Math 124: Elementary Number Theory (Fall 2001)

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

MWF 11–12

Office Hours: WF 2–3

William Stein (was@math.harvard.edu)

1 Textbooks

The main text for this course is Davenport's *The Higher Arithmetic*. From time to time I will also dip into Kato, Kurokawa, and Saito's *Number Theory 1: Fermat's Dream*. There are a huge number of web sites about elementary number theory (start with http://www.maths.uq.edu.au/~krm/web.html).

2 Course Topics

These are the main ideas of the course:

- Prime numbers
- Computer experimentation
- Congruences and the RSA public-key cryptosystem
- Sums of squares, quadratic forms
- Elliptic curves

3 Prerequisites

Math 122 is a corequisite, which you may take it concurrently with Math 124. If you haven't taken 122 you should talk to me before signing up.

4 Exams

There will be an in-class midterm exam. The final exam will be a take-home exam, which you must work on by yourself.

5 Homework

There will be one HW assignment per week, which may involve use of a computer. It will be assigned on Wednesday and due the next Wednesday. Though I will not accept any late homework, your lowest two homework grades will be dropped.

Please work together on homework problems!

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

6 Grading

Homework will be 40% of your total grade, the in-class midterm 20%, and the take-home final 40% (pending university approval).

7 Office Hours

My office is Science Center 515, which has beautiful windows and a view. I will be there waiting for you **Wednesday and Friday, 2:00–3:00pm**. You can also make an appointment with me after class if you want to see me outside of my office hours.

8 The Number Theory Lunch

Faculty members are now granted unlimited meals in undergraduate houses when accompanied by a student. So please invite me, *preferably in a group*, to lunch at your house on *Wednesday*.

9 A Note on Computer Experimentation

Computational experimentation has long played an essential role in the development of number theory. I will encourage you to use computers to explore some of the ideas we will discuss, by giving lectures on techniques for using computers to do experiments in number theory and creating homework problems that involve nontrivial computation.

Regarding actual software, I will primarily discuss the powerful and totally free open-source program PARI. You can download this program for Linux, MS Windows, and Mac from http://www.parigp-home.de.