Introduction

0.1 To the Student

The ability to store, retrieve, and transmit data accurately is a central aspect of today's society. To make this process work efficiently, *identification numbers* are used to represent or encode information pertaining to products, documents, accounts, or individuals. One such system in place today generates a Universal Product Code (UPC) for every item sold in a grocery store. A UPC identifies not only the specific product but also the type of product and its manufacturer. This gives grocery stores a convenient and effective way to maintain inventory and keep track of sales (each store associates a price with the UPC that appears on the cash register when the product's bar code is scanned at the checkout counter). Numbers are also used to identify books (International Standard Book Numbers or ISBNs), individuals (social security numbers), library holdings, bank accounts, UPS packages, drivers' licenses, credit cards, and much more.

Given that identification numbers provide a convenient way to transmit information easily and accurately, they are recorded onto documents, typed or scanned into computers, sent via the Internet, or transmitted in some other fashion millions of times a day. Banks routinely transfer money electronically by using routing and account numbers, and consumers frequently complete sales with credit card numbers. Since these types of transactions occur so frequently, errors are bound to happen. For example, the number 12345 could be transmitted and incorrectly recorded as 12346 or as 12354. A bank would not want to transfer money into the wrong bank account, and consumers and retailers do not want charges billed to the wrong credit card account.

With our heavy reliance on identification numbers to transmit information and the likelihood that sooner or later a transmission error will occur, it is crucial to know when an identification number has been transmitted incorrectly. Specifically, the receiver of that number must have a way to determine whether the number received is incorrect. If no verification system has been established, the only way of knowing is to contact the sender. But contacting the sender is not always possible or feasible, and it may be time consuming. This difficulty has motivated the creation of methods that the receiver

can use, independent of the sender, to recognize when an identification number has been transmitted incorrectly. The goal of this book is to present the mathematical methods, called *check digit schemes*, that do this.

Identification numbers, and the check digit schemes that detect when these numbers have been transmitted incorrectly, are crucial for the quick storage, retrieval, and transfer of vast amounts of information. In this book, a variety of check digit schemes are discussed. Check digit schemes vary in their ability to catch errors. Some, such as the airline ticket scheme, do not catch every occurrence of the most common type of error, while others, such as the ISBN scheme, catch most error patterns. Consequently, criteria for judging the reliability of check digit schemes are a central concern of this book.

0.2 To the Professor

This text is ideal for a liberal arts mathematics class. The book is organized to allow students to move from simple mathematical concepts and check digit schemes to more complex ideas. Not only are all mathematical concepts developed within the context of studying check digit schemes, but as each mathematical topic is studied, other applications are discussed. This will lead to a study of not only check digit schemes, but also "public key" cryptography systems, graphing data, presenting data, and symmetry.

Chapter 1 discusses a variety of identification number systems and establishes the mathematical terminology that will be used to study check digit schemes. In addition, the criteria used to determine the dependability of a scheme are presented.

Chapter 2 begins with a presentation of basic properties of integers and an introduction to modulo arithmetic. The concepts developed are then applied to an investigation of the check digit schemes used for United States' postal money orders, airline tickets, UPCs, and ISBNs. The reliability of each scheme is a central aspect of this discussion. Finding methods that address shortcomings of these schemes motivates the material covered in the remaining chapters. The same number-theoretic concepts are also applied to a discussion of cryptography, the art of sending secret messages. Special attention is paid to the RSA "public key" cryptography system, which is used to send sensitive data over the Internet.

In Chapter 3, sets, functions, and permutations are considered. These concepts play a role in the construction of more advanced check digit schemes and are central to *hashing functions*. A hashing function is the process used to take information and represent it as an identification number. The check digit scheme developed by IBM is also presented. In addition, the use of graphs to present and study functions and data is discussed.

The discussion in Chapter 4 is focused on symmetry and rigid motions. The notation established in Chapter 3 for permutations is used in a mathematical investigation of the symmetries of a variety of different shapes. The symmetries of a pentagon form the basis of the very reliable Verhoeff check digit scheme presented in Chapter 5. Furthermore, the use of rigid motions to create elaborate patterns will serve as an introduction to the discussion of group theory that begins Chapter 5.

In Chapter 5, an introduction to the fundamentals of group theory is presented. The

concepts discussed, along with those presented in the previous chapters, culminate in the Verhoeff check digit scheme, the most sophisticated and reliable scheme considered in the book. The check digit scheme used with German money, which is based on the Verhoeff scheme, is also considered.

Along with the mathematical content described above, this book provides writing and group activities. These activities can be integrated into a student-centered approach. At the beginning of each section is a preliminary activity that has the students exploring and working with the concepts to be introduced. The notions that the students develop are then cultivated in that section. At the end of the section, traditional exercises, group activities, and writing assignments are given for further exploration.

Integral to this approach is the use of writing to develop and present mathematical understanding (see [17] and [24] for more information on the use of writing in the teaching of mathematics). Writing is not only a way to express mathematical understanding, but a way to develop that understanding. As each mathematical topic is investigated, the students use writing to improve and communicate their understanding of that topic and how it is applied. Students should write at the beginning, middle, and end of the learning process. The preliminary activities have them writing to investigate. This work is then rewritten or used to complete homework exercises and group activities, which are, in turn, used to complete larger writing assignments or essays. Through this writing and rewriting process, students gain a deeper understanding of mathematics and its diverse applications.

Writing to develop mathematical understanding will also improve communication skills. Many of the components of the mathematical process are rhetorical modes or critical writing strategies. Defining, serializing, classifying, comparing, generalizing, analyzing, and arguing are skills crucial to mathematics, but each is also a strategy that must be mastered to become an effective writer. Writing and paper assignments are included to help students develop each of these strategies.