Problem Set 3: Part A

- Due Date: **2 May, 2022**
- The points for each problem is indicated on the side. The total available in this part of the set is **60 points** and you can choose to **answer any 45 points** worth of questions for a full score (anything above this threshold will be bonus points and counted towards your aggregate).
- The problem set has a fair number of questions so please do not wait until close to the deadline to start on them. Try and do one question every couple of days.
- Turn in your solution to this part electronically (PDF; preferably LaTeXed, but scanned handwritten files are also ok) on Acadly.
- Collaboration is encouraged, but all writeups must be done individually and must include names of all collaborators.
- Referring to sources other than the class notes is strongly discouraged. But if you do use an external source (eg., other text books, lecture notes, or any material available online), ACKNOWLEDGE all your sources (including collaborators) in your writeup. This will NOT affect your grades. However, not acknowledging will be treated as a serious case of academic dishonesty.
- Be clear in your writing.

1. **[Factorisation over characteristic 2]** (3 + 3 + 4 + 0)

   Fix a field $\mathbb{F} = \mathbb{F}_{2^k}$ and consider the following function $\mathrm{Tr} : \mathbb{F}_{2^k} \to \mathbb{F}_{2^k}$ defined as

   $$\mathrm{Tr}(x) = 1 + x + x^2 + \cdots + x^{2^{k-1}}$$

   (a) Show that the range of the function is in fact just $\mathbb{F}_2$. That is, 0 and 1 are the only possible outputs.

   [Hint: What happens to $\mathrm{Tr}(x) \cdot (\mathrm{Tr}(x) + 1)$?]

   (b) Show that Tr maps half the elements of $\mathbb{F}$ to 0, and half the elements of $\mathbb{F}$ to 1.

   (c) Use this to appropriately modify the Cantor-Zassenhaus algorithm to factorise univariate polynomials over the field $\mathbb{F}_{2^k}$.

   (d) Can you guess why this function is called "trace"? What is it a 'trace' of?

2. **[Computing determinants with integer entries]** (15)

   Suppose you are given an $n \times n$ matrix M with entries that are c-bit integers (that is, each entry an integer between -2^c and 2^c). Present a deterministic polynomial time algorithm (running in time $\mathrm{poly}(n, c)$) to compute the determinant of this matrix.

   [Hint: This is not a trick question. The standard Gaussian elimination might end up increasing the size of entries beyond your control. You may want to remaind yourself with some of the tools seen in this course.]

Base version: (2022-03-13 20:12:28 +0530) , 749125b

3. **[Computing a basis for a lattice]** (5 + 10)

Suppose you are given vectors $b_1, \ldots, b_m \in \mathbb{Z}^n$, and suppose these vectors span a vector space (in $\mathbb{Q}^n$) of dimension r when viewed as a set of vectors in $\mathbb{Q}^n$.

If $m > r$, we know that there is a subset of $b_1, \ldots, b_m$ of size r that forms a *basis* for this vector space. However, this may not be true when we were to think of the *lattice* generated by them and not the vector space generated by them.

(a) Construct a set of m integer vectors $b_1, \ldots, b_m \in \mathbb{Z}^n$ that span a vector space of dimension $r < m$, but no subset of $\{b_1, \ldots, b_m\}$ spans the lattice $\mathcal{L}(b_1, \ldots, b_m)$.

(b) Given vectors $b_1, \ldots, b_m \in \mathbb{Z}^n$ that space a vector space of dimension $r < m$, give an algorithm to contruct a set of vectors $b'_1, \ldots, b'_r$ such that $\mathcal{L}(b'_1, \ldots, b'_r) = \mathcal{L}(b_1, \ldots, b_m)$. That is, we can find a different set of vectors (not necessarily a subset) that does form a basis for the lattice.

[Hint: Think of vectors written down as rows in a matrix, and attempt to do a version of Gaussian elimination. As a start, can you try to keep applying row-operations in order to ensure that the first column has just one nonzero entry and this entry is the gcd of the original entries in the first column?]

4. **[Computing integer roots modulo a composite number]** (5 + 5 + 5 + 5)

You are given a polynomial $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$ (that is, $a, b, c \in Z$ are given as input), and you are also given a composite number N (think of $N = pq$ where p and q are unknown primes). You promised that there is an at least one positive integer $m \ll N^{1/12}$ such that $f(m) = 0 \bmod N$ and we want to find such an m.

There are a couple of natural approaches. If there was no modulo N, we could have just factorised $f(x)$ over integers, and $(x - m)$ would have been a root; but we are only told that there is a small integer m such that $f(m) = 0 \bmod N$ so this doesn't work. Another approach would have been to compute the roots of $f \bmod p$ and $f \bmod q$ via factorisation over $\mathbb{F}_p$ and $\mathbb{F}_q$, and use Chinese remaindering to combine them and get m. Alas, we are not told the factorisation of N and computing the factorisation of N ourselves is believed to be hard. However, LLL can help us solve this problem.

You may assume the following theorem for this problem.

Theorem 1 (Minkowski)**.** *Suppose $\mathcal{L} = \mathcal{L}(b_1, \ldots, b_n) \in \mathbb{Z}^n$ is a full-rank lattice (that is, $b_1, \ldots, b_n$ are linearly independent as vectors in $\mathbb{Q}^n$). Let K be a convex body that is symmetric about the origin ($x \in K \iff -x \in K$) such that $\mathrm{vol}(K/2) > \det(\mathcal{L})$ (where, by $\det(\mathcal{L})$, we mean the determinant of the $n \times n$ matrix whose rows are the b_i's). Then, K contains a nonzero lattice point of $\mathcal{L}$.*

(Roughly speaking, the above theorem says that if K is "large enough" compared to the "primary cell" of $\mathcal{L}$, then K must include a nonzero lattice point of $\mathcal{L}$.)

(a) If $\mathcal{L} = \mathcal{L}(b_1, \ldots, b_n) \in \mathbb{Z}^n$ is a full-rank lattice, show that there is a nonzero lattice point in $\mathcal{L}$ of ℓ_2-norm at most $\sqrt{n} \cdot (\det(\mathcal{L}))^{1/n}$.

[Hint: Choose a symmetric convex body K whose volume you know, and choose a suitable scaling of it to apply Minkowski's theorem.]

(b) Consider the following full-rank lattice $\mathcal{L} = \mathcal{L}(\{N, Nx, Nx^2, f(x), xf(x), x^2 f(x)\}) \subseteq \mathbb{Z}^6$ (where $f(x) = x^3 + ax^2 + bx + c$ that was provided to us).

Show that LLL will find a nonzero vector $u(x) = u_0 + u_1 x + \cdots + u_5 x^5 \in \mathcal{L}$ of ℓ_2-norm at most $\sqrt{200 \cdot N}$.

(c) For the $u(x)$ obtained above, show that if there is an integer $m \ll N^{1/12}$ such that $f(m) = 0 \bmod N$, then have that $u(m) = 0$ (without going modulo N).

(d) Outline an algorithm running in time $\text{poly}(\log N, k)$, where a, b, c are k-bit integers, to compute an $0 < m \ll N^{1/12}$ such that $f(x) = 0 \bmod N$ (assuming of course such an m exists).