## Primitive Root

1 Question: Show that 2 is a primitive root modulo 11 on Svitiming Indusposi

Ans: Given that,

A number q is a primitive root modulo 11,

Since 11 is prime, we need the order of 2 org bbo Ation 299

modulo 11 to be P(11) = 10.

Compute powers of 2 mod 11:

2 = 2 Q(K) = 6(2) 9 (7) = 1.6=6

22 = 9 22 = 80 N = 25001 SNH Inving. To stadming 02

29 = 16 = 5

25 = 29.2=5.2=10

2° = 10.2 = 20 = 9

27 = 9,2=18=7

28 = 7.2 = 19 = 3

2 = 32 = 6

210 = 6.2 = 12 = 1

we reached 1 first exponent 10.80 the order of 2 mod 11 is = \$ = \$ (11)

primitive

Compute :

Therefore 2 is a primitive most modulo 11.

himitive Root:

Compute powers of 2 mod 11:

2. How many incogrerent preimitive resolts iddes

Ans: Primitive roots exist for n=29 pk on Rpk with odd prime P. since 19=27, primitive roots exist

Compute:

p(K) = p(2) 9(7) = 1.6=6

so mumber of primitive roots = \$60=2

3 = 31 - Am)

2° = 2°.2 = 5°.2 = 10° € 9

E= 81= 2.6 = 40

5 = b1 = 2 . 5 = 14 = 3

5 = 35 = 6

@) Show that

Ordn (a) = Ordn (a')

Let. Ordn (a) = K (s) notro nost

That means: ak = 1 (madin)

Now, an (ak) = 1-1 (and a)

Simplify: (at ) = 1 (mod n)

That means the order of at divides k.

Hence the two orders divided eadh other

so, they are equal.

Ordn (a) = ordn (a)

(B) Show Unto (b) yes. It is a primitive root mad no then order (a) = p(m) That worden Forom pard (a), ordn (a) = ordn (a) = 46 30, a' also has order pa Therefore, at is also a primitive root modulo probro Am so, they are equal. (2) (10 = (1) (c)