The Art of Cryptography: Integral Lattices, summer 2010
PROF. DR. JOACHIM VON ZUR GATHEN, DANIEL LOEBENBERGER

6. Exercise sheet
Hand in solutions until Sunday, 30 May 2010, 23:59h.

Exercise 6.1 (Breaking truncated linear congruential generators). (14+15 points)

We consider the truncated homogenous linear congruential generators with \( x_i = ax_{i-1} \mod m \). We are given that \( m = 1009 \), \( s = \lceil \log(2, m)/2 \rceil = 5 \) and \( a = 25 \). The sequence \( y \) is defined as \( y_i := x_i \div 2^s \) which you intercepted as

\[
0, 10, 21, 25, 30, 8, 13, 13, 24, 14, 7, 6, 15, 28, 10, 3, 17, 25, 0, 15, 12, \ldots
\]

Our task is to break this generator completely. To do so, we will recover the sequence \( z_i \) with \( x_i = y_i 2^s + z_i \).

(i) Write down the matrix (over \( \mathbb{Z}/m \))

\[
A = \begin{bmatrix}
  m & 0 & 0 & 0 & 0 \\
  -a & 1 & 0 & 0 & 0 \\
  -a^2 & 0 & 1 & 0 & 0 \\
  -a^3 & 0 & 0 & 1 & 0 \\
  -a^4 & 0 & 0 & 0 & 1 \\
  -a^5 & 0 & 0 & 0 & 0
\end{bmatrix}
\]

(ii) Compute the sequence \( c_i := (a^{-1} y_1 - y_i) 2^s \) over \( \mathbb{Z} \) for \( i = 1, \ldots, 6 \).

(iii) Using lattice basis reduction compute a reduced basis \( V \) and a unimodular transformation \( U \) such that \( V = UA \).

(iv) Compute \( Uc \) and take the balanced system of representatives modulo \( m \) of your result.

(v) Now solve \( Vz = Uc \) using Gaussian elimination, obtaining the \( z_i \).

(vi) Finish by writing down the sequence \( x_i \).

(vii) Compute the next 10 values of the above sequence of \( y \)'s.

(viii) Argue that you have broken the generator.

(ix) Explain in detail why we had to use basis reduction at all.

(x) Play a bit around with your algorithms. Try different values of \( m, a \) and \( s \) and report on the successes and failures of your algorithm.
Exercise 6.2 (Dual lattices). (14 points)

Let $B \in \mathbb{R}^{n \times n}$ and let $L = \mathcal{L}(B)$ be a full-rank lattice. Consider its dual $L^* := \mathcal{L}(B)^* := \{v \in \mathbb{R}^n \mid \forall u \in L : uv \in \mathbb{Z}\}$.

(i) We now first show that $L^*$ is indeed a lattice. In particular we will show that $D := (B^T)^{-1}$ is a basis of $L^*$.
   
   (a) Show that $D$ is contained in $\mathcal{L}(B)^*$.
   (b) Conclude that $\mathcal{L}(D)$ is contained in $\mathcal{L}(B)^*$.
   (c) Show that also $\mathcal{L}(B)^*$ is contained in $\mathcal{L}(D)$. Hint: Use that $\text{span}(B) = \text{span}(D)$.

(ii) Show that we have $(L^*)^* = L$.

(iii) Prove that we have $\det(L^*) = 1/\det(L)$.

(iv) Show that $\lambda(L)\lambda(L^*) \leq n$. Hint: Use Minkowski’s bound $\lambda(L) \leq \sqrt{n} \det(L)^{1/n}$.

(v) We finish with some examples of dual lattices:
   
   (a) Compute the dual of the lattice $2\mathbb{Z}^n$.
   (b) Compute the dual of the lattice spanned by the basis $\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$.