

**COURSE SYLLABUS**

**Course Title: Introduction to Number Theory**

Abbreviated Title      Intro Number Theory  
As Appears on Transcript

Course Number:    DMAT 283

Credit Hours:    4 credits [semester credit hours]

Course Description: An introductory course in Number Theory, emphasizing computational aspects as well as a historical perspective. Topics include a study of the integers, induction, divisibility, primes, Euclidean Algorithm, Diophantine equations, congruences, Chinese Remainder Theorem, cryptography, primitive roots, quadratic residues, continued fractions, cubic and elliptic curves, Fermat's Last Theorem, and Gaussian Integers.

Prerequisite: Successful completion with grade C or higher in Precalculus or equivalent, or consent of instructor.

Course Workload: 4 semester credit hours • 3 student work hours per credit hour • 14 week Carnegie semester = 168 hours student course workload average

Examination Requirements: Proctored written and oral final examination must be passed at 70% or higher to earn passing grade in course. “B” and “A” grade paths have additional examinations and assignments. See <https://www.distancecalculus.com/grades/> for more information.

Course Professor: Robert R. Curtis, Ph.D. <[rcurtis@rwu.edu](mailto:rcurtis@rwu.edu)>, <[robert@distancecalculus.com](mailto:robert@distancecalculus.com)>  
Roger Williams University, Extension School, 1 Empire Plaza, Providence, RI, USA 02903.  
Roger Williams University, 1 Old Ferry Road, Bristol, RI 02809.  
Accredited by New England Commission of Higher Education (NECHE).  
See <https://www.rwu.edu/academics/accreditation/> for more information.

E-Textbook:

Number Theory with Computer Applications by Kumanduri & Romero

Mathematical Software:    LiveMath and Mathematica Computer Algebra & Graphing Systems

**ADA ACCOMMODATIONS**

Roger Williams University has a continuing commitment to providing reasonable accommodations for students with documented disabilities. Students with disabilities who need accommodations in order to fully

participate in this class are urged to contact Student Accessibility Services, as soon as possible, to explore the arrangements needed to be made to assure access. Student Accessibility Services is open Monday through Friday from 8:00AM to 5:00PM Eastern Time; Email: [sas@rwu.edu](mailto:sas@rwu.edu) or Voice: 401-254-3841. For more information about SAS, visit

<https://www.rwu.edu/undergraduate/academics/student-academic-success/student-accessibility-services-sas>

## **COURSE RULES**

### **Academic Honesty**

Academic Dishonesty in a Distance course includes copying or relying upon another person's work. Working with other students is good and encouraged, but the work you submit for this course must be genuinely your own work. Private tutors are allowed, but you must notify the instructor that you have obtained a private tutor to aid in your studies. Any documented instance of Academic Dishonesty will be grounds for immediate failure in this course.

### **Final (and Other) Examinations**

A written and oral proctored final exam will occur at the student's location over video with the course professor; The student must score 70% or higher on this final exam to be eligible to earn a passing grade in the course.

### **Communication**

Communication is the key to success in a Distance course. It is the student's responsibility to keep good communication channels with the instructors during the course; failure to participate in the course does not constitute "dropping" the course (Withdrawal from the course must be requested in writing to the instructors before the completion date deadline)

### **Roger Williams University Policies & Procedures**

Roger Williams University has Policies & Procedures that all students must follow, including the Roger Williams University Student Handbook. Student must agree to follow all stated rules governing student conduct listed on the Roger Williams University website, and at the [Roger Williams University Course Catalog](#)

### **Course Completion 1 Year Rule**

All Distance Calculus students are afforded 1 Year to finish their course from the Date of Enrollment. Students will be placed in the Academic Semester based upon their Date of Enrollment for academic records purposes. If a student does not finish the course, and does not request a Course Withdrawal for a W, then an "F" grade will be issued.

### **No Chatbots / AI**

Students must pledge to **not** use any Chatbot/AI at all - **period**. Student must pledge to **limit** use of search engines (Google, Bing, etc) to a minimal level. Student must pledge to not engage in dishonest disguise of any Chatbot/AI/Search Engine source of information as student's own honest academic work. Verified chatbot usage will result in an "F" course grade, and will be referred to the Roger Williams University Academic Integrity Committee.

## Learning Outcomes for DMAT 283 - Introduction to Number Theory

1. To understand the general topic of Number Theory from first principles and examples.
2. To understand the historical aspect of Number Theory.
3. To understand divisibility, primes, and modular arithmetic.
4. To understand the basic concepts of cryptography and how Number Theory is used
5. To understand the basic concepts of quadratic residues
6. To understand the basic concepts of continued fractions
7. To understand the basic concepts of Diophantine Equations and their approximate solutions.
8. To understand the basic concepts of Elliptic Curves
10. To understand and utilize visualization tools such a computer algebra systems

## Syllabus Topics Outline for DMAT 283 - Introduction to Number Theory

1. Getting Started
  - 1.1 Email and Chat
  - 1.2 Learning About the Course
  - 1.3 Required Hardware
  - 1.4 Software Fundamentals
2. Divisibility and Primes
  - 2.1. Divisibility
  - 2.2. Primes
  - 2.3. Unique Factorization
  - 2.4. Elementary Factoring Methods
  - 2.5. GCD and LCM
  - 2.6. Linear Diophantine Equations
3. Modular Arithmetic
  - 3.1. Congruences
  - 3.2. Inverses Modulo  $m$  and Linear Congruences
  - 3.3. Chinese Remainder Theorem
  - 3.4. Polynomial Congruences
  - 3.5. Magic Squares
4. Fundamental Theorems of Modular Arithmetic
  - 4.1. Fermat's Theorem
  - 4.2. Euler's Phi Function
  - 4.3. Euler's Theorem
  - 4.4. Lagrange's Theorem
5. Cryptography
  - 5.1. Classical Cryptosystems
  - 5.2. Public-Key Cryptography
  - 5.3. The RSA Scheme

6. Cryptography
  - 6.1. Classical Cryptosystems
  - 6.2. Public-Key Cryptography
  - 6.3. The RSA Scheme
  
7. Primality Testing and Factoring
  - 7.1. Pseudoprimes and Carmichael Numbers
  - 7.2. Strong Pseudoprimes and Probabilistic Primality Testing
  - 7.3. Pollard's  $(p - 1)$ -method
  
8. Primitive Roots
  - 8.1. The Concept of Order
  - 8.2. The Primitive Root Theorem
  - 8.3. The Discrete Logarithm
  - 8.4. Primality Testing
  
9. Quadratic Congruences
  - 9.1. Quadratic Residues
  - 9.2. Computing Square Roots mod  $p$
  
10. Continued Fractions
  - 10.1. Introduction
  - 10.2. Convergents
  - 10.3. Infinite Continued Fractions
  - 10.4. Quadratic Irrationals
  - 10.5. Purely Periodic Continued Fractions
  - 10.6. Classical Continued Fraction Expansions
  
11. Continued Fractions
  - 11.1. Introduction
  - 11.2. Convergents
  - 11.3. Infinite Continued Fractions
  - 11.4. Quadratic Irrationals
  - 11.5. Purely Periodic Continued Fractions
  - 11.6. Classical Continued Fraction Expansions
  
12. Diophantine Approximations
  - 12.1. Best Approximations
  - 12.2. Intermediate Convergents and Good Approximations
  - 12.3. Algebraic and Transcendental Numbers
  
13. Diophantine Equations
  - 13.1. Introduction
  - 13.2. Congruence Methods
  - 13.3. Pythagorean Triples

- 13.4. Sums of Two Squares
- 13.5. Fermat's Last Theorem

14. Elliptic Curves

- 14.1. Introduction
- 14.2. Projective Spaces
- 14.3. The Group Law on Elliptic Curves
- 14.4. Elliptic Curves Modulo Primes
- 14.5. Rational Points on Elliptic Curves