Mathematics 128S: Number Theory

Spring 2012 Tuesdays, Thursdays 1:15–2:30 pm Physics building 227

Professor: Lenny Ng
E-mail: ng AT math.duke.edu
Office: Physics 231
Office phone: 919-660-6972

Course web site: All important information (homework, handouts, etc.) will be posted on Sakai, http://sakai.duke.edu/. There is also a rudimentary web site at http://www.math.duke.edu/~ng/math128S/, but I don't expect to use this.

Textbook: There is **no required textbook**. However, *Elementary Number Theory and Its Applications*, 6th edition, by Kenneth H. Rosen is **highly recommended**. I encourage you to get this book; it will serve as a useful reference to complement the lectures.

Office hours: Two hours per week TBA, and by appointment (set up in person or by email).

Course synopsis: This course is an introduction to some of the main questions and ideas of classical number theory, with a focus on individual exploration and personal discovery. We'll begin by investigating the question "What is a number?", and see how this question led to some brilliant and celebrated breakthroughs by mathematicians such as Euler, Fermat, and Gauss. This will culminate in an examination of modern-day cryptography: how number theory allows transactions over the internet, and many more things, to be made secretly and securely.

You are not assumed to have any technical mathematical knowledge beyond the basic operations of arithmetic, only a desire to understand for yourself the surprisingly mysterious properties of the natural numbers (1, 2, 3, ...). Some previous familiarity with making precise mathematical statements and working with proofs will be very helpful, but is not absolutely necessary.

The course is roughly divided into two parts. The in-class "seminar" part is a series of lectures where we explore properties of the natural numbers. This will cover the foundations of number theory as well as modern applications to cryptography. The other part is your personal exploration of some topic in number theory that branches off from the lectures, and culminates in a mathematical paper where you explain the topic in detail, as well as a 30-minute presentation to your colleagues.

Prerequisites: If you would like to take this course and have not previously taken Math 104 (linear algebra) or equivalent, please see me so that I can make sure you're ready for the course.

Assignments: There will be weekly homework sets due on Thursdays, as well as two midterm exams. You are allowed and encouraged to work with fellow students on the homework; however, each student must write up their problem sets on their own. If you've collaborated with someone, please mention this fact (and their name) on your homework, for full disclosure.

As the culmination of this course, each of you will research a topic in number theory, chosen in consultation with me. You will write a paper on your research topic (roughly 10–15 double spaced pages) and give a 30-minute in-class presentation.

Your grade will be based on a weighted average of your grades in the various graded components: homework 15%, each midterm 25%, final project 35%.

Topics to be covered: Here is a tentative list of topics, time permitting.

- Primes, divisibility, greatest common divisor, Euclidean algorithm, Fundamental Theorem of Arithmetic
- Congruences, Chinese remainder theorem, divisibility tests, check digits
- Fermat's Little Theorem, the Euler ϕ function and other multiplicative functions (e.g. the σ and μ functions), Euler's Theorem
- Primitive roots, quadratic reciprocity
- Diophantine equations, Pythagorean triples, sums of squares
- Codes, RSA (public key) cryptography