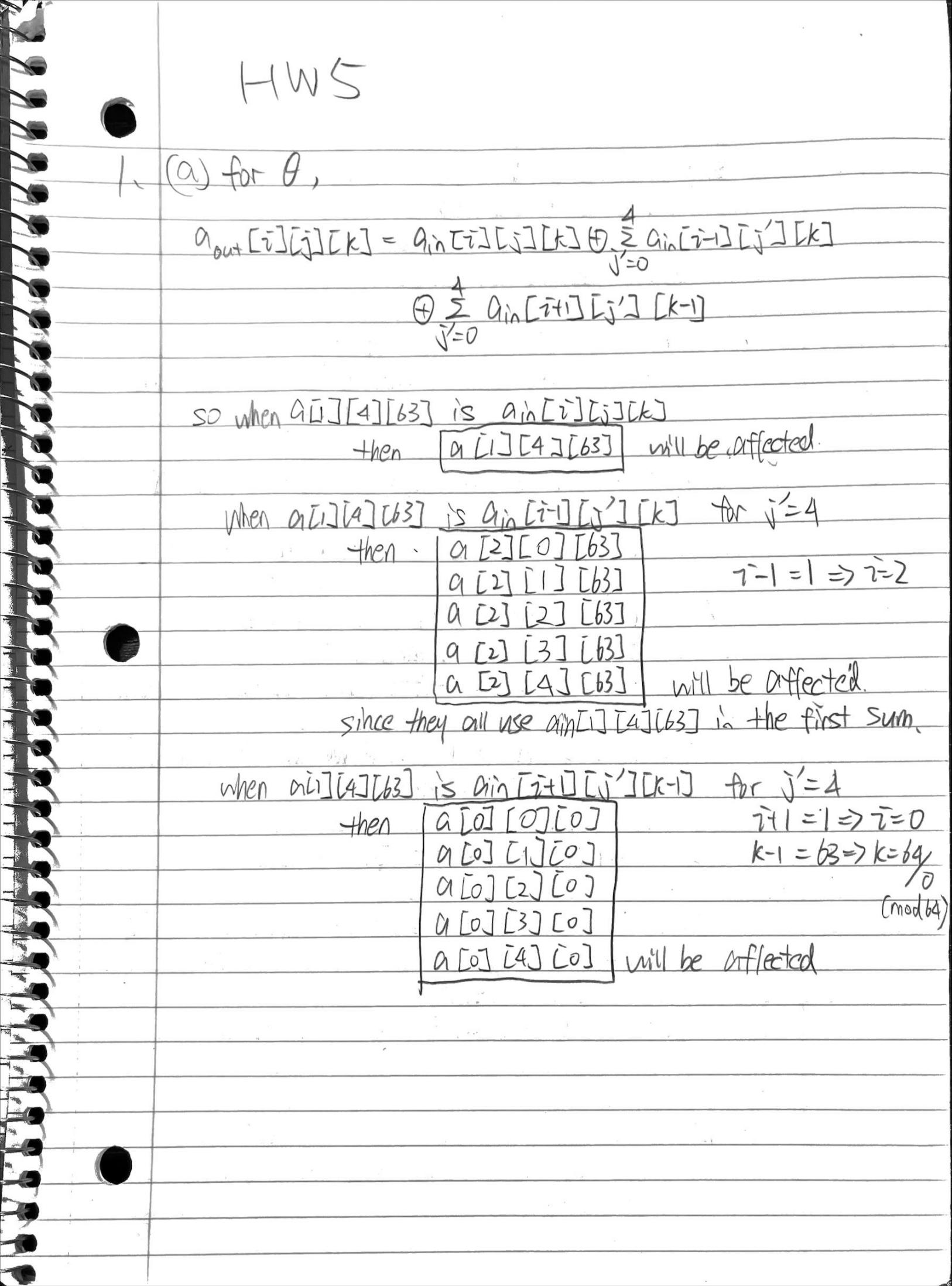
**CS181 HW5**

**Xiaoming Huang**

1a.



1b

//let B represent the output after round 1

//C represent the output after round 2

After round 1, B[1][4][63], B[2][0...4][63], B[0][0...4][0] are affected:

So in round 2:

B[1][4][63] is affected, then:

c[1][4][63], c[2][0...4][63], c[0][0...4][0], are affected

(11 intotal)

B[2][0...4][63] is affected, then:

~~C[2][0...4][63] is affected (repeat),~~

(if used in first sum: i-1= 2, so i=3; k=63)

C[3][0...4][63] are affected, (5 intotal)

(if used in second sum: i+1=2, i=1; k-1=63, k=0)

C[1][0..4][0] are affected, (5 intotal)

B[0][0...4][0] is affected, then:

~~C[0][0...4][0] are affected, (repeat)~~

(if used in first sum: i-1=0, i=1; k=0)

~~C[1][0...4][0] are affected, (repeat)~~

(if used in second sum: i+1=0, i=4; k-1=0, k=1)

C[4][0...4][1] are affected, (5 intotal)

Overall bits affected:

c[1][4][63],

c[2][0...4][63],

c[0][0...4][0],

C[3][0...4][63],

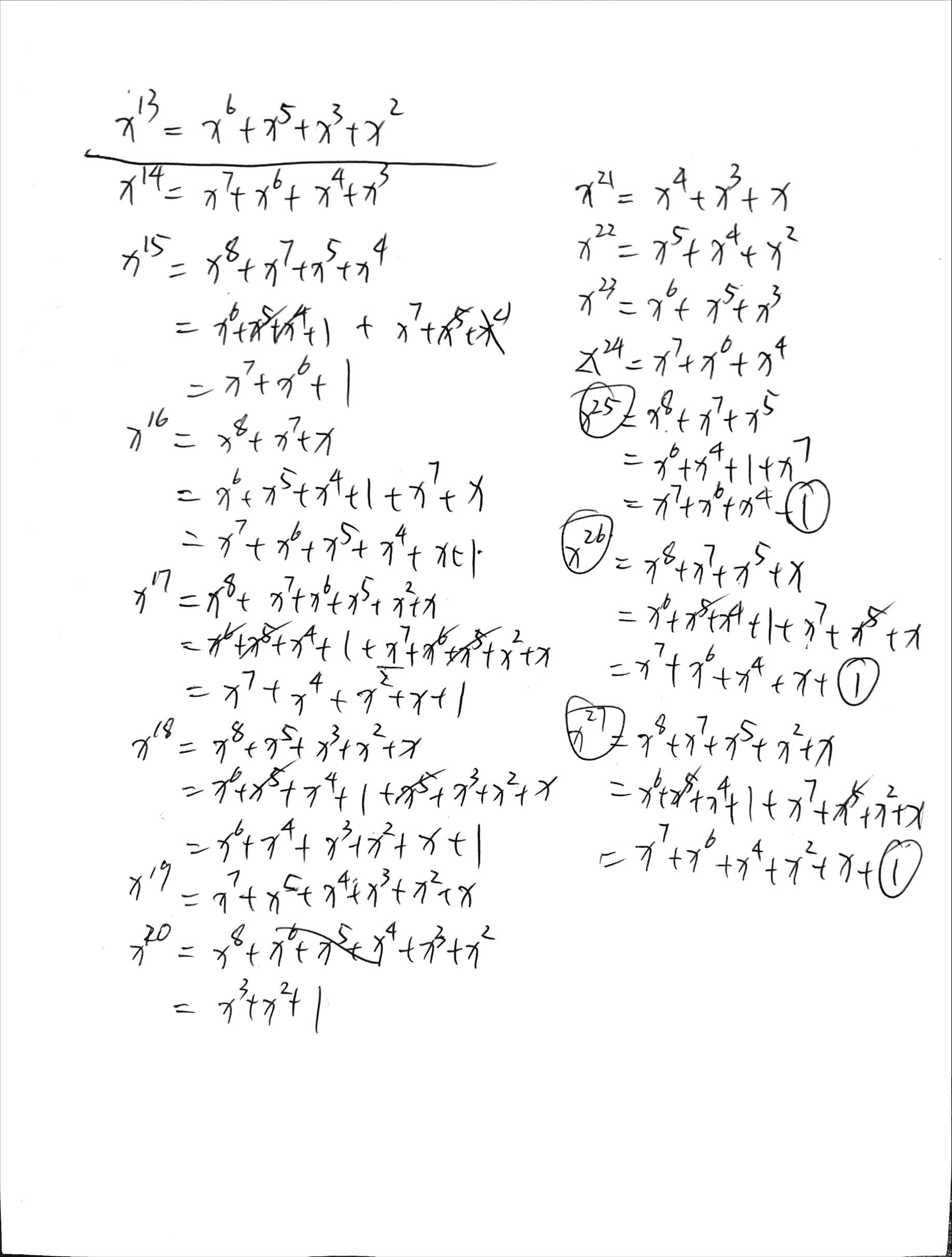
C[1][0..4][0],

C[4][0...4][1],

(26 in total)

2.

Using x^13 = x^6 + x^5 + x^3 + x^2 from the class



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| l | 2l-1 | t=l+7\*ir | x^t | Bit[0][0][2^l-1]=rc[t] |
| 0 | 0 | 21 | X^21 = x^4 + x^3 + x | 0 |
| 1 | 1 | 22 | X^22 = x^5 + x^4 + x^2 | 0 |
| 2 | 3 | 23 | X^23 = x^6 + x^5 + x^3 | 0 |
| 3 | 7 | 24 | X^24 = x^7 + x^6 + x^4 | 0 |
| 4 | 15 | 25 | X^25 = x^7 + x^6 + x^4 + 1 | 1 |
| 5 | 31 | 26 | X^26 = x^7 + x^6 + x^4 + x + 1 | 1 |
| 6 | 63 | 27 | X^27 = x^7 + x^6 + x^4 + x^2 + x + 1 | 1 |

So RC[3] has 1 on 15th,

RC[3] = 1000 0000 0000 0000 0000 0000 0000 0000

1000 0000 0000 0000 1000 0000 0000 0000

= (8000 0000 8000 8000)

This will XOR 1 to a[0][0][15], a[0][0][31], a[0][0][63]

//codes are in 345.cpp

checking for a\_out[4][3][9....18]: 0110011001

   value for a\_out[3][1][15...24]: 0011100000

checking for a\_out[4][3][9....18]: 0110110001

   value for a\_out[3][1][15...24]: 0001100010

5.

checking for a\_out[4][3][9....18]: 0110100001

   value for a\_out[3][1][15...24]: 0001101010