Math 124: Elementary Number Theory

http://modular.fas.harvard.edu/124

At Harvard University
MWF 11–12 in Science Center 103B

OFFICE HOURS: Monday 5–6 and Tuesday 2–3

Instructor: William Stein (was@math.harvard.edu)

1 Topics

The main ideas of the course are prime numbers, arithmetic modulo n, public-key cryptosystems, quadratic forms, continued fractions, and elliptic curves. This course is **unusual** for an introductory number theory course in that we will go more deeply into elliptic curves than usual, we will learn more about using computers to do number theory, and we will read a novel.

2 Prerequisites

You must already be comfortable reading and writing **proofs**. I will assume you are familiar with abelian groups, commutative rings, and fields. For the elliptic curve part of the course, I will use some basic complex analysis. You might want to attend a few of the Math 113 (complex analysis) lectures, though this isn't essential.

3 Texts

Doxiadis's little novel *Uncle Petros & Goldbach's Conjecture* is required. I selected Niven, Zuckerman, and Montgomery's *An Introduction to the Theory of Numbers* as the primary course textbook because it was highly recommended to me. I've hardly looked at it. **The primary text will be the book I'm writing**, which you can download from the course web page and print, as it is written. I will probably select some homework problems from Niven, Zuckerman, and Montgomery, and you might benefit from their alternative exposition of many of the topics we will cover.

4 Evaluation

Weekly Homework	30%
Project	20%
Take-Home Midterm	20%
Take-Home Final Exam	30%

4.1 Homework

There will be one homework assignment per week, and these may involve using a computer. Homework will be assigned on Wednesday and due the following Wednesday. The course assistant will not accept any late homework, but I will drop your two lowest homework grades.

Please work together on homework problems!

Write up your solutions individually and acknowledge those people and other sources that helped you.

4.2 Project

There will be a project that might be related to Doxiadis's novel, or the recent deterministic polynomial-time primality test, or something else number theoretic that appeals to you. This project will be due **December 4**, which is the Wednesday after the Thanksgiving break.

4.3 Exams

There will be a take-home midterm exam and, subject to university approval, the final will also be take-home. You must work on both exams by yourself.

The take-home midterm will be assigned on **Wednesday, October 16**, you will return it on Friday, October 18, and you will know your grade by October 21, which is the add/drop deadline. The midterm will be similar to what I would give as a one-hour in class exam.

4.4 Attendance

If you come to class less than half the time, you will not receive a passing grade in the course, even if you do passing work on the homework, project, and exams. Don't take this course if you don't plan to attend.

5 Office Hours

My office is Science Center 515, which is right up the stairs from the Math Department common area. I will be available to talk with you Monday 5–6, Tuesday 2–3, by appointment, or whenever you drop by.

6 Computing

I'll give lectures on techniques for using computers to do experiments in number theory, and create homework problems that involve computation.

In class I will demonstrate how to do computations using the computer algebra system MAGMA. This is not a free program, but I have a license to use it in our course, so I can give you a copy that runs on either Windows, Linux, or Mac OS X. Also, if you want access to a powerful computer with MAGMA pre-installed, I can give you an account on the MECCAH cluster.