Homework8B

Verify several points on the circular group based on

+ xy + + mod P(x)

P(x) = + x + 1

The element g = (0010) is a generator

Primitive element: P = (,)

***EX#1:*** ***(,0) + (,0)***

Point doubling, R = 2A

S =

= + 0/

= + 0

=

+ S + a = + + = + +

= + +

1010

1111

0011

0110

= = 0110 = 5

s () + + = ( + 5) + 5 + 0

= 1111

= 0110

= 1001 =9

s () + + = + 5 + 0 = + 5 = + 5

1110

0110

= = 1000 = 8

**P = (,)**

EX#2***: (,0) + (0,1)***

S = ( + ) = () =

+ s + + a = + + +0+

= + +

1100

1000

1111

0011

=1000

=

S () + + = (+) +  + 0

= 1111

= 1000

= 0111

(+) = =

= +

= 1101

= 1000

= = 0101

=

**(,)**