Monash University
FIT 5124: Advanced Topics in Security
Week 2 Tutorial Sheet

Ron Steinfeld, 7 March 2016

This week's tutorial will cover basic concepts regarding lattices and their crypto. applications. It will also introduce you to the Sage mathematical software package, which we will be using to do computational exercises throughout this unit.

1 Problems

1 **Lattice points and bases.** (based on LatticeBook, exercise 1.21). Let

$$\boldsymbol{b}_1 = \begin{bmatrix} 4 \\ -7 \end{bmatrix}, \boldsymbol{b}_2 = \begin{bmatrix} -7 \\ -8 \end{bmatrix}, \boldsymbol{b}'_1 = \begin{bmatrix} -79 \\ -44 \end{bmatrix}$$

.

a Is $\boldsymbol{b}'_1$ in the lattice $L(B)$ generated by basis $B = (\boldsymbol{b}_1, \boldsymbol{b}_2)$? Why?

b Find a lattice vector $\boldsymbol{b}'_2$ such that $B' = (\boldsymbol{b}'_1, \boldsymbol{b}'_2)$ is another basis for the lattice $L(B)$, if such a vector exists.

c Repeat questions 1a,1b with $\boldsymbol{b}_1, \boldsymbol{b}_2$ as above but

$$\boldsymbol{b}'_1 = \begin{bmatrix} -79 \\ -45 \end{bmatrix}.$$

d Repeat questions 1a,1b with $\boldsymbol{b}_1, \boldsymbol{b}_2$ as above but

$$\boldsymbol{b}'_1 = \begin{bmatrix} -158 \\ -90 \end{bmatrix}.$$

e Use Sage to check if the vector $\boldsymbol{v}$ belongs to the 4-dimensional lattice with basis B, where:

$$\boldsymbol{v} = \begin{bmatrix} -59 \\ 9 \\ 148 \\ -134 \end{bmatrix}, B = \begin{bmatrix} 4\ 5\ 34\ 12 \\ 3\ 7\ 23\ 13 \\ 9\ 8\ 22\ 18 \\ 2\ 9\ 44\ 15 \end{bmatrix}$$

2 **Multiple Bases.**

a Show, using Cramer's Rule from Linear Algebra, that if U is an integer unimodular matrix ($\det(U) \in \{-1, 1\}$), then so is U^{-1}. Then use this to prove the Lemma from the lecture: $B, B' \in \mathbb{R}^{n \times n}$ are two bases of the same lattice if and only if $B' = B \cdot U$ for some unimodular matrix $U \in \mathbb{R}^{n \times n}$.

b For the following matrices B, B', use Sage to check if B, B' generate the same lattice, and if so, compute the unimodular matrix U such that $B' = B \cdot U$ and verify that it is unimodular:

$$B = \begin{bmatrix} 4\ 5\ 34\ 12 \\ 3\ 7\ 23\ 13 \\ 9\ 8\ 22\ 18 \\ 2\ 9\ 44\ 15 \end{bmatrix}, B' = \begin{bmatrix} 249\ 150\ 421\ 132 \\ 192\ 113\ 319\ 102 \\ 260\ 104\ 359\ 118 \\ 297\ 205\ 540\ 169 \end{bmatrix}.$$

3 **Ajtai's Cryptographic Hash Function.**

a Use Sage to generate a random instance A of Ajtai's hash function with parameters $n = 5, q = 31, m = 30, d = 2$.

b Compute in Sage a basis for the SIS lattice $L_q(A)$ corresponding to the matrix A in (b).

c Use the birthday paradox attack to find a collision in the hash function of (b). How many evaluations of the hash do you expect to require to find a collision? How would you choose n to make this attack infeasible?

d Use the collision found in (c) to compute a short non-zero vector $\boldsymbol{v}$ in the SIS lattice $L_q(A)$, as in the lectures.