

**Math 522: Number Theory**  
**Spring 2021**

**Instructor:** Christopher O'Neill  
**Office:** Room 570, Geology Mathematics and Computer Science (GMCS) Building  
**E-mail:** [cdoneill@sdsu.edu](mailto:cdoneill@sdsu.edu)  
**Webpage:** <http://cdoneill.sdsu.edu/teaching/s21-522>

**Course Content:** Theory of numbers, congruences, Diophantine equations, a study of prime numbers; cryptography.

**Texts:** Content will be sampled from the following textbooks. All are optional, but will be useful references.

- *Number Theory*, Dover 1994, by George Andrews.
- *Elementary Number Theory: Primes, Congruences, and Secrets*, Springer 2008, by William Stein.

**Prerequisites:** Math 245 with a grade of C or better.

**Course Organization:** The class will be organized as follows.

- Each Tuesday class (the “lecture day”), I will give a lecture on course material.
- Each Thursday class (the “discussion day”), you will work in small groups on problems designed to lead you to discover some of the course content (in particular, these problems **will introduce new material**).

Some lecture days may include a brief “discussion session” also completed in groups, and discussion days will sometimes begin with a brief lecture.

The day before each discussion day, a short list of “preliminary problems” will be assigned, and should be completed before class on the discussion day. These assignments will be short, usually requiring at most 10 minutes to complete, and will be computational in nature (i.e. no proofs).

Although I intend to use this format throughout the course, I reserve the right to restructure the course as the term progresses, based in part on student feedback and performance. I will periodically collect anonymous feedback in class, but feel free to come talk to me if you have suggestions or concerns.

**Grading Policy:** Your grade will be determined by four oral exams, a cumulative final exam, weekly homework submissions, and a participation grade, weighted as follows.

Homework Average	50%	A = 90-100
Participation	10%	B = 80-89
Oral Exam 1	5%	C = 70-79
Oral Exam 2	10%	D = 60-69
Oral Exam 3	15%	F = 0-59
Final Exam	10%	
<hr/> Total	100%	

The Final Exam will be comprehensive, and will be a take-home exam completed during finals week. Details will be announced later in the term.

**Oral Exams:** In place of timed midterm exams, there will be several oral exams administered in one-on-one meetings throughout the term. Each oral exam will last roughly 30 minutes, and will be interactive in nature. Due to time constraints, the exams will be staggered throughout the term; a signup for exam weeks will take place early in the term. Each exam will cover material from the previous 2 weeks of the course.

**Participation:** Attendance in problem sessions is vital to success in this class, since **new material** will be covered. Your participation grade will be based on the following:

- attending and participating in lectures;
- attending and engaging in problem sessions; and
- completing the preliminary problem before each class meeting.

Missing class will result in a lowered participation grade, and only university excused absences with **advance notice** to the instructor will be accepted. I reserve the right to deduct one **additional full letter grade** if you miss too many classes, or if sufficient participation is not demonstrated during problem sessions.

If extenuating non-academic circumstances will make it difficult for you to regularly attend class at the usual time (e.g., the pandemic has forced you to live in a significantly different time zone from SDSU), please come talk to me to make alternate arrangements.

**Homework:** There will be one homework assignment given each week. Completed homework assignments will be submitted to the instructor for a grade. Collaboration on homework is encouraged, but solutions should be written individually, and **collaborators should be identified** on the front of your assignment.

Homework will be submitted through Gradescope on the course Canvas page. You are highly highly encouraged (though not required) to complete your assignments in  $\text{\LaTeX}$ ; this is a fantastic skill to develop whose utility extends far beyond this course. To use  $\text{\LaTeX}$  for free online, or to access numerous tutorials, visit <https://www.overleaf.com/>.

Homework assignments, along with their due dates, will be posted on the course webpage as they are assigned. Out of fairness to the other students, late homework assignments will **not** be accepted for credit. However, the lowest homework grade of the term will be dropped.

**Class Announcements, E-mail Policy and Communications:** Class announcements will be posted to my class web page and sent to your university e-mail account. Be sure to regularly check your e-mail. If you send me an e-mail, please include your name and course information (i.e. class and section) as well as any additional information that I might need to respond to your e-mail.

**Attendance, Absence, and Makeup Work Policies:**

- Attendance is **essential** for success in the course!
- Late homework will not be accepted. However, your lowest homework grade will be dropped.
- The last day to drop this class is **February 2nd**.

**Student Learning Outcomes:**

- Students will be able to use number-theoretic methods to solve modular equations.
- Students will be able to construct mathematical proofs of number theoretic statements, as well as find counterexamples to false statements.
- Students will be able to encode and decode messages using a variety of cryptography methods.
- Students will be able to solve challenging number theory problems in a group setting.

**A.D.A. Policy Statement:** The Americans with Disabilities Act (ADA) is a federal anti-discrimination statute that provides comprehensive civil rights protection for persons with disabilities. This legislation requires that all students with disabilities be guaranteed a learning environment that provides for reasonable accommodation of their disabilities. If you believe you have a disability requiring accommodation, please contact Student Disability Services.

If you require additional time on quizzes and/or exams, you must **contact me at the start of the course**. You will not be given extra time if you present this information just before an exam.

For additional information, visit [https://go.sdsu.edu/student\\_affairs/sds/](https://go.sdsu.edu/student_affairs/sds/).

**Student Privacy and Intellectual Property:** The Family Educational Rights and Privacy Act (FERPA) mandates the protection of student information, including contact information, grades, and graded assignments. Canvas will be used to communicate with students. Grades will not be posted in public spaces, and graded assignments will not be left in public spaces. Students will be notified at the time of an assignment if copies of student work will be retained beyond the end of the semester or used as examples for future students or the wider public. Students maintain intellectual property rights to work products they create as part of this course unless they are formally notified otherwise.

**Scholastic Dishonesty:** *An Aztec Does Not Lie, Cheat, or Steal, or Tolerate Those Who Do.* The San Diego State University Student Conduct Code will be enforced in this course. For the purpose of this course, cheating will be defined as (but not limited to) access or use of unauthorized material during exams and quizzes, collaboration between students during exams, quizzes or assignments for which group work is not allowed, perusal of another student's work during exams and quizzes, copying other student's work or allowing other students to copy your work on any assignment, quiz or exam, and having unauthorized programs or other information stored on calculators when these calculators are accessible during an exam or quiz. Note: Falsifying documentation is considered scholastic dishonesty and may result in a grade of F for the course.

For additional information, visit [http://go.sdsu.edu/student\\_affairs/srr/conduct.aspx](http://go.sdsu.edu/student_affairs/srr/conduct.aspx).