MAS 4203 Number Theory Name:______________________________

Spring 2005

FINAL EXAM - PART 1

Instructions:

- There are 4 questions. Do only **THREE** questions.
- With THREE complete problems there are 60 total points for PART 1. Full marks for PART 1 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. [$3 + 5 + 12 = 20$ points]

(i) Let a, $b \in \mathbb{Z}$. Define $a \mid b$.

(ii) Let a, b, $c \in \mathbb{Z}$. Prove that if $a \mid b$ and $b \mid c$ then $a \mid c$.

(iii) Let a, b, $c \in \mathbb{Z}$ with $(a, b) = 1$. Prove (without assuming the Fundamental Theorem of Arithmetic) that if $a \mid bc$ then $a \mid c$.

HINT: Since $(a, b) = 1$ there are integers x, y such that $ax + by = 1$.

2. [$5 + 15 = 20$ points]

(i) Let a, $b \in \mathbb{Z}$. Prove that if a and b are expressible in the form $6n + 1$, where n is an integer, then ab is also expressible in that form.

(ii) Prove that there are infinitely many prime numbers of the form $6n + 5$, where n is an integer.

HINT: Assume by way of contradiction that there are only finitely many such primes, say, $p_0 = 5$, p_1, ..., p_r. Let $N = 6(p_1 p_2 \cdots p_r) + 5$.

3. [$3 + 7 + 3 + 7 = 20$ points]

(i) Define *pseudoprime*.

(ii) Suppose that m and n are positive integers and $m \mid n$. Prove that $(2^m - 1) \mid (2^n - 1)$.

HINT: $(x^d - 1) = (x - 1)(x^{d-1} + x^{d-2} + \cdots x + 1)$.

(iii) State Fermat's Little Theorem.

(iv) Prove that $2^{11} - 1 = 2047 = (23)(89)$ is a pseudprime.

HINT: Use parts (ii),(iii).

4. [$3 + 3 + 14 = 20$ points]

(i) State Euler's Theorem.

(ii) Define the term *reduced residue system* mod m.

(iii) Let m be a positive integer $m > 2$. If $\{r_1, r_2, \ldots, r_{\phi(m)}\}$ is reduced residue system mod m, prove that

$$r_1 + r_2 + \cdots + r_{\phi(m)} \equiv 0 \pmod{m}.$$

HINT: First prove that if $(a, m) = 1$ then $(m - a, m) = 1$.