MATH 124, PROBLEM SET 3

Due: 12:00PM, September 26, 2014. ***Late submissions will not be graded.***
Note: Collaboration is permitted and encouraged. We only ask that you write up your solutions independently, and list your collaborators on your problem sets. Hard copies typed in TEX are preferred. Please separate your submissions as indicated below.

For Hirsh Jain

We saw that Euler's totient function $\phi(n)$ plays a role in the RSA cryptosystem.

1.) Recall that $\phi(n)$ is defined as the number of integers $1 \leq m \leq n$ such that $\gcd(m, n) = 1$. Prove that

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

2.) You are Person A, and you want Person B to send you messages via RSA encryption. You choose $p = 47$ and $q = 31$ to be your "large" primes.

(a) What numbers do you share with Person B? There are many valid answers.

(b) As person B, use these numbers (Person A's *public key*) to encode $m = 11$.

In class, we learned about the statement of quadratic reciprocity. We call the symbol $\left(\frac{a}{p}\right)$ the *Legendre symbol*, where for odd prime p,

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } a \equiv 0 \pmod{p} \\ +1 & \text{if } a \text{ is a quadratic residue } (\text{mod } p) \\ -1 & \text{if } a \text{ is a quadratic non-residue } (\text{mod } p). \end{cases}$$

3.) Show that

$$\left(\frac{2}{p}\right) = \begin{cases} +1 & \text{if } p \equiv 1, 7 \pmod{8} \\ -1 & \text{if } p \equiv 3, 5 \pmod{8}. \end{cases}$$

4.) Compute the following Legendre symbols:

(a) $\left(\frac{-23}{83}\right)$

(b) $\left(\frac{119}{139}\right)$

For Julian Salazar

Last time, we defined arithmetic functions as functions $\mathbb{Z}^+ \to \mathbb{C}$. Define the *Dirichlet convolution* of two arithmetic functions as

$$(f * g)(n) := \sum_{d|n} f(d) g\left(\frac{n}{d}\right).$$

It turns out that this operation turns the arithmetic functions into a *commutative ring*.

5.) Let f, g, h be arbitrary arithmetic functions.

(a) Briefly explain why this operation is commutative, i.e., $f * g = g * f$.

(b) Define id as the arithmetic function such that $id(1) = 1$ and $id(n) = 0$ for $n > 1$. Verify that it is the identity, i.e., $f * id = f$.

(c) Verify associativity: $f * (g * h) = (f * g) * h$.

We now explore the Möbius function, which holds a distinguished place in the arithmetic functions.

6.) A number is *square-free* if it is not divisible by a perfect square greater than 1. Define the *Möbius function* μ as

$$\mu(n) = \begin{cases} 0 & n \text{ is not square-free} \\ -1 & n \text{ is square-free and has an odd number of prime factors} \\ +1 & n \text{ is square-free and has an even number of prime factors.} \end{cases}$$

(a) Prove that μ is multiplicative, i.e., that $\mu(ab) = \mu(a)\mu(b)$ for $\gcd(a, b) = 1$.

(b) Define the 'conventional identity' I as $I(n) = 1$ for all n. Prove that

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & n = 1 \\ 0 & n > 1, \end{cases}$$

i.e., $I * \mu = id$ (we say I and μ are *inverses*).

(c) Let $F(n) = \sum_{d|n} f(d)$, i.e., $F = f * I$. Hence, prove the *Möbius inversion theorem*:

$$f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right).$$

(d) Use this theorem and Question 1 to deduce

$$\phi(n) = n \sum_{d|n} \frac{\mu(d)}{d}.$$