Math 3613
FIRST EXAM
9:30 – 10:20 , February 18, 2008

Name:_____

You must write your answers in complete sentences and full detail to receive full credit.

1. Definitions and Axioms (5 pts each)
(a) What is the **Well-Ordering Axiom** for the set $\mathbb{N}$ of non-negative integers?

(b). State the **Division Algorithm** theorem.

(c) What is the **greatest common divisor** $GCD\,(a, b)$ of two integers a and b. Is $GCD(0, 0)$ defined? Why not?

(d) What is a **prime number**?

2.
(a) (5 pts) Show that the function $f : \mathbb{R}^2 \to \mathbb{R}; f(x, y) = xy$ is surjective (i.e. onto).

(b) Show that the function $g : \mathbb{R} \to \mathbb{R}^2; f(x) = [x, x]$ is injection (i.e. one-to-one).

3. (10 pts) Use mathematical induction to prove the following

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2 \qquad ; \qquad \forall n \in \mathbb{Z}_{\geq 1}$$

4. (10 pts) Prove that if $a, b, u, v \in \mathbb{Z}$ are such that $au + bv = 1$, then $GCD(a, b) = 1$.

5. (10 pts) Let p be prime number. Prove that for any integer a either $GCD(p, a) = 1$ or $p|a$.

6. (5 pts) Use the Euclidean algorithm to compute $GCD(42, 144)$.

7. (10 pts) Let p be an integer $\neq 0, \pm 1$ with the following property: if $p \mid (ab)$ then $p \mid a$ or $p \mid b$. Prove that p is prime (without using Theorem 7).

8. (10 pts) Prove that if p is prime and $p|a^n$, then $p^n|a^n$.

9. (10 pts) Use the Fundamental Theorem of Arithmetic to prove that there are no nonzero integers a, b for which $a^2 = 2b^2$.

Lemmas, Propositions, Theorems, and Corollaries

PROPOSITION 1. *If $a \mid b$ then $|a| \leq |b|$.*

THEOREM 2 (The Division Algorithm). *(see Problem 1(b))*

THEOREM 3. *Let a and b be integers, not both zero, and let $d = GCD(a, b)$. Then there exists (not necessarily unique) integers u and v such that*

$$d = au + bv \quad .$$

COROLLARY 4. *Let a and b be integers, not both zero, and let d be a positive integer. Then $d = GCD(a, b)$ if and only if d satisfies*

(i) $d \mid a \quad$ *and* $\quad d \mid b$
(ii) *if $c \mid a$ and $c \mid b$, then $c \mid d$*

THEOREM 5. *If $a \mid (bc)$ and $GCD(a, b) = 1$, then $a \mid c$.*

LEMMA 6. *If $a, b, q, r \in \mathbb{Z}$ and $a = bq + r$, then*

$$GCD(a, b) = GCD(b, r) \quad .$$

THEOREM 7. *Let p be an integer with $p \neq 0, \pm 1$. Then p is prime if and only if p has this property:*

$$p \mid bc \quad \Rightarrow \quad p \mid b \quad or \quad p \mid c \quad .$$

COROLLARY 8. *If p is prime and $p \mid a_1 a_2 \cdots a_n$, then p divides at least one of the a_i.*

THEOREM 9. *Every integer n except $0, \pm 1$ is the product of primes*

THEOREM 10. *(THE FUNDAMENTAL THEOREM OF ARITHMETIC) Every integer n except $0, \pm 1$ is a product of primes. This prime factorization is unique in the following sense: If*

$$n = p_1 p_2 \cdots p_r \qquad and \qquad n = q_1 q_2 \cdots q_s$$

with each p_i,q_j prime, then $r = s$ (that is the number of factors is the same) and after reordering and relabeling the q_j's

$$\begin{aligned} p_1 &= \pm q_1 \\ p_2 &= \pm q_2 \\ &\vdots \\ p_r &= \pm q_r \quad . \end{aligned}$$

COROLLARY 11. *Every integer $n > 1$ can be written in one and only one way as*

$$n = (p_1)^{s_1} (p_2)^{s_2} \cdots (p_r)^{s_r}$$

where the s_i are positive integers and the p_i are positive prime integers such that

$$p_1 < p_2 < \cdots < p_r \quad .$$