When asked to give an algorithm, please provide pseudocode.

**Problem 1.** A polynomial is a function \( C(x) = \sum_{i=0}^{n} c_i x^i \), where \( x \) is the variable and \( c_0, \ldots, c_n \) are the constant coefficients. The only information we need to define a polynomial is this sequence of coefficients. As such, we usual represent polynomials in algorithms as coefficient arrays. The coefficients are stored so that \( c_i \) is stored at index \( i \).

The product of two polynomials \( A, B \) (of the same variable) is

\[
(AB)(x) = \sum_{i=0}^{n} \sum_{j=0}^{n} a_i b_j x^{i+j}.
\]

At a glance, an algorithm to compute \( AB \) is straightforward. In Algorithm 1, we multiply two degree \( n \) polynomials together. To multiply two different degree polynomials together, we can represent the smaller polynomial as a larger degree polynomial by padding its coefficient array with 0’s.

**Algorithm 1: MP\((A, B)\)**

- **Input:** Polynomials \( A, B \) of degree \( n \)
- Let \( C \) be a polynomial of degree \( 2n \) initialized to all 0 coefficients
- for \( i = 0 \) to \( n \) do
  - for \( j = 0 \) to \( n \) do
    - Add \( a_i b_j \) to \( c_{i+j} \)
- return \( C \)

a) What is the runtime of this multiplication algorithm?

b) Adapt a divide and conquer algorithm of similar purpose to improve the runtime.

c) State precisely what your algorithm returns.

d) Prove your algorithm is correct (that is it returns what you claimed it should).

e) Give a recurrence relation for your algorithm.

f) Determine the runtime of your algorithm using a work tree to justify it.

**Solution 1.**

a) \( O(n^2) \)
Algorithm 2: FMP($A, B$)

**Input:** Polynomials $A, B$ of degree $n$

if $n = 0$ then
    return the polynomial $a_0 b_0$

if $n + 1$ is not a power of 2 then
    Pad $A$ and $B$ until their degree is one less than the next largest power of 2
    Let $n$ be that power of 2 minus 1
    $// A = A_l + A_u x^{\frac{n+1}{2}}$ and $B = B_l + B_u x^{\frac{n+1}{2}}$
    Let $A_l = a_0 + \ldots + a_{\frac{n+1}{2}} x^{\frac{n+1}{2}}$ and $A_u = a_{\frac{n+1}{2}} + \ldots + a_n x^{\frac{n-1}{2}}$
    Let $B_l = b_0 + \ldots + b_{\frac{n+1}{2}} x^{\frac{n+1}{2}}$ and $B_u = b_{\frac{n+1}{2}} + \ldots + b_n x^{\frac{n-1}{2}}$
    $// AB = A_l B_l + (A_l + A_u)(B_l + B_u) - A_l B_l - A_u B_u) x^{\frac{n+1}{2}} + A_u B_u x^{n+1}$
    Let $C_0 = \text{FMP}(A_l, B_l)$
    Let $C_1 = \text{FMP}(A_u, B_u)$
    Let $C_m = \text{FMP}(A_l + A_u, B_l + B_u)$
    return $C_0 + (C_m - C_0 - C_1)x^{\frac{n+1}{2}} + C_1 x^{n+1}$

b) $FMP(A, B)$ returns the product $AB$.

d) Since the algorithm forces the input polynomials into a form where the number of coefficients (not the degree) is a power of two, it suffices to show that the algorithm is correct only for polynomials of this form.

In the base case, when $n = 0$, the algorithm correctly returns the product of the two constant terms.

Now assume that FMP($A,B$) is correct for any polynomials $A, B$ of degree $2^n - 1$.

Let $A, B$ be polynomials of degree $2^{n+1} - 1$. Then $A_l, A_u, B_l,$ and $B_u$ are all polynomials of degree $2^n - 1$. By assumption, $C_0 = A_l B_l, C_1 = A_u B_u, C_m = (A_l + A_u)(B_l + B_u)$.

Lastly, the identity commented in the algorithm is precisely what FMP returns. □

e) $T(n) = 3T(n/2) + O(n)$

f)
Problem 2. The discrete Fourier transform (DFT) of a function \( f : \mathbb{Z}_n \to \mathbb{C} \), where \( \mathbb{C} \) is the set of complex numbers, is given by

\[
\mathcal{F}(f)(k) = \sum_{j=0}^{n-1} f(j)e^{-\frac{2\pi i}{n}jk}.
\]

This transformation is used just about everywhere, even in places you would not expect it, though we will omit a lengthy discussion of its utility here.

Notice that the output of the Fourier transform \( \mathcal{F}(f) \) is itself a function from \( \mathbb{Z}_n \) to \( \mathbb{C} \). If we want to compute all of them, the naive approach is to compute \( \mathcal{F}(f)(k) \) directly for each value of \( k \) in \( O(n^2) \) time. However, \( e^{-\frac{2\pi i}{n}jk} \) happens to traverse a circle of radius one in the complex plane and thus has a number of symmetries we can take advantage of.

The fast Fourier transform (FFT) is the go-to algorithm we use for computing each of \( \mathcal{F}(f)(0), \ldots, \mathcal{F}(f)(n-1) \) simultaneously in \( O(n \log n) \) time (it returns an array/function/vector/etc containing these values). The key insight is the observation that

\[
\mathcal{F}(f)(k) = \sum_{j=0}^{n-1} f(2j)e^{-\frac{2\pi i}{n}jk} + e^{-\frac{2\pi i}{n}k} \sum_{j=0}^{n-1} f(2j+1)e^{-\frac{2\pi i}{n}jk}
\]

\[
= \mathcal{F}(f_e)(k) + e^{-\frac{2\pi i}{n}k} \mathcal{F}(f_o)(k)
\]

We obtain this by separating the even and odd index terms into two smaller DFTs of size \( \frac{n}{2} \). These smaller functions are denoted \( f_e \) and \( f_o \) respectively above. This division into half size problems lends itself to divide and conquer algorithms. However, there is an issue here. The smaller DFTs are not properly defined for \( k \geq \frac{n}{2} \). Luckily, symmetry saves the day. When \( n \) is even,

\[
\mathcal{F}(f)\left(k + \frac{n}{2}\right) = \mathcal{F}(f_e)(k) - e^{-\frac{2\pi i}{n}k} \mathcal{F}(f_o)(k).
\]

For the purposes of this problem, you may freely assume \( n \) is a power of two. There are a number of ways to mitigate this assumption in application, so it is largely an unimportant restriction.

a) Give an efficient divide and conquer algorithm for the FFT.

b) Show that the runtime of your algorithm is \( O(n \log n) \).

Solution 2.

a)

b)
Algorithm 3: FFT(f)

**Input:** Function $f$ of $n$ inputs

**Output:** The DFT of $f$ with $n$ inputs

if $n = 1$ then
    return the function $0 \rightarrow f(0)$

// Separate $f$ into its even and odd inputs $f_e$ and $f_o$ respectively
Let $f_e = f(2x)$ for $0 \leq x < \frac{n}{2}$
Let $f_o = f(2x + 1)$ for $0 \leq x < \frac{n}{2}$

// Compute the DFT of $f_e$ and $f_o$
Let $F_e = \text{FFT}(f_e)$
Let $F_o = \text{FFT}(f_o)$

// Create a place to build the output function
Let $F$ be a function of $n$ inputs

// Assign each output of $F$
for $k = 0$ to $\frac{n}{2} - 1$ do
    Let $l = F_e(k)$
    Let $r = e^{-\frac{2\pi i}{n}}F_o(k)$
    Assign $F(k) = l + r$
    Assign $F(k + \frac{n}{2}) = l - r$

return $F$