Fachbereich Mathematik
Elena Klimenko

WS 2017/18
Homework 13

NUMBER THEORY AND CRYPTOGRAPHY

Due in class on Friday, February 2nd, at 12:05 pm.

1. Let $L \subset \mathbb{R}^2$ be the lattice given by the basis $\mathcal{B} = \{v_1, v_2\}$, where $v_1 = (213, -437)$ and $v_2 = (312, 105)$, and let $w = (43127, 11349)$.

(a) Use Babai's algorithm to find a vector $v \in L$ that is close to w. Compute the distance $\|v - w\|$.

(b) Show that the vectors $v_1' = (2937, -1555)$ and $v_2' = (11223, -5888)$ also form a basis for the same lattice L.

(c) Use Babai's algorithm with the new basis $\mathcal{B}' = \{v_1', v_2'\}$, where v_1' and v_2' are given in (b), to find a vector $v' \in L$ that is close to w. Compute the distance $\|v' - w\|$ and compare it with your answer from (a).

(d) Which basis is good, $\mathcal{B}$ or $\mathcal{B}'$? What is the value of the Hadamard ratio in both cases?

2. (a) For given numbers N, q, and polynomials $a(x)$ and $b(x)$, compute the convolution product $c = a \star b$ in the ring $R_q = {(\mathbb{Z}/q\mathbb{Z})[x]}/{(x^N - 1)}$.

(i) $N = 3, \quad q = 7, \quad a(x) = 1 + x, \quad b(x) = 2 + 4x + 2x^2$;

(ii) $N = 7, \quad q = 3, \quad a(x) = x + x^3, \quad b(x) = x + x^2 + x^4 + x^6$.

(b) Let $N = 5$ and $q = 3$. Consider the following two polynomials in R_3:

$$a(x) = 1 + x^2 + x^3 \quad \text{and} \quad b(x) = 1 + x^2 - x^3.$$

One of these polynomials has an inverse in R_3 and the other does not. Compute the inverse that exists and explain why the other does not exist.

3. Let $a(x) \in (\mathbb{Z}/p\mathbb{Z})[x]$, where p is a prime.

(a) Prove that $a(1) \equiv 0 \pmod{p}$ if and only if $(x - 1) \mid a(x)$ in $(\mathbb{Z}/p\mathbb{Z})[x]$.

(b) Suppose that $a(1) \equiv 0 \pmod{p}$. Prove that $a(x)$ is not invertible in R_p.

4. The guidelines for choosing NTRU public parameters (N, p, q, d) require that, in particular, $\gcd(p, q) = 1$. Prove that if $p|q$, then it is very easy for Eve to decrypt the message without knowing the private key.