Math 482: Number Theory and Cryptography, Spring 2012

Instructor: Brian Sittinger
Email: brian.sittinger@csuci.edu
Office: Bell Tower 2105
Office Hours: W 3 - 4 PM, Th 12 - 1 PM, and by appointment.
Class Times: TuTh 4:30 PM-5:45 PM
Class Location: Bell Tower 2505

Prerequisite: Math 300 or equivalent.

Text: Elementary Introduction to Number Theory by Long.

Course Description from the Course Catalog: Topics include: Divisibility, prime numbers, unique factorization theorem, congruences, solutions of linear congruences, solutions of quadratic congruences, Fermat’s Little Theorem, Wilson’s Theorem, and Euler’s phi function, Cryptography.

Learning Outcomes: Through this course, students will be able to

- Prove the basic properties of divisibility in \( \mathbb{Z} \)
- Establish properties of prime numbers
- Discuss and use the unique factorization theorem
- Use the congruence formalism
- Use Wilson’s, Fermat’s, and Euler’s Theorems for theoretical and computational purposes
- Solve conditional linear and quadratic congruences
- Apply basic number theory to construct ciphers
- Express ideas of number theory and its applications in oral and written form.

Grading: Grades will be determined as follows:

- Homework (25%)
- Two Exams (25% each)
- Project (25%)
**Homework:** I will assign homework daily to be turned in on every Tuesday (unless otherwise stated) at *the beginning of lecture*. Make sure that your presentations are well-organised. If you use more than one sheet of paper, please write your name at the top of each sheet, and be sure to staple them all together. This will make my job to grade them much easier.

**Exams:** The exams will be of the *take-home* variety. You will be given one week to complete each of these. Lecture notes and the textbook may be used as resources. Please work alone, and ask me if you have any questions on them. The exams will be given around the sixth and twelfth weeks of the semester.

**Project:** Instead of a final exam, you will be given a list of possible project problems from which you will choose one to work on. This is largely an exploratory exercise, although the more you statements you prove, the merrier. This will be graded on presentation, effort, and content. More details about this will follow.

**Math 399:** Please sign up for Math 399 *Section 9*. Further instructions will be given in the lab.

**Academic Honesty:** Cheating and plagiarism will not be tolerated in this class. For information on the University’s policy, please read the University Catalog (“Policies and Regulations” section).

**Disability Statement:** Cal State Channel Islands is committed to equal educational opportunities for qualified students with disabilities in compliance with Section 504 of the Federal Rehabilitation Act of 1973 and the Americans with Disabilities Act (ADA) of 1990. The mission of Disability Accommodation Services is to assist students with disabilities to realize their academic and personal potential. Students with physical, learning, or other disabilities are encouraged to contact the Disability Accommodation Services office at (805) 437-8510 for personal assistance and accommodations.

**Disclaimer Statement:** Information contained within this syllabus, other than that mandated by the University, may be subject to change with advance notice, as deemed appropriate by the instructor.