Number Theory
Course Syllabus

Topics Covered in Course:

I. Introduction
- A. Number systems: **N, Z, Q, R, C**
  (Natural numbers, Integers, Rational numbers, Real numbers, Complex numbers)
- B. Pythagoras and the Pythagorean Theorem
  1. Two (or three) proofs of the Pythagorean theorem
  2. History
     a. Mathematics and mysticism
     b. Pythagoras and the Pythagorean Brotherhood
  3. Introduction to indirect proof (proof by contradiction)
  4. Proof that $\sqrt{2}$ is irrational
  5. Commensurability
  6. Finding square roots numerically without a calculator

II. Basic facts about the integers
- A. Proof by induction
- B. Strong induction
- C. Well-ordering principle (WOP)
- C. Well-ordering principle $\Rightarrow$ Principle of Mathematical Induction (POMI)
- D. POMI $\Rightarrow$ WOP (statement; proof on homework)

III. Elementary multiplicative number theory
- A. Definitions: factor, prime (and composite), relatively prime
- B. Basic properties of divisibility
- C. Division Theorem
- F. Sieve of Eratosthenes

IV. Euclidean Algorithm
- A. (for dividing a rectangle into squares)
- B. Incommensurability
- C. Proof that the Euclidean algorithm yields the gcd

V. Linear Diophantine equations (general potato theory)
- A. Finding a solution to a linear Diophantine equation using the Euclidean algorithm
- B. Existence of solutions for linear Diophantine equations
- C. General solution for a linear Diophantine equation
- D. Fundamental Theorem of Arithmetic
- E. Euclid's theorem on the infinitude of primes

VI. Modular arithmetic
- A. Definition of congruent mod n
- B. Addition, multiplication, exponent tables for various small mods
- C. Basic properties of congruences
- D. The Chinese Remainder Theorem
- E. Encryption using modular addition (Caesar ciphers) and modular multiplication

F. Structure of $\mathbf{Z}/n\mathbf{Z}$
    1. Rings and Fields
    2. Multiplicative inverses
    3. Cancellation
G. Encryption using modular exponentiation
H. Fermat's Little Theorem
I. Euler's Theorem
J. Primitive roots
    1. Definition
    2. Existence of primitive roots in prime mods

VII. RSA Encryption Algorithm
A. Explanation of the algorithm
B. Performing RSA on computers using Maple

VIII. Quadratic Residues

A. Definition of Quadratic Symbol $\left(\frac{a}{b}\right)$

B. Euler's Identity
C. Quadratic property of –1
D. Quadratic reciprocity

IX. Peano Axioms and Peano Arithmetic

X. Complex Numbers
A. Rectangular and polar form
B. DeMoivre's theorem

XI. Gaussian Integers
A. Definition of $\mathbf{Z}[i]$; definition of norm
B. Euclidean properties of the Gaussian Integers
    1. Definitions: unit, prime
    2. Division theorem for Gaussian Integers
    3. Unique factorization for Gaussian integers

XII. Fermat's Two Squares Theorem

XIII. Continued fractions
A. Converting rational numbers into continued fractions
   (the Wily Improper Fraction Leprechaun)
B. Converting irrational numbers into continued fractions
C. Converting infinite repeating continued fractions into radical form
D. Characterization of finite and repeating continued fractions
E. Convergents (*dis*continued fractions): how good an approximation are they?

Student Presentations:

At the end of the session, each student gives an oral presentation on a topic in number theory or the history of mathematics.