The Art of Cryptography: Integral Lattices, summer 2010

PROF. DR. JOACHIM VON ZUR GATHEN, DANIEL LOEBENBERGER

1. Exercise sheet
Hand in solutions until Sunday, 18 April 2010, 23:59h.

Reminders.

- For the course we remind you of the following dates:
  - Lectures: Monday and Thursday 13:00h-14:30h **sharp**, b-it bitmax.
  - Tutorial: Monday 11:00h-12:30h **sharp**, Room t.b.a.
- A word on the exercises. They are important. Of course, you know that. In order to be admitted to the exam it is necessary that you earned at least 20% of the credits. Just as an additional motivation, you will get a bonus for the final exam if you attended the tutorial regularly and earned more than 60% or even more than 80% of the credits.

Exercise 1.1 (Discrete sets). (3 points)

Show that the set $A := \left\{\frac{1}{n} \,\middle|\, n \in \mathbb{N}_{\geq 1}\right\}$ is discrete but the set $B := A \cup \{0\}$ is not. 3

Exercise 1.2 (Discrete groups). (9 points)

Consider a subgroup L of $(\mathbb{R}^n, +)$. For $x \in \mathbb{R}^n$ denote as in the lecture the open ball around x with radius r by $\mathcal{B}(x, r)$.

(i) Show that L is discrete if and only if for some $r > 0$ we have $L \cap \mathcal{B}(0, r) = \{0\}$. 3

Let $b_1, \dots, b_m \in \mathbb{R}^n$ be vectors and let $B := [b_1|\dots|b_m] \in \mathbb{R}^{n\times m}$. As in the lecture write $\mathcal{L}(B)$ for the set of all integral linear combinations of the b_i's.

(ii) Show that the set $\mathcal{L}([1 \quad \sqrt{2}])$ is not discrete. 2

(iii) Show that the set $\mathcal{L}(B)$ is discrete if 4

(a) $b_1, \dots, b_m \in \mathbb{Q}^n$ or

(b) $b_1, \dots, b_m$ are linearly independent. Hint: Use your result from (i) and consider the region $P = \left\{\sum_{1\leq i\leq m} x_i \cdot b_i \,\middle|\, |x_i| < 1\right\}$.

Exercise 1.3 (Lattices and the gcd). (4 points)

Let $a, b \in \mathbb{N}$ and consider the lattice $L = a\mathbb{Z} + b\mathbb{Z}$ spanned by the vectors (a) and (b).

(i) Show that $L = \gcd(a, b)\mathbb{Z}$. Hint: Extended Euclidean Algorithm! 3

(ii) Conclude that a shortest vector in L has length $\gcd(a, b)$. 1

Exercise 1.4 (Transforming bases). (5+5 points)

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

2 (i) Swap the order of the columns of B,

1 (ii) Multiply a column by -1,

2 (iii) Add an integer multiple of a column to another column, i.e. set $b_i \leftarrow b_i + ab_j$ where $i \neq j$ and $a \in \mathbb{Z}$.

+5 (iv) Show that any unimodular matrix can be expressed as a sequence of these three elementary integer column transformations.

Exercise 1.5 (Tool: Groups). (0+7 points)

In this exercise you will get comfortable with the concept of a group. Always remember: Don't PANIC. Which of the following sets, together with the given operation form a group? Check for each property (Proper, Associative, Neutral, Inverse, Commutative) if it is well-defined, and if so if it is fulfilled or not:

+1 (i) $(\mathbb{Z}, -)$: The integers $\mathbb{Z}$ with subtraction.

+1 (ii) $(\mathbb{N} \setminus \{0\}, \hat{\ })$: The positive integers $\mathbb{N} \setminus \{0\}$ with exponentiation.

+1 (iii) $(\mathbb{B}, \vee)$: The set $\mathbb{B} := \{\top, \bot\}$ with operation $\vee$ (the logical OR), defined as:

$\vee$	$\top$	$\bot$
$\top$	$\top$	$\top$
$\bot$	$\top$	$\bot$

+1 (iv) $(\mathbb{B}, \oplus)$: The set $\mathbb{B}$ with operation $\oplus$ (the logical XOR), defined as:

$\oplus$	$\top$	$\bot$
$\top$	$\bot$	$\top$
$\bot$	$\top$	$\bot$

+1 (v) $(4\mathbb{Z} + 1, \cdot)$: The set $4\mathbb{Z} + 1 := \{z \in \mathbb{Z} \mid z = 1 \text{ in } \mathbb{Z}_4\}$ with multiplication.

(vi) $(\{\mathbb{Z}_7 \to \mathbb{Z}_7\}, \circ)$: The set $\{\mathbb{Z}_7 \to \mathbb{Z}_7\} := \{f : \mathbb{Z}_7 \to \mathbb{Z}_7\}$ with concatenation $\circ$ of functions. An example: If $g_1, g_2 : \mathbb{Z}_7 \to \mathbb{Z}_7$ are two functions then $(g_1 \circ g_2)(x) := g_1(g_2(x))$ for all $x \in \mathbb{Z}_7$.

+1 (vii) $(\mathcal{S}(\mathbb{Z}_{13}), \circ)$: The set $\mathcal{S}(\mathbb{Z}_{13}) := \{f : \mathbb{Z}_{13} \to \mathbb{Z}_{13} \mid f \text{ bijective}\}$ with concatenation $\circ$.

+1 (viii) $(\mathbb{Z}_3^2, \square)$: The set $\mathbb{Z}_3^2 := \{(a, b) \mid a \in \mathbb{Z}_3, b \in \mathbb{Z}_3\}$ with the following operation $\square$:

$$\square : \begin{array}{rcl} \mathbb{Z}_3^2 \times \mathbb{Z}_3^2 & \longrightarrow & \mathbb{Z}_3^2, \\ (a, b), (c, d) & \longmapsto & (ac + bd, ad + bc) \end{array}$$