620-351 Number Theory

Credit Points:	12.50
Level:	3 (Undergraduate)
Dates & Locations:	2009, This subject commences in the following study period/s: Semester 2, - Taught on campus. Lectures and practice classes.
Time Commitment:	Contact Hours: 36 one-hour lectures (three per week) and up to 12 one-hour practice classes (one per week) Total Time Commitment: 120 hours total time commitment.
Prerequisites:	One of # 620-120 (UMEP Mathematics for High Achieving Students) (prior to 2008) # 620-121 (prior to 2008) # 620-140 (prior to 2008) # 620-141 (prior to 2008) **Or** One of # *Linear Algebra* # *Accelerated Mathematics 1* (620-157 Mathematics 1 prior to 2009), # 620-190 (UMEP Mathematics for High Achieving Students) and one of # *Calculus 2* # *Accelerated Mathematics 2* (620-158 Mathematics 2 prior to 2009)
Corequisites:	None
Recommended Background Knowledge:	None
Non Allowed Subjects:	None
Core Participation Requirements:	It is University policy to take all reasonable steps to minimise the impact of disability upon academic study and reasonable steps will be made to enhance a student's participation in the University's programs. Students who feel their disability may impact upon their active and safe participation in a subject are encouraged to discuss this with the relevant subject coordinator and the Disability Liaison Unit.
Coordinator:	Dr John Richard James Groves
Subject Overview:	This subject introduces the elementary concepts of divisibility; the basic theory and use of congruences; the properties of powers of elements in congruences, particularly Euler's theorem; the law of quadratic reciprocity; and basic properties of continued fractions and some applications. It develops applications of all of the above to primality testing, factorisation algorithms and cryptanalysis. Students should develop the ability to perform the algorithms inherent in the subject material; and to understand and present proofs related to the subject material. This subject demonstrates the extent and uses of elementary number theory, its applicability in other parts of mathematics, and its potential for application outside of mathematics. Topics include factorisation, primes and greatest common divisors; congruences; primitive roots; quadratic reciprocity; continued fractions and Pell's equation; compositeness testing and factorisation; and applications to cryptanalysis.
Objectives:	.

Assessment:	Up to 24 pages of written assignments due during the semester and a 50-minute written test held mid-semester (equally weighted, with a total of either 0% or 20%); a 3-hour written examination in the examination period (80% or 100%). The relative weighting of the examination and total assignment plus test mark will be chosen so as to maximise the student's final mark.
Prescribed Texts:	None
Breadth Options:	This subject potentially can be taken as a breadth subject component for the following courses: # **Bachelor of Arts (https://handbook.unimelb.edu.au/view/2009/D09)** # **Bachelor of Commerce (https://handbook.unimelb.edu.au/view/2009/F04)** # **Bachelor of Environments (https://handbook.unimelb.edu.au/view/2009/A04)** # **Bachelor of Music (https://handbook.unimelb.edu.au/view/2009/M05)** You should visit **learn more about breadth subjects (http://breadth.unimelb.edu.au/breadth/info/index.html)** and read the breadth requirements for your degree, and should discuss your choice with your student adviser, before deciding on your subjects.
Fees Information:	Subject EFTSL, Level, Discipline & Census Date, http://enrolment.unimelb.edu.au/fees
Notes:	This subject is available for science credit to students enrolled in the BSc (pre-2008 degree only), BASc or a combined BSc course.
Related Majors/Minors/ Specialisations:	Mathematics and Statistics (Discrete Mathematics specialisation) Mathematics and Statistics (Pure Mathematics specialisation)