USS: Introduction to mathematical cryptography
Thursday July 28 problems

1. Let $\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_n$ be linearly independent row vectors in $\mathbb{R}^n$. Form the matrix $M$ whose rows are the vectors $\vec{v}_i$. Let $\vec{a} = (a_1, \ldots, a_n)$ be a row vector with integer entries. Show that $\vec{a}M$ is a vector in the lattice generated by $\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_n$ and show that every vector in the lattice can be written in this way. (So $M$ is a generating matrix for the lattice.)

2. Please read about lattice basis reduction in two dimensions. You can find pseudocode for it on Wikipedia at `https://en.wikipedia.org/wiki/Lattice_reduction#In_two_dimensions`, and it's also covered in Trappe and Washington. For each of the following two lattices, please give a reduced basis and a shortest vector:

   (a) the lattice generated by the vectors $\vec{v}_1 = (1, 5)$ and $\vec{v}_2 = (6, 21)$

   (b) the lattice generated by the vectors $\vec{v}_1 = (3, 8)$ and $\vec{v}_2 = (5, 14)$

3. (a) Find a reduced basis for the lattice generated by the vectors $\vec{v}_1 = (53, 88)$ and $\vec{v}_2 = (107, 205)$.

   (b) Find the vector in the lattice of part (a) that is closest to the vector $\vec{v} = (151, 33)$. (This is an example of the closest vector problem. It is easier to solve when a reduced basis is known, but difficult in general.)

4. Throughout this problem, let $q = 17$. Consider the matrix

$$A = \begin{pmatrix} 1 & 2 & 0 & 16 \\ 4 & 3 & 14 & 15 \\ 14 & 0 & 4 & 1 \\ 4 & 16 & 15 & 3 \end{pmatrix}.$$

   Someone who cares about you very much tells you that if $\vec{z} = (1, -1, 1, -1)$, then $A\vec{z} \equiv 0 \pmod{17}$.

   Consider the following two sets of pairs $\{(\vec{a}_i, b_i)\}$. One of them is a set of LWE pairs, and the other is just made up with random values of $b_i$. Can you tell which is which? First set of pairs:

$$((1, 4, 14, 4), 3)$$
$$((2, 3, 0, 16), 5)$$
$$((0, 14, 4, 15), 14)$$
$$((16, 15, 1, 3), 3)$$

   Second set of pairs:

$$((1, 4, 14, 4), 8)$$
$$((2, 3, 0, 16), 16)$$
$$((0, 14, 4, 15), 14)$$
$$((16, 15, 1, 3), 5)$$