Math 259: Spring 2019
Quiz 4

NAME:

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.

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

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

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

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

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.