Math 4400 Syllabus

Summer 2017

MATH 4400-001
Introduction to Number Theory
Summer 2017
Meeting time: MWF 12:30–1:30, in LCB 215
Instructor: Daniel Smolkin
E-mail address: `smolkin@math.utah.edu`
Office: JWB 306
Office hours (tentative): Monday 3–4, Thursday 11–12, or by appointment
Course website: `http://www.math.utah.edu/~smolkin/teaching/4400/index.html`

Course text

I'll mainly be referring to *Numbers, Groups, and Cryptography* by Gordan Savin. This book is available online on my webpage. Another book I might refer to is *Elementary Theory of Numbers* by William J. LeVeque, ISBN: 0-486-66348-5. If you don't like either of these books, feel free to talk to me and I can point you to other texts.

Prerequisites

In order to take Math 4400, you need a grade of C or better in Math 2270 or Math 2250. Please see me if you do not meet this requirement.

Grading and Course Policies (the important stuff)

Grading will be based on homework, quizzes, two midterms, and a final exam. Each student's grade for the course will be broken down in the following way:

Homework	Quizzes	Exam 1	Exam 2	Final
30 %	30 %	10%	10 %	20 %

Homework: Homework is probably the most important part of this class, since you can only learn math by doing it. It will be challenging—I expect each assignment will take 5-10 hours to complete. I'll assign both proofs and computational problems for homework. Homework will be due (almost) every Monday at the start of class. **Late homework will not be accepted!** Accepting late homework in a class of 40 becomes a logistical nightmare very quickly. You are encouraged to work with your fellow classmates, but everyone is required to turn in their own assignment. I will drop everyone's lowest homework.

Quizzes: We will have a quiz (almost) every Wednesday at the end of class. Quizzes will be more or less based on the homework.

I will drop everyone's two lowest quizzes. This is to account for days you were absent, days you weren't feeling well, or maybe just days you were unlucky. If you have a planned absence on the day of a quiz, you can e-mail me to take the quiz ahead of time. However, **there will be no late quizzes**

Quizzes will be half computation-based and half proof-based. Exams will be a bit more proof-based.

Grading scale I'll use the following table to assign grades:

A	A-	B+	B	B-	C+	C	C-	D+	D	F
90	85	80	77	73	70	67	63	60	57	50

Important Dates

- Exam 1: Friday, June 16th
- Exam 2: Friday, July 21st
- Final: Friday, August 4, 12:30–2:30pm

Cell phones, etc

During quizzes and exams, any internet-connected devices in your posession must be turned **OFF**. I'll try to remind you of this rule

ADA Statement

The University of Utah seeks to provide equal access to its programs, services and activities for people with disabilities. If you will need accommodations in the class, reasonable prior notice needs to be given to the Center for Disability Services, 162 Olpin Union Building, 801-581-5020. CDS will work with you and the instructor to make arrangements for accommodations.

All written information in this course can be made available in alternative format with prior notification to the Center for Disability Services.

Course Description

Number theory is a branch of mathematics concerned with studying the structure of the integers. It is one of the oldest branches of mathematics—archeological evidence suggests the Babylonians had an algorithm for finding Pythagorean triples as early as 1800 BCE. Since that time, number theory has evolved into very active area of research with numerous applications to fields like cryptography and numerical analysis.

We'll be covering the following topics this semester:

- Proofs by induction, division algorithm
- Unique factorization, euclidean algorithm
- Fun with the Euclidean algorithm (e.g. contiued fractions)
- Modular arithmetic
- Fun with modular arithmetic (e.g. Euler's φ function and the Chinese remainder theorem)
- Groups and rings (Lagrange's theorem and generalized Chinese remainder theorem)
- RSA algorithm and the discrete log problem
- Quadratic residues
- Quadratic forms
- Gaussian integers
- When is a number the sum of two squares?
- Diophantine equations
- Diffie-Helman key exchange and Elliptic curve cryptography