Modular Arithmetic: Error-Detecting Codes

While we will make a lot of use of modular arithmetic when looking at cryptographic schemes, there is also a lot of use of cryptography in other fields. Here we look at some examples of modular arithmetic being used in *coding theory*, which studies how to ensure that information be transmitted accurately and error-free. Often a coding scheme which ensures accurate transmission of information will be being used alongside whatever cryptographic scheme is being used to keep it secret.

ISBN-10

Until 1965, when a book was published it would likely just contain information about the publisher and the author, with little else to identify the book apart from the title. After 1965 most newly published books were then assigned a Standard Book Number (SBN) and this was further developed and implemented as the International Standard Book Number (ISBN-10) in 1970.

Each book is assigned a ten-digit code, using the digits 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, X, where the 'X' stands in for the number 10. (Meaning each digit has eleven possibilities, rather than the usual ten.) The code that a book receives is not a random ten-digit number, but is based upon information such as the publisher, country, or area.

The final digit of an ISBN-10 is what interests us in terms of modular arithmetic. Given any ISBN-10, we can calculate a particular sum and check that it evaluates to 0 under modulo 11 arithmetic. If it does not return 0, then our ISBN-10 is not valid. For example, a book may be given the first nine digits of an ISBN-10 as 135023072c. The missing tenth digit is the **check digit** and is required to make the following equation equal 0 modulo 11.

$$\begin{aligned} &= (10 \times 1) + (9 \times 3) + (8 \times 5) + (7 \times 0) + (6 \times 2) \\ &+ (5 \times 3) + (4 \times 0) + (3 \times 7) + (2 \times 2) + (1 \times c) \\ &= 0 \mod 11. \end{aligned}$$

If we calculate this, we are left with

$$\begin{aligned} &= 10 + 27 + 40 + 0 + 12 + 15 + 0 + 21 + 4 + 0 + c \\ &= 129 + c \\ &= 8 + c \end{aligned}$$

$$= 0 \mod 11.$$

We then need to pick the value of c for which $8 + c = 11$, giving $c = 3$ and our final ISBN-10 as 1350230723.

This type of code is incredibly useful, since it can allow us to detect errors. For example, if we have a book with ISBN-10 0069037068 and calculate the sum

$$\begin{aligned} &= (10 \times 0) + (9 \times 0) + (8 \times 6) + (7 \times 9) + (6 \times 0) \\ &+ (5 \times 3) + (4 \times 7) + (3 \times 0) + (2 \times 6) + (1 \times 8) \mod 11 \end{aligned}$$

then we find that the result is $174 = 9 \mod 11$. Since this is non-zero, we know that at least one of the digits is wrong.

In actual fact, if we suspect that what has happened is that two adjacent digits have been transposed (swapped) then ISBN-10 can even tell us which ones. (Transposing two digits is a very common human error in data entry.) The check-sum is equal to 9, which if two digits have been swapped is equal to the difference between them. There are only two digits in the number which have a difference of 9: the fourth and fifth digits, 9 and 0. If we swap these back then the check-sum is recalculated as

$$\begin{aligned} &= (10 \times 0) + (9 \times 0) + (8 \times 6) + (7 \times 0) + (6 \times 9) \\ &+ (5 \times 3) + (4 \times 7) + (3 \times 0) + (2 \times 6) + (1 \times 8) \mod 11 \\ &= 0 \mod 11, \end{aligned}$$

giving a valid ISBN-10.

The general method is explained as follows. The last digit is a check digit, which is calculated based on the previous nine digits. Let x_i represent the digit in position i of the ISBN, e.g., in 0131862391 we have $x_1 = 0$, $x_2 = 1$, $x_3 = 3$, etc. Then, for an ISBN $x_1x_2x_3x_4x_5x_6x_7x_8x_9x_{10}$, the following checksum must be satisfied:

$$10x_1 + 9x_2 + 8x_3 + 7x_4 + 6x_5 + 5x_6 + 4x_7 + 3x_8 + 2x_9 + 1x_{10} \equiv 0 \mod 11.$$

E.g., for 0131862391 we get

$$10\times0+9\times1+8\times3+7\times1+6\times8+5\times6+4\times2+3\times3+2\times9+1\times1 = 154 = 14\times11 \equiv 0 \mod 11.$$

Test Yourself Visit the URL below to try a numbas exam:

`https://numbas.mathcentre.ac.uk/question/165497/isbn-10/embed`

ISBN-13/Barcodes

The international standard for barcodes, used on supermarket products and many other items, is similar to ISBN but uses a slightly different calculation working modulo 10. We still calculate a check digit, but the sum we work with is different. For example, if a supermarket product has barcode number 505161803079c, where the last digit is obscured, then it is calculated as follows.

$$\begin{aligned}
&(1\times 5)+(3\times 0)+(1\times 5)+(3\times 1)+(1\times 6)+(3\times 1)\\
&+(1\times 8)+(3\times 0)+(1\times 3)+(3\times 0)+(1\times 7)+(3\times 9)+(1\times c)\\
&=5+0+5+3+6+3+8+0+3+0+7+27+c\\
&=67+c\\
&\equiv 7+c \ mod\ 10
\end{aligned}$$

To calculate the check digit, we need to find the value of c for which $7+c$ will equal 0 modulo 10. This gives us $c=3$ and our valid barcode as 5051618030793.

Prior to 2007, books used 10-digit ISBN-10 as defined above, and books published since then use an ISBN-13, which is a barcode in the same sense as the previous example. Some books have both ISBN-10 and ISBN-13 codes. The last digit in each case is a check digit.

Test Yourself Visit the URL below to try a numbas exam:

`https://numbas.mathcentre.ac.uk/question/165524/isbn-13/embed`