Exercise 1 The purpose of this exercise is to support the claim made in Lecture 3 Section 2, namely that not knowing $\lambda_1(L)$ does not significantly affect the dificulty of solving SVP, at least when using the enumeration algorithm that we have considered. The formal statement takes the form of a reduction. Namely, we are given an algorithm $\mathcal{A}(r)$ as an oracle that solves SVP only when $r \geq \lambda_1(L)$, otherwise it returns an error symbol $\perp$. This algorithm is assumed to run in time at most $t(r) = a + b \cdot r^n$ for some positive constants a, b. We also assume that a lower-bound on $\lambda_1(L)$, and we denote it as r_0. We then construct the following algorithm which has oracle access to $\mathcal{A}$.

Algorithm 1: Solving SVP when $\lambda_1(L)$ is unknown.

Input : An oracle $\mathcal{A}$ as given above, a lower-bound r_0 on $\lambda_1(L)$.
Output: A shortest non-zero vector of L.

```
r ← r_0
for i = 0 to ∞ do
    v = A(r)
    if v ≠ ⊥ then
        return v
    end
    r ← r · (1 + 1/n)
end
```

You can verify that the algorithm is correct when it terminates.

i) Determine the number of loop iterations of i after which the algorithm terminates.

ii) Prove that its running time is bounded by $\left\lceil \frac{\log(\lambda_1^{(2)}(L)/r_0)}{\log(1+1/n)} \right\rceil a + e^2 \cdot (n+1) \cdot b \cdot \lambda_1^{(2)}(L)^n$.

iii) Given a *rational* basis $\mathbf{B} \in \mathbb{Q}^{n \times n}$ as input, what is the smallest positive integer f such that $f \cdot L \subset \mathbb{Z}^n$? Prove that $\log f$ is polynomial in the bitsize of $\mathbf{B}$.

iv) Show that $1/f \leq \lambda_1^{(2)}(L)$. (Hint: What is $\lambda_1^{(2)}(\mathbb{Z}^n)$?)

v) Also argue that $\log \lambda_1^{(2)}(L)$ is polynomial in the bitsize of $\mathbf{B}$.

vi) At which step is our argument specific to the Euclidean norm? Is it also valid for any ℓ_p norm?

vii) How would you adjust the above analysis to arbitrary norm? (Hint: Recall that in finite dimensional vector spaces, "all norms are equivalent". What does that mean formally?)

Exercise 2 The purpose of this exercise is to establish an alternative lower bound on the complexity of solving SVP in the Euclidean norm using FinckePohstEnum when $\mathbf{t} = 0$. This bound involves the minimal distance $\lambda_1(L)$ rather than the covering radius $\mu(L)$.

i) Prove that for any lattice L of dimension n, $|r\mathfrak{B} \cap L| \leq \left(1 + \frac{2r}{\lambda_1(L)}\right)^n$.

ii) Prove that for any lattice L with basis $\mathbf{B}$, $\lambda_1(L) \geq \min_i \|\mathbf{b}_i^\star\|_2$ (Hint: Consider the tiling $\mathcal{P}(\mathbf{B}^\star)$, and argue that it would not be packing otherwise.)

iii) Prove that the enumeration tree at level i contains at most $\left(1 + \frac{2r}{\min_{j \geq i} \|\mathbf{b}_j^\star\|}\right)^i$ points.

iv) Describe an algorithm that, given a basis $\mathbf{B}$ of L, solves ExactSVP in time at most $\left(1 + \frac{2\lambda_1(L)}{\min_i \|\mathbf{b}_i^\star\|_2}\right)^n$, up to some polynomial factor. (Hint: You don't have to re-write it all down. You can and should express it as a combination of algorithms described in the lecture notes and this exercise sheet.)

Exercise 3 As hinted in the course, there is also a depth-first version of Fincke-Pohst enumeration that is preferable as it does not require to store a large set of intermediate solutions in the enumeration tree. It is given as Algorithm 2. Note that the recursion is reversed compared to the breadth-first version: at each level of the recursion, we are considering the sublattice generated by $\mathbf{b}_1, \ldots, \mathbf{b}_{n-1}$, rather than the projected lattice $\pi_{\mathbf{b}_1}(L)$. Prove the correctness of Algorithm 2.

Algorithm 2: $\mathsf{DepthFirstFinckePohst}(\mathbf{B}, r, \mathbf{t})$: Depth-First Fincke-Pohst Enumeration Algorithm

Input : A basis $\mathbf{B} = (\mathbf{b}_1, \ldots \mathbf{b}_n) \in \mathbb{Q}^{n \times n}$ of a full rank lattice Λ, a target $\mathbf{t}$, and a radius $r \geq 0$.

Output: The closest point $\mathbf{c}$ to $\mathbf{t}$ in $L \cap (\mathbf{t} + r\mathfrak{B}_2)$ if such a point exists.

```
a ← ⟨t, b*_n⟩ / ||b*_n||
Z ← {z ∈ ℤ | (a − z||b*_n||)^2 ≤ r^2};
if n = 1 then
    return argmin_{v ∈ Z·b_n} ||v − t|| ;        // Returns error symbol ⊥ if the set is empty.
end
c ← ⊥
B' ← (b_1, ..., b_{n−1})
π ← π_{B'} ;                                   // Orthogonal projection onto, not "orthogonally to"
for z ∈ Z do
    v ← z b_n + DepthFirstFinckePohst(B', sqrt(r^2 − (a − z||b*_n||)^2), π(t − z b_n))
    if c = ⊥ or ||v − t|| < ||c − t|| then
        c ← v
    end
end
return c
```

Exercise 4 Your long time friend, currently studying chemistry, is using mass spectrometry to measure the average mass of some molecules. From context, he knows a list of atoms plausibly present in the molecule, and from the periodic table of elements, he knows the masses $(m_i)_{i \in n} > 0$ of all these atoms. Therefore, he can measure a total mass $M = \sum_{i=1}^{n} z_i m_i + e$ for some non-negative integers z_i and some measurement error e guaranteed to be in some known interval $e \in [-\varepsilon, \varepsilon]$. And he desperately wants to determine the solution(s) $\mathbf{z} \in \mathbb{Z}^n$.

i) Consider the lattice $\mathbb{Z}^n$, and construct a bounded convex set $S \subset \mathbb{R}^n$ such that $\mathbb{Z}^n \cap S$ contains the desired solutions. (Hint: Your friend just gave you $n+2$ linear inequalities.)

ii) Show that S is included in a Euclidean ball of radius $(M + \varepsilon)/\min_i m_i$. (Hint: $\|\mathbf{x}\|_2 \leq \|\mathbf{x}\|_1$.)

iii) Propose an algorithm that given $M, \varepsilon, (m_i)_{i=1}^n$ determines the set of possible solution(s).

To be continued in future exercise sheets. Spoiler: the algorithm in Exercise 4 is terribly slow.