Johns that, 2 is a primitive most modulo 11. We must show that 2 generates all nonzero residues modulo 11. The residues modulo 11 are: 1,2,3,4,5,6,7,8,9,10 bet's compute successive powens $2^{-1} \equiv 2 \pmod{11}$ $2^2 \equiv 4 \pmod{11}$ 23 = 16 = 5 (mod 11) 25= 10 (mod 11) TO addingt-01 $2^{6} = 20 = 9 \pmod{11}$ $2^{7} = 18 = 7 \pmod{11}$ $2^8 = 14 \equiv 3 \pmod{11}$ 29 = 6 (mod 11) 210=12=1 (mod11) The smallest exponent giving 1 is 10, 50 2 is a primitive root modulo 11.

2) How many incongruent primitive moots does (5 bow ond (a)= ond (a-1) Solne We know, Number of primitive roots of, n= \p(\phi(n)) if and only if n= 2,4; pk, 2pk where p is an odd prime). Here. 14=12x7, which fits the form 2p. After computation, $\varphi(14) = \varphi(2) \times \varphi(7) = 1 \times 6 = 6$ 9 (4 (14)) 00 p (6) = 20 nobro off 100 There fore, there are 2 no congruent primitive he reverse.

50. onda (a) = and a (a-1). (proved)

3) suppose, n'is a positive integen, and a-1 is the multiplicative invense of a (mod n). (a) show and (a) = and (a^{-1}) work and Let, and (a) = k.

That means:

(mod n)

(a) k = 1 (mod n)

(a) commetry ak = 1 implies Similarly of symmetry, ak = 1 implies the reverse, the reverse, and a = and n = and n (proved) 6999 a is a primitive root modulo in, must a la also rebe a primitive root? Bay sintramper es a sis a primitive rigget mod nother Modulan (a) drag planting not bold from pant (a): ordn (a^{-1}) = ordn (a) = (a) = (a) . A29 son latt offis also, a primitive riott
modulo n. The secondity. Message Top Layen secunity. Benbanus algorithm. Rydoubatdhus asusnuos tood Discussion ?