Math 565, Problem Set 7: *due Friday, February 23*

1. Alice's public key for a subset-sum cryptosystem is

$$\mathbf{M} = (5186, 2779, 5955, 2307, 6599, 6771, 6296, 7306, 4115, 7039).$$

   Eve intercepts the encrypted message $S = 26560$. 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 $\mathbf{r}$ and then decrypt the message.

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