Core
<u>Important</u>
Normal

(1) Logic
Euclidian Algorithm and GCD

$GCD(m, n)$

E0: Ensure $m > n$, swap otherwise

E1: Find $\frac{m}{n}$, set remainder r

E2: If $r = 0$, terminate, return n

E3: Set $m \leftarrow n$, $n \leftarrow r$, go to E1.

<u>Modular Arithmetic and Congruences</u>
Fermat's Little Theorem and Induction

FLT: Given a prime number p and $0 < a < p$, we have $a^p \equiv a \ (mod\, p)$ and $a^{p-1} \equiv 1 \ (mod\, p)$

Induction: Prove $P(1)$, then prove $P(n) \Rightarrow P(n+1)$ for all $n \,\varepsilon\, N$

<u>Proofs</u>

Contradiction, induction, direct

Primality Testing
Cryptography
<u>Fundamental Theorem of Arithmetic</u>

Every integer has a distinct product of primes $x = p_1 p_2 ... p_n$

<u>Exponentiation in Mod Arithmetic</u>
Infinitude of Primes

Say we have a list of all the prime $p_1,\ p_2,\ ...,\ p_n$

Take $m = p_1 p_2 ... p_n + 1$

If m is prime, new prime found.

If m is not prime, then it must be divisible by some prime number p not found in our list, as it would divide 1 if it was, which is impossible.

Either way, contradiction.

(1) Number Theory
<u>Set Theory and Proving Set Identities</u>
Translation and Symbolization

$\forall$, $\exists$, $\neg$, $\vee$, $\wedge$, $\Rightarrow$, $\Leftrightarrow$

<u>Negations in Predicate Logic</u>
Axiomatic Systems
Truth Tables

Input 1	Input 2	Output
T/F	T/F	T/F

Knights & Knaves

Venn Diagrams

Tautologies, Contradictions, Contingencies

Rules of Logic

Identity	$p \wedge 1 \equiv p$, $p \vee 1 \equiv 1$
Idempotent	$p \wedge p \equiv p$, $p \vee p \equiv p$
Complement	$p \wedge p' \equiv 0$, $p \vee p' \equiv 1$
Domination	$p \wedge 0 \equiv 0$, $p \vee 0 \equiv p$
Commutative	$p \wedge q \equiv q \wedge p$, $p \vee q \equiv q \vee p$
Associative	$p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$, $p \vee (q \vee r) \equiv (p \vee q) \vee r$
De Morgan	$(p \wedge q)' \equiv p' \vee q'$, $(p \vee q)' \equiv p' \wedge q'$
Double Negation	$(p')' \equiv p$
Absorption	$p \wedge (p \vee q) \equiv p$, $p \vee (p \wedge q) \equiv p$
Distributive	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$, $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$

Swap $\vee$ for $\cup$ and $\wedge$ for $\cap$ and we get set identities.

(2) Combinatorics

Pigeonhole Principle

Given m containers and n items, with $n > m$, then one container must have at least 2 items.

Functions

Basic Counting and Overcounting

Inclusion/Exclusion Principle

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

Erdos-Ko-Rado Theorem

Binomial Theorem and Pascal's Triangle

$(x+y)^n = (n\ ch.\ 0)x^n y^0 + (n\ ch.\ 1)x^{n-1}y^{\ 1} + (n\ ch.\ 2)x^{n-2}y^2 + \ldots + (n\ ch.\ n-1)x^1 y^{n-1} + (n\ ch.\ n)x^0 y^n$

(2) Graph Theory

Euler Tours and Circuits

An Eulerian Path is a trail which visits every edge once.

An Eulerian Circuit is an Eulerian Path which starts and ends on the same vertex.

Trees

Hamilton Cycles and Dirac's Theorem

A cycle which visits each node exactly once. A Hamiltonian Graph has one.

Dirac's Theorem: An n-vertex graph where each vertex has degree at least $n/2$ must contain a Hamilton Cycle.

Prufer Codes and Cayley's Theorem

Prufer Code:

Given a tree with n vertices

P1: Given a string of numbers length $n-2$, add 0 to the end

P2: Construct a row of numbers $\{0, 1, ..., n-1\}$ above the original, left to right, where each entry has not yet appeared in the top row and is not to the bottom and right of the current location.

P3: Create an edge joining the nodes of the rightmost pair, and create an edge joining the bottom number to a newly created top number for each subsequent pair from right to left.

Cayley's Theorem:

The number of trees on n labelled vertices is n^{n-2}.

Euler's Formula

A connected planar graph satisfies $|V|+|F|-|E|=2$

Greedy Colouring Algorithm

Marriage Theorem

Bipartite Graphs

Planar Graphs

5-Colour Theorem

K_5, $K_{3,3}$ not planar

(͡° ͜ʖ ͡°)