Mathematics 124: Number Theory

Fall 2012

Science Center 222;   Tues, Thurs, 10-11:30 a.m.

Instructor: Barry Mazur,   Sci Ctr Room 512;   mazur@math.harvard.edu

Office Hours: Wednesdays 2-3 p.m.

Wednesdays 2-3 will be devoted to this class (Math 124). You are all invited to come to my office (Room 512) during this time whether or not you have a question to ask. In each office hour I will begin by discussing the questions that people explicitly ask about, and in the remaining time we can talk about number theory following the topics of interests and the general requests of the students present at the session. Do come!

Course Assistant: Eric Larson,   Dunster J-52;   elarson3@gmail.com

Office Hours: ***to be determined***

Fourth hour: This is meant to be an integral part of the course and will be scheduled shortly.

Texts

- **Principal text:** "A Classical Introduction to Modern Number Theory" (Springer-Verlag; second edition) by Kenneth Ireland and Michael Rosen.

- **(Strongly) suggested reading:** "The Higher Arithmetic: An Introduction to the Theory of Numbers" (Cambridge University Press; seventh edition) by H. Davenport.

Prerequisites: The formal prerequisite in the catalogue reads: "Mathematics 122 (which may be taken concurrently) or equivalent," Now this is an *important* requirement, but just saying this may be less helpful to give you a sense of the type of preparation you need, than the following test that you can perform.

1. At one point in the semester you will be learning the structure of the group of units in the ring of integers mod N (for $N \geq 1$). This is in Chapter 4 of our text. You needn't know anything about the structure of this group now, but you should be comfortably acquainted with the vocabulary of that sentence, or at least feel confident that you can manage to be so as the semester progresses.

2. Take a quick look at sections 1,2 of Chapter 1 of our text (Ireland and Rosen's *A classical introduction to modern number theory*. This material, which I'll quickly review, should be familiar to you.

Course Description: The catalogue reads:

Factorization and the primes; congruences; quadratic residues and reciprocity; continued fractions and approximations; Pell's equation; selected Diophantine equations; theory of integral quadratic forms.

Specifically we will be going through the first 5 chapters of Ireland-Rosen and selected later chapters depending upon time. This will also amply cover the first 3 chapters of Davenport. Our treatment of Continued Fractions and Quadratic Forms will largely follow chapters IV and VI of Davenport.

I expect to post an hour-by-hour syllabus on the web page of the course once things get going.

Exams: There will be three in-class exams through the semester, the last of these in lieu of the standard three-hour final. The dates for these are as follows:

1. October 2

2. **November 6**

3. December 4

Homework: There will be weekly assignments each Thursday to be turned in the next Thursday (modulo holidays).

First homework assignment due September 13:
All of these exercises are taken from Ireland-Rosen.

1. **The Euclidean Algorithm**

   - *Hand in solutions to* Exercises 1 and 2 on Page 14.
   - You should also do for yourself Exercise 3 on that page, but needn't hand in the solution; just try out those calculations taking a guess beforehand at (order of magnitude) how many steps you will need (i.e., how large k is) to find the answers to each of those gcd's. Nothing to hand in about this, though.
   - *Hand in solutions to* Exercises 4,7,11 on page 15.

2. **Greatest Common Divisor and Least Common Multiple**

   - *Hand in solutions to* Exercises 13,19,20,21 on page 15.

3. *Don't hand in, but just for fun* do Exercise 12 on page 15.