Chapter 5 – Primitive Roots

5.1 The order of an integer and primitive roots.

Recall

Euler's Theorem Let $a, m \in \mathbb{Z}$, $m \geq 1$, & _____.
Then

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

Definition Let $a, m \in \mathbb{Z}$, $m \geq 1$ & $(a, m) = 1$.
The order of a mod m denoted _____ is
the

Note By Euler's Theorem ___ $\leq \text{ord}_m a \leq$ ____.

Example $m = 7$

$a = 2$

$a = 3$

$a = 4$

$a = 5$

$a = 6$

a	$\text{ord}_7 a$
1	
2	
3	
4	
5	
6	

Proposition Let $a, n \in \mathbb{Z}$, $n \geq 1$ & $(a, n) = 1$.
Then
(1) $a^n \equiv 1 \pmod{n}$ for some $n \in \mathbb{Z}^+$
if and only if .....

(2) $\text{ord}_n a$ .....

PROOF: Suppose $a, n \in \mathbb{Z}$, $n \geq 1$ & $(a, n) = 1$.
Let $k = \text{ord}_n a$ Then

(1) ($\Rightarrow$) Suppose $a^n \equiv 1 \pmod{n}$ for some $n \in \mathbb{Z}^+$

($\Leftarrow$) Suppose $\operatorname{ord}_m a = k \mid n$. Then

(2)

□

Proposition
Let $a, m, i, j \in \mathbb{Z}$, $m \geq 1$, $i, j \geq 0$ & $(a, m) = 1$.
Then
$a^i \equiv a^j \pmod{m}$ if & only if .....

PROOF Suppose $a, m, i, j \in \mathbb{Z}$, $m \geq 1$, $i, j \geq 0$ & $(a, m) = 1$.
Without loss of generality we suppose $i \geq j$.
($\Leftarrow$) Suppose $a^i \equiv a^j \pmod{m}$.

($\Leftarrow$) Suppose $i \equiv j \pmod{\operatorname{ord}_m a}$.
Let
$\operatorname{ord}_m a = k$.

Example $a = 2$, $m = 7$. Then $\operatorname{ord}_m a = \operatorname{ord}_7 2 =$ ___

Definition Let $a, m \in \mathbb{Z}$, $m \geq 1$ & $(a, m) = 1$.
The number a is a primitive root mod m
if

Example $m = 7$.

Example $m = 8$

a	$\mathrm{ord}_8\, a$
1	
3	
5	
7	

Proposition If r is a primitive root mod m
Then
$S = \{$ $\}$
is a reduced residue system mod m.

PROOF:

Proposition Let $a, m, i \in \mathbb{Z}$, $m \geq 1$, $i \geq 1$ & $(a, m) = 1$. Then

$$\text{ord}_m(a^i) =$$

Example $m = 7$, $a = 5$, $i = 4$.

Proof of Proposition:

Corollary Let $a, m, i \in \mathbb{Z}$, $m \geq 1$, $i \geq 1$ & $(a,m) = 1$.
Then
$\operatorname{ord}_m(a) = \operatorname{ord}_m(a^i)$ if & only if .....

Example $a = 2$, $m = 7$.

Corollary If a primitive root mod m exists
then there are _ _ _ _ _ _ _ _ _ _ _ _
incongruent primitive roots mod m.

Example $m = 7$.

Proof of Corollary

Ex #9 Let p be an odd prime, $r \in \mathbb{Z}$, $p \nmid r$.
Then r is a primitive root mod p
if and only if
$$r^{(p-1)/q} \not\equiv 1 \pmod{p},$$
for all prime divisors q of $p-1$.

Example

(i) Find a primitive root mod 17.

(ii) Find all incongruent integers mod 17 having order 8.