1. Give the steps of Karatsuba’s algorithm with the input polynomials $1 - x + 3x^2 - x^3$ and $1 + x + x^3$.

For all such computational questions, you are free to do the computations by hand, or to implement the algorithm and run it. If you implement it in a language like C or java, you can use floats or ints as coefficients.

2. Give the steps of the Fast Fourier Transform for $n = 4$, with the input polynomial $P = 1 + x - 2x^2 - 3x^3$. Then, perform an inverse Fast Fourier Transform to recover the polynomial $P$.

3. We start from the following recursion (which is Karatsuba’s recursion):

- $T(1) = 1$
- $T(n) = 3T(n/2) + ℓn$, for $n$ a power of 2, where $ℓ$ is a constant.

Prove that

$$T(2) = 3 + 2ℓ, \quad T(4) = 9 + 10ℓ, \quad T(8) = 27 + 38ℓ$$

and more generally, for $n ≥ 2$ (by induction)

$$T(2^n) = 3^n + 2(3^{n-1} + 2 \cdot 3^{n-2} + \cdots + 2^{n-2} \cdot 3 + 2^{n-1})ℓ.$$

Bonus question (you don’t need to complete it to get 100%): deduce that $T(2^n) = O(3^n)$, without (of course) using the master theorem.

4. Prove that you can compute the modular multiplication

$$c_0 + c_1x = (a_0 + a_1x)(b_0 + b_1x) \mod (x^2 + 2)$$

using 3 multiplications (don’t count the multiplication by a constant as a “real” multiplication).

Hint: Use Karatsuba’s algorithm.
5. You are to study an alternative to Karatsuba or Toom to multiply polynomials. Let \( f = f_0 + f_1 x + f_2 x^2 \) and \( g = g_0 + g_1 x + g_2 x^2 \), and let \( h = h_0 + h_1 x + h_2 x^2 + h_3 x^3 + h_4 x^4 \) be their product. For this size of inputs, the algorithm does the following:

(a) compute \( F_0 = f(0), F_1 = f(1), F_{-1} = f(-1), F_{x^2+2} = f \mod (x^2 + 2) \).

(b) compute \( G_0 = g(0), G_1 = g(1), G_{-1} = g(-1), G_{x^2+2} = g \mod (x^2 + 2) \).

(c) compute \( H_0 = F_0 G_0, H_1 = F_1 G_1, H_{-1} = F_{-1} G_{-1}, H_{x^2+2} = F_{x^2+2} G_{x^2+2} \mod (x^2 + 2) \).

(d) recover \( h \).

First, prove that \( H_0 = h(0), H_1 = h(1), H_{-1} = h(-1), H_{x^2+2} = h \mod (x^2 + 2) \).

There are two ways to do this: brute force computation (please don’t) or using the results on the slides (preferred). Then, show how to recover \( h \) from \( H_0, H_1, H_{-1}, H_{x^2+2} \); I’m not asking you to finish all computations, since it gets a bit messy. Finally, count how many multiplications you use. \textit{Hint: use the previous problem.}

Without giving all details, explain how you could use this trick recursively, and indicate what complexity you would expect.

6. How much time did you spend on the assignment?