Polynomials in $\mathbb{Z}_2$

A single-variable **polynomial in** $\mathbb{Z}_2$ has the form

$$f(x) = c_0 + c_1 x + c_2 x^2 + c_3 x^3 + \cdots ,$$

where the coefficients c_i are elements of $\mathbb{Z}_2$.

$\mathbb{Z}_2$ is similar to binary, except there is no carrying when adding $1 + 1$. In binary, $1 + 1 = 10$, but in $\mathbb{Z}_2$, $1 + 1 \equiv 0$ (because $2 \equiv 0 \pmod 2$). If you want, you can think of addition in $\mathbb{Z}_2$ as the XOR operation.

Since there is no carrying when adding, this also affects multiplication of polynomials. For example, when FOIL'ing $(1 + x^2)(x + x^3)$, we get $x + x^3 + x^3 + x^5$, but this simplifies to $x + x^5$. (This is because $x^3 + x^3 = 2x^3$, but in $\mathbb{Z}_2$, $2x^3 \equiv 0x^3$.)

Examples:

If you're having trouble following these examples, please ask during office hours or set up an appointment.

- $(1 + x + x^2)^2 = (1 + x + x^2) + (x + x^2 + x^3) + (x^2 + x^3 + x^4) = 1 + x^2 + x^4$
- $(1 + x^2 + x^3) + (x + x^2 + x^4) = 1 + x + x^3 + x^4$
- $(1 + x)^3 = 1 + x + x^2 + x^3$

Coding Project

You will code an addition function and a multiplication function for polynomials in $\mathbb{Z}_2$ of degree 7 or less. The inputs for these functions will be arrays of length 8. These arrays will have the form

$$[c_0, c_1, c_2, c_3, c_4, c_5, c_6, c_7]$$

where each c_i is either 0 or 1. The array contains the coefficients of the polynomial

$$c_0 + c_1 x + c_2 x^2 + c_3 x^3 + c_4 x^4 + c_5 x^5 + c_6 x^6 + c^7 x^7.$$

You may assume that your input polynomials will never be higher than degree 7. You may assume that if an input polynomial has degree less than 7, its array will be padded with zeroes so that the length of the array will be 8 elements.

3. Your first function should take two arrays as input (where the arrays are described above), and return an array representing the **sum** of the polynomials.

   Keep in mind that this is the sum in $\mathbb{Z}_2$.

   You should find this function very easy to code.

4. Your second function should take two arrays as input (again, where the arrays are described above), and return an array representing the product of the polynomials.

   Note that the product of two x^7 terms is x^{14}, and so you may need an array of length 15 for the output.

   Also keep in mind that you are working in $\mathbb{Z}_2$, so all of the coefficients in the output array should be either 0 or 1 (you should reduce any 2's that you get!).

   This will be harder than the addition function, but I hope it won't take long.

I will not grade these two functions yet, but they form part of your final project, so you should save the code you write.