1 Overview

Right off the bat we need to discuss the difference between discrete and continuous. A Discrete unit is indivisible, and we count discrete things. This gives us number such as the set of Natural numbers, $\mathbb{N} = \{0, 1, 2, 3, 4, \cdots\}$.

On the flipside, we measure with continuous units. This gives us fractions and non-negative real numbers.

We also have discrete structures which include sets, sequences, networks, matrices, permutations, and real-world data.

These structures are what the class will focus on.

Theorem 1 (Naive Set Theory). *A set is an unordered collection of objects.*

Let S be a set. If there are exactly n distinct objects in S (where n is a non-negative integer), then we say the cardinality of S is n, i.e. $|S| = n$.[1]

If x is an element of S, we say $x \in S$.

Let A and B be sets, the Cartesian product of A and B, $A \times B$, is the set of all ordered pairs (a, b) where $a \in A$ and $b \in B$, i.e. $A \times B = \{(a, b)|a \in A, b \in B\}$.

2 Principles of Counting

Theorem 2 (Multiplicative Principle of Counting[2]). *If task 1 can be done in n_1 ways, and task 2 can be done in n_2 ways, then the total number of ways to do one task **and** then the other is $n_1 \cdot n_2$.*

Theorem 3 (Additive Principle of Counting). *If task 1 can be done in n_1 ways, and task 2 can be done in n_2 ways, then the total number of ways to do one task **or** then the other is $n_1 + n_2$.*

2 .1 Pigeon-Hole Principle

Theorem 4 (The Pigeon-Hole Principle). *If n pigeons fly into k pigeon holes, and $k < n$, then some pigeon hole must contain at least 2 pigeons.*

If f is a function from a finite set x to a finite set y, and if $|x| > |y|$, then $f(x_1) = f(x_2)$ for some $x_1, x_2 \in x$ such that $x_1 \neq x_2$

Theorem 5 (The Extended Pigeon-Hole Principle). *If N pigeons are assigned to $K < N$ pigeon holes, then one of the pigeon holes must contain at least $\lfloor \frac{N-1}{K} \rfloor + 1$ or $\lceil \frac{N}{K} \rceil$ pigeons.*

[1] Cardinality is the number of elements in S. Ordinality is for ordering infinities.
[2] Product Rule

2 .2 Permutations and Combinations

Theorem 6 (Permutations). *A permutation is any linear arrangement of distinct objects in which order matters.*

Any ordered arrangement of r objects is called an r-permutation.

The number of ordered arrangements (permutations) of r objects from n objects $(0 \leq r \leq n)$ is

$$P(n, r) = \frac{n!}{(n-r)!} = P^n_r$$

In general, if there are n objects, with n_1 of type 1, n_2 of type 2, ..., to type r, then there are $\frac{n!}{n_1! n_2! \cdots n_r!}$ total permutations of the n objects.

Theorem 7. *A combinations is a sequence of objects where order does not matter. The size of a combination is the number of different elements that compose it.*

The number of combinations of size r using n different objects is expressed as

$$C(n, r) = \binom{n}{r} = C^n_r = \frac{n!}{r!(n-r)!} = \frac{P(n, r)}{r!}$$

Example 2 .1. How many different committees can be formed consisting of one chair, one vice-chair, and one treasurer from a pool of 100 people?

↪ The answer is **not** $C(100, 5)$, but rather $\frac{100!}{97!}$

Example 2 .2. Same question as before, but suppose we have one chair, one vice-chair, and two treasurers.

↪ $100 \cdot 99 \cdot \binom{98}{2}$

Example 2 .3. How many ways are there to arrange the letters in "TALLAHASSEE" without having adjacent "A"'s?

↪ First off, disregard all of the "A"'s, we'll insert those later.

$$\text{TLLHSSEE} \to \frac{8!}{2!2!2!}$$

Next, determine the possible slots for the "A"'s to go, which are in between each of the letters, as well as at the beginning and end. This leads to a total of

$$\left(\frac{8!}{2!2!2!}\right) \cdot \binom{9}{3}$$

2 .3 Binomial Coefficients

Theorem 8 (The Binomial Theorem). *Let x and y be variables, and let n be a non-negative integer, then*

$$(x + y)^n = \sum_{j=0}^{\infty} \binom{n}{j} x^{n-j} y^j$$

2 .4 Powersets

The powerset of a set is the set of all its possible subsets.

Example 2 .4. How many subsets does the set $\{1, 2, 3, 4, \cdots, n\}$ have?

↪ Let's count sets of size

- $0 \Rightarrow \binom{n}{0}$
- $1 \Rightarrow \binom{n}{1}$
- $n \Rightarrow \binom{n}{n}$

So we have a total of

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = (1 + 1)^n = 2^n (\text{Binomial Theorem})$$

2 .5 Counting Integer Solutions

The number of different, non-negative integer solutions $(y_1, y_2, \cdots, y_k)$ of the equation:

$$y_1 + y_2 + \cdots + y_k = m$$

is

$$\binom{m + k - 1}{k - 1}$$

Think of this as counting the number of ways to distribute m objects to k baskets.

2 .6 Linear Recursion

Theorem 9. *A linear recursion with constant coefficients is a recurrence relation of the form*

$$a_n = c_1 a + n - 1 + c_2 a_{n-2} + \cdots + c_k a_{n-k} + F(n)$$

where $n \geq k$, $F(n)$ is a function of n only, $c_i \in \mathbb{R}, i = 1, 2, \cdots, k$, and $c_k \neq 0$.

If $F(n) = 0$ we call this a homogeneous linear recursion of degree k with constant coefficients.

Theorem 10. *Assume a sequence $\{a_n\}$ satisfies some degree k linear recursion.*[3]

$$a_n = c_1 a_{n-1} + c_2 a_{n-2}, n \geq 2$$

Let r_1 and $_2$ be the roots of the characteristic equation

$$r^2 = c_1 r + c_2$$

[1] *If $r_1 = r_2$, then $\exists\{\alpha_1, \alpha_2 \in \mathbb{R}|a_n = (\alpha_1 + \alpha_2 n) r_1^n\}$*
[2] *If $r_1 \neq r_2$ then $\exists\{\alpha_1, \alpha_2 \in \mathbb{R}|a_n = \alpha_1 r_1^n + \alpha_2 r_2^n\}$*

Example 2 .5. Solve $a_n + a_{n-1} - 6a_{n-2} = 0, n \geq 2$

↪ Assume $a_n = cr^n$. This comes from looking at the simplest possible case: $a_n = ra_{n-1}, n \geq 1, a_0 = c \to a_n = cr^n$

$$\hookrightarrow cr^n + cr^{n-1} - 6cr^{n-2} = 0 \to 1 + r^{-1} - 6r^{-2} = 0$$
$$\hookrightarrow r^2 + r - 6 = 0 \to r_{1,2} = 2, -3$$

So $a_n = c_1 2^n$ and $b_n = c_2(-3)^n$ are solutions. In fact, since they are linearly independent solutions, the general solution is[4]

$$a_n = c_1 2^n + c_2(-3)^n$$

We can also determine these coefficients with $a_0 = 1, a_1 = 2$ giving our final answer of

$$a_n = 2^n, n \geq 0 \blacksquare$$

2 .6.1 Non-Homogeneous Linear Recursion

Theorem 11. *Recall a non homogeneous linear recursion with constant coefficients has the form*

$$a_n = c_1 a + n - 1 + c_2 a_{n-2} + \cdots + c_k a_{n-k} + F(n)$$

with the associated homogeneous form

$$a_n = c_1 a + n - 1 + c_2 a_{n-2} + \cdots + c_k a_{n-k}$$

[3] This uses a degree 2 equation
[4] since the recursion is linear

Any solution to the non-homogeneous linear recursion has the form $a_n + b_n$ where a_n is a particular solution of the non-homogeneous form, and b_n is any solution of the homogeneous form, i.e. the same equation from differential equations with

$$Solution = homogeneous + non - homogeneous$$

Suppose $\{a_n\}$ satisfies the non-homogeneous linear recursion where $F(n)$ has the form:

$$F(n) = (polynomial) \cdot (exponential) = P(n) \cdot S^n$$

1. *When S is NOT a root of the characteristic equation of the second form. Then the form is*

$$a_n = q(n) \cdot S^n$$

Where $q(n)$ is again a polynomial with degree $q \leq \deg(P)$ is n.

2. *When S IS a root of the characteristic equation, then the form is*

$$a_n = n^m \cdot q(n) \cdot S^n$$

Where m is the multiplicity of S as a root of the characteristic equation and $q(n)$ is the same.

Example 2 .6. Find the general solution of

$$a_n = 3a_{n-1} + 2^n, n \geq 1, a_0 = 1$$

↪ Note that the homogeneous linear recursion form gives us the roots

$$a_n = 3a_{n-1} \to r = 3 - a_n = \alpha 3^n, \alpha \in \mathbb{R}$$

To find the particular solution, we note that $F(n) = 2^n$, which gives us that the particular solution has the form

$$b_n = c2^n$$

2 .7 Divide and Conquer Algorithms

The divide and conquer strategy in general is to solve a given problem of size n by breaking the general problem into $a \geq 1$ sub-problems of size $\frac{n}{b}$ for $b \geq 1$.

We assume $f(n)$ satisfies $f(n) = a \cdot f\left(\frac{n}{b}\right) + g(n)$.

Let f be an increasing function that satisfies $f(n) = a \cdot f\left(\frac{n}{b}\right) + c$ where $a, b, c \in \mathbb{Z}^+$ and $b \geq 2$. If $n|b \Rightarrow$ [1] $f(n)$ will be $O(n^{\log_b(a)})$ if $a > 1$ [2] our time has growth on the order of $O(log(n))$.

Furthermore, when $a > 1$, and $n = b^k, k = 1, 2, \cdots$ then the time complexity $f(n) = c_1 \cdot n^{\log_b(a)} + c_2$ where $c_1 = f(1) + \frac{c}{a-1}$ and $c_2 = -\frac{c}{a-1}$.

2 .7.1 Master Theorem Corollary

Let f be an increasing function that satisfies $f(n) = af\left(\frac{n}{b}\right) + cn^d$ where $a, c \in \mathbb{Z}^+, b > 1 \wedge c, d \in \mathbb{R}, c > 0, d \geq 0$. If $n = b^k, k \in \mathbb{Z}^+$ then

1. $f(n)$ is $O(n^d) \Leftrightarrow a < b^d$
2. $f(n)$ is $O(n^d \cdot log(n)) \Leftrightarrow a = b^d$
3. $f(n)$ is $O(n^{\log_b(a)}) \Leftrightarrow a > b^d$

2 .8 Generating Functions

Theorem 12. *The generating function for the sequence $\{a_n\}_{n \geq 0}$ is the series*

$$A(z) = \sum_{n=0}^{\infty} a_n z^n$$

Think of the zs as placeholders. We don't actually care about their value.

Notation:

$$[z^n] A(z)$$

Is the coefficient of the z^{nth} term in the series $A(z)$.

Example 2 .7. If $a_n = 1$ for all $n \geq 0$, then the generating function is $A(z) = 1 + z + z^2 + z^3 + \cdots + z^n = \frac{1}{1-z} = \sum_{n=0}^{\infty} z^n$

Example 2 .8. Show that the generating function for $a = n, n \geq 0$ is $A(z) = \frac{z}{(1-z)^2}$.

↪ Note $\frac{d}{dz}\left(\frac{1}{1-z}\right) = \frac{1}{(1-z)^2}$

But $\frac{d}{dz}\left(\frac{1}{1-z}\right) = \frac{d}{dz}\left(\sum_{n=0}^{\infty} z^n\right) = \sum_{n=0}^{\infty} n - z^{n-1}$

So

Now

$$z \cdot \frac{1}{(1-z)^2} = z \sum_{n=0}^{\infty} nz^{n-1} = \sum_{n=0}^{\infty} nz^n = \sum_{n=0}^{\infty} a_n z^n \to a_n = n$$

Therefore the generating function is $A(z) = \frac{z}{(1-z)^2}$. 1

Theorem 13. *If $A(z)$ is the generating function for the sequence associated to $\{a_n\}_{n \geq 0}$ and if $B(z)$ is the generating function associated to $\{b_n\}_{n \geq 0}$, then*

1. *$\alpha A(z) + \beta B(z)$ is the generating function associated to $\{\alpha a_n + \beta b_n\}_{n \geq 0}$ where $\alpha, \beta \in \mathbb{R}$.*
2. *$A(z) \cdot B(z)$ is the generating function associated to*

$$\{c_n\}_{n \geq 0} = \sum_{k=0}^{n} a_k b_{n-k}$$

Example 2 .9. In how many ways can change be given for 30 cents using pennies, nickels, dimes, and quarters?

↪ Let's look at the generating functions for each currency: Pennies: $(1 + z + z^2 + z^3 + \cdots)$ Nickels: $(1 + z^5 + z^{10} + z^{15} + \cdots)$ Dimes: $(1 + z^{10} + z^{20} + z^{30} + \cdots)$ Quarters: $(1 + z^{25} + z^{50} + z^{75} + \cdots)$

The product of these polynomials is the total number of ways to make change.

$$A(z)B(z)C(z)D(z) = 1 + z + z^2 + z^3 + z^4 + 2z^5 + \cdots + 18z^{30}$$

Therefore, there are 18 ways to make change for 30 cents.

2 .9 The Inclusion/Exclusion Principle

This applies to cardinality, area, mass, volume, etc....

How many elements are there in $A \cup B$ where A and B are finite sets?

$$|A \cup B| = |A| + |B| - |A \cap B|$$

Now consider three finite sets:

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

Notation for three finite sets:

$$|A_1 \cup A_2 \cup A_3| = \sum_{1 \leq j \leq 3} |A_i| - \sum_{1 \leq i < j \leq 3} |A_i \cap A_j| + |A_1 \cap A_2 \cap A_3|$$

Theorem 14 (Inclusion/Exclusion). *Let $A_1, A_2, \cdots, A_n$ be finite sets, then*

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{1 \leq i \leq n} |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| + \cdots + (-1)^{n+1} \left|\bigcap_{i=1}^{n} a_i\right|$$

or

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{I \subset \{1,2,3,4,\ldots,n\}} (-1)^{|I|+1} \left|\bigcap_{i \in I} A_i\right|$$

or

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{I \subseteq \{1,2,3,4,\ldots,n\}} (-1)^{|I|+1} \left|\bigcap_{i \in I} A_i\right|$$

2 .9.1 Derangements

A derangement of $(1, 2, 3, \cdots, n)$ is any permutation of these numbers that leaves no number in its original position.

For a given set, $(1, 2, 3, \cdots, n)$, there are approximately $\frac{n!}{e}$ derangements, or more accurately

$$n! \cdot \left(\sum_{i=0}^{n} \frac{(-1)^i}{i!}\right)$$

3 Logic and Proofs

3 .1 Propositional Logic

Before we begin we have to define the syntax of these expressions. Let the letters $p, q, r, s, \cdots$ denote the various propositions, while T and F denote the truth value of the statement.

First we define the negation of p, denoted $\neg p$. This is expressed as the statement, "It is not the case that p."

Next we define the conjunction of p and q, denoted $p \wedge q$. This statement is true when both p and q are true, but false otherwise.

The disjunction of p and q is true when either p or q is true, and false otherwise.

The exclusive or of p and q is true when exactly one is true, and false otherwise.

The conditional statement is defined by the expression "If p; then q."

The biconditional statement is similar, except it is defined by the expression "p if and only if q."

3 .2 Propositional Equivalences

A statement that is always true is called a tautology, while a statement that is always false is called a contradiction, and a statement that is neither is a contingency.

p	q	$p \wedge q$	$p \vee q$	$q \oplus q$	$p \to q$	$p \iff q$
T	T	T	T	F	T	T
T	F	F	T	T	F	F
F	T	F	T	T	T	F
F	F	F	F	F	T	T

Table 1: Truth Table for Various Statements

Two statements are logically equivalent if $p \iff q$ is a tautology.

3 .3 Methods of Proof

3 .3.1 Direct Proof

This style of proof directly proves the statement through application of properties, definitions, or theorems. It is the most common type of proof.

3 .3.2 Proof by Contraposition

$p \Rightarrow q \equiv q \vee (\neg p) \equiv \neg p \vee \neg(\neg q)$. Therefore $\neg q \Rightarrow \neg p$.

3 .3.3 Proof by Contradiction

Suppose we wish to prove statement p, then assume $\neg p$, and then prove $\neg p$ implies a contradiction.

3 .3.4 Existence Proofs

To prove existence we can either choose a constructive approach, or a non-constructive approach. A constructive proof constructs an example satisfying the conditions, and if it's not constructive, then it has to be non-constructive.

3 .3.5 Uniqueness Proofs

First prove $(\exists x)[P(x) \Rightarrow T]$

Then prove that if $P(y) \Rightarrow T$ for any y, then show $y = x$. Else if $y \neq x$, show $P(y)$ is false.

3 .4 Induction

Theorem 15 (The Well-Ordering Principle). *Every non-empty subset of $\mathbb{Z}^+$ contains a smallest element. $\mathbb{Z}^+$ itself is well-ordered. Note, $\mathbb{Z}^+$ contains no open sets or intervals.*

Theorem 16 (The Principle of Mathematical Induction). *Let $P(n)$ be a propositional function.*

Suppose $P(1) \Rightarrow T$ and $\forall k \in \mathbb{Z}^+$ if wherever $P(k) \Rightarrow P(k+1)$, then $P(n) \Rightarrow T$ for all $n \in \mathbb{Z}^+$.

Note, induction requires two steps, the first of which being to prove $P(1)$, and the second to prove $P(k) \Rightarrow P(k+1)$.

4 Set Theory

Theorem 17. *Definitions:*

1. *A set is a list of elements where repetition and order doesn't matter.*
2. *If $p(x)$ is a propositional function with domain of speech u (the universe) then $A = \{x \in u|p(x)\}$, so $x \in A \Leftrightarrow p(x)$ is true. By definition, the negation of $x \in A$ is $x \notin A$.*
3. *Two sets are equal if they have exactly the same elements.*
4. *By definition, the only set with no elements is the Empty Set, or null set, denoted $\{\}$ or $\varnothing$. Note, $\{\varnothing\}$ is not the empty set.*
5. *A is a subset of B if $\forall x[x \in A \Rightarrow x \in B]$ is true. We write $A \subseteq B$, and $A \subseteq A$. Note, $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$.*
6. *A is a proper subset of B if A is a subset of B, and $A \neq B$. So $\exists x[x \in B \wedge x \notin A]$. $A \subset B$.*

4 .1 Operations Between Sets

1. **Union:** For $A, B \subseteq u$ we define $A \cup B = \{x \in u|(x \in A) \vee (x \in B)\}$.

$$\bigcup_{i \in I} A_i = \{x \in u|(\exists i \in I)[x \in A_i]\}$$

2. **Intersection:** For $A, B \subseteq u$, $A \cap B = \{x \in u|(x \in A) \wedge (x \in B)\}$.

$$\bigcap_{i \in I} A_i = \{x \in u|(\forall i \in I)[x \subset A_i]\}$$

3. **Set Complementation:** "The complement of A" is $A^c = \{x \in u|x \notin A\}$. $u^c = \varnothing$. $\varnothing^c = u$.

We can apply DeMorgan's Laws.

1. $$\left(\bigcup_{i \in I} A_i\right)^c = \bigcap_{i \in I} A_i^c$$

2. $$\left(\bigcap_{i \in I} A_i\right)^c = \bigcup_{i \in I} A_i^c$$

4 .2 Set Properties and Functions

Theorem 18. *Definitions:*

1. *For sets A, B, we define the cartesian product of $A \times B = \{(a, b)|(a \in A) \wedge (b \in B)\}$*
2. *The difference between A and B is $A - B = \{x \in u|(x \in A) \wedge (x \notin B)\}$.*
3. *A function from A to B is a rule that associates a unique element in B to each element of A, i.e. $f : A \to B$ is a function from A to B if $(\forall a, b \in A)[a = b \Rightarrow f(a) = f(b)]$.*
4. *If $f : A \to B$ is a function, then A is called the domain of f, B is called the codomain, and the range of f is $f(A) = \{y \in B|(\exists a \in A)[y = f(a)]\}$. Note, by definition, the range is contained in the codomain $f(a) \subseteq B$.*
5. *$f : A \to B$ is injective, $(1-1)$, or one-to-one, if for any $y \in B$ there is at most one a in A such that $f(a) = y$.*
6. *$f : A \to B$ is surjective, or onto if for any $y \in B, \exists a \in A$ such that $f(a) = y$.*
7. *If f is both one-to-one and surjective, then it is called bijective.*
8. *A set A is said to be countable if there exists a bijection $f : \mathbb{N} \to A$.*
9. *If $f : A \to B$ is a bijection, then it is invertible.*
10. *A set that is not finite nor countable is said to be uncountable.*

5 Algorithms and Integers

5 .1 Complexity

Theorem 19. *Definitions:*

1. *Let f be a function $f : [0, \infty) \to \mathbb{R}$ and $g : [-, \infty) \to \mathbb{R}$, we write $f = O(g)$ and say "f is of order g at most". If there exists constants*

Big O Form	Complexity
$O(1)$	constant
$O(log(n))$	logarithmic
$O(n)$	linear
$O(nlog(n))$	$nlog(n)$
$O(n^2)$	quadratic
$O(n^3)$	cubic
$O(n^m)$	polynomial
$O(2^n)$	exponential
$O(n!)$	factorial

Table 2: Big O Forms

$c > 0$ and $k \geq 0$ such that

$$|f(x)| \leq c|g(x)| \text{ for all } x > k$$

2. *We write $f = \Theta(g)$, "f and g are of the same order" if $f = O(g)$ and if $g = O(f)$. This is equivalent to saying $\exists c_1, c_2, k(0 < c_1 < c_2 \wedge k \geq 0)$ such that $c_1|f(x)| \leq |g(x)| \leq c_2|f(x)|, x > k$.*

Theorem 20. *If $f_1(x) = O(g_1(x))$ and $f_2(x) = O(g_2(x))$, then*

1. *$(f_1 + f_2)(x) = O(max(|g_1(x)|, |g_2(x)|))$*
2. *$(f_1 f_2)(x) = O(g_1(x) - g_2(x))$*

Theorem 21. *Definitions:*

1. *Time Complexity of an algorithm relates to the time required to give output.*
2. *Space Complexity relates to the computer memory required by the algorithm.*
3. *Worst-Case Complexity is the maximum number the algorithm for input of size n.*
4. *Average Case Complexity is the average number of operations used to solve a problem over all inputs of a given size.*

Theorem 22. *Let $P : \mathbb{R} \to \mathbb{R}$ and $q : \mathbb{R} \to \mathbb{R}$ be polynomials, then*

1. *$p = O(q) \Leftrightarrow degree(p) \leq degree(q)$*
2. *$p = \Theta(q) \Leftrightarrow degree(p) = degree(q)$*

5 .2 Greedy Algorithms

A greedy algorithm is an algorithm that makes the "best" choice at each step.

5 .2.1 Change Problem

Consider the problem of making change for n checnts using quarters, dimes, nickels, and pennies using the fewest total number of coins.

The strategy for this problem is defined as the following. At each step, choose the coin of largest denomination possible without exceeding the total.

```
def change(c1, c2, ..., c3, n):
    c = [0, 0, 0, ..., 0]   # Number of coins we have
    for i in range(0, c):
        while n >= c_i:
            c[i] = c[i] + 1
            n = n - c_i
    return c
```

Lemma: If $n \in \mathbb{Z}, n \geq 0$, then n cents in change (q, d, n, p), using the fewest coins possible, has at most $2d, 1n, 4p$ and cannot have $2d + n$. The amount of change in dnp cannot exceed 24.

5 .3 Mergesort

The algorithm is as follows:

Step One is to split the given list into two equal sublists until each list contains a single element.

Step Two is to merge the sublists until they are sorted.

Lemma: Let L_1, L_2 be the two sorted lists of ascending numbers, where L_i contains n_i elements. L_1 and L_2 can be merged into a single list, L, using at most $n_1 + n_2 - 1$ comparisons.

The worst-case complexity of mergesort is $O(n \cdot \ln(n))$

5 .4 Division Algorithm

For any integers $a, b \in \mathbb{Z}|a \neq 0$, a divides b, $a|b$ if $\exists c \in \mathbb{Z}$ such that $b = ac$.

Let a, b be positive integers, then there are unique integers q, r, $0 \leq< b$ such that $a = bq + r$.

If we consider a fixed $b > 1$ then $\exists k \geq 0$ and $\exists((a_0, a_1, \cdots, a_k) \in \{0, 1, \cdots, b-1\})$ $\left[(a_k \neq 0) \wedge \left(n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_0 = \sum_{i=0}^{k} a_i b^i\right)\right]$

5 .4.1 Uniqueness

The representation of any number $n \in \mathbb{Z}^+ \cup \{0\}$ is unique for each fixed base $b \geq 1$

5 .5 Base b Expansion

The following algorithm finds the base b representation of any integer $n \geq 0$.

```
def base_b_expansion(n,b):
    q = n
    k = 0
    while q != 0:
        a_k = q % b
        q = q / b
        k += 1
```

The complexity of the above algorithm is $\Theta(log_b(n))$

5 .6 Prime Numbers

A prime number can be defined as a positive integer $p > 1$ if the only positive factors of p are 1 and p.

If a number is not prime, it is composite.

Every integer can be written as a product of primes uniquely up to the order of the primes.

There are infinitely many primes.

If n is a composite integer then n has a prime divisor $\leq \sqrt{n}$, and contrapositively, if n doesn't have a prime divisor $\leq \sqrt{n}$, then n is prime.

5 .6.1 GCD

For integers $a, b \in \mathbb{Z}$, a positive integer c is called the greatest common divisor of a and b if

1. $(c|a) \wedge (c|b)$
2. $(d|a) \wedge (d|b) \Rightarrow (d|c) \Rightarrow (d \leq c)$

Two numbers are relatively prime if their GCD is one.

If a, b, q, r are non-negative integers such that $a = bq + r$, then the $gcd(a, b) = gcd(b, r)$.

If $a, b \in \mathbb{Z}$ and $gcd(a, b) = 1$ then $(\exists \alpha, \beta \in \mathbb{Z})\,[1 = \alpha a + \beta b]$

The corollary of the above equation is that if $a, b \in \mathbb{Z}$, then $(\exists \alpha, \beta \in \mathbb{Z})\,[gcd(a, b) = \alpha a + \beta b]$

5 .7 Modular Arithmetic

Fix $m \geq 2 (m \in \mathbb{Z})$ and if $a, b \in \mathbb{Z}$, then a is congruent to $b \mod m, a \equiv b(\mod m)$, if and only if $m|(a - b)$ and $\exists k \in \mathbb{Z}$ such that $a - b = mk \Rightarrow a = b + mk$.

1. If $a \equiv b(\mod m) \Rightarrow (a = q_1 m + r) \wedge (b = q_2 m + r)$. In other words, a and b have the same remainder after dividing by m.
2. If $a = b \Rightarrow a \equiv b(\mod m)$
3. If $a \equiv b(\mod m)$ and $a, b \in \{0, 1, 2, \cdots, m\} \Rightarrow a = b$.
4. $a \equiv a(\mod m)$
5. $a \equiv b(\mod m) \Rightarrow b \equiv a(\mod m)$
6. $a \equiv b(\mod m) \wedge b \equiv c(\mod m) \Rightarrow a \equiv c(\mod m)$
7. $a \equiv b(\mod m) \Rightarrow (a + c) \equiv (b + c)(\mod m) \wedge (ac) \equiv (bc)(\mod m)$
8. $ac \equiv bc(\mod m) \wedge gcd(c, m) = 1 \Rightarrow a \equiv b(\mod m)$
9. $gcd(a, m) = 1 \Rightarrow (\exists x \in \mathbb{Z})[ax \equiv 1(\mod m)]$, and x is called a multiplicative inverse of $a \mod m$.

5 .7.1 The Space $\mathbb{Z}_m$

Let $m = 11, \mathbb{Z}_{11} = \{x(\mod 11)|x \in \mathbb{Z}\}$ which is equivalent to $\{[0], [1], [2], \cdots, [10]\}$. Each box is $[x] = \{k \in \mathbb{Z}|k \equiv x(\mod m)\}$. These are called equivalence rings.

5 .8 Dirichlet's Approximation Theorem

For every irrational number α, there are infinitely many rational numbers $\frac{p}{q}$ such that $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$.

Lemma: For any integer $n \geq 1$ there is a rational number $\frac{p}{q}$ such that $\left|\alpha - \frac{p}{q}\right| < \frac{1}{nq}$ where $1 \leq q \leq n$.

6 Graph Theory

A graph can be defined by letting V be a finite, non-empty set of nodes and E be a set of edges. The pair of sets forms a graph.

In directed graphs we care about the direction of the nodes, and the order of the pairs in E matter.

In undirected graphs order does not matter.

Multigraphs are graphs that allow several edges between the same two nodes.

A simple graph is defined as an undirected graph with no loops and no multiple edges.

If a graph is undirected, then the total degree of the vertices is equal to twice the edges, therefore there must be an even sum of degrees.

We also have out degree and in degrees.

A graph is called bipartite if it can be written as $V = V_1 \cup V_2$ where $V_1 \cap V_2 = \varnothing$, and every edge is of the form $\{a, b\} \in G \wedge a \in V_1 \wedge b \in V_2$.

A complete bipartite graph has every node in V_1 adjacent to every node in V_2.

If we have a graph, then a proper coloring of the graph allows that each adjacent node be a different color.

The minimum number of colors to properly color a graph is called its chromatic number. A graph is bipartite if its chromatic number is 2.

We can express graphs as adjacency matrices.