

Collected Definitions for Exam #3

I can't recall the last time I didn't ask a definition question on an exam. To help you better prepare yourself for such 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.

The definitions are grouped by lecture topic, and should be in an order within each topic that is at least close to the order in which the definitions appeared in class.

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 $i | x$ and $i | y$. That is, $\text{gcd}(x, y) = i$.
- 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 $x | s$ and $y | s$. That is, $\text{lcm}(x, y) = s$.
- If $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$, then a and b are *congruent modulo m* (written $a \equiv b \pmod{m}$) iff $a \% m = b \% m$ (or, iff $m | (a - b)$). (This is just a different phrasing of the definition given in Topic 1. Either is acceptable.)
 - a and b are said to be members of the same *congruence class*.

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 , $\frac{g_{n+1}}{g_n}$ 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 the bijective mapping is to either of the sets \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 *Principle of Mathematical Induction*: To prove that $P(n)$ is true for every positive integer n , we need to show that (1) $P(1)$ is true, **and** (2) if $P(i)$ is true for all $1 \leq i \leq n$, then $P(n + 1)$ is true. (1) is called the *basis step*, and (2) is known as the *inductive step*.
- In *Strong Induction*, $P(i)$ must be true and, for any $k \geq i$, if $P(i) \wedge P(i + 1) \wedge \dots \wedge P(k - 1) \wedge P(k)$ is true, then $P(k + 1)$ is true.
- In *Weak Induction*, $P(i)$ must be true and, for any $k \geq i$, if $P(k)$ is true, then $P(k + 1)$ is true.

Topic 13: Counting

- The (*Generalized*) *Pigeonhole Principle* states that if n items are placed in k boxes, then at least one box contains at least $\lceil \frac{n}{k} \rceil$ items.
[An alternate generalized pigeonhole principle definition, in terms of functions (learn one or the other): 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, \dots, a_m) such that $f(a_1) = f(a_2) = \dots = f(a_m)$.]
- 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 $n_1 \cdot n_2 \cdot \dots \cdot n_s$ 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 $n_1 + n_2 + \dots + n_t$ 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:
 $|M \cup N \cup O| = |M| + |N| + |O| - (|M \cap N| + |M \cap O| + |N \cap O|) + |M \cap N \cap O|$
- An ordering of n distinct elements is called a *permutation*.
- An ordering of an r -element subset of n distinct elements is called an *r -permutation*.
- An *r -combination* of $X = \{x_1, x_2, \dots, x_n\}$ is an r element subset of X , denoted $C(n, r)$ or $\binom{n}{r}$ and read “ n choose r ”.