HW10

(In Hoffstein book) 7.2, 7.3, 7.5 and 7.7 (you only need to find the volume)

7.2. Use the algorithm described in Proposition 7.5 to solve each of the following subset-sum problems. If the “solution” that you get is not correct, explain what went wrong.

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

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

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

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

1. S>195, S-195=260-195=65

65>43, 65-43=22

22>19, 22-19=3

3=3,3-3=0

so the solution is [1, 0, 1, 1, 0, 1]

1. S>261, S-261=408-261=147

147>125, 147-125=22

22>11,22-11=11

11>5, 11-5=6

so the solution of the subset-sum problem doesn’t exist

1. S>257, S-257=334-257=77

77>60, 77-60=17

17>12, 17-12=5

5=5

So the solution is [0, 1, 1, 0, 1, 0, 1]

1. 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)

so the solution of the subset-sum problem doesn’t exist

7.3. Alice’s public key for a knapsack cryptosystem is M = (5186, 2779, 5955, 2307, 6599, 6771, 6296, 7306, 4115, 637).

Eve intercepts the encrypted message S = 7413. She also breaks into Alice’s computer and steals Alice’s secret multiplier A = 4392 and secret modulus B = 8387. Use this information to find Alice’s superincreasing private sequence r and then decrypt the message.

r\*A(mod B)=public key

First we need find the inverse of A, i.e.: A-1 ,

Using extended Euclidean Algorithm:

1=xgcd(4392, 8387)

8387=1\*4292+4095

4292=1\*4095+197

…

Or using Sagemath: xgcd(4392, 8387)

We get 1=2683\*4392-1405\*8387

So the inverse of 4392 is 2683

SageMath Code:

A=4392

B=8387

Inv\_A=xgcd(A, B)[1]

print 'Inverse of A is '+str(Inv\_A)

R=Integers(B)

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

print 'Private sequence r is: ',

for i in M:

print R(i\*Inv\_A),

Sp=R(Inv\_A\*25916)

print ''

print 'Disguised S is '+str(Sp)

Result:

Inverse of A is 2683

Private sequence r is: 5 14 30 75 160 351 750 1579 3253 6510

Disguised S is 4398

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]

7.5. (a) Let B = {(1, 3, 2), (2, −1, 3), (1, 0, 2)}, B’ = {(−1, 0, 2), (3, 1, −1), (1, 0, 1)}. Each of the sets B and B’ is a basis for R3. Find the change of basis matrix that transforms B’ into B.

(b) Let v = (2, 3, 1) and w = (−1, 4, −2). Compute the lengths "v" and "w" and the dot product v · w. Compute the angle between v and w.

1. SageMath Code:

B = matrix([[1, 3, 2],[2, -1, 3],[1, 0, 2]])

Bp = matrix([[-1, 0, 2],[3, 1, -1],[1, 0, 1]])

A = Bp\*B.inverse()

print 'The change of basis matrix that transforms B’ into B is:\n' + str(A.inverse())

Result:

The change of basis matrix that transforms B’ into B is:

[ 13/3 3 -11/3]

[ -1 -1 4]

[ 1/3 0 4/3]

1. SageMath Code:

v=vector([2,3,1])

w=vector([-1,4,-2])

v\_len=sqrt(2^2+3^2+1^2)

print 'length of v is '+str(v\_len.n())

w\_len=sqrt((-1)^2+4^2+(-2)^2)

print 'length of w is '+str(w\_len.n())

dot\_pro=v\*w

print 'dot product of v and w is '+str(dot\_pro)

cos\_angle=dot\_pro/(v\_len\*w\_len)

print 'The angle between v and w is '+str((180\*arccos(cos\_angle)/pi).n())+" degree"

Result:

length of v is 3.74165738677394

length of w is 4.58257569495584

dot product of v and w is 8

The angle between v and w is 62.1881568617839 degree

7.7. Let L be the lattice generated by {(1, 3, −2), (2, 1, 0), (−1, 2, 5)}. Draw a picture of a fundamental domain for L and find its volume.

SageMath Code:

A = matrix([[1, 3, -2],[2, 1, 0],[-1, 2, 5]])

print 'The volume of fundamental domain is '+ str(abs(det(A)))

Result:

The volume of fundamental domain is 35