MAS 4203 Number Theory Name:______________________________

Spring 2005

FINAL EXAM - PART 2

Instructions:

- There are 5 questions. Do only **THREE** questions.
- With THREE complete problems there are 60 total points for PART 2. Full marks for PART 2 will be given for 55 points.
- Write on **ONE** side of the paper.
- Show all necessary working and reasoning to receive full credit.
- Your work needs to be written in a proper and coherent fashion.
- When giving proofs your reasoning should be clear.
- Only scientific calculators are allowed. No programmable or graphing calculators are allowed.
- A table of primes is supplied.
- Throughout this test unless otherwise stated all variables a, b, $\ldots$ are assumed to be integers.

PLEASE GRADE THE FOLLOWING THREE QUESTIONS:

---

1. [8 + 12 = 20 points]

(i) Let $n \in \mathbb{Z}$ with $n > 1$. If $p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m}$ is the prime factorization of n, prove that

$$\phi(n) = p_1^{a_1-1} p_2^{a_2-1} \cdots p_m^{a_m-1} \prod_{i=1}^{m} (p_i - 1).$$

HINT: Use the fact that $\phi(n)$ is multiplicative and that $\phi(p^a) = p^a - p^{a-1}$, when p is prime and a is a positive integer.

(ii) Let $k \in \mathbb{Z}$ with $k > 0$. Prove that the equation $\phi(n) = k$ has at most finitely many solutions.

2. [5 + (3 + 5 + 3 + 4) = 20 points]

(i) Let k be a fixed positive integer. Prove that $f(n) = n^k$ is completely multiplicative.

(ii) Let k be a fixed positive integer. Define

$$\sigma_k(n) = \sum_{d|n} d^k.$$

(In the summation $d > 0$).

(a) Find $\sigma_2(6)$.

(b) Prove that $\sigma_k(n)$ is multiplicative, stating any theorems used in the proof.

(c) Let p be prime and suppose a is a positive integer. Find a formula for $\sigma_k(p^a)$.
HINT: $1 + x + x^2 + \cdots + x^a = \frac{(x^{a+1}-1)}{(x-1)}$, if $x \neq 1$.

(d) Suppose $n > 1$ and let $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ be a prime factorization. Find a formula for $\sigma_k(n)$, giving reasons.

3. [3 + 5 + 12 = 20 points]

(i) Define the Legendre symbol $\left(\frac{a}{p}\right)$.

(ii) Let p be an odd prime. State a theorem about the number of incongruent quadratic residues mod p.

(iii) Let a be a positive integer and let p be an odd prime with $p \nmid a$. Prove that

$$\left(\frac{a}{p}\right) + \left(\frac{2a}{p}\right) + \left(\frac{3a}{p}\right) + \cdots + \left(\frac{(p-1)a}{p}\right) = 0.$$

4. [20 points]

Prove that there are infinitely many primes of the form $4n+1$, where n is a positive integer.

HINT: Assume by way of contradiction that there are only finitely many such primes, say, $p_1, \ldots, p_r$. Let $N = 4(p_1^2 p_2^2 \cdots p_r^2) + 1$ and use the theorem about the Legendre symbol $\left(\frac{-1}{p}\right)$.

5. [20 points] Do either (A) or (B) but NOT BOTH.

(A) Explain what the RSA algorithm is and give a proof of the decoding procedure.

OR

(B) State the a-test for primality and prove that p passes the a-test for any given a, for all primes $p > a$.