6 Number Theory II: Modular Arithmetic, Cryptography, and Randomness

For hundreds of years, number theory was among the least practical of mathematical disciplines. In contrast to subjects such as arithmetic and geometry, which proved useful in everyday problems in commerce and architecture, astronomy, mechanics, and countless other areas, number theory studies very abstract ideas called numbers, and applications of the subject are not immediate. Over the course of the second half of the twentieth century, however, number theory became increasingly more applicable, and today make possible a wide range of technologies. In this section we will consider **modular arithmetic** and applications to **cryptography** and to generating "**random numbers**" by deterministic computers.

6.1 Introduction to Cryptography

Since ancient times, people desiring to transmit messages privately have devised methods of encoding messages, so that no person but the intended recipient could read the message. The ability to successfully encode and decode messages has played a central role in the development of financial markets and in history-altering military turnarounds. We use **cryptography** to refer to the study of how information can be made secretive enough so that bad people can't read it, yet still accessible enough so that good guys can. Cryptography is a very exciting and developing area of contemporary mathematics, with connections to number theory and computational complexity.

Let us consider a person Alice who would like to send a secret message to another person Bob. Perhaps Alice and Bob are childhood friends and are planning a surprise birthday party for a mutual friend. Or perhaps Alice and Bob have never met, but Alice would would like to send Bob her credit card information so she can pay for something Bob is selling. In both cases, Alice and Bob would like to guarantee several things: (a) Alice would like to ascertain that Bob has received her message; (b) both Alice and Bob would like to know that no one else has seen the secret message; (c) Bob would like to ascertain that the message he believes to have come from Alice has indeed come from Alice. It is not immediately clear how we can guarantee each of these except in the case where Alice and Bob actually meet up and Alice whispers the message into Bob's ear. What should they do, however, if they are far apart? If they send a message through the postal service, there is a small chance that (notwithstanding the serious federal crime involved in opening someone else's mail) that an eavesdropper might intercept the message before it reaches Bob. Even if they use the telephone, or an email, or a text, there is a chance that the intended message and information will make its way to the wrong hands. These kinds of questions motivate the need to develop methods of encoding and decoding information so that messages can be communicated securely.

We briefly note several methods used to solve some of the above problems. Bob can send back a note saying "I received your message", though the same security concerns relevant to the initial message will be relevant here as well. Signing one's signature to a piece of a paper is a relatively simple way in which Alice can convince that the message indeed came from her. This is partly because while reading and identifying a signature is relatively easy, actually creating it is complicated, for all except the person signing it (though of course signatures can be forged). In this section, we will focus mostly on the problem (b), that is, how can we ensure that no eavesdropper can read the message intended solely for Bob.

Simple ways of encoding messages were known since antiquity. Sometimes letters were switched for other letters, or for numbers, and so an eavesdropper quickly looking at an encoded message would only see gibberish. However, this approach has many limitation. For starters, how would Alice communicate to Bob the scheme which she used to encode the message and which he, consequently, will need to decode it? If he can determine this by himself, perhaps through some guesswork, then what would stop someone else from doing the same? Many somewhat sophisticated methods have been developed over the centuries for encoding and decoding secret messages, though in this section we will focus on one that is built on what is called **modular arithmetic**, a system of arithmetic that in some sense only has a finite number of numbers.