Subject: Date:

① show that 2 is a primitive root modulo 11.

Ans: we need to show that smallest positive integer k for which -

$2^k \equiv 1 \pmod{11}$

is $k = \phi(11) = 10$

compute powers of 2 modulo 11

$2^1 \equiv 2 \pmod{11}$

$2^2 \equiv 4 \pmod{11}$

$2^3 \equiv 8 \pmod{11}$

$2^4 \equiv 5 \pmod{11}$

$2^5 \equiv 10 \pmod{11}$

$2^6 \equiv 9 \pmod{11}$

$2^7 \equiv 7 \pmod{11}$

$2^8 \equiv 3 \pmod{11}$

Subject: ____________ Date: ____

$2^{9} \equiv 6 \pmod{11}$

$2^{10} \equiv 1\cancel{2} \pmod{11}$

~~The smallest exponent 1 is~~

so the first time we get 1 is at exponent 10. so the order of 2 modulo 11 is 10. Hence 2 is a primitive root modulo 11.

Subject: Date:

(2) How many incongruent primitive roots does 14 have?

Ans: First need to find, weather 14 has primitive root.

A number n has primitive root if only if -

$n = 2, 4, p^k$ or $2p^k$ where p is an odd number.

Here, $14 = 2 \times 7$ fits

So, 14 has primitive roots $= \phi(\phi(14))$

compute- $\phi(14) = \phi(2) \times \phi(7) = 1 \times 6 = 6$

$\phi(\phi(14)) = \phi(6) = \phi(2 \times 3) = 1 \times 2$

Therefore, 14 has 2 incongruent primitive roots.

Subject: Date:

③ suppose n is pos int and a^{-1} is the multiplicative inverse of a (mod n)

ⓐ show ord $n(a)$ = ord $n(a^{-1})$

Let, ord $n(a) = k$

Then by definition -

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

Take inverse both sides

$(a^{-1})^k \equiv 1^{-1} \equiv 1 \pmod{n}$

so ~~order~~ order of a^{-1} divides k

similarly, if $(a^{-1})^m \equiv 1 \pmod{n}$ then

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

So the order of a divides m

Hence order (a) = ord (a^{-1})

Subject: Date:

(b) If a is a primitive root mod n must a^{-1} also be a primitive root?

Since a is a primitive root

$\mathrm{ord}(a) = \phi(n)$

Form (*)

$$\mathrm{ord}_n(a^{-1}) = \mathrm{ord}_n(a) = \phi(n)$$

Therefore, a^{-1} also has order n $\phi(n)$ so, if B also a primitive root modulo n

$\therefore$ a^{-1} is also a primitive root modulo n.