18.310 Homework 11

Due Tuesday November 26th at 6PM

---

1. Determine the Discrete Fourier transform (over the complex numbers) for the sequence y_0, y_1, y_2, y_3 where $y_0 = 0$, $y_1 = 1$, $y_2 = 2$ and $y_3 = 3$.

   Now take the inverse Fourier transform for the sequence of complex numbers c_0, c_1, c_2, c_3 you just obtained. Show your calculations.

2. Suppose we want to multiply two binary numbers u and v using Discrete Fourier Transforms performed over $\mathbb{Z}_p$ for an appropriate prime p. For simplicity, let's assume that u and v have only 4 bits (for just 4 bits, it will be much more cumbersome than doing the usual long multiplication, but you probably don't want to have a homework problem in which you need to multiply two 10^6-bit integers....). It will be easier for you if you use excel for the various calculations in this exercise. We will need to compute the Discrete Fourier Transforms of u and v, multiply the corresponding coefficients, and take the inverse Fourier transform, and then perform the carryover to get the product of u and v in binary. Since the product of u and v can have 8 bits, we will be performing Fourier transforms on sequences of $n = 8$ numbers. (Thus, if we are multiplying $u = 1010$ (ten in binary) by $v = 0111$ (seven in binary), we would see these numbers as 00001010 and 00000111, and hope to get seventy in binary as the product.)

   (a) Explain why we can use $p = 17$ in this specific case of multiplying two 4-bit numbers. Can we use any smaller p (remember p has to be a prime)? Explain. What would be the smallest prime p you would use if we were multiplying two 8-bit numbers?

   (b) What are all the *primitive* 8th-root of unity over $\mathbb{Z}_{17}$ (read the lecture notes or use excel...)?

   (c) Suppose we use $z = 2$ as a primitive 8th-root of unity. What is z^{-1} (mod 17)?

   (d) Using $\mathbb{Z}_{17}$ and $z = 2$ as primitive 8th-root of unity, what is the Discrete Fourier transform for $u = 00001010$ (i.e., for the sequence with $u_i = 1$ for $i \in 1, 3$ and 0 for $i \in \{0, 2, 4, 5, 6, 7\}$)? Call it a. And what is b, the DFT for $v = 00000111$? Remember that, here, the DFT of $(y_0, y_1, \cdots, y_{n-1})$ is given by

   $$c_k \equiv \sum_{j=0}^{n-1} y_j \left(z^{-1}\right)^{jk} \pmod{17},$$

   for $k = 0, \cdots, n-1$.

   (e) Multiply the corresponding coefficients (over $\mathbb{Z}_{17}$) and compute the inverse DFT (remember that in the DFT you will be using $z = 2$ rather than z^{-1}, and that there will be an additional factor n^{-1} (mod 17). Is this what you expected? How much is uv in binary?

MIT OpenCourseWare
http://ocw.mit.edu

18.310 Principles of Discrete Applied Mathematics
Fall 2013

For information about citing these materials or our Terms of Use, visit: http://ocw.mit.edu/terms.