This problem set consists of four problems with a total of 10 subproblems. Each subproblem counts 10% towards your final grade. Remember that you can use results from previous problems, even if you did not answer the previous problem. Show your work.

Problem 1

a) Explain why 2 is irreducible in $\mathbb{Z}[\sqrt{-7}]$.

Is 2 irreducible in $\mathbb{Z}[(1+\sqrt{-7})/2]$?

b) What is the ring of integers for a number field?

What is the ring of integers for $\mathbb{Q}(\sqrt{-7})$?

Problem 2 In this problem, we will be working with column vectors.

Let $B = (\,\vec{b}_1\ \vec{b}_2\ \vec{b}_3\,) = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 2 & 5 \\ 0 & -1 & 3 \end{pmatrix}$, $\Lambda(B)$ be the lattice generated by the columns of B, and let $\vec{z} = (\,2\ 10\ 2\,)^T$.

a) Compute the Gram-Schmidt basis and the associated coefficient matrix.

b) Make the basis size-reduced (first condition for LLL-reduced).

Verify that the Lovász condition then holds (second condition for LLL-reduced, take $\delta = 3/4$).

c) Use Babai's rounding method to estimate a lattice vector close to $\vec{z}$, for the original basis and the one you got in (b).

Which is closer? Why?

Hint: Two of these three matrices may be useful:

$$\begin{pmatrix} -11/3 & 1 & -5/3 \\ 1 & 0 & 0 \\ 1/3 & 0 & 1/3 \end{pmatrix} \qquad \begin{pmatrix} 0 & 1 & 0 \\ 2/3 & 0 & -1/3 \\ 1/3 & 0 & 1/3 \end{pmatrix} \qquad \begin{pmatrix} 0 & 1 & 0 \\ 1/3 & 0 & -2/3 \\ 1/3 & 0 & 1/3 \end{pmatrix}$$

Problem 3 In this problem, we shall try to understand how to find a small zero of a monic polynomial $f(X) = \sum_{i=0}^{d} f_i X^i \in \mathbb{Z}[X]$ modulo N. We assume that for some bound $D \in \mathbb{Z}$, some unknown $x_0 \in \mathbb{Z}$ satisfies $|x_0| < D$ and $f(x_0) \equiv 0 \pmod{N}$.

a) Let $h(X) = \sum h_i X^i \in \mathbb{Z}[X]$ be s.t. $h(x_0) \equiv 0 \pmod{N}$.

Explain that if $|h(x_0)| < N$, then $h(x_0) = 0$.

Now suppose $\sum (h_i D^i)^2 < N^2/(d+1)$. Show that $h(x_0) = 0$.

Hint: Cauchy-Scharz says that for any $\vec{u} \in \mathbb{R}^n$, $\sum u_i \leq \sqrt{n}\sqrt{\sum u_i^2}$.

b) Let

$$B = \begin{pmatrix} N & 0 & \dots & 0 & f_0 \\ 0 & ND & & 0 & f_1 D \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & & ND^{d-1} & f_{d-1} D^{d-1} \\ 0 & 0 & \dots & 0 & D^d \end{pmatrix}$$

and suppose you know a non-zero $\vec{u} \in \Lambda(B)$ satisfies $\|\vec{u}\|_2^2 < N^2/(d+1)$.

Show how to find $h(X)$ satisfying the conditions of a).

Problem 4 In this problem, we shall consider how to factor $N = pq$, p, q odd primes. Here, $\mathbb{Z}_N$ denotes the integers modulo N, while $\mathbb{F}_p$ and $\mathbb{F}_q$ denote the finite fields with p and q elements, respectively.

a) Suppose you know $a, b, D \in \mathbb{Z}$ such that $a^D \equiv b \pmod{N}$ and $p-1|D$, but not $q-1|D$.

Explain a strategy for factoring N given this knowledge, and when it fails.

If a is chosen at random, how likely is it to fail?

Let $f(X) \in \mathbb{Z}[X]$ be some quadratic polynomial that is irreducible modulo both p and q.

In the ring $\mathbb{Z}_N[X]/(f(X))$, we can represent cosets with polynomials of degree at most 1.

b) Show that $\mathbb{Z}_N[X]/(f(X)) \simeq \mathbb{F}_p[X]/(f(X)) \times \mathbb{F}_q[X]/(f(X))$.

Let $a \in \mathbb{Z}_N[X]/(f(X))$. Explain how to compute quickly a representative of a^D, given D, $f(X)$ and a representative of a.

Show that $a^{(p+1)(q+1)}$ in $\mathbb{Z}_N[X]/(f(X))$ can be represented by a degree 0 polynomial?

Hint: Recall that $\mathbb{F}_p[X]/(f(X)) \simeq \mathbb{F}_{p^2}$ and $\mathbb{F}_{p^2}^*$ is cyclic and contains $\mathbb{F}_p^*$ as a subgroup.

c) Suppose you know $a, b \in \mathbb{Z}_N[X]/(f(X))$, $D \in \mathbb{Z}$ such that $a^D = b$ in $\mathbb{Z}_N[X]/(f(X))$, $p+1|D$, but not $q+1|D$.

Explain a strategy for factoring N given this knowledge, and when it fails.

If a is chosen at random, how likely is it to fail?