Further pure mathematics **(M303)** content listing

Chapter 1 *Foundations*	Proof by induction, divisibility, linear Diophantine equations
Chapter 2 *Prime numbers*	Prime numbers, Fundamental Theorem of Arithmetic, prime decomposition of integers, the τ-function, Fibonacci numbers.
Chapter 3 *Congruence*	Definition of congruence, properties of congruence, divisibility tests, linear congruences, solution of linear congruences, solving systems of linear congruences.
Chapter 4 *Fermat's and Wilson's Theorems*	Fermat's Little Theorem, Wilson's Theorem, polynomial congruences, Lagrange's Theorem (for numbers)
Chapter 5 *Examples of groups*	Group axioms, subgroups, cosets, Lagrange's Theorem (for groups), normal subgroups, quotient groups, conjugate elements, homomorphism of groups, isomorphism of groups, first isomorphism theorem, correspondence theorem.
Chapter 6 *Towards classification*	Direct product of groups, internal direct product theorem, cyclic groups, direct product of cyclic groups, decomposition of finite cyclic groups, group actions, orbits and stabilisers.
Chapter 7 *Finite groups*	Group presentations, dihedral groups, dicyclic groups, centraliser and centre of a group, groups of small order, finite p-groups, composition series, soluble groups.
Chapter 8 *The Sylow Theorems*	Sylow p-subgroup, the Sylow theorems, applications of the Sylow theorems, prime power subgroups theorem.
Chapter 9 *Multiplicative functions*	Multiplicative functions, Euler's ϕ-function, reduced set of residues, Euler's theorem, primitive roots.
Chapter 10 *Quadratic reciprocity*	Solutions of quadratic congruences, quadratic residues, Euler's criterion, the Legendre symbol, Gauss's Lemma, quadratic character of 2, the law of quadratic reciprocity, quadratic character of 3, the Jacobi symbol.
Chapter 11 *Rings and polynomials*	Ring axioms, subrings, units, fields, polynomials over fields, division algorithm for polynomials, factors of a polynomial, Euclidean algorithm for polynomials, factorising polynomials, irreducibility for polynomials, rational root test, Gauss's lemma, Eisenstein's criterion.
Chapter 12 *Fermat's Last Theorem and unique factorisation*	Pythagorean triples; integral domains; associates, irreducibles and primes in rings; integral domains, norms for integral domains; Euclidean domains; division algorithm for Euclidean domains; highest common factors in Euclidean domains; unique factorisation domains.
Chapter 13 *Distance and continuity*	Sequences in the real line; real null sequences; continuity of real-valued functions; intermediate value theorem; extreme value theorem; continuity on the plane; Euclidean distance on the plane.
Chapter 14 *Metric spaces and continuity 1*	Continuity of functions from $\mathbb{R}^n$ to $\mathbb{R}^m$, Euclidean distance on $\mathbb{R}^n$, convergent sequences in $\mathbb{R}^n$, metrics, metric spaces, convergence of sequences in metric spaces, continuity in metric spaces.
Chapter 15 *Metric spaces and continuity 2*	Induced metrics, Cantor metric, equivalent metrics, product metrics, pointwise convergence of functions, uniform convergence of functions, the max metric on $C[0,1]$.
Chapter 16 *Open and closed sets*	Open sets, closed sets, dense sets, nowhere dense sets, closure of a set, interior of a set, boundary of a set, countable sets, uncountable sets.
Chapter 17 *Rings and homomorphisms*	Fields of fractions, ring isomorphisms, primitive polynomials, ideals, principal ideals, principal ideal domain, algebra of ideals, cosets of an ideal, quotient rings, ring homomorphisms, maximal ideals, prime ideals.
Chapter 18 *Fields and polynomials*	Isomorphism of fields, field extensions, vector spaces over fields, degree of a field extension, algebraic and transcendental elements, minimal polynomials, the KLM Theorem for field extensions, finite fields, roots of unity, splitting fields, splitting polynomials, classification of finite fields.

Chapter 19 *Fields and geometry*	Subfield generated by a set, field extensions of finite degree, field of algebraic numbers, transcendental extension, ruler and compass constructions, constructible number, impossibility of doubling the cube, squaring the circle and trisecting the angle $\pi/3$.
Chapter 20 *Public-key cryptography*	RSA cryptosystem, Diffie-Hellman cryptosystem, elliptic curves, Diffie-Hellman-ElGamal cryptosystem, Menezes-Vanstone cryptosystem.
Chapter 21 *Connectedness*	Homeomorphisms, disconnections, connectedness, connected components, totally disconnected sets, connectedness in Euclidean spaces, the intermediate value theorem, path-connectedness, the topologist's cosine.
Chapter 22 *Compactness*	Sequential compactness, the Heine-Borel theorem, generalised extreme value theorem, Arzelà-Ascoli Theorem, open covers, compact metric spaces, equivalence of sequential compactness and compactness in metric spaces.
Chapter 23 *Completeness*	Cauchy sequences, complete metric spaces, the contraction mapping theorem, completion of a metric space.
Chapter 24 *Fractals*	The Hausdorff metric, self-similar sets, iterated function schemes, box dimension, open set condition.