The art of cryptography: Lattices and cryptography, summer 2013

PROF. DR. JOACHIM VON ZUR GATHEN, DR. DANIEL LOEBENBERGER

2. Exercise sheet
Hand in solutions until Sunday, 28 April 2013, 23:59h.

Exercise 2.1 (Transforming bases). (5+10 points)

Let $A \in \mathbb{R}^{\ell \times n}$ be a basis of the lattice $L = \mathcal{L}(A)$. Express each of the following matrix operations on A as a left multiplication by a unimodular matrix $U \in \mathbb{Z}^{\ell \times \ell}$, i.e. an integer matrix with $\det(U) = \pm 1$:

(i) Swap the order of the rows of A, $\boxed{2}$

(ii) Multiply a row by -1, $\boxed{1}$

(iii) Add an integer multiple of a row to another row, i.e. set $a_i \leftarrow a_i + ca_j$ where $i \neq j$ and $c \in \mathbb{Z}$. $\boxed{2}$

(iv) Show that any unimodular matrix can be expressed as a sequence of these three elementary integer row transformations. $\boxed{+10}$

Exercise 2.2 (Lattices and the gcd). (8 points)

Assume you are given two integers $a, b \in \mathbb{N}$ and consider the lattice $L = \mathcal{L}(A)$ spanned by the basis

$$A = \begin{bmatrix} 1 & 0 & \gamma a \\ 0 & 1 & \gamma b \end{bmatrix},$$

where $\gamma \in \mathbb{R}_{>1}$ is some large constant.

(i) Do some experiments with the lattice L: Select, say, 100 pairs (a, b) randomly, where a and b are at most $C = 100$ and check for which values of γ the basis reduction algorithm yields always a basis of the form $\boxed{5}$

$$B = \begin{bmatrix} x_1 & x_2 & 0 \\ s & t & \pm\gamma \gcd(a, b) \end{bmatrix},$$

with $sa + tb = \pm \gcd(a, b)$.

(ii) Try also the values $C = 500$, $C = 1000$ and $C = 5000$. Hand in a table of values of γ for which your experiment succeeded. $\boxed{3}$

Exercise 2.3 (Linear congruential generators). (17 points)

We consider the linear congruential generators with $x_i = (ax_{i-1} + b) \operatorname{rem} m$.

(i) Compute the pseudorandom sequence of numbers resulting from

2 (a) $m = 10$, $a = 3$, $b = 2$, $x_0 = 1$ and

2 (b) $m = 10$, $a = 8$, $b = 7$, $x_0 = 1$.

What do you observe?

3 (ii) You observe the sequence of numbers

$$13, 223, 793, 483, 213, 623, 593, \ldots$$

generated by a linear congruential generator. Find matching values of m, a and b.

How do you do this?

(iii) Consider $m = 100$, $a = 3$, $b = 2$, $x_0 = 1$. Compute the result of the truncated linear congruential generator, which outputs the top half of the bits.

10 (iv) Implement the truncated linear congruential generator in a programming language of your choice. Also implement the non-truncated generator together with the algorithm breaking it.