CS 473: Algorithms, Fall 2021
HW 1 (due Wednesday, Feb 10th at 8pm)

This homework contains three problems. **Read the instructions for submitting homework on the course webpage**.

Collaboration Policy: For this home work, each student can work in a group with up to three members. Only one solution for each group needs to be submitted. Follow the submission instructions carefully.

1. [**10pts**] We saw in class the FFT algorithm to compute convolutions using complex numbers. However working with complex numbers is complex and there are difficult numerical issues involved. Here we will see how to use modular arithmetic to avoid these. Recall, the field $\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$ is the field where addition and multiplication are taken *modulo* p, and the multiplicative inverse of $x \in \mathbb{Z}_p$ is a number $y \in \mathbb{Z}_p$ such that $xy \equiv 1 \mod p$.

   Suppose we have two integer valued vectors $\bar{a} = (a_0, a_1, \ldots, a_{n-1})$ and $\bar{b} = (b_0, b_1, \ldots, b_{n-1})$ whose convolution we wish to compute. We choose a sufficiently large prime number p such that we can multiply the two polynomials in the field $\mathbb{Z}_p$, which ensures that the numbers never grow too large.

   The goal of this problem is to illustrate this via a simple example which will also make you work out some of the details of the FFT algorithm. We will consider $p = 7$.

   - There is a number $\omega \in \mathbb{Z}_7$ such that all the powers $\omega, \omega^2, \ldots, \omega^6$ are distinct (modulo 7). Find this ω, and show that $\omega + \omega^2 + \ldots + \omega^6 = 0$. (Interestingly, for any prime modulus there is such a number but finding it efficiently for a given prime is not easy. If you are interested see `https://kconrad.math.uconn.edu/blurbs/grouptheory/cyclicmodp.pdf` for six different proofs of existence of such a number.)
   - Using the matrix form of the DFT, produce the transform of the sequence $(4, 1, 1, 5, 2, 5)$ modulo 7; that is, multiply this vector by the matrix $M_6(\omega)$, for the value of ω you found earlier. In the matrix multiplication, all calculations should be performed modulo 7.
   - Write down the matrix necessary to perform the inverse DFT. Show that multiplying by this matrix returns the original sequence. (Again, modulo 7.)
   - Now show how to multiply the polynomials $x^2 + 2x - 4$ and $x^3 + x + 1$ using the DFT modulo 7.
   - For multiplying two polynomials $\bar{a} = (a_0, a_1, \ldots, a_{n-1})$ and $\bar{b} = (b_0, b_1, \ldots, b_{n-1})$ with integer valued coefficients how large should a prime p be such that computing the multiplication in $\mathbb{Z}_p$ yields the correct answer?

2. [**10pts**] For any two sets X and Y of integers, the Minkowski sum $X + Y$ is the set of all pairwise sums $\{x + y \mid x \in X, y \in Y\}$.

   - Describe and analyze an algorithm to compute the number of elements in $X + Y$ in $O(n^2 \log n)$ time where $|X| = |Y| = n$.

- Describe and analyze an algorithm to compute the number of elements in $X + Y$ in $O(n + M \log M)$ time, where M is the largest absolute value of any element of $X \cup Y$. *Hint:* Use FFT.

3. **[10pts]** Consider the following problem. Given a string A of length n you want to find the smallest k such that A can be written as $A_1 \cdot A_2 \cdot \cdots \cdot A_k$ where each A_i is a palindrome.

   Hint: Use dynamic programming.