CSc 144 — Discrete Structures for Computer Science I
(McCann)

Collected Definitions Since Exam #3

Here are the definitions that we've covered since the material for the last midterm exam. I'm not going to re–print all of the definitions for the whole semester — that would be a lot of paper. If you lost a previous exam's definition handout, you can print another from the class web page or D2L.

Topic 11: 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.
- The *prime factorization* of a composite integer p is the expression of p as the product of two or more primes.
- The *Division 'Algorithm':* Let n, s, q, and r be the dividend, divisor, quotient, and remainder, respectively, of an integer division. If $n \in \mathbb{Z}, s \in \mathbb{Z}^+$, and $0 \leq r < s$, then q and r are unique.
- 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, `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 $m \mid (a - b)$). (This is just a different phrasing of the definition given in Topic 1. Either is correct.)

Topic 12: 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 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.*