MAS 4203 Number Theory Name:________________________

Spring 2010 CODE-Name:________________________

FINAL EXAM

Instructions:

- There are 8 questions. Do only **SIX** questions.
- With SIX complete problems there are 120 total points. Full marks will be given for 120 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.
- A table of primes is supplied.

---

PLEASE GRADE THE FOLLOWING SIX QUESTIONS:

---

For 4 bonus points who are the people in the photos below and what is their connection with Question 8?




**1.** [$10+10=20$ points] Prove the following without assuming the Fundamental Theorem of Arithmetic.

(i) Suppose $a$, $b$, $c \in \mathbb{Z}$ with $(a,b)=(a,c)=1$. Then

$$(a,bc)=1.$$

(ii) Suppose $a$, $b_1$, $b_2$, $\dots$, $b_n \in \mathbb{Z}$ with

$(a,b_1)=(a,b_2)=\cdots=(a,b_n)=1$. Then

$$(a,b_1b_2\cdots b_n)=1.$$

**2.** [$6+7+7=20$ points] Prove or disprove the following statements.

(i) If $a$, $b \in \mathbb{Z}$, $a$, $b>0$, $a^2 \mid b^3$, then $a \mid b$.
(ii) If $a$, $b \in \mathbb{Z}$, $a$, $b>0$, $a^2 \mid b^2$, then $a \mid b$.
(iii) If $a$, $b \in \mathbb{Z}$, $a$, $b>0$, $a^3 \mid b^2$, then $a \mid b$.

**3.** [$4+6+6+4=20$ points] Let $a$, $b$, $c$, $d$, $m \in \mathbb{Z}$ with $m>0$.

(i) Define what it means to write

$$a \equiv b \pmod{m}.$$

(ii) Prove that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ implies that $ac \equiv bd \pmod{m}$.
(iii) Let $p$ be prime. Prove that $a^2 \equiv a \pmod{p}$ implies that $a \equiv 0 \pmod{p}$ or $a \equiv 1 \pmod{p}$.
(iv) Is (iii) still true if $p$ is not prime? If not, give an example.

**4.** [$2+2+2+6+8=20$ points]

(i) State Fermat's Little Theorem.
(ii) State Euler's Theorem.
(iii) Define what it means for a positive integer $n$ to be a pseudoprime.
(iv) Prove that $1729=(7)(13)(19)$ is a pseudoprime.
(v) Let $p$ be a prime number. Prove that if $2^p-1$ is a composite number then $2^p-1$ is a pseudoprime.

(You may assume that $m \mid n$ implies $(2^m-1) \mid (2^n-1)$ provided $m$ and $n$ are positive integers).

**5.** $[2 + 2 + (8 + 8) = 20$ points$]$

(i) Define what it means for an arithmetic function to be *multiplicative.*

(ii) Define what it means for an arithmetic function to be *completely multiplicative.*

(iii) Define an arithmetic function $\rho$ by $\rho(1) = 1$ and $\rho(n) = 2^m$ when $n$ is an integer greater than 1 and where $m$ is the number of distinct prime numbers in the prime factorization of $n$.

(a) Prove that $\rho$ is multiplicative but not completely multiplicative.

(b) Find a formula for the function

$$f(n) = \sum_{d|n} \rho(d),$$

in terms of the prime factorization of $n = p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m}$.

**6.** $[5 + (2 + 4 + 5 + 4) = 20$ 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

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

(As usual, in the summation it assumed that $d > 0$).

(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.

**7.** [$2+2+8+8=20$ points]

(i) Suppose $a$, $m \in \mathbb{Z}$ with $m > 0$. Define what it means for $a$ to be a *quadratic residue modulo* $m$.

(ii) Define the Legendre symbol.

(iii) 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 $p_1$, $p_2$, $\ldots$, $p_r$. Then let

$N = 4p_1^2 p_2^2 \cdots p_r^2$.]

(iv) Find the Legendre symbol $\left(\frac{2819}{4177}\right)$.

**8.** [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.

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