Mathematics 13150–Freshman Seminar, The Magic of Numbers, spring 2014, HH DBRT 206, 2:00-2:50

Instructor	Sam Evens
Office, Phone, Email	222 HH, 631–7165, sevens@nd.edu
Office Hours	Monday 11:45–12:40 Wednesday 5:10-6:00 Or by appointment

Course Website

The website www.nd.edu/ sevens/13150.html has information about the course, including lecture notes, homework assignments, quiz and exam schedules.

Course Description

We will learn modular arithmetic (addition and multiplication on clocks) and see how it is used in the RSA algorithm, which is used in secure internet transactions. The goal of the course is for you to understand some nontrivial, accessible, and relatively abstract mathematics, and then to see how it has an important real world application.

Topics Covered

1. Counting problems (e.g., how many numbers from 7 to 356 are divisible by 8 and 12). Also some real world applications.
2. Division algorithm; find the greatest common divisor of two numbers. If m and n are relatively prime, find numbers x and y so that $xm + yn = 1$ using reverse division algorithm.
3. Prime numbers, prime factorizations, which fractions are squares of another fraction?
4. Relatively prime; how many numbers from 1 to n are relatively prime to n; answer is Euler function $\phi(n)$. Methods of computing $\phi(n)$.
5. Modular arithmetic; addition and multiplication mod n. Congruences. Division mod n using reverse division algorithm. Study of cyclical processes; when does a cyclical process reach a certain point.
6. Powers mod n using Euler's theorem and Fermat's theorem.
7. Computing kth roots mod n. If k and $\phi(n)$ are relatively prime, then every number has a unique kth root. Computing kth roots using reverse division algorithm.
8. The RSA algorithm. Roles of message sender, receiver, and spy. Modular arithmetic calculator for doing calculations with large numbers. Project to decode messages encoded with large numbers.
9. Throughout the semester, students read Simon Singh's "The CodeBook", which is a popular science history of coding.

Text

This course is based on the book *The Magic of Numbers* by Benedict Gross and Joe Harris, Prentice-hall, 2004, which was developed for a similar course at Harvard. That book is out-of-print, so instead we will use lecture notes that are posted on the course website. We will also use *The Codebook* by Simon Singh as a secondary book. *The Codebook* is a popular science book that gives a history of coding.

Quizzes

There will be quizzes roughly every two weeks, except for exam weeks. Quizzes will cover material relevant for the homework. The first quiz will be Wednesday, January 22.

Hour Exams

There will be two hour exams during the semester. They are tentatively scheduled for Friday, February 21 and Friday, March 28, and will be in class.

Final Exam

The Final Exam is scheduled for Monday, May 5, 4:15–6:15, room TBA.

Homework

There will be both in-class written work as well as take-home written work. Fridays will be largely devoted to working on problems in groups, with some lectures. In-class written work should be turned in as a single assignment for a group of no more than four people. Take-home written work should be done separately by individual students, although talking about problems together is certainly encouraged. Take-home written work is due on Wednesdays and will be announced in-class and on the course website at: www.nd.edu/∼sevens/13150.html Everyone has an automatic extension until Thursday at 5 pm, and homework can be turned in to my mailbox in the math department.

Grading

The final grade will be a weighted average of the grades on the homework, quizzes, hour exams, and final exam as follows:

Hour Exams	15% each
Final Exam	30%
Quizzes	20%
Homework	20%