The Art of Cryptography: Integral Lattices, summer 2010

PROF. DR. JOACHIM VON ZUR GATHEN, DANIEL LOEBENBERGER

3. Exercise sheet
Hand in solutions until Sunday, 2 May 2010, 23:59h.

Exercise 3.1 (The basis reduction algorithm). (32+3 points)

In this exercise we will do several experiments with the lattice basis reduction algorithm. For that (and also for later programming tasts) we need a running implementation.

(i) Implement the basis reduction algorithm in a programming language of your choice. Hand in the source code. Hint: Try to work bottom up. Implement the vector arithmetic first, afterwards scalar products and the $\mu_{i,j}$. Build from that the GSO, which in turn is used by the size-reduction and the exchange-step. Once you have all this, start writing the basis reduction algorithm. It is helpful to employ a computer algebra system for that task! [20]

If you did not succeed in making the algorithm run, use your brain or a built in function of a computer algebra system like Maple or MuPAD. Let's now try our nice example from the last sheet:

(ii) Test the algorithm! Compute $a, b \in \mathbb{Z}$ with $a^2 + b^2 = 1034353$ using your basis reduction algorithm. [3]

(iii) For which parameters δ do you obtain a solution? Note that in the Maple and MuPAD implementations the parameter δ is fixed and cannot be changed. [+2]

Let us now consider the lattice $L = \mathcal{L}(B)$ spanned by the basis $B = \begin{bmatrix} 2 & 1 & 5 & 8 \\ 7 & 2 & 5 & 5 \\ 2 & 3 & 1 & 1 \\ 5 & 8 & 9 & 9 \end{bmatrix}$.

(iv) Minkowski's theorem states that for any lattice we have $\lambda(L) \leq \sqrt{n}\,\det(L)^{1/n}$. What is the value of this bound in our example? [2]

(v) What is the length of the shortest vector in the output of the basis reduction algorithm? [1]

(vi) What is the value of the integer $\mathcal{D} = \prod_{i=1}^{4} \det(\mathcal{L}(b_1, \ldots, b_i))^2$ for the input basis? [2]

(vii) What is the number of iterations predicted by the running time analysis from the lecture? [1]

(viii) What is the value of $\mathcal{D}$ upon finding a reduced basis? [1]

(ix) Give an upper bound on the number of iterations based on the initial and final value of $\mathcal{D}$. [2]

(x) What is the number of iterations actually executed? [+1]