

Mathematics Lessons for Grades 9-12

“Break the Code”

Nathan Hamlin / nghamlin@hotmail.com / Washington State University / Culturally Relevant Engineering Applications in Mathematics

Discipline: Cryptography/ Number Theory

Grade: 9 to 10

Standards

NCTM Number and Operations Standard: Grade 9-12

Understand numbers, ways of representing numbers, relationships amongst numbers and number systems:

- Develop a deeper understanding of very large and very small numbers and of various representations of them.

Compute fluently and make reasonable estimates:

- Develop fluency in operations with real numbers, ...using mental computation or paper and pencil calculations for simple cases and technology for more complicated cases.

Connections

Recognize and apply mathematical concepts in contexts outside of mathematics.

Purpose/Goals

The students will be able to calculate using modular arithmetic, and apply appropriate multiplicative inverses within an expression. They will have a sense of some of the math used to encode messages in public-key cryptography.

Context

The activity requires addition, subtraction, multiplication and division. It greatly helps if the students are fluent with long division by pencil and paper.

Preparation

The teacher should familiarize him/ herself with the Excel spreadsheet before the activity. The teacher should examine the worksheets and get a good handle on what a “key” is: a private number used to keep a message secret.

The students will use four worksheets; two alphabet/ number charts; and an Excel spreadsheet. Three of the worksheets lead the students step-by-step through the encoding and decoding process: first by hand with multiplication, then by computer, and then with modular arithmetic. The fourth worksheet is modular arithmetic practice. The charts give students a simple way to represent letters by numbers, and provide a choice of keys. The spreadsheet allows students to type in a message in 6-letter blocks and then to have the computer do what the students had been doing in the first part by hand, except more quickly. It is the part of the project that allows the students to see some of the importance of powerful computing for cryptography. These handouts and the spreadsheet will be provided. Several computers should be available for student use if the students are going to do part two on their own, and calculators may be helpful for the other portions. The first part works best if there are some calculators that admit of ten or eleven digits.

Website

<http://www.rsa.com/rsalabs/node.asp?id=2092> has some information about the size of the “keys” used in industrial applications. This website is helpful for background information.

Motivation

Students should be reminded that because of all of the financial and personal information transmitted over the wire (internet, bank transactions, government secrets) there is a great need to keep data private. This is generally done through cryptography (i.e. code making) based on Number Theory. A good warm up exercise is to discuss with the students how arithmetic works “on a clock:” $7 + 6 = 1$, $8 + 8 = 4$, etc.

Description

In this project the students encode and decode messages to and from their classmates. There are four parts to the lesson, and two to three one-hour class periods should suffice. In the first part of the lesson, the students encode and decode one-word messages by hand (or calculator) using multiplication and division by small primes. In the second part of the lesson the students work with an Excel spreadsheet so that encoding and decoding go more quickly and so that longer messages can be used. In the third part of the lesson, the students are introduced to modular arithmetic and do some practice by hand. In the final part of the lesson the students encode/ decode messages using arithmetic mod 29 and multiplicative inverses. There are challenge questions in the third and fourth part, and in each stage it is possible for some (or all) students to send or receive multiple messages.

Assessment

Most of the learning in this project comes in the calculation of examples and the vocal interactions of the students and teacher. To assess the results one can use addition/ multiplication problems with larger moduli, and ask the students to find various inverses in those rings. The actual use of modular arithmetic in cryptography usually requires the use of exponents, and Fermat's little theorem.