Analytic Number Theory
Homework 1

Reading: If you feel comfortable with the basic notions in elementary number theory (the division algorithm, the fundamental theorem of arithmetic, modular arithmetic, and so on), there is no reading. Otherwise you can read Chapter 1 of Apostol's *Analytic Number Theory* to review.

1. (Optional review/not to turn in) If a and b are two integers, denote their greatest common divisor by (a, b). By definition, (a, b) is the unique nonnegative integer such that $d|a$, $d|b$, and if e is any other integer such that $e|a$ and $e|b$ we have $e|d$. (The notation $d|a$ means "d divides a;" i.e., there exists an integer m such that $dm = a$).
a) Prove that if $(a, b) = (a, c) = 1$, then $(a, bc) = 1$.
b) Prove that if $(a, b) = 1$ and $d|(a + b)$, then $(a, d) = (b, d) = 1$.
c) Prove that if a, b are positive, $(a, b) = 1$, and $ab = c^n$ for some integer c, then there exist integers x and y such that $a = x^n$ and $b = y^n$.

2. In class, we used that if $P_n = \prod_{i=1}^{n} p_i$ is the nth primorial, then only $\prod_{i=1}^{n}(p_i - 1)$ residue classes modulo P_n can contain any primes except $p_1, \ldots, p_n$. Let's carefully prove this and more.
a) Assume the Euclidean division algorithm: for every two integers a and b with $b \neq 0$, there exist unique integers q and r such that

$$a = bq + r$$

and $0 \leq r < |b|$. Use this fact to prove that if x_1 and x_2 are two integers with greatest common divisor d, then there exist integers c_1 and c_2 such that

$$c_1 x_1 + c_2 x_2 = d.$$

b) Define the *Euler totient function* ϕ as follows: for any natural number n, let $\phi(n)$ denote the number of integers $1 \leq i \leq n$ such that i and n are coprime (i.e., their greatest common divisor is equal to one). For example, $\phi(12) = 4$ because the numbers 1, 5, 7, and 11 are coprime to 12 and no other numbers less than 12 are. Use part a) to prove that ϕ is multiplicative: if m and n are natural numbers with $(m, n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$.
c) If p is a prime number and j a natural number, prove that

$$\phi(p^j) = p^{j-1}(p - 1).$$

d) Using previous results and the fundamental theorem of arithmetic, deduce the formula

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

e) As a special case, deduce the fact that we used in class.

3. With a tiny bit of analysis we can prove a nontrivial lower bound for the totient function. Use the explicit formula above to show that for all $\epsilon > 0$, there exists a constant $C_\epsilon > 0$ such that $\phi(n) > C_\epsilon n^{1-\epsilon}$ for all n.

4. By modifying Euclid's proof, show that there exist infinitely many primes that are equal to 2 mod 3 (i.e., equal to $3m + 2$ for some integer m). Also show that there are infinitely many primes that are equal to 3 mod 4. Why doesn't this method work to show that there are infinitely many primes equal to 1 mod 3 or 1 mod 4?