ALGORITHMIC PROBLEMS OVER LATTICES – EXERCISES

The exercises below use SageMath (`https://www.sagemath.org/`). If you don't have SageMath on your computer, you can use it online at `https://cocalc.com/`: click on "run CoCalk now", then on the project "welcome to CoCalc!" and then create a new file of type "Sage worksheet".

1 Exercise 1

1. Import the library

```
from sage.modules.free_module_integer import IntegerLattice
```

2. Start with dimension $\texttt{dim} = 10$
3. Generate a random lattice basis B with

```
B = sage.crypto.gen_lattice(n = dim//2, m=dim, q = ZZ(dim**2).next_prime())
```

4. Solve SVP in $\mathcal{L}(B)$ by running

```
IntegerLattice(B).shortest_vector(algorithm="pari")
```

5. Increase the dimension and repeat until it takes > 30 seconds

What is the maximum dimension you were able to reach?

2 Exercise 2

Do the same as in exercise 1, but replace the sampling of `B` by

```
B = random_matrix(ZZ,dim)
```

What maximum dimension can you reach now (in less than 30")?

3 Exercise 3

The objective of this exercise is to solve the SIS instance with modulus $q = 127$, dimensions $m = 10$, $n = 5$ and matrix A obtained by running

```
set_random_seed(42)
A = random_matrix(Integers(127),5,10)
```

Important note: in the slides, the vectors are columns vectors (and the matrix A is tall). In SageMath, the vectors are row vectors (so the matrix A is large). This means that in the formalism of SageMath, we want to find a small vector x such that $Ax = 0 \bmod q$ (instead of $xA = 0 \bmod q$ as in the slides).

1. Compute a matrix B whose rows generates of the lattice corresponding to the SIS instance (no need to have a basis of the lattice, any generating set is ok for now (it can contain more vectors than a basis)).
   Hint: don't forget that all the vectors $(0, 0, \cdots, 0, q, 0, \cdots, 0)$ are in this lattice.

2. The function `IntegerLattice(B)` can be used even if `B` is a generating set of the lattice and not a basis. Use this to find a short vector x in the lattice associated to the SIS instance.

3. Check that x is indeed a solution of SIS (i.e., it is short and satisfy $Ax = 0 \bmod q$.