

INSTITUTE OF MATHEMATICS
College of Science
University of the Philippines Diliman

Math 117 Course Syllabus

A. Course Catalogue Description

Course Number	Math 117
Course Title	Elementary Theory of Numbers
Course Description	Divisibility, Euclidean algorithm, primes and the fundamental theorem of arithmetic, congruences, systems of linear congruences, primitive roots, primality testing, cryptography, quadratic residues and the quadratic reciprocity law, Diophantine equations
Prerequisite	Math 108/equiv. or COI
Course Credit	3 units
Number of Hours	3 hours/week

B. Course Content

- I. Course Overview and Orientation
- II. The Integers and Divisibility
 1. Divisibility and the Division Algorithm
 2. Greatest common divisor and least common multiple
 3. Euclidean algorithm and Bezout's identity
 4. Primes and the fundamental theorem of arithmetic
 5. The distribution of primes and the Riemann zeta function
 6. Fermat and Mersenne primes
 7. Linear Diophantine equations
- III. Modular Arithmetic
 1. Congruences and congruence classes
 2. Linear congruences
 3. Systems of linear congruences and the Chinese remainder theorem
 4. Some special congruences
 - a. Wilson's theorem
 - b. Fermat's little theorem
 - c. The Euler phi-function and Euler's theorem
 5. Primitive roots
 6. Primality testing and cryptography
- IV. Quadratic congruences
 1. Quadratic residues
 2. The Legendre symbol
 3. The quadratic reciprocity law
- V. Some nonlinear Diophantine equations
 1. Primes which are sums of two squares
 2. The Pythagorean equation
 3. Infinite descent and Fermat's last theorem
- VI. Selected topics (the lecturer may choose any topic in number theory, including but not limited to the following)
 1. Elliptic curves
 2. Simple continued fractions
 3. Arithmetic functions
 4. Pell's equation

For a more detailed syllabus, send an email request to ddapr@math.upd.edu.ph.