Math 4400/6400: Number Theory

University of Georgia | Fall 2026

1. General Information

- **Instructor:** Dr. Steve Fan
- Email Address: steve.Fan@uga.edu
- Office Location: Boyd 321C
- Office Hours: 4:00 p.m.–5:00 p.m.
- **Meeting times:** MWF 12:00 p.m.–12:55 p.m., Boyd 302

2. Course Information

Course Description: Euler's theorem, public key cryptology, pseudoprimes, multiplicative functions, primitive roots, quadratic reciprocity, continued fractions, sums of two squares and Gaussian integers.

Credit Hour: 3

Course Objectives and Plans: The goal of this course is to introduce to students the classical theory of numbers, with particular attention paid to the pathbreaking accomplishments of the 18th and 19th centuries. Students are expected to understand mathematical results and their proofs and be able to apply their knowledge and skills to solve related problems.

We will start by reviewing the theory of prime factorization and congruences that you learned in MATH 4000. One of the crucial topics in MATH 4000 is the study of linear congruences of the form $ax \equiv b \pmod{m}$. Once knowing how to deal with linear congruences, it is natural to ask how to solve nonlinear ones. In this course, we will discuss the theory of quadratic congruences modulo a prime number p of the form $x^2 \equiv a \pmod{p}$. One of our major goals is to give a complete, elementary proof of one of the most important and most elegant results in number theory: the Law of Quadratic Reciprocity, which was conjectured by Euler and Legendre and first proved rigorously by Gauss. Gauss referred to this result as the "golden theorem" and contributed eight proofs of it. There are now over 230 published proofs of this theorem! As an application, we will resolve Fermat's problem on expressing a positive integer $n = 1, 2, 3, \ldots$ as $n = x^2 + y^2$ with $x, y \in \mathbb{Z}=\{0, \pm1, \pm2, \pm3, \ldots\}$.

Our discussion on quadratic congruences will be mostly based on arithmetic in the familiar ring $\mathbb{Z}$ of rational integers. Our next goal is to extend the basic properties of $\mathbb{Z}$ to larger rings. For instance, we will study the ring $\mathbb{Z}[i]$ of Gaussian integers and discuss similar rings such as $\mathbb{Z}[\sqrt{-2}]$ and $\mathbb{Z}[\sqrt{2}]$. These rings are all examples of the ring of integers of a quadratic field $\mathbb{Q}(\sqrt{d})$. Since the general theory is rather involved, we will instead focus on its subring $\mathbb{Z}[\sqrt{d}]$ with applications to solving Pell's equations $x^2 - dy^2 = 1$ in $x, y \in \mathbb{Z}$, where continued fractions naturally enter the picture. Along the way, we will also talk about the analogous problem of representing a positive integer n as $n = x^2 + 2y^2$ with $x, y \in \mathbb{Z}$, and the general solutions to the Diophantine equations $x^2 + y^2 = z^2$ and $x^2 + 2y^2 = z^2$ with $x, y, z \in \mathbb{Z}$.

Another topic of this course concerns prime numbers and arithmetic functions, which are functions defined on positive integers. The study of these objects has remained central in analytic number theory for the last two centuries. In this course, we will take a short adventure in the elementary part of the theory. In particular, we will establish simple but useful estimates for the count of prime numbers up to a certain point and briefly discuss more precise results like the Prime Number Theorem as well as open problems such as the Riemann Hypothesis. We will also study the properties of multiplicative functions, which are arithmetic functions whose values factor just as positive integers factor into primes! By using arithmetic functions, we will be able to refine our solution to Fermat's sum-of-two-squares problem with an exact counting formula for the number of solutions $x, y \in \mathbb{Z}$ to $n = x^2 + y^2$ for each given positive integer n.

If time permits, we will also explore a more advanced topic such as quaternions and Lagrange's four-square theorem, and Brun's sieve and twin primes. The former introduces a new system of numbers that is strictly larger than that of complex numbers and can be used to prove Lagrange's theorem on representing every positive integer n as the sum of four integer squares, while the latter provides a method for counting integers with certain arithmetic properties, e.g., prime numbers p such that $p + 2$ is also a prime number.

Prerequisite: MATH 4000/6000

Topical Outline:

- Prime factorization and congruences
- Quadratic congruences, the Law of Quadratic Reciprocity, sum of two squares
- Gaussian integers, integral Pythagorean triples, the ring $\mathbb{Z}[\sqrt{d}]$, units and Pell's equations
- Primes and arithmetic functions, Jacobi's two-square theorem
- Advanced topics: arithmetic of quaternions and sum of four squares, Brun's sieve and counting twin primes

Recommended Textbook: There is no required textbook for this course. Nevertheless, I recommend *Fundamentals of Number Theory* by W. J. LeVeque. This book covers all of the standard topics, covers them well, and is remarkably inexpensive, making it an excellent addition to any mathematical library.

Office Hours: There will be weekly office hours when I am available to help you with any questions you might have. You are welcome to come at any time during office hours and you do not have to stay the entire time.

Grading: The grading weights are as follows:

- Written Homework – 22%;
- Midterm Exams – 24% × 2 = 48%;
- Final Exam – 30%.

The grades will be assigned using the following scale:

92-100	88-91	86-87	81-85	78-80	76-77	71-75	68-70	60-67	<60
A	A-	B+	B	B-	C+	C	C-	D	F

The instructor reserves the right to adjust the above grading weights and scale.

3. Course Requirements

Professionalism/Attendance: Attending class is the minimal amount of effort you can put into a course, and yet it is also the easiest way to learn the material. Attendance in this course is **required**. More than four unexcused absences may result in you being withdrawn from the course. Please keep me posted whenever you have a conflict that may cause you to miss class.

Homework: There will be several written homework assignments for this course that are designed to help reinforce your understanding of the material through exercises. Homework will be collected in class, once every week or two. You are responsible for keeping track of the due dates of these assignments. Late homework will not be accepted. Your lowest HW score will be dropped at the end of the term.

Collaboration is **allowed** and in fact is very much **encouraged**. Feel free to work together and share insights with each other. You may discuss homework problems and their solutions with your classmates, but you must write your own final solutions independently and make sure you understand them yourself and are able to explain your solutions to me if requested to do. Please keep in mind that **copying** (from a textbook, another student, or a website) and **using AI tools** are not allowed.

Exams: There will be two in-class midterm exams as well as a cumulative final exam. All exams are closed book and and closed notes. The exam dates will be announced later. Please keep in mind that no make-up exams will be given, except when required by UGA policy or arranged for a documented emergency.

4. Other Information & Resources

UGA Student Honor Code: "I will be academically honest in all of my academic work and will not tolerate academic dishonesty of others." As a University of Georgia student, you have agreed to abide by the University's academic honesty policy, "A Culture of Honesty," and the Student Honor Code. All academic work must meet the standards described in "A Culture of Honesty" found at https://honesty.uga.edu/Academic-Honesty-Policy/.

Lack of knowledge of the academic honesty policy is not a reasonable explanation for a violation. Questions related to course assignments and the academic honesty policy should be directed to the instructor.

UGA Well-Being Resources: Being at the university can be stressful, and we have high expectations for all of our students. We also understand that you may face difficulties beyond what happens in the classroom and may be overwhelmed by a number of different things. Don't hesitate to reach out to me if you are struggling and feel that you are falling behind. Also, please keep in touch with Student Care & Outreach (SCO) in the Division of Student Affairs. You can contact them at 706-542-8479 or visit sco@uga.edu.

UGA provides both clinical and non-clinical options to support student well-being and mental health:

- Well-being Resources: well-being.uga.edu
- Student Care and Outreach: sco.uga.edu
- University Health Center: healthcenter.uga.edu
- Counseling and Psychiatric Services: caps.uga.edu or CAPS 24/7 crisis support at 706-542-2273
- Health Promotion/Fontaine Center: healthpromotion.uga.edu
- Accessibility and Testing: accessibility.uga.edu
- Additional information, including free digital well-being resources, can be accessed through the UGA app or by visiting https://well-being.uga.edu.

Classroom Accommodations: If you have a documented disability that may have some impact on your work in this class and for which you may require accommodations, please feel free to talk to me as well as register with the Disability Resource Center so that you have access to any accommodations that you may need throughout the semester. They can be reached by visiting Clark Howell Hall, calling 706-542-8719 (voice) or 706-542-8778 (TTY), or by visiting http://drc.uga.edu. I must have official documentation or verification prior to any assessment on which you want to use the accommodation to guarantee you this accommodation.

NOTE: The course syllabus is a general plan for the course; deviations announced to the class by the instructor may be necessary. Any information in this syllabus may be amended at the instructor's discretion.