NATURAL NUMBERS

$a+b \in \mathbb{N}$ closure

$a \times b \in \mathbb{N}$ closure

$a+b=b+a$ commutative

$(a+b)+c=a+(b+c)$ assosciative

$n \times 1 = nforalln \in \mathbb{N}$ multiplicative identity

if $m \times z = n \times z$ for some $z \in \mathbb{N}$ then $m=n$

$a \times (b+c) = (a \times b) + (a \times c)$ distributive

m is a **multiple** of n if there is a natural number r such that $m=rn$

If a and b are multiples of n the, for all $x, y \in \mathbb{N}, xa+yb$ is a a multiple of n

For any natural numbers m and n, the statement $m<n$ means that there is some $x \in \mathbb{N}$ such that $m+x=n$

If $a<b$ and $b<c$ then $a<c$

Given any natural numbers m and n, exactly one of the three statements $m<n, m=n, n<m$ is true.

Suppose that P(n) is a statement with the following properties:

(i) $P(1)$ is true; *induction basis*

(ii) if $P(k)$ is true (*induction hypothesis*) then $P(k+1)$ (*induction step*) is true for every $k \in \mathbb{N}$.

Then $P(n)$ is true for all $n \in \mathbb{N}$

strong: (ii) assume $P(i) 1 \leq i \leq k$ is true then $P(k+1)$ is true for every $k \in \mathbb{N}$

Let X be a subset of $\mathbb{N}$. An element $l \in X$ is a **least member** of X if $l \leq x$ for all $x \in X$. An element $g \in X$ is a **greatest member** of X if $g \geq x$ for all $x \in X$. Often l and g are referred to as the **minimum** and **maximum** of X.

archetype of recursive def: $A_n = \sum_{i=1}^{n} a_i$

$$A_{k+1} = \sum_{i=1}^{k+1} a_i = \sum_{i=1}^{k} a_i + a_{k+1}$$

Every non-empty subset of X of $\mathbb{N}$ has a least member.

FUNCTIONS

Suppose that X and Y are sets. We say that we have a **function** f **from** X **to** Y if for each x in X we can specify a unique element in Y, which we denote by $f(x)$.

The function f from X to Y is a **surjection** if every y in Y is a value $f(x)$ for at least one x in X. It is an **injection** if every y in Y is a value $f(x)$ for at most one x in X. It is a **bijection** if it is both a surjection and an injection, that is, if every y in Y is a value $f(x)$ for exactly one x in X.

For any set X the function $i: X \to X$ defined by $i(x)=x$ for all $x \in X$ is called the **identity** function on X. If X is a subset of Y, the function $j: X \to Y$ defined by $j(x)=x$ is called the **inclusion** function from X to Y.

If $f: X \to Y$ and $g: Y \to Z$ are injections, then so is the composite $gf: X \to Z$. If f and g are surjections then so is gf. if f and g are bijections then so is gf.

A function $f: X \to Y$ has an **inverse** function $g: Y \to X$ if, for all x in X and y in Y $(gf)(x)=x, (fg)(y)=y$. In other words gf is the identity function on X and fg is the identity function on Y.

A function has an inverse if and only if it is a bijection.

HOW TO COUNT

Let m be a natural number. Then the following statement is true for every natural number n: if there is an injection from $\mathbb{N}_n$ to $\mathbb{N}_m$, then $n \leq m$.

If there is a bijective correspondence between S and $\mathbb{N}_m$ then we say that S has size, or cardinality, m and we write $|S|=m$.

If a set S is such that $|S|=s$ and $|S|=t$, then $s=t$. (both are bijections, hence have inverse)

A set S is **finite** if it is empty of if $|S|=n$ for some $n \in \mathbb{N}$. A set which is not finite is said to be **inifite**.

The set $\mathbb{N}$ is infinite. (proof, if finite -¿ make ordered list, sum not included)

If the set S is such that there is a bijection $b: \mathbb{N} \to S$, then S is infinite.

definitions regarding properties of infinite sets: finite, countable, uncountable

INTEGERS

integer eq. class def: $(a,b)R(c,d)$ means $a+d=b+c$

def addition: $[a,b]+[c,d]=[a+c, b+d]$

def multiplic.: $[a,b]+[c,d]=[ac+bd, ad+bc]$

A **relation** R on a set X is a set of ordered pairs of members of X.

reflexive xRx, symmetric xRy, transitive xRy and yRz hence xRz

An **equivalence relation** is a relation that is **reflexive**, **symmetric** and **transitive**.

Let R be an equivalence relation on X. A non-empty set $C \subseteq X$ is an **equivalence class** with respect to R if

(i) any two members of C are R-related; and

(ii) C contains every member of X that is R-related to any member of C.

in symbols, C is such that,

if $x \in C$ then $y \in C \iff xRy$

Given an equivalence relation R on X, every member of X is one and only one equivalence class (with respect to R).

$x+0=x$ for every $x \in \mathbb{Z}$

If $x \times z = y \times z$ and $z \neq 0$ then $x=y$

For any $x \in \mathbb{Z}$ there is an element $-x$ of $\mathbb{Z}$ such that $x+(-x)=0$.

If $x \leq y$ and $0 \leq z$, then $x \times z \leq y \times z$.

The integer b is a **lower bound** for a set $X \subseteq \mathbb{Z}$ if $b \leq x$ for all $x \in X$.

If a non-empty set $S \subseteq \mathbb{Z}$ has a lower bound, then S has a least member.

DIVISIBILITY AND PRIME NUMBERS

Given positive integers a and b there exist q and r in $\mathbb{N}_0$ such that $a=bq+r$ and $0 \leq r \leq b$.

If a and b are positive integers (or zero) we say that d is the **greatest common divisor (gcd)** of a and b provided that (i) $d|a$ and $d|b$; (ii) if $c|a$ and $c|b$, then $c \leq d$.

Let a and b be positive integers, and let $d=gcd(a,b)$. Then there are integers m and n such that $d=ma+nb$.

If $gcd(a,b)=1$ then we say that a and b are **coprime**. In this case the Theorem asserts that there are integers m and n such that $ma+nb=1$.

A positive integer p is a **prime** if $p \geq 2$ and the only positive integers which divide p are 1 and p itself.

If p is a prime and $x_1, x_2, \ldots, x_n$ are any integers such that $p|x_1 x_2 \ldots x_n$ then $p|x_i$ for some $x_i (1 \leq i \leq n)$.

(The Fundamental Theorem of Arithmetic) A positive integer $n \geq 2$ has a unique prime factorization, apart from the order of the factors.

Algorithm **Eratosthenes sieve**, on a finite list of numbers.

FRACTIONS AND REAL NUMBERS

$\frac{a}{c} \oplus \frac{c}{d} = \frac{ad+bc}{bd}$

$\left(\frac{a}{b}\right)^{-1} = \frac{b}{a} (a, b \neq 0)$

Between any two rational numbers there is another one.

There are no natural numbers m, n such that $m^2=2n$.

Example: 0.5734 meaning $\frac{5}{10}+\frac{7}{100}+\frac{3}{1000}+\frac{4}{10000}$.

The set of $\mathbb{Q}$ of rational numbers is countable.

Proof array with numerator and denominator as x,y

The set of $\mathbb{R}$ of real numbers is uncountable.

Proof list of numbers with numbered decimal parts.

Ex. $a=0.31\overline{579}$. Take $b-0.\overline{579}$

$1000b-b=999b \to 579.\overline{579}-0.\overline{579}=579$

$\to 999b=579 \to b=\frac{579}{999}$

$a=0.31\overline{579}$

$100a=31.\overline{579}$

$100a-31=0.\overline{579}=b=\frac{579}{999}$ solve for a

PRINCIPLES OF COUNTING

If A and B are non-empty finite sets, and A and B are disjoint (that is $A \cap B = \varnothing$, the empty set), then $|A \cup B| = |A| + |B|$. Addition principle

Let X and Y be finite non-empty sets, and let S be a subset of $X \times Y$. Then the following results hold. (i) The size of S is given by

$$|S| = \sum_{x \in X} r_x(S) = \sum_{y \in Y} c_y(S)$$ where $r_x(S)$ and $c_y(S)$ are the row and column totals as described above. (ii) If $r_x(S)$ is a constant r, inependent of x and $c_y(S)$ is a constant c, independent of y, then $r|X| = c|Y|$. (iii) (The multiplication principle) The size of $X \times Y$ is given by $|X \times Y| = |X| \times |Y|$.

Eulers's function: let $\phi(n)$ denote the number of integers x in the range $1 \leq x \leq n$ such that x and n are coprime. $\phi(p)=p-1$ (p prime).

For any positive integer n, $\sum_{d|n} \phi(d) = n$.

Let X and Y be non-empty finite sets, and let F denote the set of functions from X to Y. if $|X|=m$ and $|Y|=n$, then $|F|=n^m$.

Equivalently, we may say that the number of words of length m in an alphabet Y of n symbols is n^m. In general we can say that a function from $\mathbb{N}_m$ to Y is a mathematical model of an **ordered selection with repetition of** m **things from the set** Y.

How many subsets to a set with n elements can be done by 2^n

The number of **ordered selections, without repetition, of** m **things from a set** Y **of size** n is the same as the number of injections from $\mathbb{N}_m$ to Y, and is given by $n(n-1)(n-2)\ldots(n-m+1)$.

If $m=n$ then ordered selection, without repetition is a **permutation**

The following properties hold in the set S_n of all permutations of $\{1, 2, \ldots, n\}$. (i) If π and σ are in S_n, so is $\pi\sigma$. (ii) For any permutations π, σ, τ in S_n, $(\pi\sigma)\tau = \pi(\sigma\tau)$. (iii) The identity function, denoted by id an defined by $id(r)=r$ for all r in $\mathbb{N}_n$, is a permutation and for any σ in S_n we have $id\sigma = \sigma id = \sigma$. (iv) For every permutation π in S_n there is an inverse permutation $\pi^{-1} = \pi^{-1}\pi = id$.

SUBSETS

Unordered selection without repetition: $\binom{n}{r}$ spoken n *choose* r.

If n and r are positive integers satisfying $1 \leq r \leq n$ then $\binom{n}{r} = \binom{n-1}{r-1} + \binom{n-1}{r}$.

If n and r are positive integers satisfying $1 \leq r \leq n$, then $\binom{n}{r} = \frac{n(n-1)\ldots(n-r+1)}{r!} = \frac{n!}{r!(n-r)!}$ (proof by recursion formula and induction).

unordered selections with repetition, The number of unordered selections, with repetition, of r objects from a set of n objects is: $\binom{n+r-1}{r} = \binom{n+r-1}{n-1}$. Since the selections are unordered, we may arrange matters so that, within each selection, all the objects of one given kind come first, followed by the objects of another kind, and so on.

binominal theorem: Let n be a positive integer. The coefficient of the term $a^{n-r}b^r$ in the expansion of $(a+b)^n$ is the binominal number $\binom{n}{r}$. Explicitly, we have $(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \cdots + \binom{n}{n}b^n$.

sieve principle: If $A_1, A_2, \ldots, A_n$ are finite sets then $|A_1 \cup A_2 \cup \ldots A_n| = \alpha_1 - \alpha_2 + \alpha_3 - \cdots + (-1)^{n-1}\alpha_n$, where α_i is the sum of the cardinalities of the intersections of the sets taken i at a time $(1 \leq i \leq n)$.

formula for $\phi(n)$: Let $n \leq 2$ be an integer whose prime factorization is $n = p_1^{e_1} p_2^{e_2} \ldots p_r^{e_r}$. Then $\phi(n) = n(1-\frac{1}{p_1})(1-\frac{1}{p_2})\ldots(1-\frac{1}{p_r})$.

PARTITION, CLASSIFICATION, DISTRIBUTION

Let $S(n,k)$ denote the number of partitions of an n-set X into k parts, where $1 \leq k \leq n$. Then $S(n,1) = 1$, $S(n,n) = 1$,
$S(n,k) = S(n-1,k-1) + kS(n-1,k)$ $(2 \leq k \leq n-1)$.
The numbers $S(n,k)$ are sometimes called **Stirling Numbers** (of the second kind). As a consequence of Theorem 12.1 they may be tabulated in much the same way as the binominal numbers are arranged in Pascal's triangle.
If R is an equivalence relation on a set X then the distinct equivalence classes with respect to R form a partition of X.
Distribution: Let J denote the set of surjections from an n-set X to a k-set Y. Then $|J| = k!S(n,k)$ (where $k!$ is the number of ways how we can write the parts of a partition in different sequences)
Given any positive integers $n, n_1, \ldots, n_k$ satisfying $n_1 + n_2 + \cdots + n_k = n$, we have $\binom{n}{n_1,n_2,\ldots,n_k} = \frac{n!}{n_1!n_2!\ldots n_k!}$ (how many words with n letters, accounting for identical letters).
For any positive integers n and k
$(x_1 + x_2 + \cdots + x_k)^n =$
$\sum \binom{n}{n_1,n_2,\ldots,n_k} x_1^{n_1} x_2^{n_2} \ldots x_k^{n_k}$, where the sum is taken over all k-tuples of non-negative integers $(n_1, n_2, \ldots, n_k)$ such that $n_1 + n_2 + \cdots + n_k = n$.
General formula for classification of permutations: $\frac{n!}{1^{\alpha_1}2^{\alpha_2}\ldots n^{\alpha_n}\alpha_1!\alpha_2!\ldots\alpha_n!}$

MODULAR ARITHMETIC

Let x_1 and x_2 be integers, and m a positive integer. We say that x_1 is **congruent** to x_2 **modulo** m, and write $x_1 \equiv x_2 \pmod{m}$ whenever $x_1 - x_2$ is divisible by m.
Let m be a positive integer and x_1, x_2, y_1, y_2 integers such that $x_1 \equiv x_2 \pmod{m}$, $y_1 \equiv y_2 \pmod{m}$. Then (i) $x_1 + y_1 \equiv x_2 + y_2 \pmod{m}$, (ii) $x_1 y_1 \equiv x_2 y_2 \pmod{m}$.
The set of **integers modulo m**, written as $\mathbb{Z}_m$, is the set of distinct equivalence classes under the relation of congurence modulo m in $\mathbb{Z}$.
The operations $\oplus$ and $\otimes$ satisfy the following rules, where a, b, c denote any members of $\mathbb{Z}_m$, and $0 = [0]_m$, $1 = [1]_m$. **M1**$a \oplus b$ and $a \otimes b$ are in $\mathbb{Z}_m$. **M2**$a \oplus b = b \oplus a$, $a \otimes b = b \otimes a$.
M3$(a \oplus b) \oplus c = a \oplus (b \oplus c)$,
$(a \otimes b) \otimes c = a \otimes (b \otimes c)$. **M4**$a \oplus 0 = a$, $a \otimes 1 = a$. **M5**$a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$. **M6**For each a in $\mathbb{Z}_m$ there is an unique element $-a$ in $\mathbb{Z}_m$ such that $a \oplus (-a) = 0$).
An element r in $\mathbb{Z}_m$ is said to be **invertible** if there is some x in $\mathbb{Z}_m$ such that $rx = 1$ in $\mathbb{Z}_m$. In the case, x is called the **inverse** of r, and we write $x = r^{-1}$..
The element r in $\mathbb{Z}_m$ is invertible if and only if r and m are coprime in $\mathbb{Z}$. in particular, when p is a prime every element of $\mathbb{Z}_p$ except 0 is invertible.
If y is invertible in $\mathbb{Z}_m$ then $y^{\phi(m)} = 1$ in $\mathbb{Z}_m$.
Euler's Theorem: if gcd(y,m) = 1 then $y^{\phi(m)} \equiv 1 \pmod{m}$.
Fermat's Theorem: if $p \nmid y$ then $y^{p-1} \equiv 1 \pmod{p}$.
A **latin square** of order n is an $n \times n$ array in which each one of n symbols occurs once in each row and once in each column.
Let p be a prime and t a non-zero element of $\mathbb{Z}_p$. Then the rule $L_t(i,j) = ti + j$ $(i,j \in \mathbb{Z}_p)$ defines a latin square. Furthermore, when $t \nmid u$ the latin square L_t and L_u are orthogonal.
Let f be a function from $\mathbb{N}$ to $\mathbb{N}$. We say that $f(n)$ is $O(g(n))$ if there is a positive constant k such that $f(n) \leq kg(n)$ for all n in $\mathbb{N}$ (with possibly a finite number of exceptions). The symbol $(O(g(n))$ is pronounced 'big-oh of $g(n)$'

ALGORITHMS AND THEIR EFFICIENCY

bubblesort Compare adjacent terms in the list and switch them if they are in the wrong order. The operations involved in bubble sort are comparisons and switches. At the jth path, $n - m$ comparisons are made, adn so the total nmber of comparisons is
$(n-1) + (n-2) + \cdots + 2 + 1 = \frac{1}{2}n(n-1)$, which is n^2. **listsort** The basic idea of insertion sorting is to begin with the list $L = (x_1)$ and insert xi in its correct place in the list for $i = 2, 3, \ldots, n$. Insertions can be done **sequential** or preferentially by the **bisection** method.

GRAPHS

A **graph** G consists of a finite set V, whose members are called **vertices**, and a set E of 2-subsets of V, whose members are called **edges**. We usually write $G = (V, E)$ and say that V is the **vertex set** and E is the **edge set**.
Let us say that two vertices x and y of a graph are *adjacent* whenever $\{x, y\}$ is an edge. (We say also that x and y are **neighbours**.) Then we can represent a graph $G = (V, E)$ by its **adjacency list**, wherein each vertex v heads a list of those vertices adjacent to v.
Two graphs G_1 and G_2 are said to be **isomorphic** when there is a bijection α from the vertex set of G_1 to the vertex set of G_2 such that $\{\alpha(x), \alpha(y)\}$ is an edge of G_2 if and only if $\{x, y\}$ is an edge of G_1. The bijection α is said to be an **isomorphism**.
The **degree** of a vertex v in a graph $G = (V, E)$ is the number of edges of G which contain v. We shall use the notation $\delta(v)$ for the degree of v, so formally $\delta(v) = |D_v|$, where $D_v = \{e \in E | v \in e\}$.
The sum of the values of the degree $\delta(v)$, taken over all the vertices v of a graph $G = (V, E)$, is equal to twice the number of edges:
$\sum_{v \in V} \delta(v) = 2|E|$.
The number of odd vertices is even.
A **walk** in a graph G is a sequence of vertices $v_1, v_2, \ldots, v_k$, such that v_i and v_{i+1} are adjacent $(1 \leq i \leq k-1)$. If all its vertices are distinct, a walk is called a **path**.
Suppose $G = (V, E)$ is a graph and the partition of V corresponding to the equivalence relation is $V = V_1 \cup V_2 \cup \cdots \cup V_r$. Let $E_i (1 \leq i \leq r)$ denote the subset of E comprising those edges whose ends are both in V_i. Then the graphs $G_i = (V_i, E_i)$ are called the **components** of G. If G has just one component, it is said to be **connected**.
We say that a graph T is a **tree** if it has two properties: (T1) T is connected; (T2) there are no cycles in T.
If $T = (V, E)$ is a tree with at least two vertices, then: (T3) for each pair of x, y of vertices there is a unique path in T from x to y, (T4) the graph obtained from T by removing any edge has two components, each of which is a tree; (T5) $|E| = |V| - 1$
A **vertex coloring** of a graph $G = (V, E)$ is a function $c : V \to \mathbb{N}$ with the property that $c(x) \neq c(y)$ whenever $\{x, y\} \in E$. The **chromatic number** of G, written $\chi(G)$, is defined to be the least integer k for which there is a vertex coloring of G using k colors.
Greedy algorithm for vertex coloring. Not always perfect, but ok. Suppose we have arranged the vertices in some order $v_1, v_2, \ldots, v_n$. We assign color 1 to v_i for each $v_i (2 \leq i \leq n)$ we form the set S of colors assigned to vertices $v_j (1 \leq j < i)$ which is adjacent to v_i; and we give v_i the first color not in S.
If G is a graph with maximum degree k, then (i) $\chi(G) \leq k + 1$, (ii) if G is connected and not regular, $\chi(G) \leq k$.
A graph is bipartite if and only if it contains no cycles with odd length.

TREES, SORTING, SEARCHING

A vertex in a rooted tree is said to be a **leaf** if it is at level $i (i \geq 0)$ and it is not adjacent to any vertices at level $i + 1$. A vertex which is not a leaf is an **internal** vertex. The **height** of a rooted tree is the maximum value of k for which level k is not empty.
The height of an m-ary rooted tree with l leaves is at least $log_m l$.
The **heapsort** algorithm involves two stages. First, the unsorted list is transformed into a special kind of list know as *heap*, and secondly, the heap is transformed into the sorted list. The characteristic property of a heap is that each father is smaller than his sons. Heapsort $O(n \log(n))$.
Suppose that $G = (V, E)$ is a connected graph, and T is a subset of E such that (i) every vertex of G belongs to an edge in T; (ii) the edges in T form a tree. In this case, we say that T is a **spanning tree** for G.
Minimum Spanning Tree MST for the weighted graph G. A simple algorithm for the MST problem is based on applying the greedy principle to the tree-growing method given above. Specifically: at each stage we add the *cheapest* edge joining a new vertex to the partial tree.
Let $G = (V, E)$ be a connected graph with weight function $w : E \to \mathbb{N}$, and suppose that T is a spanning tree for G constructed by the greedy algorithm, then $w(T) \leq w((U)$ for any spanning tree U of G.
Depth-First-Search. Let v be a vertex of the graph G and let T be the subset of the edges of G constructed according to the DFS method. Then T is a spanning tree for the component of G which contains v. (Stack procedure)
Breadth-First-Search. Let v be a vertex of the graph G, and let T be the subset of the edges of G constructed according to the BFS algorithm. Then T is a spanning tree for the component of G which contains v. (Queue procedure)
shortest path problem Dijkstras algorithm, greedy

BIPARTITE GRAPHS AND MATCHINGS

Let $G = (X \cup Y, E)$ be a bipartite graph and let $\delta(v)$ denote the degree of a vertex v in G. Then $\sum_{x \in X} \delta(x) = \sum_{y \in Y} \delta(y) = |E|$.
Let G be a graph with edge set E. A coloring of E is said to be an *edgecoloring* of G if any two edges containing the same vertex have the different colors.
If $G = (X \cup Y, E)$ is a bipartite graph, then the minimum number of colors needed for an edge coloring of G is equal to the maximum degree of G.
Any $m \times n$ latin rectangle with $1 \leq m \leq n$ can be completed to form an $n \times n$ latin square.
Let R be a partial $m \times p$ latin rectangle in which the symbols $\{s_1, s_2, \ldots, sn\}$ are used, and let $n_R(s_i)$ denote the number of times s_i occours in $R (1 \leq i \leq n)$. Then R can be completed to an $n \times n$ latin square if and only if
$n_R(s_i) \geq m + p - n$ $(1 \leq i \leq n)$.
A **matching** in a bipartite graph $G = (X \cup Y, E)$ is a subset M of E with the property that no two edges in M have a common vertex.
We shall say that a matching M is a **maximum matching** for $G = (X \cup Y, E)$ if no other matching has a greated cardinality. If $|M| = |X|$ (all the people get jobs), then we say that M is a **complete matching**.
If $G = (X \cup Y, E)$ and A is a subset of X, let $J(A) = \{y \in Y | xy \in E \text{ for some } x \in A\}$ so that $J(A)$ is the set of jobs for which the people in A are collectively qualified.
The bipartite graph $G = (X \cup Y, E)$ has a complete matching if an only if Hall's condition is satisfied, that is $|J(A)| \geq |A|$ for all $A \subseteq X$.