



ORIGINAL COURSE IMPLEMENTATION DATE: September 2002  
 REVISED COURSE IMPLEMENTATION DATE: September 2026  
 COURSE TO BE REVIEWED (six years after UEC approval): February 2032  
 Course outline form version: 29/08/2024

## OFFICIAL UNDERGRADUATE COURSE OUTLINE FORM

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

<b>Course Code and Number:</b> MATH 355	<b>Number of Credits:</b> 3 <a href="#">Course credit policy (105)</a>												
<b>Course Full Title:</b> Number Theory and Applications <b>Course Short Title:</b> Number Theory & Applications													
<b>Faculty:</b> Faculty of Science	<b>Department/School:</b> Mathematics & Statistics												
<b>Calendar Description:</b> 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 its applications (divisibility tests, hashing functions, check digits), number-theoretic functions and cryptology.													
<b>Prerequisites (or NONE):</b>	MATH 265.												
<b>Corequisites (if applicable, or NONE):</b>	None.												
<b>Pre/corequisites (if applicable, or NONE):</b>	None.												
<b>Antirequisite Courses</b> <i>(Cannot be taken for additional credit.)</i> Former course code/number: Cross-listed with: Equivalent course(s): <i>(If offered in the previous five years, antirequisite course(s) will be included in the calendar description as a note that students with credit for the antirequisite course(s) cannot take this course for further credit.)</i>	<b>Course Details</b> Special Topics course: <b>No</b> <i>(If yes, the course will be offered under different letter designations representing different topics.)</i> Directed Study course: <b>No</b> <i>(See <a href="#">policy 207</a> for more information.)</i> Grading System: <b>Letter grades</b> Delivery Mode: <b>May be offered in multiple delivery modes</b> Expected frequency: <b>Every other year</b> Maximum enrolment (for information only): <b>24</b>												
<b>Typical Structure of Instructional Hours</b> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 80%;">Lecture/seminar</td> <td style="width: 20%; text-align: center;">50</td> </tr> <tr> <td> </td> <td> </td> </tr> <tr> <td style="text-align: right;"><b>Total hours</b></td> <td style="text-align: center;"><b>50</b></td> </tr> </table>	Lecture/seminar	50									<b>Total hours</b>	<b>50</b>	<b>Prior Learning Assessment and Recognition (PLAR)</b> PLAR is available for this course.
Lecture/seminar	50												
<b>Total hours</b>	<b>50</b>												
<b>Scheduled Laboratory Hours</b> Labs to be scheduled independent of lecture hours: <b>No</b>	<b>Transfer Credit</b> <i>(See <a href="#">bctransferguide.ca</a>.)</i> Transfer credit already exists: <b>Yes</b> Submit outline for (re)articulation: <b>No</b> <i>(If yes, fill in <a href="#">transfer credit form</a>.)</i>												
<b>Department approval</b>	<b>Date of meeting:</b> June 16, 2025												
<b>Faculty Council approval</b>	<b>Date of meeting:</b> September 5, 2025												
<b>Undergraduate Education Committee (UEC) approval</b>	<b>Date of meeting:</b> February 27, 2026												

**Learning Outcomes** (These should contribute to students' ability to meet program outcomes and thus Institutional Learning Outcomes.)

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

1. Define the central concepts of elementary number theory such as prime numbers, gcd, modular arithmetic, and arithmetic functions.
2. State key theorems such as the Division Algorithm, the Prime Number Theorem, Fundamental Theorem of Arithmetic, the Euler's Totient Theorem, Chinese Remainder Theorem, and Fermat's Last Theorem.
3. Apply core theorems and algorithms (for example the Chinese Remainder Theorem, Euclidean Algorithm) to prove related properties.
4. Construct rigorous proofs, illustrative examples, and relevant counterexamples concerning core number-theoretic concepts and their interrelations.
5. Apply the theory of congruences to solve problems such as constructing divisibility tests, solving linear Diophantine equations, polynomial congruences, and systems of linear congruences.
6. Implement course concepts in applications such as cryptography and error correction.
7. Perform calculations by hand and computer algebra systems.

**Recommended Evaluation Methods and Weighting** (Evaluation should align to learning outcomes.)

Final exam:	40%	Assignments:	15%	%
Quizzes/tests/midterm:	45%		%	%

**Details:**

Students must achieve at least 40% on the final exam in order to receive credit for this course.

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

**Typical Instructional Methods** (Guest lecturers, presentations, online instruction, field trips, etc.)

This course is primarily lecture based, with some computational support provided by a computer algebra system. It is well-suited to student presentations, if feasible (depending on class size). The course is learner centred, inquiry and experiential-learning based, recognizes awareness of all people in equal measure, and supports a variety of learning styles (through class discussion, written assignments, and class presentations, for example).

**Texts and Resource Materials** (Include online resources and Indigenous knowledge sources. [Open Educational Resources](#) (OER) should be included whenever possible. If more space is required, use the [Supplemental Texts and Resource Materials form](#).)

Type	Author or description	Title and publication/access details	Year
1. Textbook	JK Strayer	Elementary Number Theory, Waveland Press	2002
2. Textbook	GA Jones and JM Jones	Elementary Number Theory (SUMS series book), Springer	1998
3. Textbook	Kenneth H Rosen	Elementary Number Theory and its Applications, Addison Wesley	2011
4.			
5.			

**Required Additional Supplies and Materials** (Software, hardware, tools, specialized clothing, etc.)**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 Remainder Theorem, polynomial congruences, systems of linear congruences)
- Applications of congruences (divisibility tests, hashing functions, check digits)
- Special congruences (Fermat's Theorem, Euler's Theorem, Wilson's Theorem, pseudoprimes with applications to primality testing)
- Number-theoretic functions (multiplicative functions, Euler's phi-function, Möbius Inversion, perfect numbers, Mersenne primes)
- Cryptology (block ciphers, exponentiation ciphers, public key cryptography, knapsack ciphers)
- Computer algebra systems for number theory (Maple, Mathematica, SageMath, Maxima, PARI/GP, Yacas)
- 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)