EXERCISES

The exercises 1 to 6 in this sheet are the most interesting ones and should be prioritized. Exercises 7 to 10 are more advanced, and are targeted for students who already have some knowledge about lattices, and want to learn more (exercise 10 is available only in the online version: `https://apelletm.pages.math.cnrs.fr/page-perso/documents/enseignement/CIMPA_school_Pondicherry/exercises.pdf`).

Exercises 1 to 4, and advanced exercises 7, 8, 10 can be done after the first lecture. Exercise 5 can be done after the second lecture (if we go fast enough), exercise 6 can be done after the third lecture, and exercise 9 can be done after the fourth lecture.

1 Lattice bases ($\star$)

The objective of this exercise is to prove a bunch of properties regarding bases of lattices. Throughout this exercise, the matrix B (or the matrices B_1, B_2) are invertible matrices in $\mathrm{GL}_n(\mathbb{R})$ for some dimension $n > 0$. Recall that we write $\mathcal{L}(B)$ for the lattice spanned by the columns of the matrix B.

1. Let $B_1, B_2 \in \mathrm{GL}_n(\mathbb{R})$. Show that $\mathcal{L}(B_1) = \mathcal{L}(B_2)$ if and only if $B_1 = B_2 \cdot U$ for some $U \in \mathbb{Z}^{n \times n}$ such that $\det(U) = \pm 1$. Such a matrix U is called unimodular. It is an invertible integer matrix whose inverse is also an integer matrix.

2. Let B_1 and B_2 be two bases of the same lattice $\mathcal{L}$. Prove that $|\det(B_1)| = |\det(B_2)|$.
   This shows that the quantity $|\det(B)|$ does not depend on the choice of the basis B of $\mathcal{L}$, but only on the lattice $\mathcal{L}$. It is usually called the volume or the determinant of the lattice $\mathcal{L}$, and written $\mathrm{vol}(\mathcal{L})$ or $\det(\mathcal{L})$.

3. Let $\mathcal{L}_1$ and $\mathcal{L}_2$ be two lattices of rank n. Show that if $\mathcal{L}_1 \subseteq \mathcal{L}_2$, then $\det(\mathcal{L}_1) = k \cdot \det(\mathcal{L}_2)$ for some integer $k > 0$. This integer k is called the index of $\mathcal{L}_1$ inside $\mathcal{L}_2$ and is written $[\mathcal{L}_2 : \mathcal{L}_1]$.

   The determinant of a lattice is an important quantity, mostly useful in cryptography thanks to Minkowski's first theorem. This theorem states that in any lattice $\mathcal{L}$ of dimension n, there exists a non-zero vector $v \in \mathcal{L}$ such that $\|v\| \leq \sqrt{n} \cdot \det(\mathcal{L})^{1/n}$.

4. Show that the upper bound in Minkowski's first theorem can be quite loose for some lattices: construct a lattice with $\det(\mathcal{L}) = 1$ and which contains a non-zero vector v whose euclidean norm is arbitrarily close to 0.

   The objective of the next questions is to observe that when dealing with lattices, a maximal set of independent vectors is not always a basis, and a minimal set of generating vectors is also not always a basis (which differs from what we are used to in vector spaces).

5. Exhibit a family of n linearly independent vectors in $\mathbb{Z}^n$ which do not form a $\mathbb{Z}$-basis of $\mathbb{Z}^n$.

6. Exhibit a family of $n+1$ vectors generating $\mathbb{Z}^n$ such that it is not possible to remove any vector from this set to obtain a $\mathbb{Z}$-basis of $\mathbb{Z}^n$.

7. Compute a basis for the lattice generated by $c_1 = (2\pi, 4)^T$, $c_2 = (0, 3)^T$ and $c_3 = (4\pi, 4)^T$. Same question for $c_1 = (1, 0)^T$, $c_2 = (1, 1)^T$ and $c_3 = (1, \pi)^T$. ($\star\star$)
   (Hint: the question might be lying to you. In this case, show what is wrong in the question. :)).

2 HNF basis $(\star\star)$

In this exercise, we will see how to compute a special basis of a lattice $\mathcal{L}$, called the HNF basis of $\mathcal{L}$. The main advantage of this basis is that it can be computed in polynomial time from any *basis of $\mathcal{L}$, hence, it is a "worst possible" basis: revealing this basis does not leak more information on $\mathcal{L}$ than what any other basis would leak.*

The algorithm to compute the HNF basis is very similar to the way one would use Gaussian elimination to compute the echelon form of matrices over a field. The main difference is that since we are only allowed to perform integer linear combinations over the vectors of our basis, we cannot multiply by the inverse of a coefficient, in order to annihilate the other coefficients on the same row.

1. Let's review Gaussian elimination a little. Run Gaussian elimination (over $\mathbb{R}$) on the columns of the matrix $M = \begin{pmatrix} 2 & 3 \\ 3 & 4 \end{pmatrix}$ in order to obtain a triangular matrix of the form $\begin{pmatrix} * & 0 \\ * & * \end{pmatrix}$. (Here, running Gaussian elimination on the columns means that you are only allowed to perform operations on the columns of the matrix. Said differently, you can only multiply M by invertible matrices on the right).

2. In the previous question, the operations we performed on the columns were not integer. We now want to focus on integer operations on the columns of M. Show that there exists an integer matrix U with determinant 1 such that $M \cdot U = \begin{pmatrix} 1 & * \\ * & * \end{pmatrix}$.

3. More generally, show that for any matrix $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ there is a unimodular matrix U such that $M \cdot U = \begin{pmatrix} \gcd(a,b) & * \\ * & * \end{pmatrix}$. $(\star\star)$

4. Using the previous question, show that for any matrix $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ there is a unimodular matrix U such that $M \cdot U = \begin{pmatrix} \gcd(a,b) & 0 \\ * & * \end{pmatrix}$.

5. Compute a matrix U as in the previous question for $M = \begin{pmatrix} 9 & 2 \\ 3 & 1 \end{pmatrix}$.

6. Let $M_1 = \begin{pmatrix} 2 & 1 & 0 \\ 8 & 1 & 4 \\ 0 & 1 & 7 \end{pmatrix}$. Generalize the algorithm from the previous questions to compute a matrix M_2 such that $M_2 = M_1 \cdot U$ for some unimodular matrix U and M_2 is of the form $M_2 = \begin{pmatrix} * & 0 & 0 \\ * & * & 0 \\ * & * & * \end{pmatrix}$.

7. Let $\mathcal{L}$ be a lattice of dimension n. Show that there is a unique basis B of $\mathcal{L}$ such that $b_{i,j} = 0$ when $j > i$, $b_{i,i} > 0$ and $0 \leq b_{i,j} < b_{i,i}$ for $j < i$. This is the basis which is called the Hermite normal form (HNF) basis of $\mathcal{L}$. $(\star\star)$

3 LWE and SIS lattices $(\star\star)$

Let q ,$m \geq r > 0$ be integers and $A \in \mathbb{Z}_q^{m \times r}$. Recall that the SIS lattice associated to A is defined by $\Lambda^{\perp}(A) := \{x \in \mathbb{Z}^m \,|\, x^T \cdot A = 0 \bmod q\}$. Recall similarly that the LWE lattice associated to A is $\Lambda(A) := \{x \in \mathbb{Z}^m \,|\, \exists s \in \mathbb{Z}^n \text{ s.t. } As = x \bmod q\}$.

1. Show that $\Lambda(A)$ is generated by the columns of A and the m vectors $q \cdot e_i$ (with $1 \leq i \leq m$), where e_i is the vector with a 1 at the i-th position and 0's everywhere else.

2. Assume that q is prime. Using the previous question, exhibit a set of generating vectors for the lattice $\Lambda^{\perp}(A)$. (Hint: you might want to show that $\Lambda^{\perp}(A) = \Lambda(B)$ for some well chosen matrix B).

3. Assume again that q is prime. Assume also that the rank of A modulo q is r (i.e., the r column vectors of A are linearly independent modulo q). Show that up to permuting the rows of A (i.e., permuting the coefficients of the vectors in $\Lambda(A)$), there exists a basis of $\Lambda(A)$ of the form $\begin{pmatrix} I_r & 0_{n\times(m-r)} \\ A' & q\cdot I_{m-r}\end{pmatrix}$, for some integer matrix $A' \in \mathbb{Z}^{(m-r)\times r}$. $(\star\star)$

   Similarly, show that up to permuting the rows of A, there exists a basis of $\Lambda^{\perp}(A)$ of the form $\begin{pmatrix} I_{m-r} & 0_{(m-r)\times r} \\ B' & q\cdot I_r\end{pmatrix}$, for some integer matrix $B' \in \mathbb{Z}^{r\times(m-r)}$.

4. Assuming that q is prime and that A has rank n modulo q, show that the SIS lattice $\Lambda^{\perp}(A)$ contains a non-zero vector of norm $\leq \sqrt{m}\cdot q^{r/m}$ and that the LWE lattice $\Lambda(A)$ contains a non-zero vector of norm $\leq \sqrt{m}\cdot q^{1-r/m}$.

4 Solving the closest vector problem $(\star)$

Babai's round-off algorithm solves the approximate closest vector problem as follows. Given as input a basis $(b_i)_{1\leq i\leq n}$ of the lattice $\mathcal{L}$ (of dimension n) and a target t, the algorithm writes $t = \sum_{i=1}^{n} t_i b_i$ with $t_i \in \mathbb{R}$ and output the vector $s = \sum_i \lceil t_i \rfloor b_i$.

1. Show that Babai's round-off algorithm finds a point $s \in \mathcal{L}$ such that $\|t - s\| \leq 1/2 \cdot n \cdot \max_i \|b_i\|$.

5 LWE is a BDD problem $(\star\star)$

In this exercise, we will fix an LWE instance (A, b), with a prime modulus q, with $A \in (\mathbb{Z}/q\mathbb{Z})^{m\times n}$ (where $m \geq n > 0$ are integers), and with $b = A\cdot s + e \bmod q$ for some secret $s \in (\mathbb{Z}/q\mathbb{Z})^n$ and $e \in \mathbb{Z}^m$ satisfying $\|e\| \leq B$ (for some bound $B > 0$). We will show that, under some conditions on the parameters B, q, m and n, it is possible to recover the secret s by solving a BDD instance in the lattice $L := \Lambda(A)$ from Exercise 3 (hence the name "LWE lattice").[1]

1. Let $t \in \mathbb{Z}^m$ be any lift of b in $\mathbb{Z}^m$ (i.e., $t \bmod q = b$). Show that there exists a vector $v_0 \in L$ such that $\|v_0 - t\|_2 \leq B$. Show also that if one recovers v_0, then one can recover the secret s of the LWE instance.

   To prove that s can be recovered by solving a BDD instance in L, is then "only" remains to prove that $B \leq 1/\gamma \cdot \lambda_1(L)$ for some $\gamma > 2$ (this is actually the hardest part of the proof): this will prove that t is a γ-BDD instance in L, with closest vector v_0, and so solving BDD in L with target t will recover v_0 and hence we can obtain the secret s.

   In Exercise 3, we have shown that $\lambda_1(L) \leq \sqrt{m}\cdot q^{1-n/m}$ (when A has rank n). The next questions will be devoted to the proof that this bound is close to optimal (with overwhelming probability over the random choice of A). Recall that we asked that q is prime.

2. Let $\rho \in (0, q)$ be some bound, and write $\mathcal{B}_\rho$ the m-dimensional euclidean ball centered in 0 and of radius ρ. Show that
$$\Pr_A\big(\lambda_1(\Lambda(A)) \leq \rho\big) \leq \sum_{\substack{y\in\mathcal{B}_\rho\cap\mathbb{Z}^m \\ x\in(\mathbb{Z}/q\mathbb{Z})^n\setminus\{0\}}} \Pr_A\big(Ax = y \bmod q\big),$$
   where A is sampled uniformly at random in $(\mathbb{Z}/q\mathbb{Z})^{m\times n}$.
   (Hint: you may want to use a union bound)

[1] More precisely, this will be possible with overwhelming probability over the random choice of A.

3. Show that for any $x \in (\mathbb{Z}/q\mathbb{Z})^n \setminus \{0\}$ and $y \in \mathbb{Z}^m$ fixed, it holds that $\Pr_A\big(Ax = y \bmod q\big) = q^{-m}$.
(Hint: this is where you use that q is prime)

4. Conclude that
$$\Pr_A\big(\lambda_1(\Lambda(A)) \leq \rho\big) \leq |\mathcal{B}_\rho \cap \mathbb{Z}^m| \cdot q^{n-m}.$$

5. Show that $|\mathcal{B}_\rho \cap \mathbb{Z}^m| \leq (2\rho + 1)^m$.
(Hint: the ball $\mathcal{B}_\rho$ is contained in $\mathcal{B}_\rho^\infty := \{z \in \mathbb{R}^m \mid \|z\|_\infty \leq \rho\}$).

6. Assume that m, n and q satisfy $q^{1-n/m} \geq 4$ (e.g., if $m \geq 2n$ and $q \geq 16$). Conclude that
$$\Pr_A\Big(\lambda_1(\Lambda(A)) \leq \frac{q^{1-n/m}}{4} - 1\Big) \leq 2^{-m}.$$

__Remark:__ there is a gap of the order of $O(\sqrt{m})$ between the upper bound on $\lambda_1(L)$ from exercise 3 and the lower bound we just proved. This gap can be reduced by being more careful when upper bounding the quantity $|\mathcal{B}_\rho \cap \mathbb{Z}^m|$.

7. Conclude that if $q^{1-n/m} \geq 16 \cdot B$ (e.g., if $q \geq 2^{16}$, $B = \sqrt{q}$ and $m \geq 4n$), then with probability at least $1 - 2^{-m}$ over the choice of A, it is possible to solve the LWE instance (A, b) by solving a γ-BDD instance in the lattice $L := \Lambda(A)$ with $\gamma = \frac{q^{1-n/m}}{8B}$.

6 Hashing with SIS ($\star\star$)

The objective of this exercise is to study a construction of a collision resistant hash function based on SIS.

Let F be a family of functions from a set X to a set Y (which we will call "hash functions", but really they are just functions) and let D_F be a distribution over this set of functions.

Definition: The advantage of a probabilistic polynomial time (p.p.t.) algorithm $\mathcal{A}$ against the collision resistance of the family of hash functions (F, D_F) is defined as

$$\mathrm{Adv}_F(\mathcal{A}) := \Pr_{f \leftarrow D_F}\Big(\mathcal{A}(f) = (x, x') \in X^2 \text{ with } f(x) = f(x') \text{ and } x \neq x'\Big),$$

where the probability is taken over the random choice of f and the internal randomness of $\mathcal{A}$.

Recall also the SIS problem, which is as follows.

Definition: Let q, m, n be integers with $m \geq n$ and $B > 0$ be some bound. The advantage of a p.p.t. adversary $\mathcal{A}$ against the $\mathrm{SIS}_{q,n,m,B}$ problem is defined as

$$\mathrm{Adv}_{\mathrm{SIS}}(\mathcal{A}) := \Pr_{A \leftarrow \mathcal{U}(\mathbb{Z}_q^{m\times n})}\Big(\mathcal{A}(A) = x \in \mathbb{Z}^m \text{ with } x^T \cdot A = 0 \bmod q \text{ and } 0 < \|x\| \leq B\Big),$$

where the probability is over the random choice of A and the internal randomness of $\mathcal{A}$.

We will consider the following family F of functions, from $\{0,1\}^m$ to $\mathbb{Z}_q^n$. The functions of F are indexed by a matrix $A \in \mathbb{Z}_q^{m\times n}$ and are defined as

$$\begin{aligned} f_A : \{0,1\}^m &\to \mathbb{Z}_q^n \\ x &\mapsto x^T \cdot A \end{aligned}$$

The distribution D_F over F is obtained by sampling $A \in \mathbb{Z}_q^{m\times n}$ uniformly at random and outputting f_A.

1. Assume that $B \geq \sqrt{m}$. Show that if there exists an adversary $\mathcal{A}$ against the collision resistance of (F, D_F) with advantage $\varepsilon > 0$, then there exists an adversary $\mathcal{B}$ against the $\mathrm{SIS}_{q,n,m,B}$ problem with advantage $\geq \varepsilon$. This proves that (F, D_F) is a family of collision resistant functions, provided that the SIS problem is hard.

7 QR-factorization ($\star\star$)

The objective of this exercise is to define the QR factorization of a matrix and prove useful properties of this decomposition, which will be used in exercise 8.

In this exercise, we admit the following result:
Lemma: There exists a polynomial time algorithm that takes as input any matrix $B \in \mathrm{GL}_n(\mathbb{R})$, and outputs two matrices $Q, R \in \mathrm{GL}_n(\mathbb{R})$ such that

- $B = Q \cdot R$;
- Q is orthonormal, i.e., $Q^{-1} = Q^T$;
- R is upper triangular and has non negative diagonal coefficients.

The pair (Q, R) is called a *QR-factorization* of the matrix B. We will see below that it is unique. In the rest of this exercise sheet, it might be useful to remember that an orthonormal matrix Q has the following properties:

- all the rows and columns of the matrix Q have euclidean norm 1;
- the rows (resp. columns) of Q are orthogonal;
- for any vector v it holds that $\|Qv\| = \|v\|$.

1. Let $B \in \mathrm{GL}_n(\mathbb{R})$. Show that the QR-factorization of B is unique (i.e., show that if $B = QR = Q'R'$ with Q, Q' orthonormal and R, R' upper triangular with positive diagonal coefficients, then $Q = Q'$ and $R = R'$) ($\star\star$)

   We say that a basis B of a lattice is *size-reduced* if its QR-factorization (Q, R) satisfies the following property: for all $j \geq i$, $|r_{i,j}| \leq r_{i,i}$ (remember that $r_{i,i} > 0$). In other words, the diagonal coefficients of R are the largest coefficients of their rows (in absolute value).

2. Let $B \in \mathrm{GL}_n(\mathbb{R})$ and (Q, R) be its QR-factorization. Show that there exists an efficiently computable unimodular matrix U such that $B \cdot U$ is size-reduced and has QR-factorization (Q, R') with $r'_{i,i} = r_{i,i}$ for all i. ($\star\star$)
   (You do not have to describe the algorithm very properly, getting the idea is sufficient.)

   In the rest of this exercise sheet, we call `size_reduce` the polynomial time algorithm that takes as input a matrix B and returns a sized-reduced matrix $B' := B \cdot U$ as in the above question, i.e., with $r_{i,i} = r'_{i,i}$ and $\mathcal{L}(B') = \mathcal{L}(B)$.

3. Let $B \in \mathrm{GL}_n(\mathbb{R})$ and (Q, R) be its QR-factorization. Let b_j be the column vectors of B. Show that $\max_j r_{j,j} \leq \max_j \|b_j\|$. If B is size-reduced, show that we also have the inequality $\max_j \|b_j\| \leq \sqrt{n} \cdot \max_j r_{j,j}$ (in other words, the size of the diagonal coefficients of R are a relatively good approximation of the size of the vectors of B when B is size-reduced). ($\star\star$)
   (Hint 1: observe that $b_j = Q \cdot r_j$ with r_j the j-th column of R)
   (Hint 2: remember the property that $\|Qv\| = \|v\|$ for any vector v)

8 Computing a short basis from a short generating set ($\star\star$)

The objective of this exercise is to show that given an arbitrary basis B of a lattice $\mathcal{L}$ and a set of n linearly independent (short) vectors S in $\mathcal{L}$, then one can create a new basis $\tilde{B}$ of $\mathcal{L}$ with vectors of length not much larger than the ones of S. In other words, finding short linearly independent vectors in $\mathcal{L}$ is sufficient to obtain a short basis of $\mathcal{L}$.
This exercise uses results from exercise 7.

1. Let B be a basis of a lattice $\mathcal{L}$ and $S \in \mathrm{GL}_n(\mathbb{R})$ be a set of n linearly independent vectors in $\mathcal{L}$. Make sure you remember why there exists an integer matrix X such that $S = B \cdot X$. Is X unimodular?

2. Let Y be the HNF basis of the lattice $\mathcal{L}(X^T)$ and let U be the unimodular matrix such that $X^T = Y \cdot U$. Verify that $B' = B \cdot U^T$ is a basis of $\mathcal{L}$ and that $S = B' \cdot Y^T$.

3. Let $S = Q_S \cdot R_S$ be the QR factorization of the matrix S and $B' = Q_B \cdot R_B$ be the one of B'. Show that $Q_S = Q_B$ and that $R_S = R_B \cdot Y^T$.
   (Hint: use the unicity of the QR-factorization that you proved in exercise 7)

   Let $\tilde{B} = \texttt{size\_reduce}(B')$. Our objective is to show that $\tilde{B}$ is a basis of $\mathcal{L}(B)$ which has vectors almost as short as the ones of S. (You can check from the way we defined it that $\tilde{B}$ can be computed in polynomial time from B and S).

4. Let $(\tilde{Q}, \tilde{R})$ be the QR-factorization of $\tilde{B}$. Show that $\max_j \tilde{r}_{j,j} \leq \max_j \|s_j\|$.
   (Hint 1: remember from question 2 in exercise 7 that $\tilde{r}_{j,j} = (R_B)_{j,j}$ when we use the size-reduction algorithm)
   (Hint 2: observe that the triangular matrix Y is integral and has positive diagonal coefficients, hence its diagonal coefficients are ≥ 1.)

5. Conclude that $\tilde{B}$ is a new basis of $\mathcal{L}$ with columns vectors $\tilde{b}_j$ satisfying $\max_j \|\tilde{b}_j\| \leq \sqrt{n} \cdot \max_j \|s_j\|$. In other words, the vectors of $\tilde{B}$ are almost as short as the linearly independent vectors from S.
   (Hint: this question consists mainly in combining what you have seen in this exercise and in exercise 7.)

9 Ideal lattices (⋆⋆)

Let R be the ring $\mathbb{Z}[X]/(X^d+1)$ where d is a power-of-two (so that X^d+1 is irreducible, and $K = \mathbb{Q}[X]/(X^d+1)$ is a field). An ideal in R is a subset I of R such that for all $x, y \in I$, the sum $x+y$ is also in I, and for any $x \in I$ and $\alpha \in R$, the product $x \cdot \alpha$ is in I.

1. Recall that the coefficient embedding

$$\Sigma : K \to \mathbb{Q}^d$$
$$a = \sum_{i=0}^{d-1} a_i X^i \mapsto (a_0, \cdots, a_{d-1})$$

   maps elements of K to vectors in $\mathbb{Q}^d$ (and elements of R to vectors in $\mathbb{Z}^d$). Show that if $a \in K$ is non-zero, then the d vectors $\Sigma(a \cdot X^i)$ for $i = 0$ to $d-1$ are linearly independent. (⋆⋆)
   (Hint 1: assume you have a $\mathbb{Q}$-linear relation $\sum_{i=0}^{d-1} y_i \cdot \Sigma(a \cdot X^i) = 0$ with the y_i's in $\mathbb{Q}$ and not all zero and try to obtain a contradiction.)
   (Hint 2: Σ is a $\mathbb{Q}$-morphism and is a bijection between K and $\mathbb{Q}^d$. Also, K is a field so all non-zero elements are invertible.)

   Remember that during the lecture, we have seen that a principal ideal is an ideal of rank d once embedded into $\mathbb{Q}^d$ via the canonical embedding. The objective of the next question is to show that this is true for all ideals (not only the principal ideals).

2. Show that for any non-zero ideal I, the set $\Sigma(I)$ is a lattice of rank d in $\mathbb{R}^d$. (⋆⋆)

3. Let I be an ideal of R and $s \in I$ be a non-zero element of I. Show that one can efficiently construct d elements s_i (for $1 \leq i \leq d$) in I such that the vectors $\Sigma(s_i)$ are linearly independent and have euclidean norm $\|\Sigma(s_i)\| = \|\Sigma(s)\|$. (⋆⋆)

4. Conclude that in an ideal lattice $\Sigma(I)$, finding one short vector $v \in \Sigma(I)$ is sufficient to construct a short basis B of $\Sigma(I)$ where all vectors b_i of B have euclidean norm at most $\sqrt{d} \cdot \|v\|$.
   (Hint: you may want to use the result of question 5 from exercise 8)

   Note: in this exercise, we used special properties of the ring R. In more generality, from one short vector $v \in \Sigma(I)$, one can construct a short basis with vectors of norm at most $\gamma_K \cdot \|v\|$ for some γ_K depending on the number fields K. For most number fields K used in cryptography, this quantity γ_K is small (and so the intuition that "one short vector in an ideal is sufficient to have a short basis" is true).

10 Lagrange-Gauss algorithm $(\star\star\star)$

Recall the Lagrange-Gauss algorithm: given as input a basis (b_1, b_2) of a lattice in $\mathbb{R}^2$, the algorithm finds $x \in \mathbb{Z}$ that minimizes $\|b_2 - xb_1\|$ and replaces b_2 by $b_2 - xb_1$ (finding x efficiently is done by computing the QR factorization of the basis B, this step is not important for this exercise). The algorithm then switches b_1 and b_2 and starts again. The algorithm stops when no progress is made for two consecutive iterations (which means that we cannot reduce b_1 by b_2 nor b_2 by b_1 anymore).

1. Let b_1 and b_2 be two non-zero vectors in $\mathbb{R}^2$. Show that if $\|b_1\| \leq \|b_1 + b_2\|$, then for any $\alpha \in (1, +\infty)$ it holds that $\|b_1 + b_2\| \leq \|b_1 + \alpha b_2\|$. $(\star\star)$

2. Show that if the Lagrange-Gauss algorithm terminates, then either b_1 or b_2 is a shortest non-zero vector of $\mathcal{L}$. (Hint: you may want to consider a shortest non-zero vector $s = x_1 b_1 + x_2 b_2$ and write it as $s = x_1 \cdot (b_1 + \alpha b_2)$ with $\alpha = x_2/x_1$ if $x_1 \neq 0$.) $(\star\star\star)$