

MODULE I

Computers, Codes, and Binary Numbers

The essence of mathematics lies in its freedom. – Georg Cantor

There are three kinds of people in the world—those that can count and those that can't. — Old Math Joke

$$1 + 1 = 2$$

$$2 + 2 = 4$$

$$4 + 4 = 8$$

$$8 + 8 = 17$$

— Prof Moriarty's Blackboard

from the movie *Sherlock Holmes' Smarter Brother*

1. Goal

To familiarize you with the mathematical ideas behind some of the technology used in our society.

- Computer architecture uses **binary numbers** in fixed sizes, called **bytes**.
- Megabyte of memory is (approx) one million bytes.
- Gigabyte of memory is (approx) one billion bytes.

3. Error-correcting codes

In **error-correcting** codes, we encode information so that if an error occurs in reading the information, we can still recover the original data.

Compact disk technology utilizes this type of coding, where small scratches on a CD need not damage the sound reproduction.

2. Encoding Information

We are particularly interested in the mathematical concepts used to **encode** information.

Two purposes for encoding information:

- (1) **Error-correcting** codes
- (2) **Encryption**

4. Secret codes

A second purpose of coding information is to make it **secure**, so that unauthorized persons cannot read private messages.

Secret codes have obvious military, industrial, and personal applications.

Our simple encryption-decryption method relies on some basic facts about “clock-arithmetic” and on a method for solving what we call “the pails-of-water” problem.