Homework 8A

Verify several points on the circular group based on

+ 2 + 2 mod 17

Primitive element: P = (5,1)

**Ex#: (9,16) + (9,16)**

P = (9,16), Q = (9,16), R = (,)

- - mod 17

s ( - ) - mod 17

Because P =Q, hence

s = (3

s = (3 = (381+2)

7 8 mod 17

5 mod 17

- - 7 mod 17

s ( - ) - = 5(9-7) -16 11 mod 17

**R = (7,11)**

**Ex#: (9,16) + (5,16)**

P = (9,16), Q = (5,16), R = (,)

- - mod 17

s ( - ) - mod 17

Because P Q, hence

s = ( - ) mod 17

s = ( - ) mod 17 0 mod 17

- - mod 17 3 mod 17

s ( - ) - = 0 -16 1 mod 17

**R = (3,1)**