Math 400 Fall 2017
Cryptology HW 9 Solutions
Due Thursday, November 2

1. Solve the following knapsack problems:

   (a) $\mathbf{M} = (3, 7, 19, 43, 89, 195), S = 260$

   (b) $\mathbf{M} = (5, 11, 25, 61, 125, 261), S = 408$

   (c) $\mathbf{M} = (4, 12, 15, 36, 75, 162), S = 214$

   Solution:

   (a) $260 = 195 + 43 + 19 + 3$

   (b) $408 = 261 + 125 + 11 + 11$. (This isn't really a solution; I wrote a bad problem. I gave full credit to people with this solution and to people with no solution; I took points off if you gave me a false solution).

   (c) $214 = 162 + 36 + 12 + 4$. Note this isn't superincreasing so the algorithm doesn't work.

2. Alice publishes the public key $\mathbf{M} = (18, 89, 90, 110, 185, 141)$

   (a) Supposeyou wish to send the message $\mathbf{x} = (1, 1, 0, 1, 1, 0)$ (corresponding to 27 in binary). What ciphertext should you send?

   (b) Suppose you intercept someone else's message of $S = 430$. Express the problem of decrypting this message as a shortest-vector problem, as in section 9.5 of the notes.

   (c) Now decrypt the message corresponding to $S = 430$. You don't need to use lattice methods to do this.

   Solution:

   (a) We have $S = 18 + 89 + 110 + 185 = 402$.

   (b) Let L be the lattice generated by

   $$\mathbf{v}_1 = (2, 0, 0, 0, 0, 0, 18) \qquad \mathbf{v}_2 = (0, 2, 0, 0, 0, 0, 89)$$
   $$\mathbf{v}_3 = (0, 0, 2, 0, 0, 0, 90) \qquad \mathbf{v}_4 = (0, 0, 0, 2, 0, 0, 110)$$
   $$\mathbf{v}_5 = (0, 0, 0, 0, 2, 0, 185) \qquad \mathbf{v}_6 = (0, 0, 0, 0, 0, 2, 141)$$
   $$\mathbf{v}_7 = (1, 1, 1, 1, 1, 1, 430).$$

   Then we wish to find the shortest vector in L.

(c) Trial and error shows that $S = 89 + 90 + 110 + 141$ so the message is $\mathbf{x} = (0, 1, 1, 1, 0, 1) = 46$.

3. Alice chooses the superincreasing sequence

$$\mathbf{r} = (2, 5, 13, 28, 60, 144)$$

with the numbers $A = 53$ and $B = 300$.

(a) What public key does Alice publish?

(b) Alice receives the ciphertext $S = 681$. What is the plaintext message?

Solution:

(a) We have $A = 53$ so $A^{-1} \equiv 17 \mod 300$. Then we have

$$\mathbf{M} = (106, 265, 89, 284, 180, 132).$$

(b) We compute $A^{-1}S = 17 \cdot 681 = 11577 \equiv 177$. Thus she sees the solution is $\mathbf{x} = (0, 1, 0, 1, 0, 1)$.

4. Suppose Alice's public key for a knapsack cryptosystem is

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

Eve intercepts the encrypted message $S = 26560$. She also manages to steal from Alice the secret numbers $A = 4392$ and $B = 8387$. Use this information to find Alice's superincreasing sequence $\mathbf{r}$ and then decrypt the message.

Solution: We have $A^{-1} \equiv 2683 \mod 8387$, so we have

$$\mathbf{r} = A^{-1}\mathbf{M} = (5, 14, 30, 75, 160, 351, 750, 1579, 3253, 6500).$$

To decrypt we calculate $S' = A^{-1}S = 2683 \cdot 26560 \equiv 4528 \mod 8387$. Then we write

$$S' = 3253 + 750 + 351 + 160 + 14.$$

Thus the message is $(0, 1, 0, 0, 1, 1, 1, 0, 1, 0) = 314$ in decimal (or 370 if you read it backwards).

5. Which of the following matrices are invertible over $\mathbb{Z}$? Find inverses for the ones that are.

(a) $\begin{bmatrix} 3 & 1 \\ 2 & 2 \end{bmatrix}$

(b) $\begin{bmatrix} 3 & -2 \\ 2 & -1 \end{bmatrix}$

(c) $\begin{bmatrix} 3 & 2 & 2 \\ 2 & 1 & 2 \\ -1 & 3 & 1 \end{bmatrix}$

(d) $\begin{bmatrix} -3 & -1 & 2 \\ 1 & -3 & -1 \\ 3 & 0 & 2 \end{bmatrix}$

Solution:

(a) The determinant is $6 - 2 = 4$ so the matrix is not invertible over $\mathbb{Z}$.

(b) The determinant is $-3 + 4$ so the matrix is invertible over $\mathbb{Z}$. The inverse is

$$\begin{bmatrix} -1 & 2 \\ -2 & 3 \end{bmatrix}.$$

(c) The determinant is -9 so the matrix is not invertible over $\mathbb{Z}$.

(d) The determinant is 41 so the matrix is not invertible over $\mathbb{Z}$.

6. Let L be the lattice generated by the basis $B = \{(3, 1, -2), (1, -3, 5), (4, 2, 1)\}$. Which of the following sets of vectors are also bases for L? For each one that is, find the change of basis matrix and write the new basis in terms of the basis B.

(a) $B_1 = \{(5, 13, -13), (0, -4, 2), (-7, -13, 18)\}$

(b) $B_2 = \{(4, -2, 3), (6, 6, -6), (-2, -4, 7)\}$.

(a) We have $\mathbf{w}_1 = -3\mathbf{v}_2 + 2\mathbf{v}_3$, $\mathbf{w}_2 = \mathbf{v}_1 + \mathbf{v}_2 - \mathbf{v}_3$, and $\mathbf{w}_3 = -2\mathbf{v}_1 + 3\mathbf{v}_2 - \mathbf{v}_3$. Thus we have the matrix

$$U = \begin{bmatrix} 0 & -3 & 2 \\ 1 & 1 & -1 \\ -2 & 3 & -1 \end{bmatrix}$$

We have $\det U = 1$ so this is a basis.

(b) We have

$$\begin{aligned} \mathbf{w}_1 &= \mathbf{v}_1 + \mathbf{v}_2 \\ \mathbf{w}_2 &= \mathbf{v}_1 - \mathbf{v}_2 + \mathbf{v}_3 \\ \mathbf{v}_3 &= -\mathbf{v}_1 + \mathbf{v}_2 \end{aligned}$$

Then we have

$$U = \begin{bmatrix} 1 & 1 & 0 \\ 1 & -1 & 1 \\ -1 & 1 & 0 \end{bmatrix}$$

and $\det U = -2$ so this isn't a basis.

7. A lattice L has dimension $n = 251$ and determinant $\det(L) \approx 2^{2251.58}$. How long do you expect the shortest vector to be?

Solution: By the Gaussian heuristic, we estimate the shortest length to probably be

$$\sigma(L) = \sqrt{\frac{251}{2\pi e}}(2^{2251.58})^{1/251} \approx 1923.$$