UNIVERSITY OF THE FRASER VALLEY

ORIGINAL COURSE IMPLEMENTATION DATE: September 2002
REVISED COURSE IMPLEMENTATION DATE: September 2016
COURSE TO BE REVIEWED: (six years after UEC approval) February 2021
Course outline form version: 09/15/14

OFFICIAL UNDERGRADUATE COURSE OUTLINE FORM

Note: The University reserves the right to amend course outlines as needed without notice.

Course Code and Number: MATH 355	**Number of Credits:** 3 Course credit policy (105)
Course Full Title: Number Theory and Applications **Course Short Title (if title exceeds 30 characters):**	
Faculty: Faculty of Science	**Department (or program if no department):** Mathematics & Statistics

Calendar Description:

An introduction to the fundamental properties of the integers and their consequences, with applications in computation, cryptography, and communications. Topics include primes and gcds, congruence, (modular arithmetic), and applications (hashing functions, check digits), factorization methods, and cryptology.

Prerequisites (or NONE):	MATH 265 with a grade of C or better.
Corequisites (if applicable, or NONE):	
Pre/corequisites (if applicable, or NONE):	

Equivalent Courses (cannot be taken for additional credit)
Former course code/number:
Cross-listed with:
Equivalent course(s):
Note: Equivalent course(s) should be included in the calendar description by way of a note that students with credit for the equivalent course(s) cannot take this course for further credit.

Transfer Credit
Transfer credit already exists: ☐ Yes ☒ No
Transfer credit requested (OReg to submit to BCCAT):
☐ Yes ☒ No (if yes, fill in transfer credit form)
Resubmit revised outline for articulation: ☐ Yes ☒ No
To find out how this course transfers, see **bctransferguide.ca**.

Total Hours: 45
Typical structure of instructional hours:

Lecture hours	45
Seminars/tutorials/workshops	
Laboratory hours	
Field experience hours	
Experiential (practicum, internship, etc.)	
Online learning activities	
Other contact hours:	
Total	**45**

Special Topics
Will the course be offered with different topics?
☐ Yes ☒ No
If yes, different lettered courses may be taken for credit:
☐ No ☐ Yes, repeat(s) ☐ Yes, no limit
Note: The specific topic will be recorded when offered.

Maximum enrolment (for information only): 36

Expected frequency of course offerings (every semester, annually, every other year, etc.): Every 2 to 3 years

Department / Program Head or Director: Cynthia Loten	**Date approved:**	September 29, 2014
Faculty Council approval	**Date approved:**	October 2014
Campus-Wide Consultation (CWC)	**Date of posting:**	January 23, 2015
Dean/Associate VP: Lucy Lee	**Date approved:**	October 17, 2014
Undergraduate Education Committee (UEC) approval	**Date of meeting:**	February 27, 2015

Learning Outcomes

Upon successful completion of this course, students will be able to:

1. Precisely design the central concepts and results of elementary number theory such as prime number, gcd, Fundamental Theorem of Arithmetic, the Chinese Remainder Theorem, and Euler's Theorem.
2. Construct proofs, examples, and counterexamples concerning these concepts and their interrelations.
3. Apply the theory of congruences to other problems (for example, constructing divisibility tests, solving linear Diophantine equations, polynominal congruences, and systems of linear congruences).
4. Precisely define and implement applications of the ideas above to techniques such as cryptology and error correction. Perform all the necessary computations by hand (in principle) and in a computer algebra environment such as Maple or Sage.

Prior Learning Assessment and Recognition (PLAR)

☒ Yes ☐ No, PLAR cannot be awarded for this course because

Typical Instructional Methods (guest lecturers, presentations, online instruction, field trips, etc.; may vary at department's discretion)

This course will be primarily lecture based, with some computational support provided by a computer algebra system such as Maple or Sage. This course is well-suited to student presentations, if feasible (depending on class size).

Grading system: Letter Grades: ☒ Credit/No Credit: ☐ Labs to be scheduled independent of lecture hours: Yes ☐ No ☒

NOTE: The following sections may vary by instructor. Please see course syllabus available from the instructor.

Typical Text(s) and Resource Materials (if more space is required, download Supplemental Texts and Resource Materials form)

	Author (surname, initials)	Title (article, book, journal, etc.)	Current ed.	Publisher	Year
1.	Kenneth H Rosen	Elementary Number Theory and its Applications	☒	Addison Wesley	2011
2.	GA Jones & JM Jones	Elementary Number Theory (SUMS series book)	☒	Springer	1998
3.	JK Strayer	Elementary Number Theory	☒	Waveland Press	1994
4.			☐		
5.			☐		

Required Additional Supplies and Materials (software, hardware, tools, specialized clothing, etc.)

Typical Evaluation Methods and Weighting

Final exam:	40%	Assignments:	20%	Midterm exam:	30%	Practicum:	%
Quizzes/tests:	**10**%	Lab work:	%	Field experience:	%	Shop work:	%
Other:	%	Other:	%	Other:	%	Total:	100%

Details (if necessary): Students must achieve at least 40% on the final exam in order to receive credit for this course.

Typical Course Content and Topics

- Fundamental properties of the integers; divisibility and factorization (prime numbers, gcds, Euclidean algorithm, Fundamental Theorem of Arithmetic, factorization methods, linear Diophantine equations)
- Congruences (linear congruences, Chinese reminder theorem, polynomial congruences, systems of linear congruences)
- Applications of congruences (divisibility tests, hashing functions, check digits)
- Special congruences (Fermat's and Euler's Theorem, Wilson's Theorem, pseudoprimes (applications to primality testing)
- Number-theoretic functions (Multiplicative functions, Euler's phi-functions, Mobius Inversion, perfect numbers, Mersenne primes)
- Cryptology (block ciphers, exponentiation ciphers, public key cryptography, knapsack ciphers)
- Computer algebra systems for number theory (Maple, Yacas, Sage, Maxima, PARI/GP)
- Additional topics as time permits such as: Gaussian integers and norms (sums of squares), quadratic reciprocity, continued fractions, primitive roots (order of an integer, existence of primitive roots, primality tests)