Introduction to Number Theory
Final Project First Details

Spring 2016

Last Updated: March 24, 2016

---

1. Final Project

Unless you choose to take a final exam, you will need to do a final project. You will choose a topic and a group. I will provide some suggested reading material. You will then read about the topic (it may be necessary for you to go beyond the initial reading material I suggest), write a 5-10 page article giving an overview of the topic, and give a short presentation to the class on the topic.

You should write your paper at a level so that a student in this class, but not in your project group, could fully understand. Your presentation should be expository and designed to inform. More details about the paper and project will be given once topics are assigned.

The presentations will occur during class-time during Reading Period, beginning on Tuesday 3 May 2016. [Depending on the number of groups that form, we may begin on Thursday 28 April 2016.] The papers will be due on Tuesday 3 May 2016, even if your group doesn't present until afterwards.

Over spring break, you should start thinking about what topics you are interested in. If there are other students in class with whom you would like to work, you should begin to talk and consider topics. At the end of this document is a list of potential topic ideas, but I encourage you to be daring! If you want to pursue something that I haven't listed, email me and I'm confident we can arrange something.

You should email me with a preliminary topic selection by Monday, April 4th [the day you get back from spring break, and one month before the project deadline]. I need to make sure that there aren't too many students pursuing the same topic, so I encourage you to let me know what you are thinking about as soon as possible.

Topics and student groups will be finalized by Thursday, April 7th.

As a final note: this project is an opportunity for you to learn about or investigate something that has caught your interest. I hope you will find the process fun and enriching.

2. Some Initial Suggestions for Project Ideas

Here is a brief list, with brief explanations, of some projects that you might find interesting. You do not have to choose one of these projects!

You might be inspired by one of these projects to choose something on your own!

(1) Factorization Techniques

How do we factor a composite integer in a non-naive way? There are many factorization algorithms out there. How fast are they, which work and how well do they work? Some good things to look at are the references in exercise 18.6 in the book.

(2) Pseudoprimes and Carmichael Numbers

Fermat's little Theorem tells us that $a^p \equiv a \pmod{p}$ when p is prime. Conversely, if $a^n \not\equiv a \pmod{n}$, then n is not prime. But when do composite n satisfy $a^n \equiv a \pmod{n}$ despite being composite? These are called pseudoprimes, and there are special pseudoprimes called Carmichael Numbers.

(3) The Prime Number Theorem and Related Topics

We mentioned in class that $\pi(X) \sim \frac{X}{\log X}$, or rather that the number of primes up to X is about $\frac{X}{\log X}$. Most proofs are somewhat technical, but the history and progress towards the problem is fascinating and varied.

(4) An Alternative to RSA: Discrete Logs

The "hard problem" behind RSA is factorization. Another hard problem is the "discrete log" problem. Investigating discrete logarithms leads to the ElGamal cryptosystem and the Diffie-Helmann key exchange. How are these related to RSA?

(5) Other Alternatives to RSA

There are other "hard problems" that allow public-key cryptosystems to work too. Some are "lattice-based." Others include "elliptic-curve cryptography." This topic is a bit open-ended.

(6) The Riemann Hypothesis and the Riemann Zeta Function

How does $\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s}$ have anything to do with counting prime numbers? What does $\zeta(s)$ even mean when $s < 1$? How do the locations of the zeroes of $\zeta(s)$ affect number theory, and other areas of mathematics? (Note that this is quite open-ended, and might involve a lot of exploratory reading.)

(7) Fermat's Last Theorem: An Overview

What are some of the big ideas that go into proving Fermat's Last Theorem? This is a big and hard question, but it really goes through a tour-de-force of mathematics!

(8) Fermat's Last Theorem: Specific Cases like $n = 3, 4$.

How hard is it to show that $x^4 + y^4 = z^4$ has no nontrivial solutions? What about $x^3 + y^3 = z^3$? More generally, how far can we get proceeding in a totally elementary way, similar to how we looked at solutions to $x^2 + y^2 = z^2$? (Note: there is a chapter in the book based on the $n = 4$ case of FLT).

(9) Other Topics in Cryptography

Cryptography is a huge subject! Did you know that you can craft a set of 40 keys so that it takes any 10 to decrypt a message, but no set of 9 will do? This is known as "secret-sharing," where many people each get part of the secret. We mentioned "zero-knowledge proofs" and "electronic voting" and "digital signatures" and "onion routing" and "digital currency" (like bitcoin) in class. Some subsets of these could make nice projects.

(10) Quantum Computing

How does quantum computing work? What makes it hard and is it worth the effort? How would a quantum computer allow someone to factor integers? In this project, you would try to understand how Shor's Algorithm for factorization works.

(11) Applications of Congruences

One can use the Chinese Remainder Theorem to speed up parallel computation in computers. One can create ISBNs cleverly to allow scanners to partially auto-correct even if the item is incorrectly scanned. Or you can understand and create divisibility tests for a wide variety of integers. Did you know that one way of testing for divisibility by 11 is to see the the sum of the even-placed digits minus the sum of the odd-placed digits is divisible by 11?

Alternately, Google (and other search engines) use "hashing functions" a lot, which usually involve congruences. In fact, these are tremendously important objects. One can schedule tournaments or know the day of the week of December 21st, 2067 immediately (or any day, really), all through playing with congruences.

There are a lot of topics here.

(12) Number Theory with Polynomials

Here is a guiding question: to what extent are polynomials with integer coefficients similar to the integers? Is there unique factorization, for instance? What does the Chinese Remainder Theorem mean here? This is a rich and interesting area.

(13) Primality Checking

Determining whether a number is prime is different than factoring that number. There is the now-famous AKS primality test, which runs quite quickly (and much much faster than previously thought). There are also probabilistic primality tests, which are perhaps more commonly used, such as the Miller-Rabin test.

(14) Elliptic Curves

This is a very large topic, but many of the last chapters in the book are dedicated to elliptic curves. In just a few words, these are special curves with very many nice properties, and which happen to have been very useful in the proof of Fermat's Last Theorem. For more, I encourage you to glance through some of the material in the book.

(15) Binomial Coefficients, Linear Recurrences, and Generating Functions

These are other chapters in the book with beautiful and nice ideas. For a better idea, I encourage you to glance through some of them.

(16) Quaternions and Sums of 4 Squares

In class, we will use $\mathbb{Z}[i]$ to understand which primes can be written as sums of 2 squares, $p = a^2 + b^2$. It is possible to look at an even more "exotic" number system called the quaternions and investigate which numbers can be written as sums of 4 squares.

(17) Continued Fractions and Pell's Equations: The Return of Square-Triangular Numbers

We've investigated square-triangular numbers repeatedly. In class, we will return once more and prove (yet again) that there are infinitely many square-triangular numbers. More generally, we will investigate how many solutions there are to $X^2 - DY^2 = 1$. But we won't do a good job of actually finding them. You can, though! A great resource for this material is the textbook, including the online supplementary material. (There are additional chapters available online).

I should note it is also a nice project to think about continued fractions not as related to Pell's Equation. A continued fraction is an infinite fraction that looks like

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}}$$

and they have many very interesting properties.

(18) Something else not on this list

There are so many interesting things out there!