Proofs and logic	
Direct proof- $p \to q$	Proof by contrapositive - ${\sim}q \to {\sim}p$
Division into cases $(p \vee q) \to r \equiv (p \to r) \wedge (q \to r)$	Transitivity - $p \to q, q \to r, \therefore p \to r$
Elimination - $(p \vee q),\ {\sim}q, \therefore\ p$	Specialisation - $(p \wedge q), \therefore p, \therefore q$
Inverse error - ${\sim}p \to {\sim}q$	Converse error - $q \to p$
Uniqueness $\exists!\, x, P(x) \equiv \exists x, P(x) \wedge \forall a \forall b, \big(P(a) \wedge P(b)\big) \to a = b$	
Number theory	
Direct proof/Contrapositive	Pigeonhole principle
Constructive	Example/Counterexample – for existential statements
Contradiction (assume $p \to q$ and get a contradiction)	Division into cases (**modulo**, **even/odd**, **+/-/0**)
Mathematical Induction	
Strong PMI – use of every base case	PMI – 1 base case and 1 inductive step
Multiple base cases	PMI –inductive steps in both ways

Logical axioms	
Commutative: $p \wedge q \equiv q \wedge p$	Associative: $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$, $(p \vee q) \vee r \equiv p \vee (q \vee r)$
Distributive: $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	Identity: $p \wedge true \equiv p,\ p \vee false \equiv p$
Negation: $p \vee {\sim}p \equiv true, p \wedge {\sim}p \equiv false$	Idempotent: $p \vee p \equiv p \wedge p \equiv p$
De Morgan: ${\sim}(p \vee q) \equiv {\sim}p \wedge {\sim}q, {\sim}(p \wedge q) \equiv {\sim}p \vee {\sim}q$	Absorption: $p \vee (p \wedge q) \equiv\ p \wedge (p \vee q) \equiv p$
Universal bound: $p \vee true \equiv true, p \wedge false \equiv false$	Cases $(p \vee q) \to r \equiv (p \to r) \wedge (q \to r)$
Conditional: $p \to q \equiv {\sim}p \vee q$	Biconditional: $p \leftrightarrow q \equiv p \to q \wedge q \to p$
Number system - $\mathbb{R}, \mathbb{Q}, \mathbb{Z}$	
Identity: $x + 0 = x,\ x \cdot 1 = x$	Inverse: $x + (-x) = 0,\ x \cdot \left(\frac{1}{x}\right) = 1$ if $x \neq 0$
Commutative: $x + y = y + x,\ x \cdot y = y \cdot x$	Associative: $x + (y + z) = (x + y) + z,\ x \cdot (y \cdot z) = (x \cdot y) \cdot z$
Distributive: $x \cdot (y + z) = x \cdot y + x \cdot z$	
Closure properties	
Integers: closed under addition and multiplication	**Rational numbers:** addition, multiplication, division
Even integers: closed under addition and multiplication	**Odd integers:** closed under multiplication

Number Theory	
Tut3, q1: n is even if and only if n^3 is even *extension*: n^k is even/odd if and only if n is even/odd	Tut3, q8: If a is even, and $a^2 = b^3$, then $4 \mid a$ and $4 \mid b$
$a \mid b \wedge b \mid a \Longrightarrow a = \pm b$	4.1.1: If $n \in \mathbb{Z}$ then $n^2 + n$ is even
4.1.2: If $n \in \mathbb{Z}$, then $3 \mid n^3 - n$ *(proven by mod cases)*	4.1.4: Pigeonhole principle – if m pigeons go into r pigeonholes, at least one hole has more than one
Tut4, q5: There are no integers a and n with $n \geq 2$ and $a^2 + 1 = 2^n$	4.3.6: **Standard factored form** of $\forall n > 1, n \in \mathbb{Z}$ is $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ where $p_1 \dots p_k$ are primes, $e_1 \dots e_k$ are positive integers, and $p_1 < p_2 < \cdots < p_k$
5.2.1: Every positive integer can be written as the sum of distinct powers of any integer	Bernoulli inequality: $\forall x \in \mathbb{R}, x > -1, n \in \mathbb{Z}, n \geq 2,$ $1 + nx < (1 + x)^n$
Rational numbers	
3.3.5: $\forall$ positive $x, y \in \mathbb{R}, x \neq y, \frac{x}{y} + \frac{y}{x} > 2$	3.3.6: A rational number in its lowest term $\frac{m}{n}$
Congruence/Modulo	
Symmetric: $a \equiv b \bmod n \leftrightarrow b \equiv a \bmod n$	Transitive:$a \equiv b \bmod n \wedge b \equiv c \bmod n \to a \equiv c \bmod n$
$\forall\ a \in \mathbb{Z}$ and $n \in \mathbb{Z}^+, a \equiv r \bmod n$ for exactly one integer r such that $0 \leq r \leq n - 1$	$a \equiv b \bmod n$ and $c \equiv d \bmod n \Rightarrow a + c \equiv b + d \bmod n$
$a \equiv b \bmod n$ and $c \equiv d \bmod n \Rightarrow ac \equiv bd \bmod n$	$a \equiv b \bmod n \Rightarrow a^k \equiv b^k \bmod n$ for all $k \in \mathbb{Z}^+$
Absolute value	
Triangle inequality: $\forall x, y \in \mathbb{R}, \lvert x + y \rvert \leq \lvert x \rvert + \lvert y \rvert$	Tut4, q1a: $\forall x, y \in \mathbb{R},\ \lvert xy \rvert = \lvert x \rvert \lvert y \rvert$
Primes: No factors except 1 and itself	**Composites**: Not a prime

Tut4, q4: The set of primes is infinite	
4.2.3-derived: Let $p_1, p_2, \ldots p_n$ be a sequence of primes. For any prime $p_n, p_{n+1} \leq p_1 p_2 \ldots p_n + 1$	Assn1, q5b: $n < p < n!, \forall n \in \mathbb{Z}, n > 2$
Irrational Numbers($\sqrt{2}$) Definition: Not rational	
Sum of a rational and irrational number is irrational	Product of a rational and irrational number is irrational
Tut3, q4a: if x is irrational then $\sqrt{x}$ is irrational *extension*: any root of x is irrational	$\sqrt{p}$ is an irrational number
$\sqrt{2}+\sqrt{3}$ is irrational	Assn1, q4b$\sqrt{2}+\sqrt{3}+\sqrt{5}$ is irrational
Sequences	
AP: $\sum_{k=m}^{n} k = \frac{(n+m)(n-m+1)}{2}$	**GP:** Given a series $a + ar + ar^2 + ar^3 + \cdots + ar^{n-1}$, where $r \neq 1, \sum_{k=1}^{n} ar^{k-1} = \frac{a(1-r^n)}{1-r}$
Sum of squares: $\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$	Product: $\prod_{k=m}^{n} a_k = a_m \cdot a_{m+1} \cdot a_{m+2} \cdot \ldots \cdot a_n$
2nd-Order Linear Homogeneous Recurrence Relation:	
Expression: $a_k = Aa_{k-1} + Ba_{k-2}$	Characteristic eqn: $t^2 - At - B = 0$
2 roots r and s: $a_k = Cr^k + Ds^k$	1 root r: $a_k = Cr^k + Dkr^k$
Sets	
Notations: Listing {1,2,…} or Set builder $\{x \in U \mid p(x)\}$	**Operators**: ∪,∩, −, complement
Laws: Idempotent, Commutative, Associative, Distributive, De Morgan's	Distributive law on Cartesian products: $A \times (B\ op\ C) = (A \times B) op (A \times C)$
Functions	
$f: A(domain) \rightarrow B(codomain)$ $f(x) = y \Longrightarrow y$ = image of x and x = preimage of y under f, $y \in range(f)$	**Injective:** $\forall x, y \in A, x \neq y \rightarrow f(x) \neq f(y)$ **Surjective:** $\forall y \in B, \exists x \in A\ such\ that\ y = f(x)$ **Bijective**: Injective and Surjective
Relations	
aRb implies $(a,b) \in R = \{(a,b) \in A \times B \mid\ p(x,y)\}$ $a \in dom(R) \Leftrightarrow \exists b\ such\ that\ (a,b) \in R$ $b \in range(R) \Leftrightarrow \exists a\ such\ that\ (a,b) \in R$	**Reflexive**: $\forall x \in A, (x,x) \in R$ **Symmetric**: $if\ (x,y) \in R\ then\ (y,x) \in R$ **Transitive**: $if\ (x,y)\ and\ (y,z) \in R\ then\ (x,z) \in R$
Equivalence relation when R is reflexive, symmetric and transitive	**Equivalence classes**: $[a]_R = \{x \in (x,a) \in R\}$ $(a,b) \in R \Leftrightarrow [a]_R = [b]_R$ $(a,b) \notin R \Leftrightarrow [a]_R \cap [b]_R = \emptyset$
Counting	
repetition allowed, order matters: n^k (multiplication rule)	repetition allowed, order does not matter: $\binom{r+n-1}{r}$ (r-combination with repetition)
repetition not allowed, order matters:$\frac{n!}{(n-r)!}$ (r-permutation)	repetition not allowed, order does not matter: $\binom{n}{k} = \frac{n!}{r!(n-r)!}$ (r-combination)
permutations of n objects with indistinguishable elements: $\frac{n!}{n_1! n_2! n_3! \ldots n_k!}$	generalized inclusion/exclusion rule: $N(A_1 \cup \ldots \cup A_n) = \sum_{1 \leq i \leq n} N(A_i) - \sum_{1 \leq i < j < n} N(A_i \cap A_j) + \cdots + (-1)^{n+1} N(A_1 \cap A_2 \cap \ldots \cap A_n)$
Graphs	
Graph: A graph $G = \{V, E\}$ Consists of a *nonempty* set of vertices $V(G)$ and set of edges $E(G)$	Simple graph: No loops or parallel edges
Bipartite graph: graph with distinct vertices v and w such that there are no edges between any v's or w's	Handshake theorem: In any graph, the total degree of a graph is twice the number of edges, and is always even
10.1.9: In any graph, there are an even number of vertices with an odd degree	Trail: No repeat edges Path: Trail with no repeat vertices
Closed walk: Starts and ends at same vertex Circuit: Closed walk with no repeat edges Simple circuit: Circuit with no repeat vertices	Euler circuit: Visits every edge of G. G must be connected and all vertices with positive even degrees
Isomorphism: G and $G`$are isomorphic iff ∃ bijective functions $g: V(G) \rightarrow V(G`)$ and $h: E(G) \rightarrow E(G`)$ Graph isomorphism is an equivalence relation	Isomorphic invariants: vertex/edge/degree count, possible circuits, connectedness