Compsci 120

Number Theory

Sets of Numbers

$\mathbb{Z}$	Integers
$\mathbb{N}$	Natural Numbers (not 0)
$\mathbb{R}$	Real Numbers
$\mathbb{Q}$	Rational Numbers
$\mathbb{I}$	Irrational Numbers

Even and Odd Numbers

By definition, a number ’n‘ is even if $n = 2k$, $k \in \mathbb{Z}$.

By definition, a number ’n‘ is odd if $n = 2k + 1$, $k \in \mathbb{Z}$.

$\implies$ 0 is neither odd or even.

The sum of any two even numbers is even

Let n and m be two even numbers.

By definition, $n = 2k$, $m = 2l$

Then, $n + m = 2k + 2l = 2(k + l) = 2(\text{another integer})$

The product of any two odd numbers is odd

Let n and m be two odd numbers.

By definition, $n = 2k + 1$, $m = 2l + 1$

Then, $n + m = (2k + 1) \times (2l + 1) = 4kl + 2k + 2l = 2(\text{another integer}) + 1$

Divisibility

For two integers ‘a’ and ‘b’, we say ‘a divides b’ if you can write $b = k \times a$ for some integer k.

FACT 1: 1 and a are always divisors of any integer a.

FACT 2: Any integer is a divisor of 0

FACT 3: If a divides b and b divides c, then a divides c

Prime Numbers

A positive integer ‘p’ is said to be prime if it has only two distinct positive factors 1 and p.

Composite Numbers

A composite number is any positive integer that can be written as the product of two integers ‘a’ and ‘b’ where ‘a’ and ‘b’ are at least 2.

FACT 4: Any positive integer is either prime, composite or 1

Rational Numbers

Any number is said to be a natural number if it can be written as a ratio $\frac{x}{y}$ where x, y are integers and $y \neq 0$. Notice that an irrational number cannot be expressed as a ratio of two integers.

Prime Factorisation

A prime factorisation of a positive integer n is any way to write n as a product of prime numbers. e.g.

$$12 = 2 \times 6$$
$$540 = 2 \times 2 \times 3 \times 3 \times 3 \times 3 \times 5$$

Modulo

Modulo can be considered the ‘remainder operator’. It is represented here with ‘ mod ’ but appears in the text book and elsewhere as ‘%’.

Algorithm

$a \geq n$	subtract n from a until $a < 0$. This is $a \bmod n$
$a < 0$	add n to a until $a \geq 0$. This is $a \bmod n$
$0 \leq a \leq n - 1$	a is $a \bmod n$

Congruence

$$a \bmod n \equiv b \implies a \bmod n = b \bmod n$$

$$a \bmod n = b \bmod n$$

$$\implies a - b = nk, k \in \mathbb{Z}$$

This gives us the operations:

$$\begin{aligned}
&(a + c) \bmod n = (b + d) \bmod n \\
&(ac) \bmod n = (bd) \bmod n \\
&(a^k) \bmod n = (b^k) \bmod n
\end{aligned}$$

Finding the last digit

The last digit of any decimal number a can be found by a mod 10 for example,

> Finding the last digit of 213047^{129314}
> 213047^{129314} mod 10
> Observe, 213047 mod 10 = 7
> $\implies 213047^{129314} \bmod 10 = 7^{129314} \bmod 10$ (from eqn. 3)
> Notice, $(7^2) \bmod 10 = 49 \bmod 10 = 9$
> Notice, $(7^2 \cdot 7^2) \bmod 10 = 81 \bmod 10 = 1$
> So for any k, $(7^{4k}) \bmod 10 = (7^2 \cdot 7^{4k}) \bmod 10 = 1$
> Because $129314 = 129300 + 12 + 2$
> We have $(7^{129314}) \bmod 10 = 9$
> So the last character is 9

Strings

Alphabets

An alphabet is just a collection of symbols. It is denoted Σ. e.g. the binary alphabet will be $\Sigma = \{0, 1\}$.

Definitions

A string s over an alphabet Σ is just a sequence of elements from Σ. An empty string is denoted by λ. The length of any string is the number of characters in that string. e.g. the length of 'Alex' is 4. Concatenation of strings is like the addition of strings. You just 'glue' them together.

Prefix, Suffix, Substring

Given a string 's' and a string 't' we say s is a prefix of t if t=su, we say s is a suffix of t if t=us, we say s is a substring of t if we can write t=usv

Sets

A set is simply defined as a collection of well defined objects e.g. a collection of strings = $\{\text{cats}, \text{dogs}, \text{cats}\}$. A set does not have to contain anything. An empty set is represented by Φ. Order does not matter within a set and in CS120 we cannot have duplicate values.

Set Operators

$a \in b$	An item a is 'in' a set b
$a \subseteq b$	Every element of a is in b
$a \cup b$	The set of all the elements in a and b
$a \cap b$	The set of elements that are in both a and b
$a \setminus b$	The set of elements in a that are not in b
$a = b$	Every element of a is in b

You can generate sets using a property

$$\{x \mid \text{property of x}\}$$

Combinatorics and Probability

Ordered means that order matters e.g. a pattern of letters. With repetitions means that repeated values will have separate outcomes. Remember that it is, "given n items choose k".

Combinatorics

Ordered Choice WITH Repetitions	n^k
Unordered Choice WITH Repetitions	$\frac{(k-1+n)!}{k!(n+k1)!} = \binom{n+k-1}{k}$
Ordered Choice without Repetitions	$\frac{n!}{k!}$
Unordered Choice without Repetitions	$\frac{n!}{k!(n-k)!} = \binom{n}{k}$

Probability

The probability of an event occuring is given by

$$P(E) = \frac{\text{the no. of ways E can happen}}{\text{the total no. of outcomes}}$$

Functions

There are some requirements for a function to ‘exist’ mathematically.

- Every input should have exactly one output
- For a function to exist the domain of g must equal the co-domain of f

Domain, Co-domain, Range

The domain is the collection of all possible input values. Conversely, the co-domain is the collection of elements describing the output. Range is the set of all values in the co-domain that the function actually send values to.

$$\text{Range } = \{b \in \text{co-domain} \mid f(a) = b \text{ for some a in the domain}\}$$

Function Composition

If $f : B \to C$ and $g : A \to B$ then the function composition is defined by

$$f \circ g(x) = f(g(x))$$

Limits

$$\lim_{n\to\infty} \frac{1}{n} = 0$$
$$\lim_{n\to\infty} n = +\infty$$
$$\lim_{n\to\infty} \log_2(n) = +\infty$$

Growth

You can determine which functions grow faster by evaluating the limit

$$\lim_{n\to\infty} \frac{|f(n)|}{|g(n)|}$$

If the limit evaluates to $+\infty$ then $f(n)$ grows faster than $g(n)$

Heuristics

$$n << n^2 << n^3 << n^4 << \ldots$$

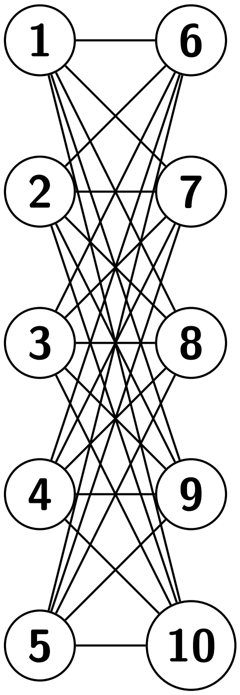
$$2^n << 3^n << 4^n << 5^n << \ldots$$

$$\text{Constants} << \text{Logarithms} << \text{Polynomials} << \text{Exponentials}$$

Graphs

In cs120, graphs are simple undirected loopless graphs. A simple undirected loopless graph G consists of two things: a set V of vertices which represents the objects, abd another set E of edges which corresponds to connections between the objects.

A complete bipartite graph $K_{5,5}$



The Degree Sum Formula

The degree of a vertex is the number of edges in this vertex. Denoted deg(x). If G is a graph, then the sum of the degrees of the vertices in G is always twice the number of edges in G.

Trees

A tree is a graph T that is connect and has no cycle graph C_n as a subgraph.

Proofs

Direct Proof

A direct proof is when you take simple known facts, axioms and theorems and work them algebraically until you prove the thing you are looking for is true or false. For statements like 'p implies q' or 'if p then q' we can assume p is true and use our known facts/algebra to prove q.

Proof by Contradiction

Say we have a fact p we want to prove is true. We assume p is false then reach a contradiction so in fact p must be true. Say we want to prove p implies q. Then we can assume p is true, but q is false. Then we reach a contradiction.

Proof by Cases

Say we want to prove a statement in the form 'for all numbers/graphs/etc' but the 'numbers/graphs/etc' can be thought of as several families so we deal with each separately in different 'cases'. Eg. we could consider odd & even numbers.

Proof by Construction

Proof by construction is a bit of an odd ball but can be brought down to simply producing an example of what you are trying to prove. If the statement is of the form "there exists x" it is a valid proof to just produce a numerical/physical example otherwise you must work in general i.e ”a graph with n vertices”.

Proof by Induction