MAT 255- Number Theory

MWF 2:30-3:25 PM

Cunningham 209

Instructor: Claire Merriman

Email: clmerriman@davidson.edu

Office: Chambers 3043

Office Hours:

Mondays 9-10

Tuesdays TBD

Wednesdays 1-2

Thursdays 11:05-12:15

Course Grades:

Preparation Assignments	5%
In Class Activities	5%
Homework	20%
Papers	30%
Weekly Quizzes	30%
Final Presentation	10%

Grading Scale:

A	93-100	A-	90-92		
B+	87-89	B	83-86	B-	80-82
C+	77-79	C	73-76	C-	70-72
D+	67-69	D	60-66	F	0-59

Paper Due Dates:

February 16

March 1

March 27

April 26

Final Presentation

During exam week, May 3-8

Course Information

The primary topics are in Chapters 1 through 6 of the Strayer textbook, as well as part of Chapter 8. These include properties of the integers and related sets, including divisibility properties, prime numbers and their distribution, congruences, Diophantine equations, arithmetic functions, primitive roots, quadratic residues, and cryptology.

The first three weeks of the course will cover introduction to proofs along with Chapter 1 of the Strayer textbook. Additional proof techniques will be introduced throughout the course.

This course also introduces methods of proof and emphasizes writing clear mathematical arguments. The standard for writing and presentation will be higher than in a calculus class, including on homework.

Course Goals

- Understand primes and factorization
- Understand modular arithmetic and some methods for solving systems of congruences
- Connect modular arithmetic to integer valued functions
- Solve problems using quadratic reciprocity
- Understand several techniques for solving Diophantine (integer solution) equations
- Increase student confidence in their ability to solve difficult math problems by using previous results, trying different methods, asking questions, and working with others
- Increase student confidence in their ability to judge when a solution is “done."
- Improve student’s mathematical communication skills
- Improve student’s mathematical writing

Textbook and other readings

Elementary Number Theory by James K. Strayer. A copy is on reserve at the library.

Introduction to Proof via Inquiry-Based Learning by Dana Ernst. The author’s website has various options for free pdf versions.

Mathematical Reasoning: Writing and Proof by Ted Sundstrom. You can also access a pdf version here.

Rough course notes are available on Moodle

Other required materials

In Class Work: You will work on problems with your classmates in class. You should bring a pen or pencil to work on the paper copies.

Online Homework Submission: All homework, papers, and preparation assignments will be submitted on Gradescope. You will also find your grades and feedback on all assignments on Gradescope. To get started, follow the invite link to create an account on Gradescope using your Davidson College email address or join our course using the code.

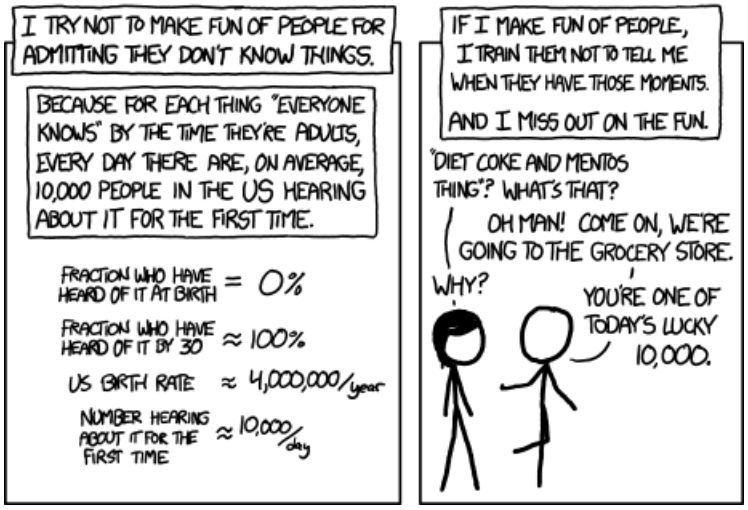
Typesetting: After the first homework, all homework and papers must be written in LaTeX. I suggested using Overleaf with either the provided homework files or the default homework template.

Classroom Expectations

Learning mathematics requires you *do* mathematics. This means that you will spend part of class working on math problems, and you will have times that you struggle to solve them. The goal is for this to be a *productive struggle*, where you emerge with a greater understanding of the concepts.

I expect this course to be a place where you will be treated with respect. All members of this class are expected to contribute to a respectful, welcoming, and inclusive environment for every other member of the class.

The topics in this course may also be more or less familiar depending on what other courses you have taken. If you have already seen a concept that we cover in class, view this as an opportunity to learn about it from a different perspective and practice explaining math to others.



Discrimination against any individual based on age, color, disability, gender identity or expression, national origin, race, religion, sex, sexual orientation, or veteran status will not be tolerated.

Assignment Descriptions

Preparation

You will have short assignments due before the start of each class to get familiar with the topics we will cover in class. Sometimes these questions will be short calculations, but they will often ask you to explain steps in the examples given in the textbook. These questions will be graded on a mix of completion and accuracy with the following rubrics:

0 points: Missing or minimal effort, such as only writing down the problem or a definition.
1 point: Contains a reasonable attempt to answer at least one question with significant mathematical errors or omissions (such as only answering one of two questions).
2 points: Contains a reasonable attempt to answer all questions with some mathematical errors.
3 points: Answers to all questions demonstrate understanding of the mathematical concepts, possibly with some minor errors.

Preparation assignments for the week will be available on the preceding Saturday. These assignments have a soft deadline of 1:30 pm and will **not be accepted more than 5 minutes after the start of class**. I will do my best to grade any assignments submitted by the soft deadline before the start of class and use the answers to adjust the lecture for the day.

The lowest 2 grades will be dropped.

In class activities

You will have problems to work on in groups throughout class time. These will range from calculation problems that check for understanding to more in-depth problems that benefit from group discussion. I will provide paper copies and collect them at the end of class. We may also do some other activities throughout class.

I will only grade one submission per group, so you should all work together. These problems typically require some amount of discussion. Often homework problems are continuations of the group questions.

In class activities are primarily graded on a mix of accuracy and completions out of 10 points. Since the lecture portion of class is important for being able to contribute to group discussion, excessive tardiness or leaving early will result in a reduced individual score:

- 5 to 10 minutes late or leave 5 to 10 minutes early: 3 points deducted from score.
- 10 to 15 minutes late or leave 10 to 15 minutes early: 5 points deducted from score.
- More than 15 minutes late, leave more than 15 minutes early, or unexcused absence: 0 points.

The instructor reserves the right to deduct additional points for distracting behavior, creating a hostile group environment, or lack of active participation in group work.

Lowest 3 grades will be dropped.

Homework

Weekly homework assignments will cover the material from the past week's lecture and reading assignments. You are encouraged to work together on the problems; however, **you must write up your own solutions and submit them individually**.

All homework assignments must have a correctly completed **Homework Cover Sheet**. Each homework assignment will have two sections: "Proofs and Writing" and "Calculations and Algorithms". The rubrics for the "Proofs and Writing" questions will be on the corresponding assignment page on Moodle before the assignment is due. "Proofs and Writing" questions are always worth 4 points. The total point value will vary each week, but each assignment is counts towards 2% of your final course grade.

You must type all Homework assignments after Homework 1. I will provide TeX files for each homework assignment. All problems will be graded on accuracy of the mathematical argument and clarity of the explanation. The answer to some problems are in the back of the book—you may use them to check your work, but a full credit answer will include more details.

Homework is due at the beginning of class. Late homework assignments will receive a 20 percentage-point penalty per day, unless you are using one of your late passes. You may not use more than one late pass per assignment.

After the homework is graded, **you may revise your answers to the Proofs and Writing question based on the feedback and resubmit for a new grade** due one week after the original due date. You may only resubmit problems where you had a reasonable attempt at a solution on the first submission. A reasonable attempt includes enough information to receive feedback. If the graded assignments are not returned by the class before the resubmission deadline, this deadline will be adjusted.

Weekly Quizzes

There will be a 10 minute, 1-3 question quizzes at the start of class each Friday. These questions will be similar to the "Calculations and Algorithms" questions on the Homework. The total point value will vary each week, but each quiz is counts towards 3% of your final course grade.

Lowest 2 scores are dropped.

Papers

An important part of mathematical communication is writing proofs. The papers will be similar to long homework assignments, where all of the problems are related, due at the beginning of. These assignments must be typed in LaTeX.

You may work with your classmates on the problems; however, you must write up your own solutions and submit them individually. **You may not use any outside sources, unless directed by the problem instructions**.

The total point value will vary for each paper, but each is 7.5% of your final course grade.

Late papers will receive a 20 percentage-point penalty per 24 hours, unless you are using one of your late passes. You may not use more than one late pass per assignment.

Final Presentation

There will be a final presentation during Finals Week, on a number theory topic of your choice that requires some techniques from Diophantine equations. More details will be posted on Moodle.

Ways to get help

The best way to succeed in this course is to ask for help before you fall behind. This includes working with your classmates and asking questions during class. Here are other ways to get help:

- **Office hours**: Office hours are a time I am in my office to help you with the material in the course. They can also be a time to meet or work with other students in the class.
- **Slack:** For questions about course material or logistics, check the Slack—someone else may have already asked the same question. If not, you should post, as other students likely have the same question. Other students in the course and can answer your questions in Slack.
- **Email**: For questions containing private information such as grades or absences, contact me by email. I will respond to Slack messages and emails within 24 hours on weekdays.
- **Study Groups**: I strongly encourage you to work with your peers on homework and when studying for reviews

Other course policies

Late Work

You may use 4 late passes during the semester. A late pass will allow you to turn in homework or labs up to 24 hours late without penalty—you may not use more than one late pass on the same assignment. You do not need to ask ahead of time, just write LATE PASS on the assignment. You are responsible for keeping track of when you have used all of your late passes.

Late work will receive a 20 percentage-point penalty per 24 hours. That is, an assignment with 20 total points will receive a 4 point deduction per 24 hours, a 50 point assignment will receive a 10 point deduction, etc. No work will be accepted more than 5 days after the deadline.

Honor Code

The Honor Pledge of Davidson College states: “On my honor I have neither given nor received unauthorized information regarding this work, I have followed and will continue to observe all regulations regarding it, and I am unaware of any violation of the Honor Code by others.” This pledge applies to all work for our course.

Your preparation assignments and homework assignments will be submitted individually. Though you may discuss your solutions with any of your classmates, you are expected to write your final submissions on your own. If you work on a problem with someone else (in or out of class) you should acknowledge this collaboration on the cover page for the homework assignments and on the preparation assignments.

Any copying of work which is not your own is an Honor Code violation. In addition, allowing others to copy your work (in person or by making it available electronically) is an academic integrity violation.

If you use a source that is not our course notes or a linked resource on Moodle, you must cite them on the cover page for the assignment. You do not need to use any specific format for your citations–just provide enough information that I can find the resource. You may not look up solutions to any problem assigned in the course on the internet. Once you have seen a full solution, it is not possible to independently develop a solution.

Academic Access

The college welcomes requests for accommodations related to disability and will grant those that are determined to be reasonable and maintain the integrity of a program or curriculum. To make such a request or to begin a conversation about a possible request, please contact the Office of Academic Access and Disability Resources by emailing ***AADR@davidson.edu***. It is best to submit accommodation requests within the drop/add period; however, requests can be made at any time in the semester. Please keep in mind that accommodations are not retroactive.

Important Dates

January 16	Classes Begin
January 16, 7 am**- January 19,** 5 pm	Add/Drop Week 1 available to all students on Banner Self-Service
January 19, 5 pm**-January 26,** 5 pm	Add/Drop Week 2 available through the Add/Drop Permission Form only ($20 fee). Adds or Drops not permitted after September 9.
March 4-8	Spring Break, No Classes
March 29	No Classes
April 11	Spring Convocation, No Afternoon Classes
May 1	Verna Miller Case Research & Creative Works Symposium, No Classes
May 2	Reading Day, No Classes
May 3-8 (May 3-6 for seniors)	Final Exams

Tentative Course Schedule—Subject to change, Defer to Schedule on Moodle

Date	Topic	Assignments Due
January 17	Introduction to the course, Strayer §1.1 Divisibility Introduction to "Doing" Mathematics	None
January 19	Strayer §1.1 Divisibility Direct Proofs, Logic, Proof by Contradiction	Prep: Ernst Ch 1 and §2.1, Strayer p. 1-5
January 22	Strayer §1.1 Divisibility Quantifiers	Prep: Ernst Ch 1 and §2.3
January 24	Strayer §1.1 Divisibility, Strayer §1.2 Prime Numbers Using other proofs as a guide for new theorem, Well-Ordering Principle	Prep: Strayer §1.2
January 26	Strayer §1.2 Prime Numbers, Strayer §1.3 Greatest Common Divisors Mathematical Induction	Prep: Appendix A: Mathematical Induction Homework 1 & Quiz 1: Strayer §1.1, Logic, Proof by Contradiction
January 29	Strayer §1.3 Greatest Common Divisors, Strayer §1.4 The Euclidean Algorithm Mathematical Induction	Prep: Appendix A: Mathematical Induction
January 31	Strayer §1.4 The Euclidean Algorithm	Prep: Strayer §1.5
February 2	Strayer §1.5 The Fundamental Theorem of Arithmetic	Prep: Strayer §1.5 Homework 2 & Quiz 2: Strayer §1.2, Induction
February 5	Strayer §1.5 The Fundamental Theorem of Arithmetic	Prep: Strayer §1.5
February 7	Strayer §2.1 Congruences	Prep: Appendix B: Equivalence Relations
February 9	Peer Feedback on Homework Questions that are on Paper 1, Strayer §2.1 Congruences	Prep: Strayer §2.1 Homework 3: Strayer §1.3-1.5, Induction Quiz 3: Strayer §1.3-1.4, Induction
February 12	Strayer §2.1 Congruences	None
February 14	Strayer §2.2 Linear Congruences in one variable, Strayer §6.1 Linear Diophantine Equation	None
February 16	Strayer §2.3 The Chinese Remainder Theorem	**Paper 1—Arithmetic Progressions** Quiz 4: Strayer §1.5, 2.1
February 19	Strayer §2.3 The Chinese Remainder Theorem, Strayer §2.4 Wilson's Theorem	Prep: Strayer §2.4
February 21	Strayer §2.5 Fermat's Little Theorem	Prep: Strayer §2.5
February 23	Strayer §2.6 Euler's Theorem	Prep: Strayer §2.6

		Homework 4 & Quiz 5: Strayer §2.2-2.3
February 27	Strayer §3.2 The Euler Phi-Function	None
February 28	Strayer §5.1 The Order of an Integer; Primitive Roots	None
March 1	Strayer §5.1 The Order of an Integer; Primitive Roots	**Paper 2—Pseudoprime or Carmichael Numbers** Quiz 6: Strayer §2.4-2.6
March 4-8	**No Classes—Spring Break**	
March 11	Strayer §5.2 Primitive Roots for Prime Numbers	Prep: Strayer §5.2
March 13	Strayer §5.2 Primitive Roots for Prime Numbers	Prep: Strayer §5.2
March 15	Strayer §5.3 The Primitive Root Theorem	Prep: Strayer §5.3 Homework 5: Strayer §2.4-2.6, 3.2, 5.1 Quiz 7: Strayer §3.2, 5.1
March 18	Additive and Multiplicative cyphers, Diffie-Helman Key Exchange	Prep: Notes uploaded to Moodle
March 20	Strayer §8.2 Cryptography; The RSA Encryption System	Prep: Strayer §8.2
March 22	Strayer §8.3 Primality Testing	Prep: Strayer §8.3 Homework 6 & Quiz 8: Strayer §5.2-5.3
March 25	Strayer §6.2 Nonlinear Diophantine Equations; A Congruence Method	None
March 27	Strayer §6.5 Representations of an Integer as a Sum of Squares (Sum of Two Squares)	**Paper 3—Primitive roots for composite moduli or More encryption**
March 29	**No Classes**	
April 1	Strayer §4.1 Quadratic Residues	Prep: Strayer §4.1
April 3	Strayer §4.2 The Legendre Symbol	Prep: Strayer §4.2
April 5	Strayer §6.5 Representations of an Integer as a Sum of Squares (Sum of Three Squares)	Prep: Strayer §6.5 Homework 7 Strayer §8.2-8.3, 6.2, 6.5 Quiz 9: Strayer §6.2, 6.5 (Two squares)
April 8	Strayer §4.3 Quadratic Reciprocity	Prep: Strayer §4.3
April 10	Strayer §4.3 Quadratic Reciprocity	Prep: Strayer §4.3
April 12	Strayer §6.5 Representations of an Integer as a Sum of Squares (Sum of Four Squares)	Prep: Strayer §6.5 Homework 8 & Quiz 10: Strayer §4.1-4.2, 6.5 (three squares)
April 15	Strayer §6.5 Representations of an Integer as a Sum of Squares (Sum of Four Squares	Prep: Strayer §6.5
April 17	Strayer §6.5 Representations of an Integer as a Sum of Squares (Sum of Four Squares)	Prep: Strayer §6.5

April 19	Strayer §6.3 Pythagorean Triples	Prep: Strayer §6.3 Homework 9 Strayer §6.5 (four squares) Quiz 11: Strayer §4.3, 6.5 (four squares)
April 22	Strayer §6.3 Pythagorean Triples, Strayer §6.4 Fermat's Last Theorem	None
April 24	Strayer §6.4 Fermat's Last Theorem	None
April 26	Strayer §3.1 Arithmetic Functions; Multiplicity, Strayer §3.3 The Number of Positive Divisors Function, Strayer §3.4 The Sum of Positive Divisors Function	**Paper 4—Jacobi symbol, Quadratic residues** Quiz 12: Strayer §6.3
April 29	TBD	Prep: TBD
April 30	TBD	Homework 10 Strayer §6.3-6.5
May 3-8	**Final Presentation—Schedule TBD**	