Math 259: Spring 2019
Quiz 4

NAME: SOLUTIONS

Are you taking this class for graduate credit?

Time: **30 minutes**

Problem	Value	Score
1	3	
2	6	
3	6	
4	5	
TOTAL	20	

Problem 1 : (3 points) Let L be the lattice generated by the vectors

$$\vec{v}_1 = (3, 2, -1), \quad \vec{v}_2 = (-1, 0, 3), \quad \vec{v}_3 = (0, 5, 1).$$

Give two vectors that belong to this lattice. Please show all of your work.

Easy options: $\vec{v}_1 = (3, 2, -1)$
$\vec{v}_2 = (-1, 0, 3)$
$\vec{v}_3 = (0, 5, 1)$

all belong to the lattice

other options:

$\vec{v}_1 + \vec{v}_2 = (2, 2, 2)$

$2\vec{v}_2 - \vec{v}_1 + \vec{v}_3 = (-5, 3, 8)$

all belong to the lattice

etc

Finally, by HW5#4, any

$$\vec{v} = (a_1\ a_2\ a_3)\begin{bmatrix} 3 & 2 & -1 \\ -1 & 0 & 3 \\ 0 & 5 & 1 \end{bmatrix}$$

belongs to the lattice if $a_1, a_2, a_3 \in \mathbb{Z}$

Problem 2 : (6 points) Suppose that you have set up a **Regev** LWE cryptosystem with $q = 17$ and $\vec{s} = (4, 3, 14, 1)$. Decrypt the pair

$$((13, 5, 1, 6), 3).$$

Decryption is

$$b - \vec{a} \cdot \vec{s} = 3 - (13, 5, 1, 6)(4, 3, 14, 1)$$

$$= 3 - (52 + 15 + 14 + 6)$$

$$= 3 - 87$$

$$= -84$$

Then see if the remainder modulo $q = 17$ is closer to $\lfloor \frac{q}{2} \rfloor = \lfloor \frac{17}{2} \rfloor = \lfloor 8.5 \rfloor = 8$ than to 0 modulo 17

$$-84 = -34 - 34 - 16 \equiv -16 \equiv 1 \pmod{17}$$

$$\begin{array}{r} 84 \\ -68 \\ \hline 16 \end{array}$$

This is closer to 0, so we decrypt the message to be

$$\boxed{0}$$

Problem 3 : (6 points) Give a reduced basis and the shortest vector for the lattice generated by the vectors

$$\vec{v}_1 = (-1, 3), \quad \vec{v}_2 = (-2, 3).$$

Since $|-1| < |-2|$, $\vec{v}_1$ is shorter than $\vec{v}_2$

First round of reducing:

- $\dfrac{\vec{v}_1 \cdot \vec{v}_2}{\vec{v}_1 \cdot \vec{v}_1} = \dfrac{2+9}{1+9} = \dfrac{11}{10}$

- the nearest integer to $\frac{11}{10}$ is $t = 1$

- we replace $\vec{v}_2$ with $\vec{v}_2 - t\vec{v}_1 = (-2,3) - (-1,3)$
  $= (-1, 0)$

Now $(-1,0)$ is shorter than $(-1,3)$ so we set
$\vec{v}_1 = (-1,0)$ $\vec{v}_2 = (-1,3)$

Second round of reducing:

- $\dfrac{\vec{v}_1 \cdot \vec{v}_2}{\vec{v}_1 \cdot \vec{v}_1} = \dfrac{1+0}{1} = 1$

- the nearest integer to 1 is $t = 1$

- we replace $\vec{v}_2$ with $\vec{v}_2 - t\vec{v}_1 = (-1,3) - (-1,0)$
  $= (0,3)$

Now $(-1,0)$ is still shorter than $(0,3)$ so we set $\vec{v}_1 = (-1,0)$ $\vec{v}_2 = (0,3)$

Third round of reducing:

- $\frac{\vec{v}_1 \cdot \vec{v}_2}{\vec{v}_1 \cdot \vec{v}_1} = \frac{0}{1} = 0$

- the nearest integer to 0 is $t=0$

When $t=0$ the algorithm terminates.

So the reduced basis is $\vec{v}_1 = (-1,0)$ $\vec{v}_2 = (0,3)$

and a shortest vector is $\vec{v}_1 = (-1,0)$.

Problem 4 : (5 points) Let $n = 3$ and $q = 11$. Generate $m = 2$ **Regev** LWE pairs, each of length $n = 3$ with entries in $\mathbb{Z}/11\mathbb{Z}$. Please show all of your work.
When you are supposed to generate random numbers or draw from a distribution, just make up numbers that are plausible in context.

Let $\vec{s} = (3, -2, 5)$

$\vec{a}_1 = (-1, 4, 2)$

$\vec{a}_2 = (2, 0, -2)$

$e_1 = 1 \quad e_2 = 0$

} these are all values I just made up

then $\vec{a}_1 \cdot \vec{s} + e_1 = (-3 - 8 + 10) + 1 = -1 + 1 = 0 = b_1$

$\vec{a}_2 \cdot \vec{s} + e_2 = (6 + 0 - 10) + 0 = -4 = b_2$

My 2 pairs are

$((-1, 4, 2), 0)$ OR in $\mathbb{Z}/11\mathbb{Z}$: $((10, 4, 2), 0)$

$((2, 0, -2), -4)$ $((2, 0, 9), 7)$