Spring 2024 **Exercise 2** **L. Ducas**

Lattices and their Algorithms **Discussion on 22/02/18** **Leiden**

Exercise 1 In each of the following, decide whether the set $M \subseteq \mathbb{R}^n$ is a lattice:

i) $M = \{0\}$.

ii) Let $\alpha \in \mathbb{R}$ be irrational. $M = \{x + \alpha y : x, y \in \mathbb{Z}\}$.

iii) Let $\mathbf{v}_1, \ldots, \mathbf{v}_m \in \mathbb{Q}^n$, where $m \leq n$, and $\mathbf{B} = (\mathbf{v}_1, \ldots, \mathbf{v}_m) \in \mathbb{Q}^{n \times m}$. $M = L(\mathbf{B})$.

iv) Let $\mathbf{v}_1, \ldots, \mathbf{v}_m \in \mathbb{Q}^n$, where $m > n$. Then $M = \{x_1\mathbf{v}_1 + \ldots + x_m\mathbf{v}_m : x_1, \ldots, x_m \in \mathbb{Z}\}$.

v) Let L be a lattice and define $M = \{x \in \mathrm{Span}_{\mathbb{R}}(L) : \langle x, y \rangle \in \mathbb{Z} \ \forall \ y \in L\}$.

vi) Let $L \subseteq \mathbb{R}^n$ be a lattice and define $M = \{x \in \mathbb{R}^n : \langle x, y \rangle \in \mathbb{Z} \ \forall \ y \in L\}$.

vii) Let $\mathbf{B} \in \mathrm{GL}_n(\mathbb{R})$, and $M = L(\mathbf{B})$.

Exercise 2 Consider a prime $p \equiv 1 \mod 4$, and let $L = \{(x, y) \in \mathbb{Z}^2 : x + jy \equiv 0 \mod p\} \subset \mathbb{R}^2$, where $j \in \mathbb{Z}$ is such that $j^4 \equiv 1 \mod p$ and $j^2 \equiv -1 \mod p$. Such a j exists since 4 divides the order of $(\mathbb{Z}/p\mathbb{Z})^\times$.

i) Show that L is a lattice.

ii) Find $\det(L)$.

iii) Show that for any $\mathbf{v} \in L$, $p \mid \|\mathbf{v}\|_2^2$.

iv) Show that there exists an element $\mathbf{v} \in L$ with $\|\mathbf{v}\|_2^2 = p$.

v) Prove that if $p \equiv 3 \mod 4$ then there does not exist an $x, y \in \mathbb{Z}$ with $p = x^2 + y^2$.

Parts (iv) and (v) give Fermat's Theorem: an odd prime p can be written $p = x^2 + y^2$ for integers $x, y \in \mathbb{Z}$ if and only if $p \equiv 1 \mod 4$.

Exercise 3 Let $\mathbf{B}$ be a non-singular $n \times n$ matrix with rational coefficients. In this exercise, we show that inversion of $\mathbf{B}$ can be done in *polynomial time*. That is, the time can be bounded above by some polynomial in n and the maximum size of the input. Here, the maximum size of the input will be $\max_{b_{i,j} \in \mathbf{B}} \left(h(b_{i,j})\right)$, where $h(\cdot)$ is the *height* of a rational number: $h\left(\frac{c}{d}\right) = 2\max(\log|c|, \log|d|)$. The height is the number of *bits* required to represent the rational number.

i) Show that the Gauss-Jordan (i.e. Gaussian elimination) method of inverting an $n \times n$ matrix can be done in Cn^3 arithmetic operations, for some constant $C > 0$ (you do not need to give a value for C).

ii) Show that if α, β are rational numbers, then $h(\alpha\beta) \leq h(\alpha) + h(\beta)$, and $h(\alpha + \beta) \leq 2h(\alpha)h(\beta)$, and $h(\alpha^{-1}) = h(\alpha)$.

iii) Prove that for any $n \times n$ matrix M, $|\det(M)| \leq n!(\max_{i,j} |m_{i,j}|)^n$, and therefore if a matrix can be written in a polynomial number of bits, then so can its determinant.

iv) Show that if a matrix M can be written in polynomially many bits, then so can its inverse.

Now we need to show that during the Gauss-Jordan process, the coefficients in the matrices in question do not get too large. We will show that the intermediate matrices in the elimination are quotients of rational numbers of polynomially-bounded height.

Let $\mathbf{B}^{(k)}$ be the matrix $\mathbf{B}$ after k iterations of the main loop (i.e. when the first k rows and columns make a $k \times k$ identity matrix. We will assume without loss of generality that the pivot is on the main diagonal. Let $D^{(k)}$ be the submatrix of the first k rows and columns of $\mathbf{B}$, and let $D^{(k)}_{i,j}$ (for $i, j \geq k$) be the submatrix of $\mathbf{B}$ made up of the rows $1, \ldots, k, i$ and the columns $1, \ldots, k, j$.

v) Show that

$$\mathbf{B}^{(k)}_{i,j} = \frac{\det(D^{(k)}_{i,j})}{\det(D^{(k)})}.$$

vi) Explain why all the matrices involved in the gaussian elimination and therefore the inversion have height bounded by some polynomial in terms of the original heights.