COURSE IMPLEMENTATION DATE: September 2002
COURSE REVISED IMPLEMENTATION DATE: September 2006
COURSE TO BE REVIEWED: September 2009
(Four years after UPAC Final Approval Date) (MONTH YEAR)

OFFICIAL COURSE OUTLINE INFORMATION

Students are advised to keep course outlines in personal files for future use.
Shaded headings are subject to change at the discretion of the department and the material will vary - see course syllabus available from instructor

FACULTY/DEPARTMENT: **Science, Health & Human Services / Mathematics & Statistics**

MATH 355		**3**
COURSE NAME/NUMBER	FORMER COURSE NUMBER	UCFV CREDITS

Number Theory and Applications
COURSE DESCRIPTIVE TITLE

CALENDAR DESCRIPTION:

An introduction to the fundamental ideas of number theory, with attention to applications in computation, cryptography and communications.
Topics include primes and gcds, congruence, and applications (hashing functions, check digits), factorization methods and cryptology (ciphers, public key cryptography, etc.) and continued fractions.

PREREQUISITES: One of Math 214, Math 265, Math 221, or Math 225.
COREQUISITES:

SYNONYMOUS COURSE(S)
(a) Replaces: _____ *(Course #)*
(b) Cannot take: _____ *(Course #)* for further credit.

SERVICE COURSE TO:
_____ *(Department/Program)*
_____ *(Department/Program)*

TOTAL HOURS PER TERM: **45**
STRUCTURE OF HOURS:

Lectures:	**45**	Hrs
Seminar:		Hrs
Laboratory:		Hrs
Field Experience:		Hrs
Student Directed Learning:		Hrs
Other (Specify):		Hrs

TRAINING DAY-BASED INSTRUCTION
LENGTH OF COURSE: _____
HOURS PER DAY: _____

MAXIMUM ENROLLMENT: **36**
EXPECTED FREQUENCY OF COURSE OFFERINGS: **Every 2 to 3 years**

WILL TRANSFER CREDIT BE REQUESTED? (lower-level courses only)	☐ Yes	☐ No
WILL TRANSFER CREDIT BE REQUESTED? (upper-level requested by department)	☐ Yes	☒ No
TRANSFER CREDIT EXISTS IN BCCAT TRANSFER GUIDE:	☐ Yes	☒ No

AUTHORIZATION SIGNATURES:

Course Designer(s): Susan Milner
Chairperson: *(Curriculum Committee)*
Department Head: Greg Schlitt
Dean: Jacalyn Snodgrass
PAC Approval in Principle Date:
PAC Final Approval Date: September 30, 2005

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. Please check online at http://www.ucfv.ca/math/challenge.htm for the departmental challenge policy.

TEXTBOOKS, REFERENCES, MATERIALS:

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

Chosen by departmental curriculum committee. An example:

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

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 t midterms, and the comprehensive final exam must be worth from 30% to 50% of the final grade. A student must obtain at least 40% o exam to pass the course.

An 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, psuedoprimes (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)