Exercise 1 Let L be a lattice for which $\lambda_2(L)/\lambda_1(L) \geq (\gamma_2 + \varepsilon)^n$. Show that an instance of ε-LLL reduction on a basis for L will find a shortest vector.

Exercise 2 Let q, n, m be integers with $n < m$, q prime and m even. Let $\gamma > \frac{\sqrt{2\pi e}}{q^{n/m} \sqrt[n]{\pi n}}$. Here we prove that for a lattice $L := \Lambda_q^{\perp}(\mathbf{A})$ where $\mathbf{A}$ is a random matrix $\mathbf{A} \leftarrow \mathcal{U}(\mathbb{Z}_q^{n\times m})$, it holds except with probability at most γ^{-n} that:

$$\lambda_1^{(2)}(L) > \frac{q^{n/m}\gamma \sqrt[n]{\pi n}\sqrt{n}}{\sqrt{2\pi e}} - \frac{\sqrt{n}}{2}.$$

The proof is the same strategy as that of Lemma 6, except with different analysis of the number of elements of $\mathbb{Z}^m$ with norm less than β. Use, without proof, that for even $m = 2k$, the volume of the Euclidean m-ball of radius 1 is $\frac{(\pi e)^k}{k^k\sqrt{2\pi k}}(1 + o(1))$, where the little-oh is with respect to rising k.

i) Show that, when $\beta > \sqrt{m}/2$, we have

$$|\{\mathbf{x} \in \mathbb{Z}^m : \|\mathbf{x}\|_2 \leq \beta\}| \leq \frac{1}{\sqrt{2\pi k}} \left((\beta + \sqrt{m}/2) \left(\sqrt{\frac{2\pi e}{m}} \right) \right)^m (1 + o(1)).$$

We once again have that for a given non-zero $\mathbf{x} \in \mathbb{Z}^m$,

$$\mathbb{P}_{\mathbf{A}}\left[\mathbf{A}\mathbf{x} = 0 \mod q\right] = q^{-n}.$$

ii) Following the strategy from Lemma 5, prove that $\lambda_1^{(2)}(L) \geq \frac{(q/\gamma)^{n/m} \sqrt[2m]{\pi m}\sqrt{m}}{\sqrt{2\pi e}} - \frac{\sqrt{m}}{2}$ except with probability γ^{-n}.

Exercise 3 This exercise is about reductions to and from $\mathrm{SIS}_{n,m,q,\beta}$.

i) Give a reduction from $\mathrm{SIS}_{n,m',q,\beta}$ to $\mathrm{SIS}_{n,m,q,\beta}$ for integers $m' < m$. That is, show how to use an oracle that solves $\mathrm{SIS}_{n,m,q,\beta}$ to solve $\mathrm{SIS}_{n,m',q,\beta}$.

ii) Recall from Section 2.2 that for a random q-ary lattice L, $\lambda_1(L) \approx q^{n/m}$. This means if $\beta \geq (\gamma_2 + \varepsilon)^m \cdot q^{n/m}$, the problem can be solved by running ε-LLL on the lattice L. Find the optimal m' to use in part i).

Exercise 4 The Merkle-Damgård (MD) construction we saw in the lecture was for an input of length lb, which is a multiple of the blocksize b. Consider the following MD construction for arbitrary length input.

As before, let $f : \mathcal{K} \times \{0,1\}^m \to \{0,1\}^n$ with $m > n$ be any function. Let $b = m - n > 0$. For a message $\mu \in \mathcal{M}$ of length r, let $\mu' = (\mu|r|0^s)$, where s is the smallest integer such that μ' has length that is a multiple of b. Such a string of 0's is called *padding*. Then let $\ell = \mathrm{length}(\mu')/b$, and define

$$\begin{aligned} f_{MD} &: \mathcal{K} \times \{0,1\}^{\ell\cdot b} \to \{0,1\}^n \\ & f_{MD}(\mu') = f_k(\cdots f_k(f_k(f_k(0^n|\mu'_1)|\mu'_2)|\mu'_3)\cdots)|\mu'_\ell), \end{aligned}$$

where $\mu' = (\mu'_1 \ldots \mu'_\ell)$

i) Show that if f is collision resistant, then so too is f_{MD}.

ii) Can you think of a reason why we also include the message length in the message that is to be hashed?

Exercise 5 (Generic Collision Attack) Let $(h_i)_{i\geq 1}$ be sampled independently and uniformly at random from a set of size S. Let c denote the first *collision index*, that is the smallest c such that their exists $i < c$ with $h_i = h_c$.

1. Compute the probability that $c < \bar{c}$ for a given $\bar{c} \in \mathbb{N}$.
2. Deduce that $\mathbb{E}[c] \leq O(\sqrt{S})$.
3. Reach the same conclusion without the uniformity assumption.
4. Deduce a generic attack (i.e. a similar attack that would apply to any hash function) that runs in expected time $O(\sqrt{|\mathcal{H}|})$