18.781 Problem Set 4

Due Monday, March 4 in class.

1. I have made a toy RSA encryption system. I announce to you the public modulus $m = 221$ and the public encryption key $k = 77$. To encrypt a message a to me (which can be any positive number between 1 and 220), you must calculate $a^{77} \pmod{221}$.

1(a). Suppose that you wish to send me the private message 2. What is the encrypted message you should send?

1(b). Not content with the ability to send me private messages, you have decided to try to *read* my private messages. You find that the Dean has sent me the encrypted message 95. What was the Dean's actual message to me?

2. Recall that Euler's ϕ function is defined for every positive integer m as

$$\phi(m) = \text{number of integers } 1 \leq a \leq m \text{ such that } \gcd(a, m) = 1.$$

In particular, this means that $\phi(1) = 1$.

2(a). Suppose that d is a positive divisor of m, and that $1 \leq a \leq m$. Prove that $\gcd(a, m) = d$ if and only if $d|a$ and $\gcd(a/d, m/d) = 1$.

2(b). Suppose that d is a positive divisor of m. Prove that

$$\phi(m/d) = \text{number of integers } 1 \leq a \leq m \text{ such that } \gcd(a, m) = d.$$

2(c). Prove Gauss's formula

$$\sum_{d|m} \phi(m/d) = m.$$

2(d). You know that if p is a prime number, then $\phi(p) = p - 1$. Use this fact and part (c) to calculate $\phi(21)$.

3. This problem is stolen from a text "Discrete math for computer science students" by Ken Bogart and Cliff Stein. The goal is to factor $N = 224,551$, in order to get some sense of how difficult factoring large numbers might really be. You may assume (as you might verify by trial divisions by hand) that N has no prime factors less than or equal to 59. You may also assume (as you might verify with a calculator) that $N^{1/2} = 473.86\ldots$ and $N^{1/3} = 60.78\ldots$.

3(a). Prove that if N is not prime, then it must be the product of exactly two prime factors $p_1 < p_2$, with $61 \leq p_1 \leq 467$.

3(b). Find a table of prime numbers. How many are there between 61 and 467?

3(c). Suppose that some kindly oracle tells you that p_1 is between 400 and 450. Use trial divisions (with the table of primes you located in (b)) to find a prime factorization of N.