**Cryptography Assignment - 11**

**Pramod Aravind Byakod**

**(In Hoffstein-Pipher-Silverman book, second edition) 7.2, 7.3 (use S = 25916), 7.5 and 7.7 (you only need to find the volume)**

**Exercise 7.2**

**(a) M = (3, 7, 19, 43, 89, 195), S = 260**

S>195

S-195=260-195=65

65>43

65-43=22

22>19

22-19=3

3=3

3-3=0

Solution is **[1, 0, 1, 1, 0, 1]**

**(b) M = (5, 11, 25, 61, 125, 261), S = 408**

S>261

S-261=408-261=147

147>125

147-125=22

22>11

22-11=11

11>5

11-5=6

**Solution doesn’t exist in this case**

**(c) M = (2, 5, 12, 28, 60, 131, 257), S = 334**

S>257

S-257=334-257=77

77>60

77-60=17

17>12

17-12=5

5=5

Solution is **[0, 1, 1, 0, 1, 0, 1]**

**(d) M = (4, 12, 15, 36, 75, 162), S = 214**

S=214>162

S-162=214-162=52

52>36

52-36=16

16>15

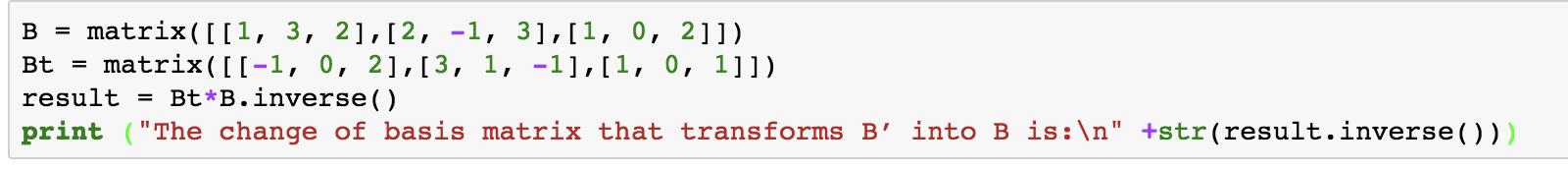
16-15=1

1<4(the smallest value of M)

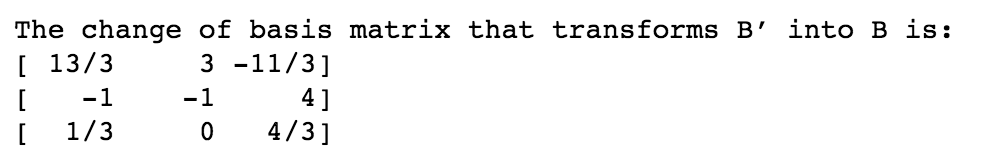
**Solution doesn’t exist in this case**

**Exercise 7.5**

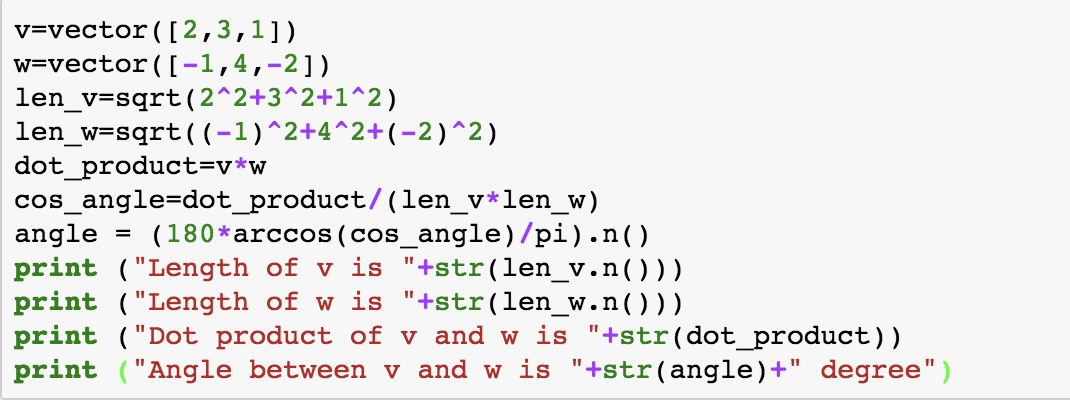
(a)



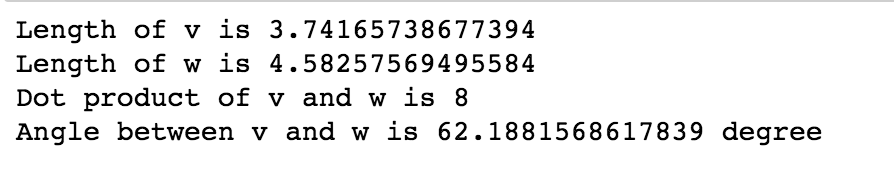
Output:



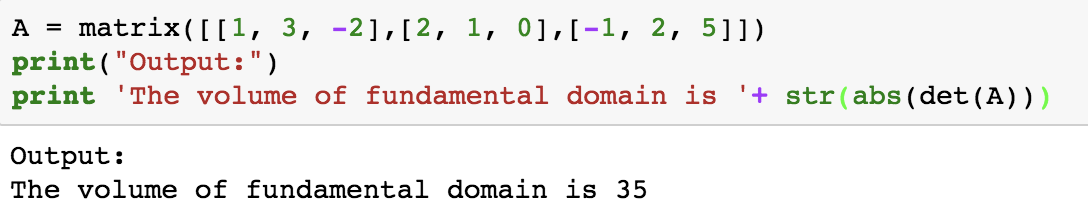
(b)

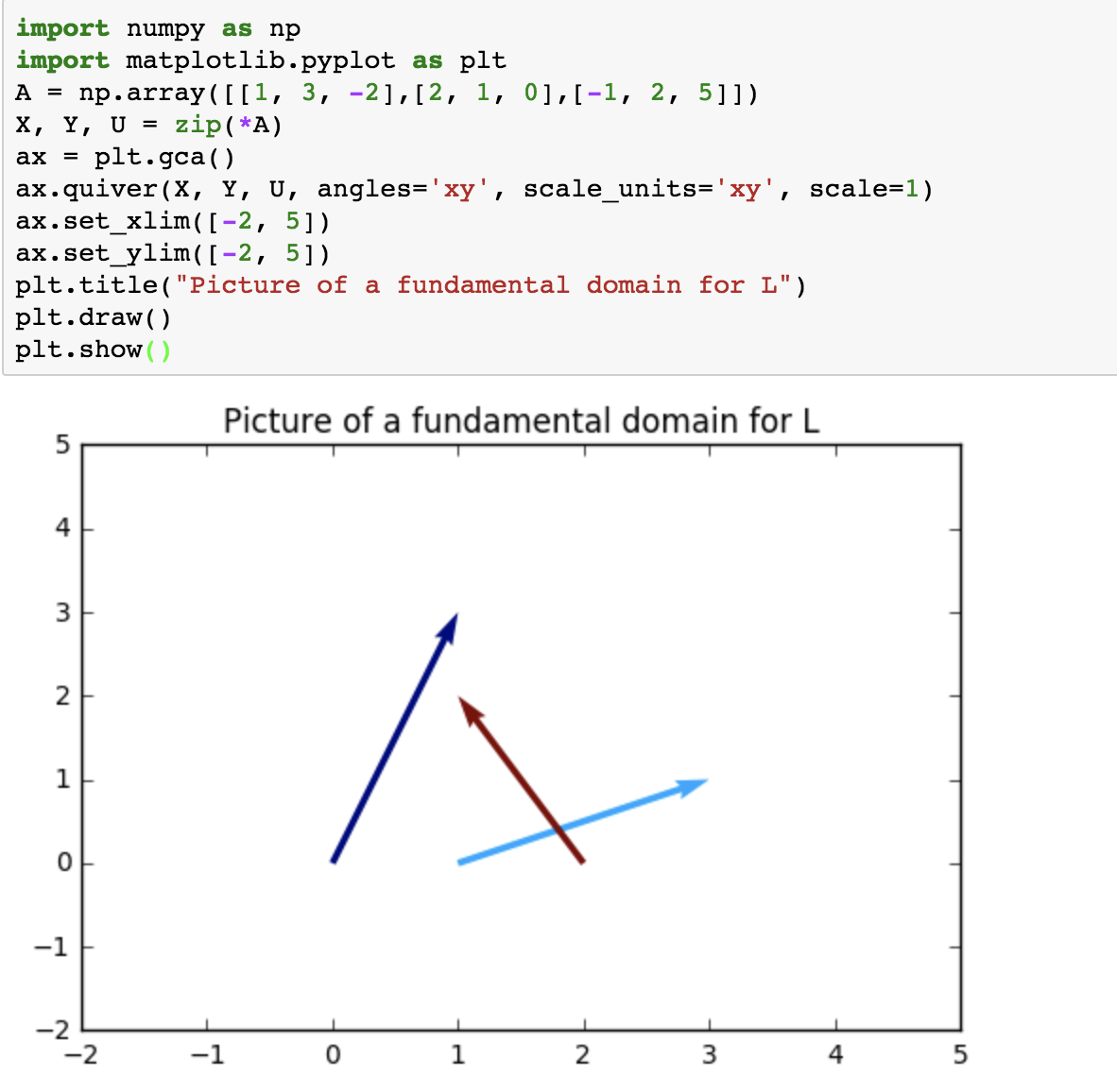


Output:



**Exercise 7.7**





**Exercise 7.3**

M = (5186, 2779, 5955, 2307, 6599, 6771, 6296, 7306, 4115, 637)

S = 25916

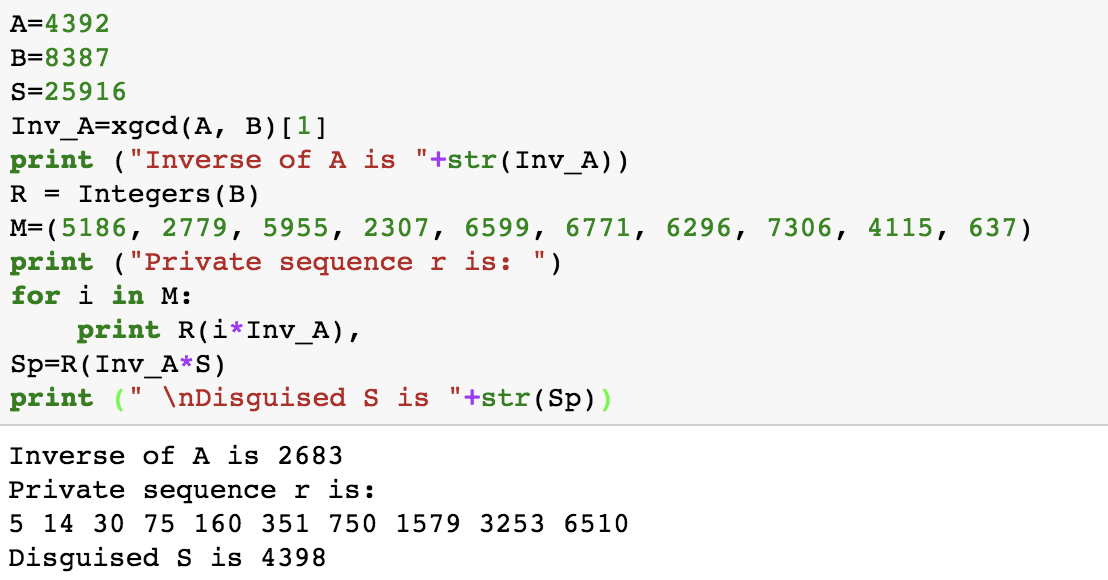
A = 4392

B = 8387

Using Sage, xgcd(4392, 8387) = (1, 2683, -1405)

We can write 1=2683\*4392-1405\*8387

Therefore, inverse of 4392 is 2683



Decrypt the message:

Sp=4398

4398>3253

4398-3253=1145

1145>750

1145-750=395

395>351

395-351=44

44>30

44-30=14

14=14

So, the result is **[0, 1, 1, 0, 0, 1, 1, 0, 1, 0]**