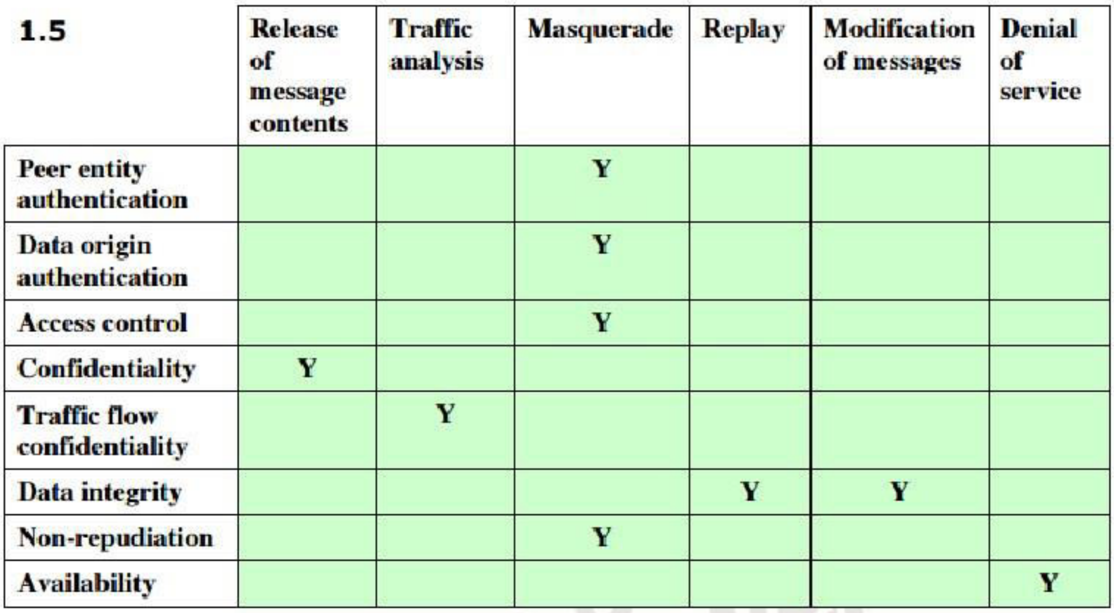
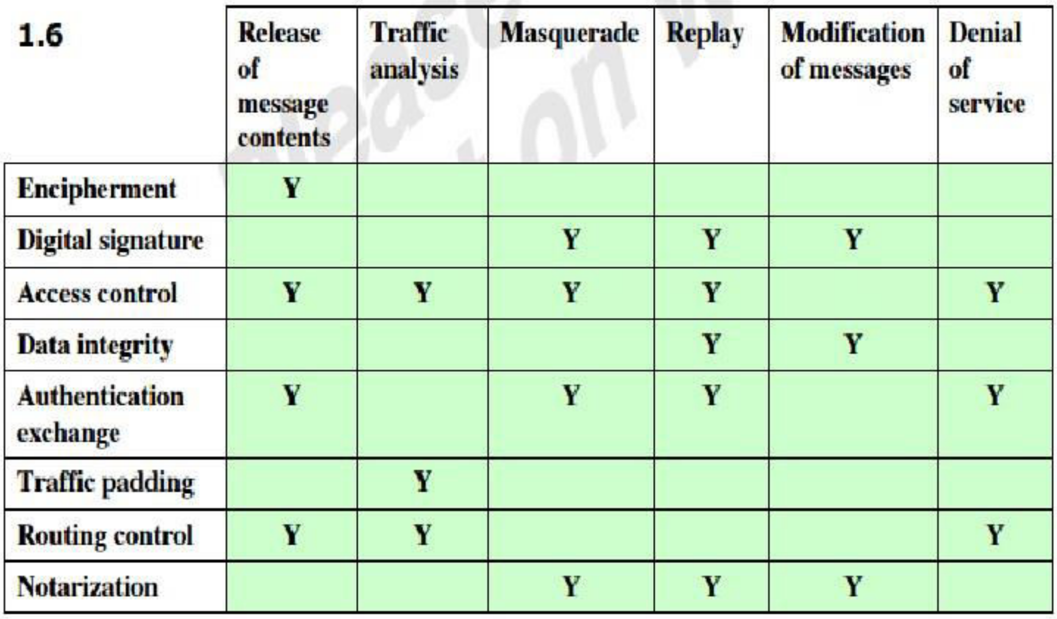
Assignment 1 Solutions

1.5 Draw a matrix similar to table to 1.4 that shows relationship between security services and attacks.



1.5	Release of message contents	Traffic analysis	Masquerade	Replay	Modification of messages	Denial of service
Peer entity authentication			Y			
Data origin authentication			Y			
Access control			Y			
Confidentiality	Y					
Traffic flow confidentiality		Y				
Data integrity				Y	Y	
Non-repudiation			Y			
Availability						Y

1.6 Draw a matrix similar to table to 1.4 that shows relationship between security services and attacks.



1.6	Release of message contents	Traffic analysis	Masquerade	Replay	Modification of messages	Denial of service
Encipherment	Y					
Digital signature			Y	Y	Y	
Access control	Y	Y	Y	Y		Y
Data integrity				Y	Y	
Authentication exchange	Y		Y	Y		Y
Traffic padding		Y				
Routing control	Y	Y				Y
Notarization			Y	Y	Y	

2.3) Answers.

a) 2

b) 3

c) 4.

2.7 1, 2, 4, 6, 16, 12.

2.12

a) 34

b) 35.

2.16

a) 3239

b) No inverse escists

c) 550.

2.27

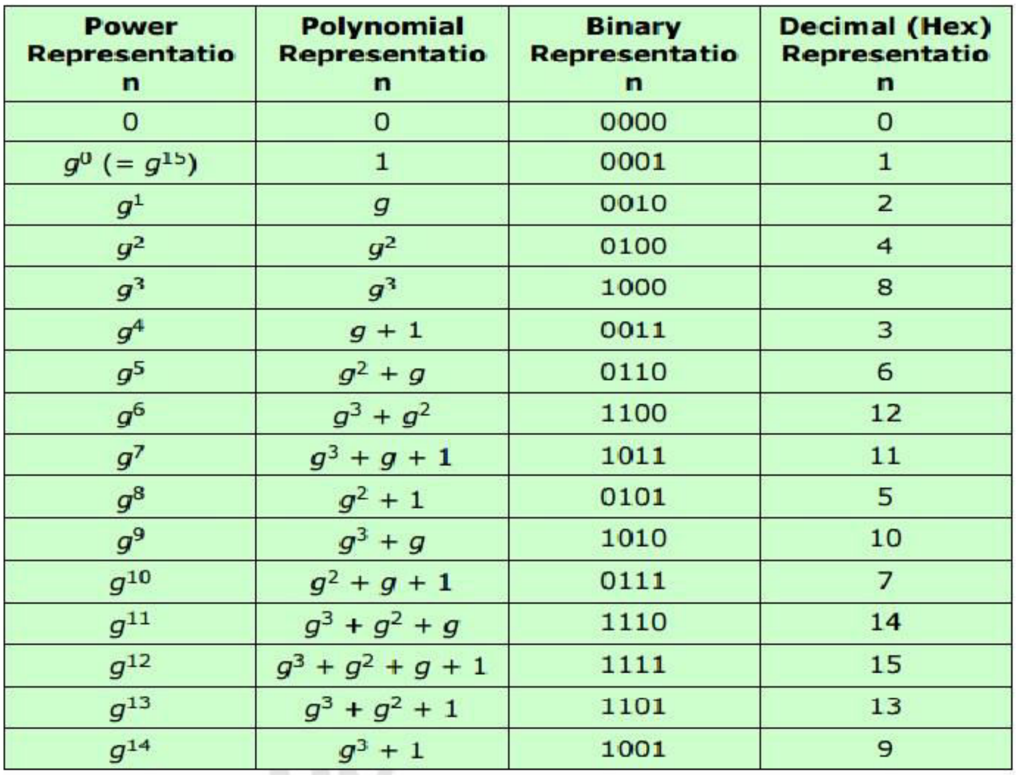
a) $\phi(41) = 40$

b) $\phi(27) = \phi(3^3) = 3^3 - 3^2 = 18$.

c) $\phi(231) = \phi(3) \times \phi(7) \times \phi(11) = 2 \times 6 \times 10 = 120$.

d) $\phi(440) = \phi(2^3) \times \phi(5) \times (11) = (2^3 - 2^2) \times 4 \times 10 = 160$.

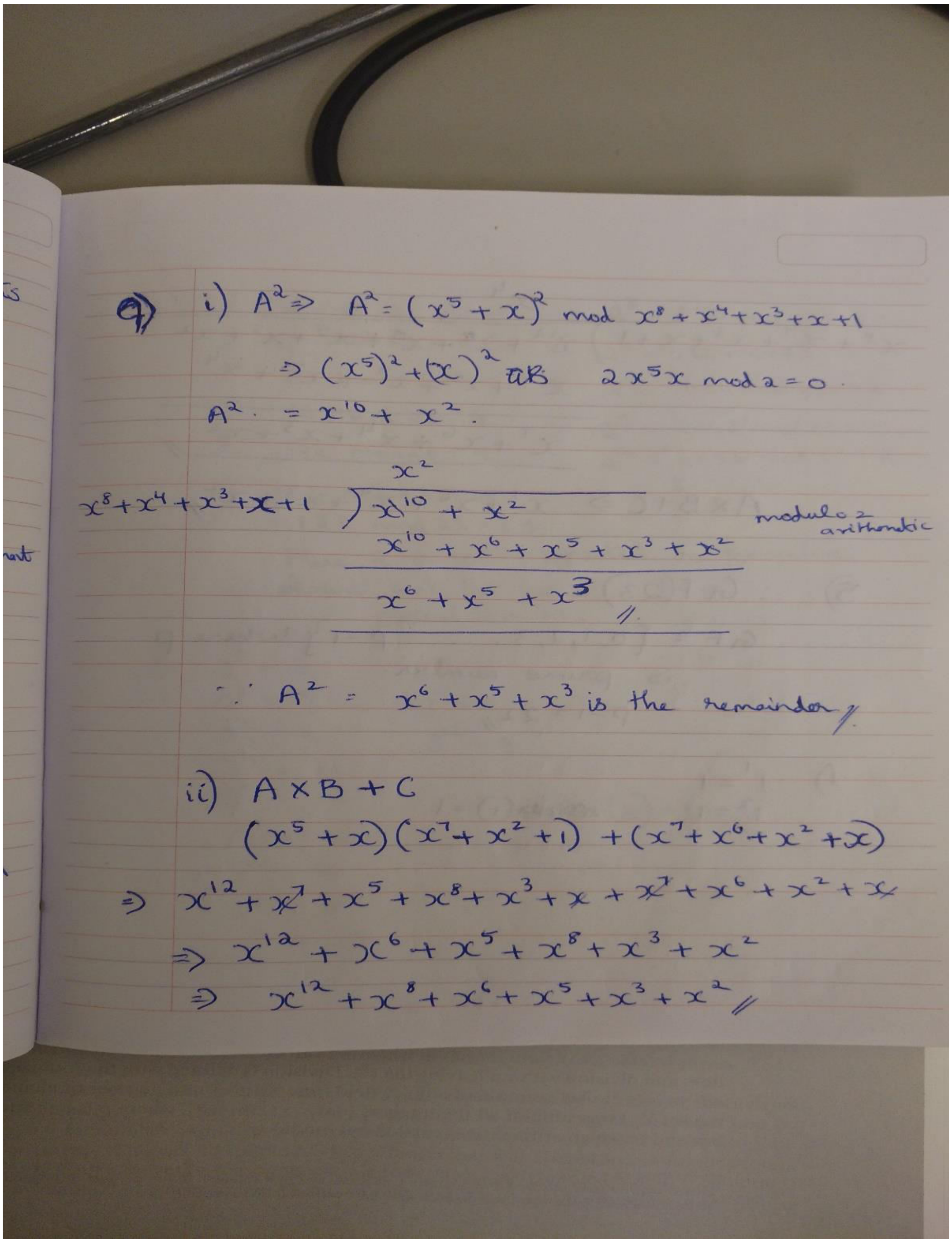
5.12



Power Representation	Polynomial Representation	Binary Representation	Decimal (Hex) Representation
0	0	0000	0
g^0 (= g^{15})	1	0001	1
g^1	g	0010	2
g^2	g^2	0100	4
g^3	g^3	1000	8
g^4	$g + 1$	0011	3
g^5	$g^2 + g$	0110	6
g^6	$g^3 + g^2$	1100	12
g^7	$g^3 + g + 1$	1011	11
g^8	$g^2 + 1$	0101	5
g^9	$g^3 + g$	1010	10
g^{10}	$g^2 + g + 1$	0111	7
g^{11}	$g^3 + g^2 + g$	1110	14
g^{12}	$g^3 + g^2 + g + 1$	1111	15
g^{13}	$g^3 + g^2 + 1$	1101	13
g^{14}	$g^3 + 1$	1001	9

8

The Primitive elements which has maximum order are 2,3,10,13,14,15,16,17.



9) i) $A^2 \Rightarrow A^2 = (x^5 + x)^2 \bmod x^8 + x^4 + x^3 + x + 1$

$\Rightarrow (x^5)^2 + (x)^2$ ~~AB~~ $\quad 2x^5x \bmod 2 = 0.$

$A^2. = x^{10} + x^2.$

$$\begin{array}{r|l} & x^2 \\ x^8+x^4+x^3+x+1 & x^{10} + x^2 \\ & x^{10} + x^6 + x^5 + x^3 + x^2 \\ \hline & x^6 + x^5 + x^3 \quad // \end{array}$$

modulo 2 arithmetic

$\therefore A^2 = x^6 + x^5 + x^3$ is the remainder //

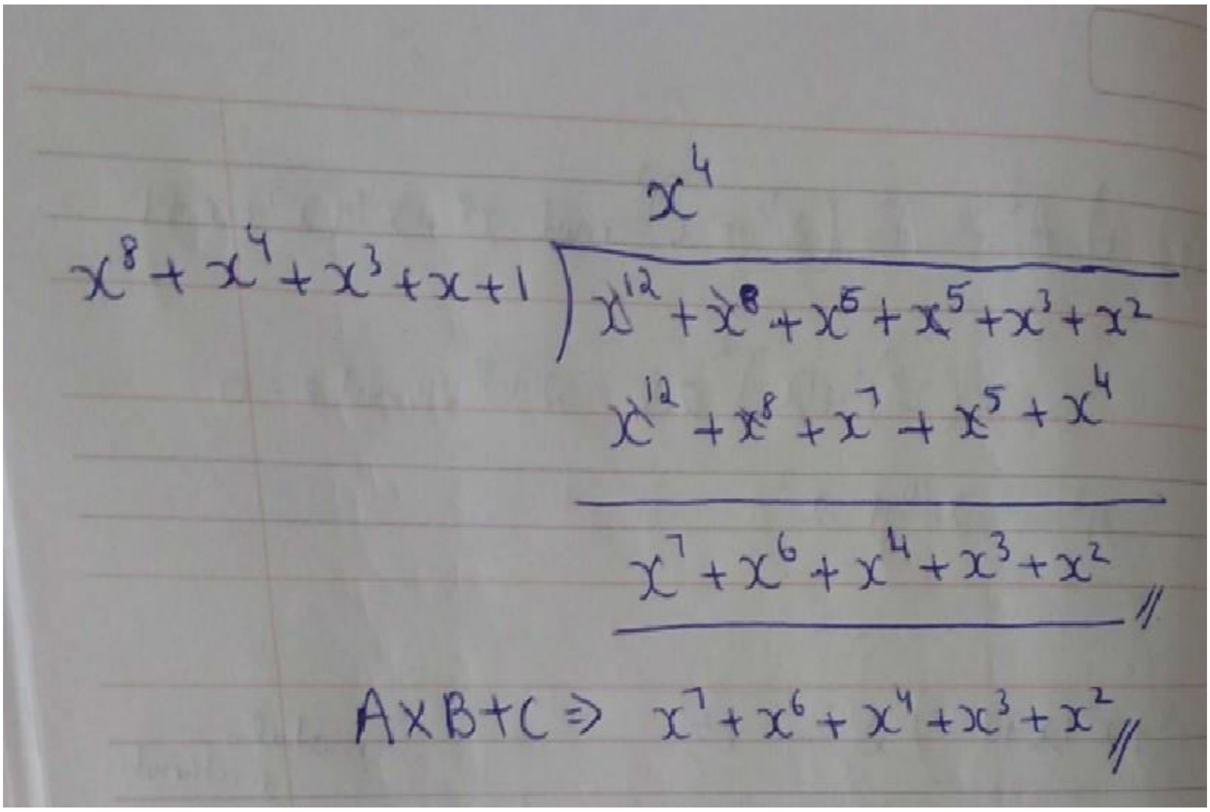
ii) $A \times B + C$

$(x^5 + x)(x^7 + x^2 + 1) + (x^7 + x^6 + x^2 + x)$

$\Rightarrow x^{12} + \cancel{x^7} + x^5 + x^8 + x^3 + \cancel{x} + \cancel{x^7} + x^6 + x^2 + \cancel{x}$

$\Rightarrow x^{12} + x^6 + x^5 + x^8 + x^3 + x^2$

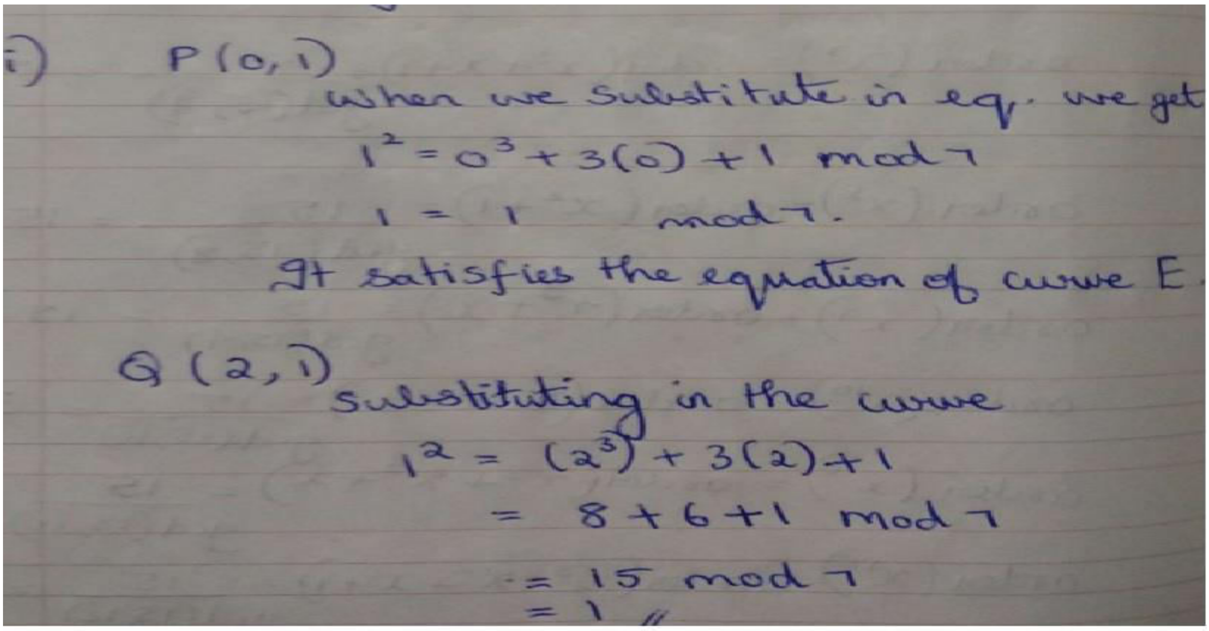
$\Rightarrow x^{12} + x^8 + x^6 + x^5 + x^3 + x^2 \;//$



$$\begin{array}{r|l} & \qquad x^4 \\ \hline x^8+x^4+x^3+x+1 & x^{12}+x^8+x^6+x^5+x^3+x^2 \\ & x^{12}+x^8+x^7+x^5+x^4 \\ \hline & x^7+x^6+x^4+x^3+x^2 \\ \cline{2-2} & \quad // \end{array}$$

$$A \times B + C \Rightarrow x^7+x^6+x^4+x^3+x^2 \; //$$

10



i) $P(0,1)$

when we substitute in eq. we get

$1^2 = 0^3 + 3(0) + 1 \mod 7$

$1 = 1 \quad \mod 7.$

It satisfies the equation of curve E.

$Q(2,1)$

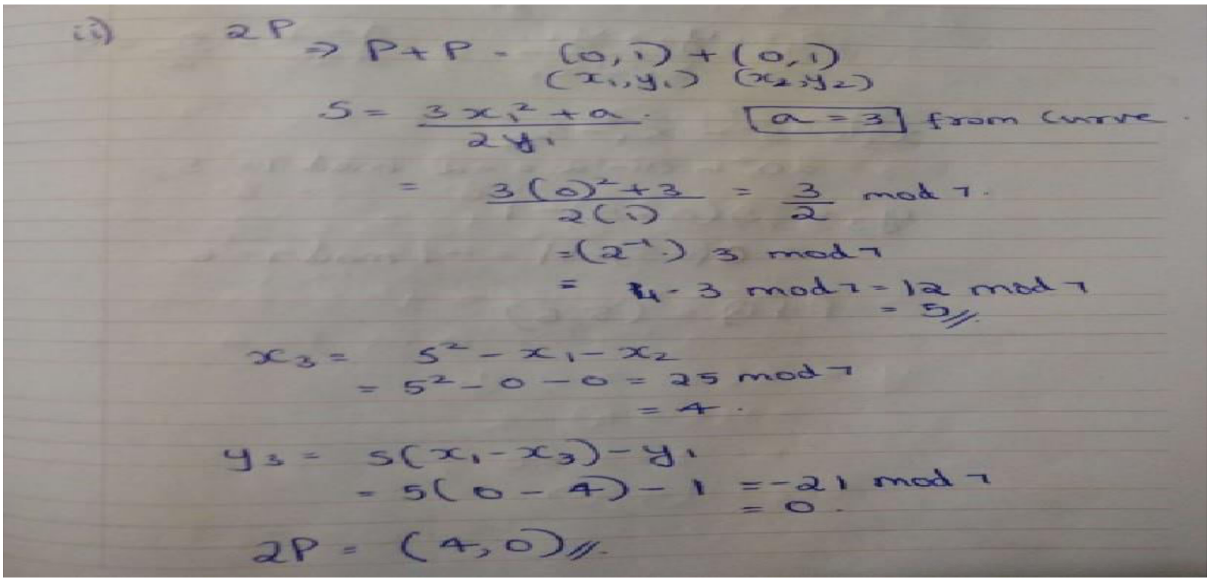
substituting in the curve

$1^2 = (2^3) + 3(2) + 1$

$= 8 + 6 + 1 \mod 7$

$= 15 \mod 7$

$= 1$ //



ii) $2P$

$\Rightarrow P + P - \underset{(x_1,y_1)}{(0,1)} + \underset{(x_2,y_2)}{(0,1)}$

$S = \dfrac{3x_1^2 + a}{2y_1}.$ $\boxed{a = 3}$ from curve.

$= \dfrac{3(0)^2 + 3}{2(1)} = \dfrac{3}{2} \mod 7.$

$= (2^{-1}) 3 \mod 7$

$= 4 \cdot 3 \mod 7 = 12 \mod 7$

$= 5$ //.

$x_3 = 5^2 - x_1 - x_2$

$= 5^2 - 0 - 0 = 25 \mod 7$

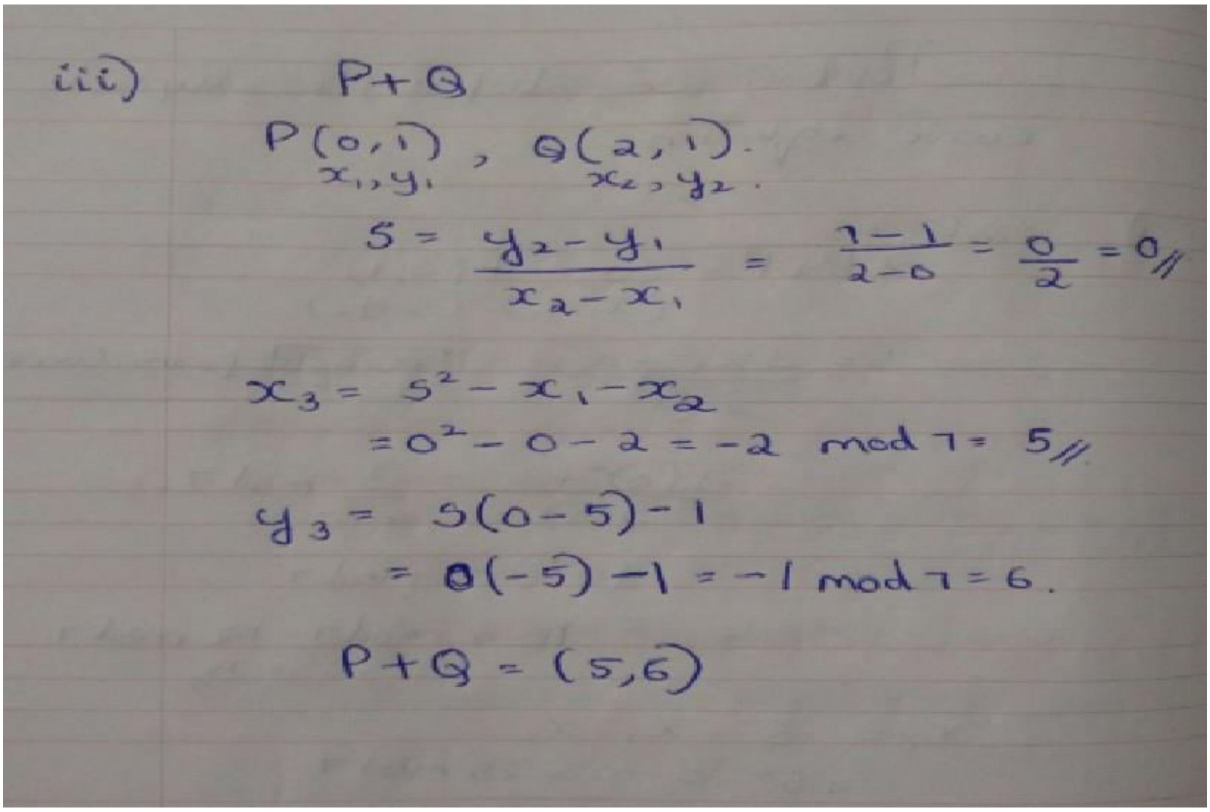
$= 4.$

$y_3 = 5(x_1 - x_3) - y_1$

$= 5(0 - 4) - 1 = -21 \mod 7$

$= 0.$

$2P = (4,0)$ //.



iii) $P+Q$

$P(0,1)$, $Q(2,1)$.

x_1, y_1 $\quad$ x_2, y_2.

$$s = \frac{y_2 - y_1}{x_2 - x_1} = \frac{1-1}{2-0} = \frac{0}{2} = 0 /\!/$$

$$x_3 = s^2 - x_1 - x_2$$

$$= 0^2 - 0 - 2 = -2 \bmod 7 = 5 /\!/$$

$$y_3 = s(0-5) - 1$$

$$= 0(-5) - 1 = -1 \bmod 7 = 6.$$

$P+Q = (5,6)$