MAS 4203 - SPRING 2010 TEST 1

2 BONUS PTS: Who is this guy? State his famous Theorem.

FRIDAY, FEBRUARY 5 Name: ____________________

Instructions: Answer all questions. Show all necessary working and reasoning. Your work should be written in a proper and coherent fashion, and in a way that any student in the class can follow your work. When giving proofs your reasoning should be clear. Only scientific calculators are allowed. 50 points total.

1. [$2 + 4 = 6$ pts]

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

(b) Suppose a, $b \in \mathbb{Z}$. Prove that if $3 \mid a$ and $4 \mid b$ then $12 \mid (8a - 9b)$.

2. [$2 + 3 + 5 = 10$ pts]

(a) Suppose a and b are integers that are not both zero. Define (a, b).

(b) Complete the following

Proposition. Let a, $b \in \mathbb{Z}$ and suppose that a and b are not both zero. Then

$$(a, b) = \min\{\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\}.$$

(c) Suppose a, b, $c \in \mathbb{Z}$ with $(a, b) = 1$. Prove that if $a \mid c$ and $b \mid c$, then $ab \mid c$ using the Proposition in (b) (and NOT the Fundamental Theorem of Arithmetic).

3. [$2 + 6 = 8$ pts]

(a) Define the term *prime*.

(b) Prove or disprove the following statement.

If $a \in \mathbb{Z}$, $a > 0$, p is prime, and $p^7 \mid a^3$, then $p^3 \mid a$.

[Hint. Write the prime factorization of $a = p^{e_0} p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ where each $e_i \geq 0$.]

4. [$3 + 3 + 6 = 12$ pts]

(a) Use the Euclidean algorithm of compute $(1340, 1274)$.

(b) Hence find integers x and y such that

$$1340x + 1274y = (1340, 1274).$$

(d) Suppose a, b are integers not both zero, let $d = (a, b)$ and suppose $c \in \mathbb{Z}$. Prove that there are integers x, y such that

$$ax + by = c$$

if and only if $d \mid c$.

5. [$2+5+5+2=14$ pts]

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 $a^2 \equiv b^2 \pmod{p}$ implies that $a \equiv \pm b \pmod{p}$.

(iv) Is (iii) still true if p is not prime? If not, give an example.