COURSE NAME:	**NUMBER THEORY**
COURSE CODE:	**MATH 3405**
LEVEL:	**III**
NUMBER OF CREDITS:	**3**
SEMESTER:	**I**
PREREQUISITES:	**MATH2401: Elements of Mathematical Analysis** **MATH2411: Introduction to Abstract Algebra**

RATIONALE: As the eminent mathematician Gauss once said, mathematics is the queen of the sciences and number theory is the queen of mathematics. Number Theory was anchored even more firmly at the centre of modern mathematics when the historic Fermat's Last Theorem was proved in 2000. Number Theory is not only fascinating, but it is linked to other mathematical subjects such as Analysis, Algebraic Geometry and Topology. In recent times it is shown to have extremely useful applications that were not foreseen like cryptography (eg. internet security). In particular, its cryptoanalytic application makes it relevant. Moreover, any concepts of Algebra originated in Number Theory.

COURSE DESCRIPTION: This course is for third-year mathematics majors and interested students in computing and related areas. It gives a thorough introduction to and analysis of principles of divisibility using Diophantine equations, Bezout's Identity, the classes of prime numbers, Euler's function and its application and group of units. Also, it prepares students for graduate study in Algebra, Number Theory, or related areas in Computing such as Cryptanalysis.

LEARNING OUTCOMES: On successful completion of the course, the student should be able to:

- Prove new and elementary results in Number Theory using results and methods introduced in the course.

- Solve Diophantine Equations, Linear and Nonlinear Congruences.

- Use advanced techniques such as the Extended Chinese Remainder Theorem to produce original proofs of new results.

COURSE CONTENT:

1. **Divisors:** Elementary results on divisors, Bezout's Identity, Linear Diophantine Equations

2. **Prime Numbers:** Prime-Power Factorizations, Distribution of Primes, Fermat and Mersenne Primes

3. **Congruences:** Modular Arithmetic, Linear Congruences, Simultaneous Linear Congruences, Simultaneous Nonlinear Congruences, the extended Chinese Remainder Theorem

4. C**ongruences with a Prime Power Modulus:** The arithmetic of Z_p, Pseudoprimes and Carmichael Numbers, solving Congruences mod p^n.

5. **Euler's function:** Units, Euler's Function, Applications of Euler's Function.

6. **The Group of Units:** The group U_n, Primitive Roots, The group U_n when $n = p^k$ Applications of Primitive Roots.

TEACHING METHODOLOGY

The abstract concepts, illustrated with numerous examples, will be presented during the interactive lectures. The total of 39 contact hours may be accounted for as follows: 26 hours of expository and proof-orientated lectures and 13 hours of problem based learning tutorials. Students will receive weekly problem sets designed to solidify their understanding of the course content. The problem sets will also form the foundation for future incourse tests and the final examination. Course material, including practice problems, will be posted on the course webpage, currently supported by OurVLE

ASSESSMENT:

The course assessment has two components:

- Two (1 hour) midterm tests; (20% each) **40%**
- Final written examination paper (2 hours); **60%**

REFERENCE MATERIALS:

Books:

Prescribed

1. Jones G, and Jones M, *1998, Elementary Number Theory*, Springer Undergraduate Mathematics Series, *ISBN-13: 978-3540761976*

Highly Recommended

2. Stillwell J, *2010, Elements of Number Theory*, Springer, *ISBN-13: 978-1441930668*

3. Marshall D, Edward O, and Starbird M, *2007, Number Theory Through Inquiry*, Mathematical Association of America, *ISBN-13: 978-0883857519*

Online Resources:

1. www.artofproblemsonlving.com/Resources/Papers/SatoNT.pdf This is a 45-page paper by Prof Sato giving the basics of number theory in an accessible way. It also contains many links to other websites.

2. www.dmoz.org/Science/Math/Number_Theory/ This site gives a good overview of number theory and contains many links to other websites.

3. www.math.usf.edu/~wclark/#ELEMENTARY_NUMBER_THEORY This is a free textbook in number theory and makes a very accessible companion to a standard textbook.