Collected Definitions for Exam #3

This is the ‘official’ collection of need-to-know definitions for Exam #1. I can’t recall the last time I didn’t ask a definition question on an exam. To help you better prepare yourself for definition questions, I’ve assembled this list. My pledge to you: If I ask you for a definition on the exam, the term will come from this list. Note that this is not a complete list of the definitions given in class. You should know the others, too, but I won’t specifically ask you for their definitions on the exam.

Once in a while a student will express disappointment that I ask definition questions on exams. My justification is that I think it’s important for you to know what the core terms mean so that you can use them correctly and effectively. At the same time, I don’t require that you memorize the exact wording of the definitions you see here. If you provide a definition in your own words that captures all of the detail found here, without adding anything incorrect, that’s fine.

**Topic 9: Functions**

- A function from set X to set Y, denoted \( f : X \to Y \), is a relation from X to Y. If \( (x, y) \in f \), then y is the only value returned from \( f(x) \). Further, \( f(x) \) is defined \( \forall x \in X \).

- For each of the following, let \( f : X \to Y \) be a function, and assume \( f(n) = p \).
  - X is the domain of f; Y is the codomain of f.
  - f maps X to Y.
  - p is the image of n; n is the pre-image of p.
  - The range of f is the set of all images of elements of X. (Note that the range need not equal the codomain.)

- The floor of \( n \), denoted \( \lfloor n \rfloor \), is the largest integer \( \leq n \).

- The ceiling of a value \( m \), denoted \( \lceil m \rceil \), is the smallest integer \( \geq m \).

- A function \( f : X \to Y \) is injective (a.k.a. one-to-one) if, for each \( y \in Y \), \( f(x) = y \) for at least one member of X.

- A function \( f : X \to Y \) is surjective (a.k.a. onto) if \( f \)’s range is Y (the range = the codomain).

- A bijective function (a.k.a. a one-to-one correspondence) is both injective and surjective.

- The inverse of a bijective function \( f \), denoted \( f^{-1} \), is the relation \( \{(y, x) \mid (x, y) \in f\} \).

- Let \( f : Y \to Z \) and \( g : X \to Y \). The composition of \( f \) and \( g \), denoted \( f \circ g \), is the function \( h = f(g(x)) \), where \( h : X \to Z \).

- A function \( f : X \times Y \to Z \) (or \( f(x, y) = z \)) is a binary function.

**Topic 10: Properties of Integers**

- Let \( i \) and \( j \) be positive integers. \( j \) is a factor of \( i \) when \( i \% j = 0 \).

- A positive integer \( p \) is prime if \( p \geq 2 \) and the only factors of \( p \) are 1 and \( p \).

- A positive integer \( p \) is composite if \( p \geq 2 \) and \( p \) is not prime.

- Let \( x \) and \( y \) be integers such that \( x \neq 0 \) and \( y \neq 0 \). The Greatest Common Divisor (GCD) of \( x \) and \( y \) is the largest integer \( i \) such that \( i \mid x \) and \( i \mid y \). That is, \( \gcd(x, y) = i \).

- If the GCD of \( a \) and \( b \) is 1, then \( a \) and \( b \) are relatively prime.

- When the members of a set of integers are all relatively prime to one another, they are pairwise relatively prime.

- Let \( x \) and \( y \) be positive integers. The Least Common Multiple (LCM) of \( x \) and \( y \) is the smallest integer \( s \) such that \( x \mid s \) and \( y \mid s \). That is, \( \text{lcm}(x, y) = s \).

(Continued ...)
**Topic 11: Sequences and Strings**

- A **sequence** is the ordered range of a function from a set of integers to a set \( S \).
- In an **arithmetic sequence** (a.k.a. arithmetic progression) \( a \), \( a_{n+1} - a_n \) is constant. This constant is called the common difference of the sequence.
- In a **geometric sequence** (a.k.a. geometric progression) \( g \), \( \frac{a_{n+1}}{a_n} \) is constant. This constant is called the common ratio of the sequence.
- An **increasing** (a.k.a. non-decreasing) sequence \( i \) is ordered such that \( i_n \leq i_{n+1} \).
- A **strictly increasing** sequence \( i \) is ordered such that \( i_n < i_{n+1} \).
- A **non-increasing** (a.k.a. decreasing) sequence \( i \) is ordered such that \( i_n \geq i_{n+1} \).
- A **strictly decreasing** sequence \( i \) is ordered such that \( i_n > i_{n+1} \).
- Sequence \( x \) is a **subsequence** of sequence \( y \) when the elements of \( x \) are found within \( y \) in the same relative order.
- A **string** is a contiguous finite sequence of zero or more elements drawn from a set called the **alphabet**.
- A set is **finite** if there exists a bijective mapping between it and a set of cardinality \( n, n \in \mathbb{Z}^+ \).
- A set is **countably infinite** (a.k.a. denumerably infinite) if there exists a bijective mapping between the set and either \( \mathbb{Z}^+ \) or \( \mathbb{Z}^* \).
- A set is **countable** if it is either finite or countably infinite. If neither, the set is **uncountable**.

**Topic 12: Induction**

- The First Principle of Mathematical Induction: if (i) \( P(a) \) is true for the starting point \( a \in \mathbb{Z}^+ \), **and** (ii) if \( P(k) \) is true for any \( k \in \mathbb{Z}^+ \), then \( P(k+1) \) is true, **then** \( P(n) \) is true for all \( n \in \mathbb{Z}^+ \), \( n \geq a \).
- The Second Principle of Mathematical Induction: if (i) \( P(a) \) is true for the starting point \( a \in \mathbb{Z}^+ \), **and** (ii) (for any \( k \in \mathbb{Z}^+ \)) if \( P(j) \) is true for any \( j \in \mathbb{Z}^+ \) such that \( a \leq j \leq k \), then \( P(k+1) \) is true, **then** \( P(n) \) is true for all \( n \in \mathbb{Z}^+ \), \( n \geq a \).

**Topic 13: Counting**

- I present two definitions of the (Generalized) **Pigeonhole Principle**; learn either one (or both!):
  (a) if \( n \) items are placed in \( k \) boxes, then at least one box contains at least \( \lceil \frac{n}{k} \rceil \) items.
  (b) Let \( f : X \rightarrow Y \), where \( |X| = n \) and \( |Y| = k \), and let \( m = \lceil \frac{n}{k} \rceil \). There are at least \( m \) values \((a_1, a_2, \ldots, a_m)\) such that \( f(a_1) = f(a_2) = \ldots = f(a_m) \).

- The **Multiplication Principle** (a.k.a. the **Product Rule**): If there are \( s \) steps in an activity, with \( n_1 \) ways of accomplishing the first step, \( n_2 \) of accomplishing the second, etc., and \( n_s \) ways of accomplishing the last step, then there are \( n_1 \cdot n_2 \cdot \ldots \cdot n_s \) ways to complete all \( s \) steps.

- The **Addition Principle** (a.k.a. the **Sum Rule**): If there are \( t \) tasks, with \( n_1 \) ways of accomplishing the first, \( n_2 \) ways of accomplishing the second, etc., and \( n_t \) ways of accomplishing the last, then there are \( n_1 + n_2 + \ldots + n_t \) ways to complete one of these tasks, assuming that no two tasks interfere with one another.

- The **Principle of Inclusion-Exclusion for Two Sets** says that the cardinality of the union of sets \( M \) and \( N \) is the sum of their individual cardinalities excluding the cardinality of their intersection. That is:
  \[ |M \cup N| = |M| + |N| - |M \cap N| \]

- The **Principle of Inclusion-Exclusion for Three Sets** says that the cardinality of the union of sets \( M, N, \) and \( O \) is the sum of their individual cardinalities excluding the sum of the cardinalities of their pairwise intersections and including the cardinality of their intersection. That is:
  \[ |M \cup N \cup O| = |M| + |N| + |O| - (|M \cap N| + |M \cap O| + |N \cap O|) + |M \cap N \cap O| \]