MAT-255, Number Theory

TR 9:40-10:55 am

Chambers 3209

Instructor: Claire Merriman

Email: clmerriman@davidson.edu

Office: Chambers 3043

Office Hours: TBD

Embedded Tutor: Jack McCalpin

Email:

Location:

Office Hours:

Course Grades:

Reading Assignments	5%
In Class Activities	5%
Homework	9%
Written Investigation	25%
Chapter Reviews	36%
Final Review	20%

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

Written Investigation Due Dates:

February 9

March 2

March 30

April 20

Review Dates:

May 6-8: Self Scheduled Final Review for Seniors

May 6-12: Self Scheduled Final Review for Non-Seniors

Course Information

The primary topics are in Chapters 1 through 6 of the 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.

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

The main goals of the course are to:

- 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

The goals of this course format and homework grading are to:

- 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 Course Notes

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

We will likely also use parts of *Elementary Number Theory* by Gareth A. Jones and J. Mary Jones, which is linked under Course Reserves - (Leganto) on Moodle. Additional readings will be uploaded or linked to Moodle.

Rough course notes are available on Moodle—these notes are a plan for the week, not notes from class. The notes will be updated with solutions to the reading assignment questions and any major changes after class each day.

Other 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 Assignment Submission: Preparation assignments and written investigations will be submitted and graded on Moodle.

Typesetting: Written investigations and one of the first two homework assignments must be typed. I suggested using Overleaf with either the provided homework files or the default homework template. Microsoft equation editor may be sufficient if tedious for the purposes of this course. Google Docs does not have a built-in equation editor—you need to install an add on.

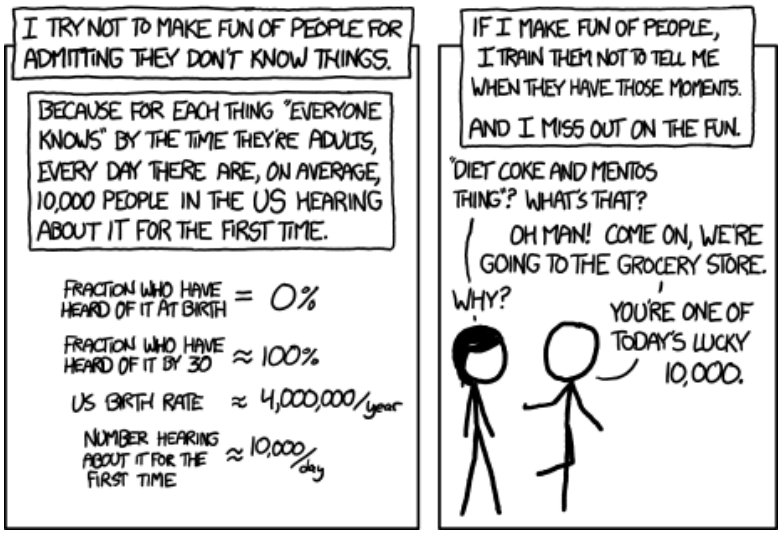
Classroom Expectations

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.

It is also important that you come to class on time having completed the reading assignment for the day and stay until the end of class.

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.



Conduct violating the Student Handbook, including Honor Code violations and discrimination or harassment based on race, color, national origin, religion, gender, orientation, age or disability will not be tolerated. Contributing to a hostile classroom environment may result in lost points on In Class Activities.

Assignment Descriptions

Reading

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.

Reading assignments for the week will be available on the preceding Saturday. These assignments have a soft deadline of 8:40 am the day of class 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. Class will start by going over the answers to these questions.

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 at the start of each class 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 on accuracy and completion. These are an opportunity for feedback before homework. You can earn up to 5 points per class session for active participation. You must arrive on time and stay for the whole session. Absence or tardiness will result in a lower participation score for the day.

- 10 to 15 minutes late or leave 5 to 10 minutes early: 3 points maximum
- 15 to 20 minutes late or leave 10 to 15 minutes early: 1 point maximum.
- More than 20 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.

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**, found in the General Course Materials section of Moodle. 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.

Assignments should be legible–you should work out problems then write up a new, final version. Homework should be on a separate page or in a separate file from you course notes. Problems or assignments that are messy may result in lower grades. You must type either Homework 1 or Homework 2 in preparation for the Written Investigations. I will provide TeX files for each homework assignment.

Homework is due at the beginning of class. There are no homework assignments during the weeks with a Review. Late homework assignments will receive a 20 percentage-point penalty per day, unless you are using one of your late passes or I have granted an extension before the assignment is due. 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.

Written Investigations

An important part of mathematical communication is writing proofs. The Written Investigations are short papers that are similar to long homework assignments, where all of the problems are related, due at the beginning of class on the same day as the chapter reviews. These assignments must be typed.

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**.

Late written investigations will receive a 20 percentage-point penalty per 24 hours, unless you are using one of your late passes or I have granted an extension before the assignment is available for completion. You may not use more than one late pass per assignment.

Chapter Reviews

There will be four 35-minute in class reviews, roughly corresponding to a chapter of the textbook. The questions will be similar to Calculations and Algorithms homework questions, as well as some very short proofs.

Final Review

The final review will be cumulative, with a slight emphasis on material covered since Review 4.

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.
- **Embedded tutor**: Jack McCalphin
- **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 Jack 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
- **Math and Science Center (MSC)**: Jack should be your primary source for peer assistance and learning support this semester. The Math & Science Center (MSC) will also have a small number of additional peer tutors available on a drop-in or by-appointment basis. The embedded, drop-in, and by-appointment tutors are trained and highly qualified peers that demonstrated deep understanding and succeeded in this course themselves. Located in the Center for Teaching & Learning (CTL) on the first floor of the College Library, the MSC's drop-in hours are Sunday through Thursday, 8-11 PM, beginning Sunday, January 22. Prior to visiting for drop-in help, be sure to look at the tutor schedules to determine when an appropriate tutor for your course/topic will be present. Tutor schedules for drop-in assistance, as well as links to schedule an appointment with a tutor, can be found at https://www.davidson.edu/offices-and-services/center-teaching-and-learning/student-resources/math-science-and-economics-center (click on "Meet with Math or Science Tutor"). Peer assistance is free to Davidson students at the point of service. For more information, contact Dr. Mark Barsoum, Director of the CTL (mabarsoum@daivdson.edu or ext. 2796).

Make-up Policy

If you need to miss class due to excused absence, we will schedule a time for you to complete the in-class assignments. Note: this is not a replacement for attending class and intended for short term (less than one week) illnesses, family emergency, college sponsored travel, or religious holidays. Excused absences may require documentation, particularly for midterms and the final.

If you are dealing with longer term illnesses or other life events that are interfering with your ability to attend class or complete assignments, reach out to me about how to handle assignments. These may require documentation.

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 reading 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 reading 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 Honor Code violation. Honor Code violations will be reported to the Honor Council. Assignments with Honor Code violations will receive a 0.

If you use a source that is not our textbook, course notes, or a 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, which is located in the Center for Teaching and Learning in the E.H. Little Library: Beth Bleil, Director, bebleil@davidson.edu, 704-894-2129; or Alysen Beaty, Assistant Director, albeaty@davidson.edu, 704-894-2939. 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 17	Classes Begin
January 17 (7 am)- 20 (5 pm)	Add/Drop Week 1 available to all students on Banner Self-Service
January 20 (5:01 pm)- 27 (5 pm)	Add/Drop Week 2 available through the Add/Drop Permission Form only ($20 fee). Drops not permitted after January 27.
March 6-10	Spring Break, No Classes
April 7	April Break, No Classes
May 4-5	Reading Day, No Classes
May 6-12	Final Exams for Non-Seniors
May 6-8	Final Exams for Seniors

Tentative Course Schedule—Subject to change

Date	Topic	Assignments Due
January 17	Introduction to the course, §1.1 Divisibility, Introduction to Proofs	None
January 19	§1.1 Divisibility, §1.2 Prime Numbers, Introduction to Mathematical Writing	Prep §1.2
January 24	§1.3 Greatest Common Divisors, §1.4 The Euclidean Algorithm	Prep §1.3, 1.4
January 26	Number systems without unique factorization, §1.5 The Fundamental Theorem of Arithmetic	Prep on other number systems (§1.5 Exercise 77), Homework 1
January 31	§1.5 The Fundamental Theorem of Arithmetic	Prep §1.5
February 2	§2.1 Congruences, Peer Review Homework 2 questions that are on Written Investigation 1.	Prep §1.5, Homework 2
February 7	§2.1 Congruences	None
February 9	§2.2 Linear Congruences in one variable **Review 1 In Class** Chapter 1	**Written Investigation 1**
February 14	§2.2 Linear Congruences in one variable, §6.1 Linear Diophantine Equations	Prep §2.2
February 16	§2.3 The Chinese Remainder Theorem	Prep §2.3, Homework 3
February 21	§2.3 The Chinese Remainder Theorem, §2.4 Wilson's Theorem	Prep §2.4
February 23	§2.5 Fermat's Little Theorem, §2.6 Euler's Theorem	Prep §2.5, Homework 4
February 28	§3.2 The Euler Phi-Function §5.1 The Order of an Integer; Primitive Roots	None
March 2	§5.1 The Order of an Integer; Primitive Roots **Review 2 In Class** Chapter 2 and Section 6.1	**Written Investigation 2**
March 6-10	**No Classes—Spring Break**	
March 14	§5.2 Primitive Roots for Prime Numbers	Prep §5.2
March 16	§5.3 The Primitive Root Theorem	Prep §5.2, Homework 5
March 21	Additive and Multiplicative cyphers, Diffie-Helman Key Exchange	Prep Notes uploaded to Moodle
March 23	§8.2 Cryptography; The RSA Encryption System, §8.3 Primality Testing	Prep §8.2, Homework 6
March 28	§6.2 Nonlinear Diophantine Equations; A Congruence Method, §6.5 Representations of an Integer as a Sum of Squares (Sum of Two Squares)	None
March 30	§4.1 Quadratic Residues **Review 3 In Class** Sections 3.2, 5.1-5.3, and 8.2-8.3; Additive and Multiplicative cyphers; and Diffie-Helman Key Exchange	**Written Investigation 3**
April 4	§4.2 The Legendre Symbol	Prep §4.2

April 6	§4.2 The Legendre Symbol, §6.5 Representations of an Integer as a Sum of Squares	Prep §4.2, Homework 7
April 11	§4.3 Quadratic Reciprocity	Prep §4.3
April 13	§4.3 Quadratic Reciprocity, §6.5 Representations of an Integer as a Sum of Squares	Prep §6.5, Homework 8
April 18	§6.3 Pythagorean Triples	None
April 20	§6.3 Pythagorean Triples **Review 4 In Class** Sections 4.1-4.5 and Sections 6.2 and 6.5	**Written Investigation 4**
April 25	§4.6 Fermat's Last Theorem	Prep §4.6
April 27	§3.1 Arithmetic Functions; Multiplicity, §3.3 The Number of Positive Divisors Function, §3.4 The Sum of Positive Divisors Function	Prep §3.1, Homework 9
May 6-12	**Final Exam—self scheduled,** taken in Chambers Exam Center	**Written Investigation 5**