École normale supérieure **2022-2023**
Département d'informatique

Introduction à la cryptologie
TD n° 6 : Elliptic Curves and Lattices.

We will use the following notation throughout.

— $\langle \vec{u}, \vec{v} \rangle$ is the standard Euclidean inner product of $\mathbb{R}^n$, that is $\langle \vec{u}, \vec{v} \rangle = \sum_{i=1}^{n} u_i v_i$.
— The Euclidean norm : $\|\vec{u}\|^2 = \langle \vec{u}, \vec{u} \rangle$.
— span() denotes the sub(vector)space generated by the vectors or the set inside the parentheses. It is the smallest subspace containing the vectors or the set inside the parentheses.
— $\mathcal{B}_r(\vec{v}) = \{\vec{w} \in \mathbb{R}^n, \|\vec{v} - \vec{w}\| < r\}$ is the open ball of $\mathbb{R}^n$ of center $\vec{v}$ and radius r.

Exercice 1 (Properties of lattices)**.** Let L be a discrete subgroup of $\mathbb{R}^n$. Show that :

1. There exists $r > 0$ s.t. for all $\vec{v} \in L$, $L \cap \mathcal{B}_r(\vec{v}) = \{\vec{v}\}$.
2. Show that any convergent sequence of L is stationary : in particular, L is closed.
3. For all $r > 0$ and $\vec{v} \in \mathbb{R}^n$, $L \cap \mathcal{B}_r(\vec{v})$ is finite.
4. L is countable.

Exercice 2 (Discreteness of subgroups)**.** Let L be a subgroup of $\mathbb{R}^n$. Show that L is discrete if and only if one of the following conditions holds :

1. 0 is isolated in L, *i.e.* there exists $r > 0$ s.t. $L \cap \mathcal{B}_r(\vec{0}) = \{\vec{0}\}$.
2. There is no injective sequence of L converging to zero.

Exercice 3 (Examples of lattices)**.** Let L be a discrete subgroup of $\mathbb{R}^n$. Show that :

1. Show that $\mathbb{Z}^n$ is a lattice.
2. Show that any subgroup of $\mathbb{Z}^n$ is a lattice.
3. Let $\vec{b}_1, \ldots, \vec{b}_d$ be vectors in $\mathbb{Z}^n$. Show that the set of all integral linear combinations $\mathcal{L}(\vec{b}_1, \ldots, \vec{b}_d) = \{\sum_{i=1}^{d} x_i \vec{b}_i, x_i \in \mathbb{Z}\}$ is a lattice.
4. Let $\vec{b}_1, \ldots, \vec{b}_d$ be linearly independent vectors in $\mathbb{R}^n$. Show that $\mathcal{L}(\vec{b}_1, \ldots, \vec{b}_d)$ is a lattice.

Exercice 4 (Duality)**.** Let L be a lattice of $\mathbb{R}^n$. Show that :

1. For any group homorphism $f : L \to \mathbb{Z}$, there exists a unique $\vec{v} \in \mathrm{span}(L)$ s.t. for all $\vec{w} \in L$, $f(\vec{w}) = \langle \vec{v}, \vec{w} \rangle$.
2. The set $L^\times$ of all $\vec{v} \in \mathrm{span}(L)$ such that for all $\vec{w} \in L$, $\langle \vec{v}, \vec{w} \rangle \in \mathbb{Z}$ is a lattice, called the *dual lattice* of L.
3. The additive group of all group homorphisms $f : L \to \mathbb{Z}$ is isomorphic to $L^\times$.

Exercice 5 (Elliptic curves)**.** Let C be a non-singular cubic curve $C : y^2 = f(x) = x^3 + ax^2 + bx + c$. We denote by $\mathcal{O} = (\inf, \inf)$ the neutral element. Show the following :

1. A point $P = (x, y) \neq \mathcal{O}$ on C has order 2 iff $y = 0$.
   Tip : The inverse of P is $(x, -y)$.
2. The curve C has exactly four points of order 1 or 2.
3. A point $P = (x, y) \neq \mathcal{O}$ on C is of order 3 iff $x(2P) = x(P)$, where $x(P)$ is the x coordinate of P.
4. A point $P = (x, y) \neq \mathcal{O}$ on C has order 3 iff x is a root of the polynomial $\psi_3(x) = 3x^4 + 4ax^3 + 6bx^2 + 12cx + 4ac - b^2$.
   Tip : Use the identity $x(2P) = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c}$.

Algorithm 1 Lagrange's reduction algorithm.

Require: a basis $(\vec{u}, \vec{v})$ of a two-rank lattice L.
Ensure: a Lagrange-reduced basis of L.

1: **if** $\|\vec{u}\| < \|\vec{v}\|$ **then**
2:     swap $\vec{u}$ and $\vec{v}$
3: **end if**
4: **repeat**
5:     $\vec{r} \leftarrow \vec{u} - q\vec{v}$ where $q = \left\lfloor \frac{\langle \vec{u}, \vec{v} \rangle}{\|\vec{v}\|^2} \right\rceil$ and $\lfloor x \rceil$ denotes an integer closest to x.
6:     $\vec{u} \leftarrow \vec{v}$
7:     $\vec{v} \leftarrow \vec{r}$
8: **until** $\|\vec{u}\| \leq \|\vec{v}\|$
9: Output $(\vec{u}, \vec{v})$.

Exercice 6 (Lagrange's Algorithm)**.** In 1773, Lagrange published a two-dimensional reduction algorithm (Algorithm 1) which is an ancestor of the LLL algorithm.

1. Consider Line 5 of Algorithm 1 : show that this choice of $q \in \mathbb{Z}$ minimizes $\|\vec{u} - q\vec{v}\|$.
2. Show that Lagrange's algorithm terminates, *i.e.* that the repeat/until loop is not infinite.
3. Consider the integer q of Step 5. Show that :
   — if $q = 0$, then this must be the last iteration of the loop.
   — if $|q| = 1$, then this must be either the first or last iteration of the loop.
4. Show that the number τ of iterations of the repeat/until loop is bounded by : $\tau = O(1 + \log B - \log \lambda_1(L))$ where B denotes the maximal Euclidean norm of the input basis vectors $\vec{u}$ and $\vec{v}$.
5. Show that when $L \subseteq \mathbb{Z}^n$, the bit-complexity of Lagrange's algorithm is polynomial in $\log B$.