LECTURE 10

Review Session for First Examination

1. Techniques of Proof

- Contrapositive Method
- Proof by Contradiction
- Proof by Induction

2. Definitions (things to be memorized)

- **Well Ordering Axiom:** Every non-empty subset of $\mathbb{N}$ has a least element.
- **Even and Odd Integers:** an integer z is even if $z = 2k$ for some integer k; z is odd if $z = 2k + 1$ for some integer k.
- **surjective function:** a function $f : A \to B$ is surjective if

$$b \in B \quad \Longrightarrow \quad b = f(a) \text{ for some } a \in A$$

- **injective funtion:** a function $f : A \to B$ is injective if

$$f(x) = f(x') \quad \Longrightarrow \quad x = x'$$

- **bijective function:** a function $f : A \to B$ is bijective if it is both injective and surjective.
- **the Division Algorithm:** For any $a, b \in \mathbb{Z}$, $b \neq 0$, there exists unique integers p, q such that
  (i) $a = bq + r$
  (ii) $0 \leq r < b$
- **Greatest Common Divisor:** The greatest common divisor, $GCD(a, b)$ of two integers a, b not both zero is the unique integer d such that
  - $d|a$ and $d|b$
  - If $c|a$ and $c|b$ then $c \leq d$
- **relatively prime:**Two integers not both zero are relatively prime if $GCD(a, b) = 1$.
- **prime number:** An integer $p \neq 0, \pm 1$ is said to be prime if its only factors are $\{\pm 1, \pm p\}$.

3. Sets and Functions

- Sets - See HW problems
- Functions: 1:1, onto, and bijective functions

4. Chapter 1.

THEOREM 10.1. *(THE DIVISION ALGORITHM) Let a, b be integers with $b > 0$. Then there exists unique integers q and r such that*

$$\begin{array}{ll} (i) & a = bq + r \\ (ii) & 0 \leq r < b \quad . \end{array}$$

COROLLARY 10.2. *Let a, b be integers with $b \neq 0$. Then there exists unique integers q and r such that*

$$\begin{array}{ll} (i) & a = bq + r \\ (ii) & 0 \leq r < |b| \quad . \end{array}$$

THEOREM 10.3. *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*

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

N.B. The converse of this theorem is not true.

COROLLARY 10.4. *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*

$$\begin{array}{ll} (i) & d \mid a \quad \textit{and} \quad d \mid b \\ (ii) & \textit{if } c \mid a \textit{ and } c \mid b, \textit{ then } c \mid d \quad . \end{array}$$

THEOREM 10.5. *If $a \mid (bc)$ and $GCD(a, b) = 1$, then $a \mid c$.*

LEMMA 10.6. *If $a, b, q, r \in \mathbb{Z}$ and $a = bq + r$, then*

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

THEOREM 10.7. *Let p be an integer with $p \neq 0, \pm 1$. Then p is prime if and only if p has this property:*

$$p \mid bc \quad \Rightarrow \quad p \mid b \quad \textit{or} \quad p \mid c \quad .$$

COROLLARY 10.8. *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 10.9. *Every integer n except $0, \pm 1$ is the product of primes*

THEOREM 10.10. *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*

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

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

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

COROLLARY 10.11. *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

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