Math 437/537 Homework #4

due Friday, October 31, 2003 at the beginning of class

I. Solve Problem 8.5 from the "Cryptography" handout you received in class. Do all of the computations by hand and show your work, with the exception that once you do one modular exponentiation in full detail, you can use mechanical aids for the others if you want and simply quote your answers.

II. Niven, Zuckerman, and Montgomery, Section 4.3, p. 196, #18

III. Recall that $f_\alpha(n) = n^\alpha$ and $\sigma_\alpha(n) = \sum_{d|n} d^\alpha$.

(a) For any fixed real numbers β and γ, find a formula for $f_\beta * f_\gamma$ in terms of the functions f_α and σ_α.

(b) Suppose that f and g are two totally multiplicative functions such that their (value-wise) product is not equal to the "identity function" ι. Prove that $f * g$ is multiplicative but never totally multiplicative. Conclude that none of the functions σ_α are totally multiplicative. (Remark: having their value-wise product equal to ι is in fact equivalent to their Dirichlet convolution being totally multiplicative.)

IV. Determine all Dirichlet characters with period 7; with period 24. (Remember that the values may be complex numbers.)

V. Prove that $\phi(n) + d(n) \leq n + 1$ for all integers n. (Hint: think about the definitions of $\phi(n)$ and $d(n)$.)

VI. Prove that for every number n, there is a number x such that $d(nx) = n$.

VII. The largest perfect number known through the end of the second millennium was $n_{38} = 2^{p-1}(2^p - 1)$, where $p = 6{,}972{,}593$. Determine how many digits n_{38} has, and find the first three digits (on the left).

VIII. For any positive integer n, define $r_1(n)$ to be the number of positive divisors of n that are congruent to 1 (mod 3) and $r_2(n)$ to be the number of positive divisors of n that are congruent to 2 (mod 3). Find, with proof, the smallest positive integer n that is relatively prime to 6 and satisfies $r_1(n) > r_2(n) > 0$.

(continued on back of page)

IX. When n is a positive integer, a *primitive nth root of unity* is a complex number of the form $e^{2\pi ik/n}$ where $(k,n) = 1$. Equivalently, a primitive nth root of unity is a complex number z such that $z^n = 1$ but $z^m \neq 1$ for any $0 < m < n$. Define the nth cyclotomic polynomial $\Phi_n(x)$ to be the polynomial whose roots are precisely the $\phi(n)$ primitive nth roots of unity. For example, $\Phi_6(x) = (x - e^{\pi i/3})(x - e^{5\pi i/3}) = x^2 - x + 1$.

(a) Prove that

$$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}.$$

For example, $\Phi_6(x) = (x-1)^1(x^2-1)^{-1}(x^3-1)^{-1}(x^6-1)^1 = x^2 - x + 1$.

(b) Define the *von Mangoldt Lambda-function*

$$\Lambda(n) = \begin{cases} \ln p, & \text{if } n = p^r \text{ with } p \text{ prime and } r \geq 1, \\ 0, & \text{otherwise.} \end{cases}$$

So for example, $\Lambda(125) = \ln 5$. Prove the two identites

$$\sum_{d|n} \mu(n/d) \ln d = \Lambda(n) \quad \text{and} \quad \sum_{d|n} \mu(d) \ln d = -\Lambda(n).$$

(Hint: $\ln d = \ln n - \ln(n/d)$.)

(c) Evaluate $\Phi_n(1)$ for every $n \geq 1$. (Hint: cancel factors of $x - 1$.)