

There are three parts to the course: Number Theory -- Cryptoclub -- Problem solving
Number Theory contains many topics that can be used to understand encryption techniques. Crypto Club activities provide examples of using Number theory in the real world and an interesting application to use with middle school students.

Number theory is the study of integers (no fractions or irrational numbers!) and their properties relative to the operations of addition, subtraction, multiplication, and division. The topics of number theory that we cover are using different bases, arithmetic progressions, combination charts, factoring and prime numbers, lcm and gcd, solving Diophantine equations, modular arithmetic, solving congruence equations and powers of numbers in modular arithmetic.

The **problems** are designed to inform the number theory – in advance of our study it motivates our conversations as we discover valuable techniques to use in number theory.

In **The Cryptoclub** we will cover Caesar ciphers, Vigenère ciphers, multiplicative and affine ciphers and RSA encryption. For each type of cipher we will first need to know how to encode, then how to decode given key information, and finally, how to crack a cipher given only what type of cipher is used. Cryptography will show us valuable applications of number theory – even number theory that is learned in middle school.

Technology: We will be using TI-84 calculators, EXCEL, and several internet games and activities available on the internet. TI-84 will be available during class but you should consider purchasing your own or asking your school to provide one for you. A TI-83 will work as well. If you do not have access to a computer on which you can make EXCEL files and experiment with the online games, you may use the computers in room 600 by appointment. If you get your UIC ID card you can check out a lap-top computer for use in the Math Learning Center on the fourth floor of SEO.

Class Structure each class day:

- 4:00: Office hours
- 5:00: Quiz and/or opener (Late-comers may make-up the work at 8:00)
- 5:15: Problem presentations
- 5:30: Activity one
- 6:30: Break
- 6:45: Technology application
- 7:00: Activity two.
- 8:00: Class ends. Computers available. Make-up quiz

Grading

- 20% Problem Portfolio
- 20% Presentation and Teaching application
- 20% CryptoClub Workbook and CryptoQuizes
- 20% Midterm, TBA
- 20% Final, December 7

The following course outline is subject to change.

WEEK1 Place Value and arithmetic algorithms, using ascii code to code letters into numbers

WEEK2 Arithmetic Progressions and Combination Charts.

WEEK3 LABORDAY CryptoClub: Units 1 and 2, CryptoClub website, Frequency Analysis

WEEK4 CryptoQuiz through Unit 2

Basic rules about numbers, foundations of Arithmetic, proofs, division algorithm, definition divisibility

WEEK5 CryptoQuiz though Chapter 9

Factors, multiples and Prime numbers, Sieve of Eratosphenes, GCD algorithms,

WEEK6 Crypto Day, Vigierne Ciphers

WEEK7 Basic rules of divisibility and proofs, Euclidean algorithm for finding GCD

WEEK8 Extended Euclidean Algorithm – why it works, Solving Diophantine equations, Fundamental Theorem of Arithmetic

WEEK9 Lure of the Labyrinth Day

WEEK10 Introduction to Modular Arithmetic, Basic rules and proofs, Multiplication tables, Multiplication cipher -- Multiplication tables mod 26

WEEK11 Finding inverses in modular arithmetic, solving congruence equations
Decipher multiplicative and affine codes

WEEK12 Prime Number Projects

WEEK13 Finding powers in modular arithmetic, Using powers to encode, Patterns in power tables, little Fermat's theorem. RSA coding.

WEEK14 CryptoClub Unit 7 RSA coding schemes

WEEK15 Final Presentations – Treasure Hunts – etc