



Mathematics (MATH) 409

Number Theory (Revision 2)

Status:

Replaced with new revision, see the [course listing](#) for the current revision

Delivery mode:

Individualized study online

Credits:

3

Area of study:

Science

Prerequisites:

MATH 265, MATH 266, MATH 270, MATH 271 and MATH 309, or equivalent courses from another university.

Precluded:

None

Challenge:

MATH 409 is not available for challenge.

Faculty:

Faculty of Science and Technology

Overview

Mathematics 409 is a course in elementary number theory, the branch of mathematics concerned with the properties of numbers, including but not limited to divisibility, prime numbers, modular arithmetic, quadratic congruences, Pythagorean triples, and the theorems, conjectures, definitions and lemmas that permit exploration of these topics.

Outline

MATH 409 comprises 11 units:

- Unit 0: Introduction to Mathematics 409
- Unit 1: Division and Linear Diophantine Equations
- Unit 2: Introduction to the Prime Numbers
- Unit 3: Modularity
- Unit 4: Fermat's Little Theorem and Euler's Theorem
- Unit 5: Introduction to Cryptography
- Unit 6: Primitive Roots
- Unit 7: Quadratic Reciprocity
- Unit 8: Pythagorean Triples and Sums of Squares
- Unit 9: Rational Approximation and Pell Equations
- Unit 10: Finding Prime Numbers



Learning outcomes

Upon successful completion of this course, you should be able to

- demonstrate a foundational understanding of number theory, including the definitions, conjectures, and theorems that permit exploration of topics in the field.
- define and determine whether a number is a prime.

- state and apply the fundamental theorem of arithmetic.
- work with numbers and polynomials modulo a prime, linear congruences, and systems of linear congruences, including their solution via the Chinese remainder theorem.
- define the order of a number relative a prime and be able to restate and apply Fermat's little theorem, Euler's theorem and Wilson's theorem.
- state and apply Lagrange's theorem, define a primitive root of a prime p , and derive properties of the Euler ϕ -function.
- define quadratic residues and non-residues for primes p , determine whether a number is a quadratic residue for a prime, and state and prove the law of quadratic reciprocity.
- define Pythagorean triples and primitive Pythagorean triples and derive their properties.
- use number theory to design an effective encryption system through an exploration of the RSA public key cryptosystem.

Evaluation


To **receive credit**  for MATH 409, you must achieve a course composite grade of at least a **C- (60%)**  and a combined grade of at least 50% on the midterm and final assessments.

The weighting of the composite grade is given below:

Activity	Weight
Course notebook (10 units)	70%
Midterm assessment	10%
Final assessment	20%
Total	100%

To learn more about assignments and examinations, please refer to

Materials

Marshall, D. C., Odell, E., & Starbird, M. (2007). *Number theory through inquiry* (1st ed.). Mathematical Association of America, Inc.  (Print)





Special Course Features

The teaching method employed in MATH 409 is a version of the Moore method, adjusted for online education. This method is based on the finding that students gain a deeper understanding of a topic when they explore it for themselves.

As a record of your exploration, you will keep a course notebook, divided into units, in which you write out solutions to exercises, proofs of theorems, answers to questions, general ideas on the course material, and other observations relevant to the course. This notebook is your record of progress in your exploration of number theory. When you complete each unit in the course, you will send a copy of the corresponding pages of your notebook to your instructor for grading.

Your notebook will be graded on the basis of the solutions to exercises, answers to questions, and the proofs they contain. You are not expected to be able to answer every question, work every exercise, or prove every theorem; rather, your notebook will be graded on what you accomplish and on your improvement over the length of the course. Your grades for each unit will reflect your growing understanding both of number theory and of how to think creatively in mathematics.

Important links

- › [Academic advising](#) 
- › [Program planning](#) 
- › [Request assistance](#) 
- › [Support services](#) 

Athabasca University reserves the right to amend course outlines occasionally and without notice. Courses offered by other delivery methods may vary from their individualized study counterparts.

Opened in Revision 2, April 25, 2015

Updated September 17, 2024

View **previous revision** [↗](#)
