Department of Mathematics & Statistics
Concordia University

MATH 392
Elementary Number Theory
Winter 2026

Instructor: Dr. Tian Wang
Email: tian.wang@concordia.ca

Class Schedule: Mondays & Wednesdays, 16:15-17:30, FB S109 (SGW Campus).

Office Hours: Mondays, 14:00-15:30, or by appointment in LB 915-5.

Course Description: Welcome to *Elementary Number Theory!* Number theory is a classical subject with results dating back thousands of years, yet it is also the most modern of subjects, with new discoveries being made at a rapid pace. In this course, we will explore a wide range of foundational topics in number theory. These include integers, prime numbers, congruences, cryptology, primitive roots, quadratic residues, continued fractions, and Diophantine equations. In addition, this course will help you develop your skills in problem-solving, proof writing, logical reasoning, collaboration, and communication.

Prerequisite: MATH 251 or higher.

Moodle: Important information about the course will be posted on Moodle; please check it out frequently.

Textbook: *Elementary Number Theory*, *6th Edition* by Kenneth H. Rosen.

Students may find the textbook online. The course material mostly follows from this book.

Grading Scheme: Your overall score is determined by the maximum of the following weighted average.

Assignment	30%
Midterm	25%
Final	45%

Assignment	20%
Midterm	30%
Final	50%

Although participation is not graded, the most successful students in this class regularly attend lectures, arrive on time, engage deeply with the material, and collaborate with peers.

If the grading scheme for this course includes graded assignments, a reasonable and representative subset of each assignment may be graded. Students will not be told in advance which subset of the assigned problems will be marked and should therefore attempt all assigned problems.

Exams: The course includes one midterm exam and one final exam. The midterm will be held **in class** on **Wednesday, February 25, 2026**. Students are expected to plan accordingly. The date and time of the final exam will be announced at a later time. All exams are conducted in person, and collaboration is strictly prohibited. Exam dates and updates will be posted on **Moodle**.

Assignments: Homework assignments are typically posted on Moodle on Wednesdays and are due approximately two weeks later. Students are encouraged to work in small groups; however, all submitted work must be completed independently. A reasonable and representative subset of each assignment will be graded. Students will not be informed in advance which problems will be marked and should therefore attempt all assigned problems.

Assignment	Post Day	Due Day
1	01.12	01.26
2	01.14	02.02
3	01.21	02.09
4	01.28	02.16
5	02.09	02.23
6	03.04	03.18
7	03.09	03.23
8	03.16	03.30
9	03.23	04.08

Tentative Schedule for Covered Sections

Weeks	Monday	Wednesday	Topics Covered
Week 1 (01.12 - 01.14)	1.1,1.2,1.3, 1.5, 2.1	3.3, 3.4	Representations of Integers, Mathematical Induction, proof by contradiction, integers, gcd and lcm, Euclidean division, The division algorithm

Week 2 (01.19 - 01.21)	3.1, 3.2	3.5, 3.7	sieve of Eratosthenes, infiniteness of primes, prime number theorem, Dirichlet's theorem, fundamental theorem of arithmetic, linear Diophantine equations, introduction to congruences and moduli
Week 3 (01.26 - 01.28)	4.1, 4.2, 4.3	4.4, 5.1	introduction to congruences, solving linear congruences, the Chinese Reminder Theorem, reduced residue system, Hensel's lemma, divisibility tests
Week 4 (02.02 - 02.04)	6.1, 6.2, 6.3	7.1, 7.2, 7.3	Pseudoprimes, perfect numbers and Mersenne Primes, Wilson's Theorem, Fermat's Little Theo-rem, Euler phi function, sum of divisors function,
Week 5 (02.09 - 02.11)	7.5, 2.3	8.4, 8.6	partition, complexity, RSA, Diffie-Hellman Key Exchange, Digital Signatures,
Week 6 (02.16 - 02.18)	9.1, 9.2,	11.1	The order of an integer, primitive roots, primitive roots for primes, Quadratic Residues and Non-residues
Week 7 (02.23 - 02.25)	Review	Midterm	Bring the your questions to class
Reading Week (03.02.- 03.08)	Reading Week	Reading Week	
Week 8 (03.09 - 03.11)	11.2, 11.3	11.4, 11.5	Jacobi symbol, Quadratic reciprocity, Zero-Knowledge Proofs
Week 9 (03.16 - 03.18)	13.1	13.2	Pythagorean Triples, Diophantine equations of the form $x^a + y^b = z^c$
Week 10 (03.23 - 03.25)	13.3, 14.1	13.5	Sums of squares, Gaussian Integers and Gaussian Primes, the congruent number problem
Week 11 (03.30 - 04.01)	12.1, 12.2	12.3	finite and infinite continued and real numbers
Week 12 (04.06 - 04.08)	Easter Holiday	12.4, 13.4	periodic continued fractions, application to Pell's Equation
(04.13)	Final Review Makeup class (04.06)		

Calculators: Only calculators approved by the Department (with a sticker attached as proof of approval) are permitted for the class test and final examination.
For the list of approved calculators see:
https://www.concordia.ca/artsci/math-stats/services.html#calculators

Late Work: An extension will only be granted for sickness, religious holidays, or other appropriate circumstances. Homework solutions are typically posted 24 hours

after the due date, or any late submissions after that time can only be accepted for partial credit.

Student Services
You may wish to access the many services available to you as a Concordia student. An overview of these resources can be found here: https://www.concordia.ca/students/services.html

Academic Integrity and the Academic Code of Conduct
This course is governed by Concordia University's policies on Academic Integrity and the Academic Code of Conduct as set forth in the Undergraduate Calendar and the Graduate Calendar. Students are expected to familiarize themselves with these policies and conduct themselves accordingly. "Concordia University has several resources available to students to better understand and uphold academic integrity. Concordia's website on academic integrity can be found at the following address, which also includes links to each Faculty and the School of Graduate Studies: https://www.concordia.ca/conduct/academic-integrity.html" *[Undergraduate Calendar, Sec 17.10.2]*

Behaviour
All individuals participating in courses are expected to be professional and constructive throughout the course, including in their communications.

Concordia students are subject to the Code of Rights and Responsibilities which applies both when students are physically and virtually engaged in any University activity, including classes, seminars, meetings, etc. Students engaged in university activities must respect this Code when engaging with any members of the Concordia community, including faculty, staff, and students, whether such interactions are verbal or in writing, face to face or online/virtual. Failing to comply with the Code may result in charges and sanctions, as outlined in the Code.

AI Tools
The use of AI Tools (such as ChatGPT, Gemini, or Claude) is **strictly prohibited** on all assignments in this class. Relying on AI tools significantly diminishes the educational value of the assignments and is very likely to result in lower quiz and exam grades. More importantly submitting work that is not your own (whether generated by AI, copied from a peer, or taken from the internet, etc.) is a violation of the honor code. Any suspected violations will be reported to the Honor and Ethics Council. You may use AL tools as supplementary resources for studying outside of completing assignments. Please be aware that AI tools often produce incorrect or misleading answers, particularly in mathematics. It is strongly recommended that you verify any AI-generated content against reliable resources, such as the course textbook.

Intellectual Property
Content belonging to instructors shared in online courses, including, but not limited to, online lectures, course notes, and video recordings of classes remain the intellectual property of the faculty member. It may not be distributed, published or broadcast, in whole or in part, without the express permission of the faculty member. Students are also forbidden to use their own means of recording any elements of an online class or lecture without express permission of the instructor. Any unauthorized sharing of course content may constitute a breach of the Academic Code of Conduct and/or the Code of Rights and Responsibilities. As specified in the Policy on Intellectual Property, the University does not claim any ownership of or interest in any student IP. All university members retain copyright over their work.

Extraordinary circumstances
In the event of extraordinary circumstances and pursuant to the Academic Regulations the University may modify the delivery, content, structure, forum, location and/or evaluation scheme. In the event of such extraordinary circumstances, students will be informed of the change.