MATH 565: NUMBER THEORY

WINTER TERM 2018, LAWRENCE UNIVERSITY

Professor: Scott Corry
Office: 408 Briggs Hall, x7287
Office Hours: 11-12 MW, 2-3 TR, and by appointment
E-mail: scott.corry@lawrence.edu
Webpage: www.lawrence.edu/fast/corrys
Text: *An Introduction to Mathematical Cryptography* (Springer), Hoffstein, Pipher, Silverman.

1. Overview

To begin, Number Theory is the study of properties of the natural numbers

$$\mathbb{N} = \{1, 2, 3, 4, 5, \dots\}.$$

From an algebraic point of view, it quickly becomes clear that one should actually study the *ring* of integers

$$\mathbb{Z} = \{\dots, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, \dots\}.$$

This course is all about the ring $\mathbb{Z}$ and its remarkable applications to public-key cryptography, which plays an enormous role in our everyday lives.

In our attempt to understand a particular natural number n and its role in the ring of all integers $\mathbb{Z}$, we will find it extremely helpful to study the quotient ring

$$\mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, 3, \cdots, n-1\},$$

where the operations of addition and multiplication are carried out modulo n. In the case when $n = p$ is a prime number, $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ is a finite field with p elements.

While these rings and fields are extremely simple to define, their arithmetic is sufficiently complex to harbor hard problems (such as the factorization and discrete logarithm problems) forming the basis of cryptographic schemes (such as RSA and Diffie-Hellman). However, these cryptosystems are susceptible to attack by quantum computers. After a brief discussion of quantum algorithms, we will end the course with a discussion of lattice-based cryptography, which may be more resistant to quantum attack.

2. Practicalities

2.1. **Homework, Exams, Presentations.** There will be regular homework assignments, and problems will be carefully graded on the following five point scale:

5 = perfect – correct and well-written
4 = one minor error
3 = one major error or several minor errors
2 = several major errors
1 = indicative of relevant thought

Remember that the quality and clarity of your writing are important. Take the time to make your solution set neat and legible, and strive to effectively convey your ideas. Homework will count for 70% of your final grade, and **absolutely no late homework will be accepted**.

We will have one in-class midterm (date TBD, worth 15% of your course grade). Instead of a final exam, we will have group presentations (also worth 15% of your course grade) on topics of your choice ... more details on that to come.

2.2. **Office Hours and Other Details.** Please feel free to come by my office, whether you are having difficulty or just want to chat about mathematics. Of course, I may not be in, or I may be otherwise engaged and unable to talk. To ensure that you have my undivided attention, you should come during my office hours, which are listed above. Of course, if these times are impossible for you, you can always make an appointment with me.

In addition to talking with me, I encourage you to speak with each other about the course, and even to work together on the problems if that suits your style of learning. That being said, I expect you to spend some time thinking privately about the problems before collaborating, and each of your writeups should be the result of your own cogitation and exposition. If you like to work together, a good model would be to make a first pass through the problems on your own, then get together to talk about difficulties and share ideas, and finally find a solitary place to write a polished (and unique) solution set. Of course, all of your work for this course is governed by the Lawrence University Honor Code.

2.3. **Statement on Disability.** Lawrence University is committed to providing reasonable accommodations for students with disabilities. Students establish eligibility and request accommodations through the Center for Academic Success. View the Accessibility Services web page at go.lawrence.edu/cas for more information.