MATH 4400
HOMEWORK 3
DUE 2/12/08

Instructions: Math 6400 students should do all the problems. Math 4400 students should do Problems 1-5.

Problem 1: Let $\lambda(n) = (-1)^{a_1+\ldots+a_k}$, where $n = p_1^{a_1} \cdots p_k^{a_k}$. What is

$$\sum_{d|n} \lambda(d)?$$

If we define $f(n) = \sum_{d|n} \lambda(d)$, show that $f(n)$ is not completely multiplicative (but that it is multiplicative).

Problem 2: (a) Recall that $\mathbf{1}(n) = 1$ for all n. What is $\mathbf{1} \star \mathbf{1}$?

(b) Show that

$$\sigma_1(n) = \sum_{d|n} \varphi(d)\sigma_0\left(\frac{n}{d}\right).$$

(Hint: use part (a), and convolution.)

Problem 3: (a) For which n is $\sigma_0(n)$ odd?

(b) A prison with 1000 inmates is overcrowded. The warden decides to let certain prisoners go free, via the following scheme:

The cells, one for each prisoner, are arranged in a circular fashion, with a small gap between cell 1 and 1000. In Step n, a guard goes to every nth cell (starting with cell n and ending with the cell numbered with the largest multiple of n less than or equal to 1000) and changes its state–if it's locked, he unlocks it; if it's unlocked, he locks it.

The guards start by locking every cell. No prisoner is allowed to leave until the process is completely finished. The guards first execute Step 1, then Step 2, then Step 3, and so on all the way through Step 1000 (which changes the state of cell 1000 but leaves the other ones unchanged; in fact, Steps 501 through 1000 only change the state of one cell each). Whichever prisoner's cell is unlocked at the end of the process is free to go.

So which prisoners go free? (Hint: use part (a).)

Problem 4: (a) Show that if f is a multiplicative function such that $f(1) \neq 0$, there exists a function g such that $f \star g = \delta$. (Recall that $\delta(n) = 1$ if $n = 1$ and 0 otherwise.) Hint: define g inductively; if $g(k)$ is defined for all $k \leq n$, find a formula for $g(n)$ that we can use to define it.

(b) Show that if f and $f \star g$ are multiplicative, then g is multiplicative. Deduce that if f is multiplicative, then the function g defined in part (a) is as well.

Problem 5: Let D_n be the set of positive divisors of n. Show that if a and b are relatively prime, the natural map

$$\psi\colon D_a \times D_b \to D_{ab}$$

defined by $\psi(d, e) = de$ is a bijection.

Problem 6: Let S_n be the set of solutions in $\mathbb{Z}/n\mathbb{Z}$ to the congruence $x^2 \equiv 1 \bmod n$. For the rest of the problem, let p be an odd prime. Of course $S_2 = \{1\}$ and $S_p = \{\pm 1\}$.

(a) Show that $S_{p^k} = \{\pm 1\}$. (Hint: induction on k.)

(b) Show that $S_{2p^k} = \{\pm 1\}$.

(c) Show that if $\gcd(a, b) = 1$, then the bijection $(\mathbb{Z}/ab\mathbb{Z})^* \to (\mathbb{Z}/a\mathbb{Z})^* \times (\mathbb{Z}/b\mathbb{Z})^*$ restricts to a bijection $S_{ab} \to S_a \times S_b$.

(d) Show that $S_4 = \{\pm 1\}$ and $S_{2^k} = \{\pm 1, \pm 1 + 2^{k-1}\}$ for $k \geq 3$. (Induction again.)

(e) Now for the punchline: Show that the product

$$\prod_{\substack{1 \leq x \leq m \\ \gcd(x,m)=1}} x = \prod_{x \in S_m} x,$$

and deduce a formula for this product in terms of the prime factorization of m. (This might be a little tough, but the ingredients are all there.)

Problem 7: This exercise is devoted to the proof of the *Erdös-Ginzburg-Ziv Theorem*: Let $a_1, \ldots, a_{2n-1}$ be integers. Then there is some subset I of $\{1, \ldots, 2n-1\}$ such that $\sum_{i \in I} a_i$ is divisible by n.

(a) First, note that the $2n - 1$ is sharp: find a sequence of $2n - 2$ integers such that no subsequence of n of them has a sum divisible by n. (Hint: use 0's and 1's.)

(b) Now let p be a prime. We will prove the theorem for $n = p$ next, as follows: Define, in $\mathbb{F}_p[x_1, \ldots, x_{2p-1}]$,

$$f(x_1, \ldots, x_{2p-1}) = x_1^{p-1} + \cdots + x_{2p-1}^{p-1}, \quad g(x_1, \ldots, x_{2p-1}) = a_1 x_1^{p-1} + \cdots + a_{2p-1} x_{2p-1}^{p-1}.$$

Show that f and g have a nontrivial common zero.

(c) Explain why the nontrivial common zero you found in part (b) proves the theorem for $n = p$.

Now we proceed to prove the theorem for general n by induction: Let $n = mp$ for some prime p, and suppose we have proved the theorem for m.

(d) Show that we can find $2m - 1$ subsets $I_1, \ldots, I_{2m-1}$ of $\{1, \ldots, 2n-1\}$ such that each I_j has p elements, and $b_j = \sum_{i \in I_j} a_i$ is divisible by p.

(e) Now apply the inductive hypothesis to the set $\{b_1/p, \ldots, b_{2m-1}/p\}$. Finish the proof.