Math 4400/Number Theory/Fall 2012 Syllabus

Course webpage: www.math.utah.edu/~bertram/4400

Class meets: MWF 10:45-11:35 in AEB 306

Instructor: Aaron Bertram Office: JWB 302

Email: bertram@math.utah.edu Phone: 581-6964

Office Hours: Mondays 12-1, Fridays 9:30-10:30 and by appointment.

Materials: The main textbook for the class is available online, titled *Numbers, Groups and Cryptography* by my colleague Gordan Savin, available at www.math.utah.edu/~savin/book_08_12.pdf. You may print them, but please do not distribute them. There is an additional book which I ask you to purchase on your own (amazon.com has good prices), *Number Theory. An approach through history* by André Weil.

Grading: Grades will be based on homework, exams and a project.

Homework: Problem sets are assigned Mondays, collected Fridays. You are encouraged to discuss the problem sets among yourselves and with me at office hours, but the final write-up must be your own. Each problem set is worth 10 points, and only the top 10 scores will count. There will be at least 12 problem sets. In addition, there will be assigned readings from the Weil book each weekend.

Midterms: Three midterms, the lowest one of which will be dropped.

1st Midterm: Friday, September 21, in class (100 points).

2nd Midterm: Friday, October 26, in class (100 points).

3rd Midterm: Friday, November 30, in class (100 points).

Project: This will be a book report to be presented orally to the class, carefully explaining one of the readings from the Weil book.

Final: Thursday, December 13, 10:30-12:30 (150 points).

Total: 10 Problem Sets + 2 Midterms + Project + Final = 500 points

Prerequisites: Calculus and linear algebra are required, and analysis is recommended. If you have not had these courses recently, see me.

ADA Statement: The Americans with Disabilities Act requires that reasonable accomodations be provided for every student with physical, sensory, cognitive, systemic, learning, and psychiatric disabilities. Contact me at the beginning of the semester to discuss whether any such accommodations are necessary.

Course Description: This is a course in the Theory of Numbers. These numbers are, primarily, the integers, though, as we will see, the finite fields consisting of numbers *modulo* a given prime number p will play an important role. There is a surprising amount of structure to these numbers, including their unique factorization into primes, as well as solutions to various (linear and quadratic) equations modulo p. We'll look into all this in some detail. Although the study of numbers started as the purest of mathematics, it has been shown to be extremely useful in cryptography. This course is self-contained, but it is also good preparation for a course in cryptography that I will give this Spring.

Course Outline: We will cover Chapters 1-9 of Savin's notes.

1. Euclidean Algorithm.

- **a.** Euclid's Algorithm and Continued Fractions
- **b.** Integer solutions to $ax + by = c$.
- **c.** Unique factorization of integers.
- **d.** How fast is Euclid's algorithm?

2. Groups and Arithmetic.

- **a.** What is a group?
- **b.** Numbers modulo n.
- **c.** The group of units moduli p.
- **d.** Lagrange's Theorem.
- **e.** The Chinese Remainder Theorem.

3. Rings and Fields.

- **a.** Wilson's Theorem and the field of integers modulo p.
- **b.** Fields of characteristic p.
- **c.** Quadratic numbers.

4. Primes.

- **a.** There are infinitely many.
- **b.** Primes in arithmetic progressions.
- **c.** Perfect numbers and Mersenne primes.
- **d.** The Lucas-Lehmer primality test.

5. Roots.

a. What is a root modulo n?

b. The Euler function.

c. Primitive roots.

d. The discrete logarithm.

e. Cyclotomic polynomials.

6. Quadratic Reciprocity.

a. Perfect squares modulo p.

b. Fields with p^2 elements.

c. When is 2 a perfect square modulo p?

d. Quadratic reciprocity.

7. Applications of quadratic reciprocity.

a. Fermat primes.

b. Quadratic fields and the circle group.

c. Lucas-Lehmer revisited.

8. Sums of Two Squares.

a. Sums of two squares.

b. Gaussian integers.

c. The method of descent.

9. Pell's Equation.

a. Shape numbers and induction.

b. Square-triangle numbers and Pell.

c. Dirichlet approximation.

d. Classifying the solutions to Pell's equation.

e. Continued fractions.

First Homework Assignment. Due this Friday, August 24

Savin, Page 9. Problems 1-8.