18.310A Homework 7

Due Fri May 8th at 10AM in lecture

Instructions: Collaboration on homework is permitted, but you must write the solutions yourself; no copying is allowed. Please list the names of your collaborators; if you worked alone, state this. Also indicate any sources you consulted beyond the lecture notes.

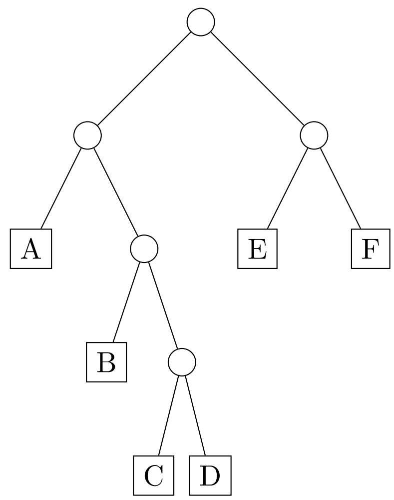
1. Using the Fermat and/or Miller-Rabin test, decide if $p = 3,855,619$ is prime. Start by computing a^{p-1} modulo p by repeated squaring where a is the day of the month of your birthday plus 1 (to avoid a be 1 if you were born the first of the month). If this is inconclusive (even by the Miller-Rabin test), choose one other value of a. You are welcome to use excel, or any programming language, but show your calculations.

2. (a) What is the Discrete Fourier Transform over $\mathbb{C}$ of $y = (1, 1, 0, i)$?
   (b) What is $z = y * y$ where $*$ denotes the convolution (with indices taken modulo 4)?
   (c) Using the result in (a) above, what is the Discrete Fourier Transform of z?

3. In this exercise, you will multiply two numbers s and t, where $0 \leq s, t \leq 124$. Assume s and t are given in base 5 so that their base-5 expansion consist of at most 3 symbols (eg., $s = 117$ in base-10 is written as 432 in base-5, and we would let $s_0 = 2, s_1 = 3$ and $s_2 = 4$). Instead of doing this the elementary school way, you'll use the technique shown in lecture by computing Discrete Fourier Transforms of s and t over $\mathbb{Z}_p$ for an appropriate prime p, multiply the corresponding coefficients, and take the inverse Fourier transform to get st.

   (a) What is the smallest prime p one could choose to be able to recover st? Justify.
   (b) What is the smallest n one could choose? Justify.
   (c) Suppose we choose $p = 61$ and $n = 5$. Without trying to find one, does there exists a primitive 5th root of unity over $\mathbb{Z}_{61}$? Justify.
   (d) Let z be the smallest primitive 5th root of unity modulo $\mathbb{Z}_{61}$. What is the multiplicative inverse of z? Is it also a primitive 5th root of unity?
   (e) For $n = 5$, $p = 61$ and your z, what is the Fourier transform of s where $s_0 = 2$, $s_1 = 3$ and $s_2 = 4$ (and $s_3 = 0$ and $s_4 = 0$)? (s corresponds to 432 in base-5 or 117 in base-10.)
   (f) Consider now the convolution of s with itself: $u = s * s$. What is the Discrete Fourier Transform (over $\mathbb{Z}_{61}$) of u?
   (g) Give the inverse Fourier transform of u.
   (h) Deduce from it the base-5 expansion of 117^2 (this is written in base-10). (Check your answer the elementary school way!)

4. The following binary tree corresponds to a prefix code.



(a) Find a probability distribution on the letters A, B, C, … F, for which Huffman's algorithm could construct this prefix code.

(b) Can you select the probability distribution above such that this prefix code is not just the best *prefix* code (in terms of the expected length of an encoded letter) but also achieves Shannon's lower bound? Explain.

5. Lempel-Ziv.

(a) Suppose you encode n digits from the sequence

$$1234567891011121314151617181920212 2\cdots$$

obtained by concatenating all natural numbers. Approximately how many bits will this take to encode using Lempel-Ziv?

(b) Suppose you encode n bits from the sequence

$$0101010101010101010101\cdots$$

obtained by alternating 0's and 1's. Approximately how many bits will this take to encode using Lempel-Ziv?