thm, we know that $n \in Z^+$, $n > 1$, processes a primitive root iff $n = 2, 4, p^t$, or $2p^t$, where p is an odd prime and $t \in Z^+$.

Thus, if $n \in Z^+$ and is odd and
if $\exists\, x \in Z^+ \ni x$ is a primitive root satisfying

$$x^{n-1} = 1 \bmod n,$$

then n is prime.

Note: If $n = p^t > 1$, then $x^{\phi(n)} = 1 \bmod n$, where $\phi(n) = p^{t-1}(p-1) \neq n-1$.

Thm:

If $n \in Z^+$ and if $\exists\ x \in Z^+ \ni$

$$x^{n-1} = 1 \bmod n$$

and

$$x^{(n-1)/q} \neq 1 \bmod n$$

for all prime divisors q of $n - 1$, then n is prime.

Proof:

$x^{n-1}=1 \bmod n$, $\Rightarrow$ $\mathrm{ord}_n x|(n-1)$. If $\mathrm{ord}_n x \neq n-1$, then $\exists\, k \in$ $n-1= k \cdot \mathrm{ord}_n x$, then

$$x^{\frac{n-1}{q}} = x^{\frac{k\times \mathrm{ord}_n x}{q}} = \left(x^{\mathrm{ord}_n x}\right)^{\frac{k}{q}} = 1 \bmod n$$

$$\left(x^{\frac{n-1}{q}} \neq 1 \bmod n, \forall q \,|\, n-1\right)$$

Where q is a prime divisor of k. However, this contradicts the hypothese of the theorem

$\therefore$.$\mathrm{ord}_n x = n-1$, $\mathrm{ord}_n x \leq n-1$, we conclude that $\phi(n) = n-1 \Rightarrow n$ is prime.

Corollary:

If $n \in$ odd positive integer and if $x \in Z^+ \ni$

$$x^{(n-1)/2} = -1 \bmod n$$

and

$$x^{(n-1)/q} \neq 1 \bmod n$$

for all prime divisors q of $n - 1$, then n is prime.

This primality test is a deterministic test and is presented by Lucus.

1. In order to use this primality test, it needs to factor n-1 in advance. If n-1 cannot be factored, then the method is infeasible.
2. This test is very useful for test the primality of Fermat numbers.

Thm:

If n is composite, this can be proved with $O((\log_2 n)^2)$ bit operations.
(When the appropriate information is know).

Proof:

If n is composite , then $\exists$ a and b with $1< a <n$, $1< b <n$ and $n = ab$. Taking $O((\log_2 n)^2)$ bit operations to proof that n is composite.

Thm :

If n is prime, this can be proven using $O((\log_2 n)^4)$ bit operations.
(When the appropriate information is known)

Proof :

Let $f(n)$ be the total number of multiplications and modular exponentiations need to verify that the integer n is prime.

We want to show that $f(n) \le 3\left(\frac{\log n}{\log 2}\right) - 2$ (1)

$f(2)=1 \Rightarrow$ (1) is true .

Assume that for all primes q , $q < n$ the

inequality $f(q) \le 3\left(\frac{\log n}{\log 2}\right) - 2$ is true .

If n is prime , then $\exists\ 2^n q_1 \ldots\ldots q_t$ and x satisfy

i. $n-1 = 2^a q_1 \ldots\ldots q_t \Rightarrow$ t multiplications.

ii. q_i is prime $\forall 1 \le i \le t \Rightarrow f(q_i),\ \forall 1 \le i \le t$

iii. $x^{\frac{n-1}{2}} = -1 \bmod n \rightarrow 1$ exponentiations

iv. $x^{\frac{n-1}{q_j}} \ne 1 \bmod n, \forall 1 \le i \le t$ exponentiations

$$\therefore f(n) = t + (t+1) + \sum_{i=1}^{t} f(q_i) \le 2t + 1 + \sum_{i=1}^{t} 3\frac{\log q_i}{\log 2} - 2 \le 3\frac{\log n}{\log 2} - 2$$

$$= 3\log_2 n - 2$$

1 moddular exponentiation requires $O((\log_2 n)^3)$

$\therefore$Total number of bit operations needed is $O((\log_2 n)^4)$.

Remark :

1. Above theorem cannot be used to find this short proof of primality, since the

   factorization of n -1

   and

   the primitive root x of n

   are required.

2. An efficient primality test requires fewer than $(\log_2 n)^{c \log_2 \log_2 \log_2 n}$ bit operations, where c is a constant.

9.6 Universal Exponents

Def:

A universal exponent of positive integer n is a positive U such that

$$a^U = 1 \bmod n,$$

for all integers a relatively prime to n.

Remark: If $n = p_1^{t_1} p_2^{t_2} \ldots p_m^{t_m}$ and $(a,n) = 1$, then

$$a^{\phi(p^{t_i})} = 1 \bmod p^{t_i},$$

where $p^{t_i} \mid n$.

$$\Rightarrow a^U = 1 \bmod n \text{ if } U = lcm(\phi(p_1^{t_1}), \phi(p_2^{t_2}), \ldots, \phi(p_m^{t_m})),$$

$$\Rightarrow U \text{ exixt for all } n \in Z^+.$$

Problem :

1. Given n, what is the least universal exponent of n?

2. How to find a ∋

$$\text{ord}_n a = \lambda(n),$$

where $\lambda(n)$ is the least universal exponent

Def :

The least universal exponent of the positive integer n is called the *minimal universal exponent* of n, and is denoted by $\lambda(n)$.

Remark :

1. If n has a primitive root , then $\lambda(n) = \phi(n)$.

 (a) $n = p^t$, then $\lambda(p^t) = \phi(p^t) = p^{t-1}(p-1)$, where p is odd prime and $t \in Z^+$.

 (b) $n = 2$, then $\lambda(2) = \phi(2) = 1$.

 (c) $n = 4$, then $\lambda(4) = \phi(4) = 2$.

 (d) $n = 2p^t$, then $\lambda(2p^t) = \phi(2p^t) = p^{t-1}(p-1)$.

Remark :

1. If n has a primitive root, then $\lambda(n) = \phi(n)$.

   (a) $n = p^t$, then $\lambda(p^t) = \phi(p^t) = p^{t-1}(p-1)$,
   where p is odd prime and $t \in Z^+$.

   (b) $n = 2$, then $\lambda(2) = \phi(2) = 1$.

   (c) $n = 4$, then $\lambda(4) = \phi(4) = 2$.

   (d) $n = 2p^t$, then $\lambda(2p^t) = \phi(2p^t) = p^{t-1}(p-1)$.

2. If $n = 2^t$, $t \geq 3$, then $\lambda(2^t) = 2^{t-2}$,

   $\therefore$ If $(a,n) = 1 \Rightarrow a$ is odd and $a^{2^{t-2}} = 1 \bmod 2^t$

Thm : Let $n = 2^{t_0} p_1^{t_1} \dots p_m^{t_m}$, then $\lambda(n) = [\lambda(2^{t_0}), \phi(p_1^{t_1}), \dots, \phi(p_m^{t_m})]$.

Moreover, $\exists a \in Z^+ \ni ord_n a = \lambda(n)$.

Proof : Let $a \in Z^+$, and $(a,n) = 1$ and

let $M = \text{lcm}[\lambda(2^{t_0}), \phi(p_1^{t_1}), \dots, \phi(p_m^{t_m})]$

$a^{\lambda(p^t)} = a^{\phi(p^t)} = 1 \text{ mod } p^t$, for all $p^t \mid n$.

$\therefore a^M = 1 \text{mod} p^t \rightarrow a^M = 1 \text{mod} n, (\text{CRT})$

Now , we prove that M is the least universal exponent.

Let r_i be a primitive root of $p_i^{t_i}$.

Consider the system of simultaneous congruences .

$$a = 5 \ \bmod \ 2^{t_0} \Rightarrow ord_{2^{r_0}} a = \lambda\left(2^{t_0}\right)$$

$$a = r_1 \ \bmod \ p_1^{t_1} \Rightarrow ord_{p_1^{r_1}} a = \lambda\left(p_1^{t_1}\right) = \varphi\left(p_1^{t_1}\right)$$

$$\vdots$$

$$a = r_m \ \bmod \ p_m^{t_m} \Rightarrow ord_{p_m^{r_m}} a = \lambda\left(p_m^{t_m}\right) = \varphi\left(p_m^{t_m}\right)$$

Then, by CRT, $\exists a \ni ord_n a = M$, and $1 \le a \le n-1$

Remark : Above thm tells us a method to find $a \ni$ $\left(a,n\right) = 1$ and $ord_n a = \lambda\left(n\right)$

Note: A carmichael number n is a composite integer that satisfies

$$b^{n-1} = 1 \bmod n,$$

for $\forall b \in Z^{+}$, and $(b, n) = 1$.

We have proved that if $n = q_1 q_2 ... q_k$,

where $q_1 q_2 ... q_k$ are distinct primes satisfying

$$(q_j - 1) \mid (n-1), \forall 1 \le j \le k,$$

then n is a Carmichael number in Thm5.7 (p.195).

Here ,we prove the converse of the result.

Thm : If $n > 2$ is a Carmichael number, then $n = q_1 q_2 \ldots q_k$, where the $g_j s$ are distinct primes $\ni (q_j - 1) \mid (n-1)$ for all $j = 1, 2, \ldots, k$

Proof : If n is a Carmichael number m then $b^{n-1} = 1 \bmod n, \forall (b,n) = 1$

however , $\exists a \in Z^+$, such that $ord_n a = \lambda(n)$ and $(a,n) = 1$.

$\therefore \lambda(n) \mid n-1$

(1)n must be odd , Θ if n is even , then $n-1$ is odd , but $\lambda(n)$ is even $(n > 2)$, contradicting $\lambda(n) \mid n-1$.

(2)n must be the product of distinct primes , i.e. $n = q_1 q_2 \ldots q_k$ $\therefore$ If $p^t \mid n, t \geq 2$, then $\lambda(p^t) = \varphi(p^t) = p^{t-1}(p-1) \mid \lambda(n) \mid n-1$, which s impossible $p \mid n$.

(3) If $n = q_1 q_2 \ldots q_k$, where q_js are distinct primes , $1 \le j \le k$,

then $\lambda(q_j) = \varphi(q_j) = (q_j - 1) \mid \lambda(n)(n-1)$.

Thm : A Carmichael number must have at least three different odd prime factors .

Proof : Let n be a Carmichael number . Since n is the product of distinct primes .Let $n = pq$,where p and q are odd primes with $p > q$, then $n - 1 = pq - 1 = (p-1)q + (q-1)$

q - $1 \neq 0 \bmod p - 1. \rightarrow (p-1) \nmid (n-1)$, it is impossible , $\therefore$ n cannot be a Carmichael number.