18.310 Exam 3 practice questions

Collection of problems from past quizzes and other sources. It does not necessarily reflect what will be on the exam on Friday.

1. What is the gcd of 161 and 119. Show your calculations.

   For each of the following numbers, write it as a linear combination of 161 and 119, if possible; if it is not possible, explain why not.

   - 21
   - 15

2. (From final, spring 2013.)

   1. State Lagrange's theorem.
   2. Let p be a prime number, and suppose that $(G, \cdot)$ is a group of order p^2. Let $x \in G$, with $x \neq e$ (e being the identity element of the group).
      Let $H = \{x^k : k \in \mathbb{Z}\}$. Prove that either $H = G$, or else $|H| = p$.

3. (From quiz Spring 2012)

   Alice chooses primes $p = 5$ and $q = 11$. The public key she generates is the pair $(55, 7)$ and the private key is $(55, 23)$. Bob wants to encrypt the message $m = 53$ and send it to Alice. What is the encrypted message?

4. (From quiz, Fall 2010.)

   Suppose a message m is encoded using RSA with the public key $N = 77$ and $z = 43$, i.e.

   $$s \equiv m^z \pmod{77},$$

   and the encoded message is $s = 2$. Compute (numerically) m. Explain your steps.

5. (From quiz Spring 2012)

   1. How many elements of $\{0, 1, 2, \ldots, 134\}$ are divisible both by 3 and by 5? (Note that $135 = 3^3 \cdot 5$).
   2. Determine the cardinality (number of elements) of the multiplicative group $(\mathbb{Z}^*_{135}, \otimes)$.

6. (From quiz spring 2012)

   Let $a_0, a_1, \ldots, a_{n-1}$ be real numbers. Let $c_0, c_1, \ldots, c_{n-1}$ be the coefficients associated to the sequence $a_0, a_1, \ldots, a_{n-1}$ by the Discrete Fourier Transform. Let $c'_k = c_k$ for all $k = \{0, \ldots, n-1\}$ except $c'_1 = c_1 + 1$. Let $a'_0, a'_1, \ldots, a'_{n-1}$ be the number obtained from $c'_0, c'_1, \ldots, c'_{n-1}$ by the inverse Discrete Fourier Transform. Express $a'_0, a'_1, \ldots, a'_{n-1}$ in terms of $a_0, a_1, \ldots, a_{n-1}$.

7. (From quiz, spring 2012)

   Let z be a primitive 32nd root of unity modulo p.

   1. Give two possible values for p.
   2. Write the formula for the discrete Fourier transform $a_0, a_1, \cdots, a_{31}$ of a sequence $y_0, y_1, \cdots, y_{31}$ modulo p and using z as 32nd root of unity.
   3. Let $y_i = 1$ for $i = 0, \cdots, 31$. What is its discrete Fourier transform?

8. (From quiz, Fall 2012; was one out of 5 questions.)

   Suppose you have a random source which outputs independent letters from an alphabet of size k, and each letter is equally likely (its probability is thus $1/k$).

   1. In expectation, how many bits does the best code use to compress a string of n letters from this source?
   2. Give a value of k for which the best code is not a prefix code. Explain.
   3. Give values of k for which this best code can be chosen to be a prefix code. Justify your answer.

9. (From quiz, Fall 2010; was one of 4 questions.)

   Consider the following probabilities for the alphabet $A = \{A, B, C, D, E, F\}$.

A	0.15
B	0.13
C	0.2
D	0.1
E	0.34
F	0.08

   (a) Derive the optimum Huffman code for A with the probabilities above.

   (b) How would you encode CAFE?

   (c) What is the expected number L of bits per encoded letter?

10. (From quiz Fall 2012; was one out of 5 questions.)

    Suppose we have two sequences of length 32, f_k and a_k, related by

$$f_k = \sum_{j=0}^{31} a_j e^{-2\pi ijk/32}$$

    for $k = 0, 1 \cdots, 31$.

    1. Give a formula for a_j in terms of the f_k's.

2. Suppose that

$$f_k = e^{-20\pi ik/32},$$

for $k = 0, 1 \cdots, 32$. Give an explicit expression for the numbers a_j. This answer should have no summation.

11. (From quiz Spring 2012)

Consider a source which outputs independent random letters from the alphabet $A = \{a, b, c, d, e\}$ with probabilities $p_a = 1/4$, $p_b = 1/4$, $p_c = 1/6$, $p_d = 1/6$ and $p_e = 1/6$.

1. Give a Huffman code for this source.
2. Let L_n be the random length of the Huffman code for a random sequence of n letters from that source. Compute the expectation $\mathbb{E}(L_n)$.
3. Let L_n be the (random) length of the Lempel-Ziv code for a random sequence of n letters from that source. Say if $\lim_{n\to\infty} \frac{\mathbb{E}(L_n)}{n}$ and $\lim_{n\to\infty} \frac{\mathbb{E}(L'_n)}{n}$ are equal, and if not which one is larger.

12. Consider the message

$$aababcabcdabcde.$$

Describe the decomposition into phrases that will be used by Lempel-Ziv, and give the encoded string obtained using Lempel-Ziv. When encoding a letter, use the mapping

$$a \to 000, \quad b \to 001, \quad c \to 010, \quad d \to 011, \quad e \to 100.$$

18.310 Principles of Discrete Applied Mathematics
Fall 2013