(154) -A

Order: Let $n > 1$ and $\gcd(a, n) = 1$. The order of a modulo n is the smallest positive integer k such that

$$a^k \equiv 1 \pmod{n}.$$

Def: If gcd $(a, n) = 1$ and

$$o(a) = \phi(n) \pmod{n}$$

then a is primitive root of the integer n.

e.g As $3^6 \equiv 1 \pmod 7 \Rightarrow 3$ is a primitive root of 7.

Theorm: Let $o(a) = k \pmod n$, then

$$a^h \equiv 1 \pmod n \text{ iff } k \mid h.$$

In particular $k \mid \phi(n)$.

Proof: Let $k \mid h \Rightarrow h = jk,\ j \in \mathbb{Z}$

$$\because a^k \equiv 1 \pmod n$$

$$\therefore a^h = a^{jk} = (a^k)^j \equiv 1^j \pmod n$$
$$\equiv 1 \pmod n$$

Conversely, let $a^h \equiv 1 \pmod n$

156

By Division algorithm, $\exists$ q and r such that

$$h = qk + r, \quad 0 \le r < k.$$

$$a^h = (a^k)^q a^r$$

$$a^h \equiv 1 \pmod n$$

$$a^k \equiv 1 \pmod n$$

$$\Rightarrow \quad a^r \equiv 1 \pmod n \quad \text{if} \quad 0 < r < k$$

a contradiction

$$\therefore \quad r = 0$$

$$\Rightarrow \quad h = qk \Rightarrow k \mid h$$

Theorem: If $o(a) = k \pmod n$, then

$$a^i \equiv a^j \pmod n \quad \text{iff} \quad ~~\text{k}~~ \; i \equiv j \pmod k$$

Proof: suppose $a^i \equiv a^j \pmod n$

$+ \quad i \geq j$

$\because \quad (a, n) = 1$

$\Rightarrow \quad a^{i-j} \equiv 1 \pmod{n}$

$\Rightarrow \quad k \mid i-j$

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

Conversely, let $i \equiv j \pmod{k}$

$\Rightarrow \quad i = j + qk$

& $\quad a^{k} \equiv 1 \pmod{n}$

$\Rightarrow \quad a^{i} \equiv a^{j+qk} \pmod{n}$

$\equiv a^{j} \pmod{n}$

<u>Corollary</u>: If $O(a) = k \pmod{n}$, then $a, a^2, \ldots, a^k$ are incongruent modulo n.