MATH 124, PROBLEM SET 2

Due: 12:00PM, September 19, 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 say that an arithmetic function $f : \mathbb{N} \to \mathbb{C}$ is a *multiplicative function* if $f(mn) = f(m)f(n)$ when $(m, n) = 1$ (GCD is often denoted by parentheses only).

1.) Show that for $n = \prod_{i=1}^{k} p_i^{e_i}$, *Euler's totient function* $\phi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$, and conclude that $\phi(n)$ is multiplicative.

2.) Let ψ be a multiplicative function. Prove that $\Psi(n) = \sum_{d|n} \psi(d)$ is also multiplicative, and conclude that the sum-of-divisors $\sigma(n)$ and the number-of-divisors $d(n)$ are multiplicative.

A *primitive root mod* n is a number for which every a such that $(a, n) = 1$ is congruent to a power of the primitive root (we say that a primitive root *generates* the ring of units of n).

3.) Using the fact that 2 is a primitive root of 29:
(a) Solve $x^4 \equiv 1 \pmod{29}$.
(b) Solve $1 + x + x^2 + x^3 \equiv 0 \pmod{29}$.

In class, we learned about Fermat's little theorem and its generalization due to Euler.

4.) Prove Euler's theorem, i.e., $a^{\phi(n)} \equiv 1 \pmod{n}$ for all a such that $(a, n) = 1$.

For Julian Salazar

Euler's and Fermat's results lead to very concrete numerical statements:

5.) For which numbers $n > 1$ does n^{40} not end in ...01?

6.) Prove that $19 \mid 2^{2^{6k+2}} + 3$ for all non-negative k (recall that a^{b^c} is evaluated as $a^{(b^c)}$).

Confirm your comfort with congruence classes:

7.) Let $\{a_i\}$ be a set of n integers. For $s > n$, show there exists c such that $s \nmid a_i + c$ for all a_i.

8.) Let $b, n \geq 1$. Show that the sequence

$$b, b^b, b^{b^b}, b^{b^{b^b}}, \ldots \pmod{n}$$

(i.e., the sequence $a_1 = b, a_{i+1} = b^{a_i}$ modulo n) is eventually constant.

(**Hint:** Proceed by contradiction. For any b, suppose there exists n where the sequence never becomes constant, and consider the smallest such n.)