# Math 124, Number Theory

**Instructor**: Frank Calegari, 432 Science Center.

**Class time**: MWF, 11:00–12:00.

**Office hours**: Tue, 11:00–12:00, Thurs, 2:00–3:00, and by appointment. Please come!

**Course Web Page**: `www.math.harvard.edu/~fcale/124.html`
The homework will be available on the web in postscript and pdf format.

**Prerequisites**: Math 122 (which may be taken concurrently).

**Textbook**: "The Higher Arithmetic" by H. Davenport. This is a nice book; it is written in a conversational style, however, and does not always delineate between theorems and proofs. I therefore strongly recommend that you download (for free) William Stein's textbook:

`http://modular.fas.harvard.edu/edu/Fall2002/124/stein/`

(there is a link to this site on the course web page). This book covers the material taught in 124 over the previous two years. This year's course this year will be slightly different (less computational, and less time spent on elliptic curves), but you should still find this book very useful. Some of the homework exercises will come from this book.

**Grading policy**: Homework will account for 40% of your course grade, the midterm 20%, and the final exam 40%.

**Exams**: The Midterm and Final will both be *take-home* exams, pending administration approval (this should be a formality).

**Collaboration**: On the homework sets, collaboration is not only allowed but encouraged. However, you must write up and understand your own individual homework solutions, and you may not share written solutions. If you learn how to solve a problem by talking to a classmate or looking it up in a book, you should cite the source in your homework write-up, just as you would reference your sources in a literature or history class. You are not allowed to collaborate on either the midterm or final exam.

## What is Number Theory?

One simple answer is that number theory studies the arithmetic properties of the integers and the rational numbers. This is in contrast to calculus and analysis, which concentrate on continuous properties of the real numbers. The rational numbers do not form a "continuum"; there are "gaps" on the plane given by irrational numbers. This makes study of the rational numbers less obviously amenable to analysis.

Another way to describe what number theorists do is to describe some of the problems that number theorists consider. Here are a few such problems.

- What are the last two digits of $7^{2003}$? last *five* digits?
- What integers can be written as the sum of two squares? *three* squares? *four* squares?
- What are the *integer* solutions to $a^2 + b^2 = c^2$?
- Can $x^2 + 1$ ever be divisible by a number of the form $4k + 3$?
- What are the *integer* solutions to $x^n + y^n = z^n$?

Some of these problems may at first seem ad hoc; by changing coefficients one can seemingly generate an endless supply of them. Indeed, number theory often presents itself as a series of tricky "puzzles". However, there turns out to be a surprising amount of beautiful structure underlying the solutions to all of these problems, and the generalisation of these ideas is very much the topic of current research.