

COURSE NAME/NUMBER**LEARNING OBJECTIVES / GOALS / OUTCOMES / LEARNING OUTCOMES:**

This course will serve as an introduction to the fundamental ideas of number theory, a foundational and historically important part of “pure” mathematics, but with close attention paid throughout the course to the many modern applications to computing and communications. On completion of the course the successful student will thus:

1. Be able to precisely define and elucidate the central concepts and results of elementary number theory such as prime number, gcd, congruences and their solution methods, Euler’s theorem, and continued fractions
2. Be able to structure correct arguments (proofs) concerning these concepts and their interrelations
3. Be able to precisely define and implement applications of the ideas above to techniques such as cryptology and error correction
4. Be able to perform all the necessary computations by hand (in principle) and in a computer algebra environment such as Maple.

Many students require a number theory course as a prerequisite for PDP programs. This course will serve as such a prerequisite.

METHODS:

The course will be primarily lecture-based, with some computational support provided by a computer algebra system such as Maple. Evaluation will include quizzes, tests, assignments and a final exam.

PRIOR LEARNING ASSESSMENT RECOGNITION (PLAR):

Credit can be awarded for this course through PLAR (Please check :) Yes No

METHODS OF OBTAINING PLAR:

Course challenge

TEXTBOOKS, REFERENCES, MATERIALS:

[Textbook selection varies by instructor. An example of texts for this course might be:]

Elementary number theory and its applications (4th ed), Kenneth H. Rosen, Addison Wesley (1992)

SUPPLIES / MATERIALS:

Access to a computer algebra system

STUDENT EVALUATION:

[An example of student evaluation for this course might be:]

The weighting of the various components may vary from instructor to instructor and from year to year, although there must be at least two midterms, and the comprehensive final exam must be worth from 30% to 50% of the final grade. A student must obtain at least 40% on the final exam to pass the course.

A example of student evaluation for this course:

Quizzes	10%
Assignments	20%
Tests (2)	30%
Final exam	40%

COURSE CONTENT:

[Course content varies by instructor. An example of course content might be:]

1. The integers (sequences, sums, induction, divisibility)
2. Computer operations with integers (representation and complexity)
3. Prime numbers and gcds (prime numbers, gcds, Euclidean algorithm, fundamental theorem of arithmetic, factorization methods, linear Diophantine equations)
4. Congruences (linear congruences, Chinese remainder theorem, polynomial congruences, systems of linear congruences)

5. Applications of congruences (divisibility test, hashing functions, check digits)
6. Special congruences (Euler's theorem, Wilson's theorem, pseudoprimes (applications to primality testing))
7. Multiplicative functions (Euler phi-functions, perfect numbers, Mersenne primes)
8. Cryptology (block ciphers, exponentiation ciphers, public key cryptography, knapsack ciphers)
9. Decimal fractions and continued fractions
10. (If time permits) Primitive roots (order of an integer, existence of primitive roots, primality tests)