TOPIC NAME: Assignment - 6

1. Show that 2 is a primitive root modulo 11.

$\Rightarrow$

2 is a primitive root modulo 11 because its powers generate all residues 1 - 10 :-

$2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 5$

$2^5 = 10$, $2^6 = 9$, $2^7 = 7$, $2^8 = 3$

$2^9 = 6$, $2^{10} = 1$.

Hence, order of 2 is $10 = \varphi(11)$

2. How many incongruent primitive roots does 14 have?

$\Rightarrow$ Given, $n = 14 \Rightarrow \phi(14) = 6$

and $\phi(\phi(14)) = \phi(6) = 2$

So, 2 incongruent primitive roots.

TOPIC NAME :

DAY :

TIME : DATE : / /

3. Suppose n is a positive integer, and a^{-1} is a multiplicative inverse of $a \pmod n$.

a. Show $ord_n\, a = ord_n (a^{-1})$

b. If a is a ~~positive~~ primitive root modulo n, must a^{-1} also be a primitive root ?

a. since $a \cdot a^{-1} \equiv 1 \pmod n$, both have the same order.

$ord_n (a) = ord_n (a^{-1})$

b. If a is a primitive root modulo n, then a^{-1} must also be a primitive root because it has the same order $\varphi(n)$.