Cosmos Multidisciplinary Research E-Journal
Online Available at www.cmrj.in
Recognized International Peer Reviewed Journal
ISSN No. 2456-1665

Modular Arithmetic Approach to Check Digits

Dr. Aruna M. Kulkarni
Department of Mathematics
SAJVPM'S Smt.S. K. Gandhi College, Kada,
Dist. Beed, Maharashtra
abhiarud@gmail.com

Abstract

The purpose of this paper is to discuss on Modular Arithmetic and application to real life situation.

INTRODUCTION

Modular arithmetic is a special type of arithmetic that involves only integers. It is a system of arithmetic for integers which considers the remainder. It an abstraction of a method of counting. Under modular arithmetic the only numbers are

0, 1, 2, 3,……..N-1.

Division algorithm will be an important application to modular arithmetic.

When $a = q_{n+r,}$ where $q\ is\ the\ quotient\ and\ r\ is\ the\ \boldsymbol{remainder}$ upon dividing a by n we write

$$a\ mod\ n = r\ or$$

$$a = r\ mod\ n$$

Example- $11 mod 3 = 2$

In our applications, we will use addition and multiplication mod n as

$$(ab) mod\ n = \big((a\ \boldsymbol{mod}\ n)(b\ mod\ n)\big) mod\ n$$

Similarly

$$(a + b) mod n \quad \big((a\ mod\ n) + (b\ mod\ n)\big)$$

Modular arithmetic is often used in assigning an extra digit to identification number for the purpose of detecting forgery or errors.

Check Digit

A check digit is a decimal (or alphanumeric) digit added to a number for the purpose of detecting the sorts of errors humans typically make on data entry. It is not uncommon to make errors when handling numbers like writing down a phone number, giving out a credit card number, writing down a street address and so on.

Application- 1

The United States postal service money order has identification number 10 digits together with an extra digit called a check. The check digit is the 10 digit number mod 9.

Thus the number 8800016502 has the check digit 3 since (8+8+0+0+0+1+6+5+0+2) mod 9 = 3. If the number 88000165023 were incorrectly entered into computer program as, say, 88001165023 (an error in the fifth position) the machine would calculate the check as 4 whereas the entered check digit would be 3. Thus the error would be detected.

Example-

Suppose that the money order has ID number 719-8164036, can you determine the missing term?

Yes we can,

Let the missing term be a_4

Since $(7+1+9+a_4+8+1+6+4+0+3) \bmod 9 = 6$

$(39+a_4) \bmod 9 = 6$

Gives $a_4 = 3$

Application-2

Airline companies, United parcel service and Avis and National rental car companies use the modulo 7 values of identification number to assign check digits.

Airline Companies.

An airline ticket identification number is a 14- digit number. The check digit is the number between 0 and 6 that represents what the identification number is equivalent to using a mod 7 clock. Thus the check digit is just the remainder when the identification number is divided by 7.

Example-

What is the check digit for airline identification number 10061559129884?

Since

$$10061559129884 = 7 \times 1437365589983 + 3$$
$$\therefore 10061559129884 \equiv 3 \; mod \; 7$$

So the check digit is 3.

United parcel service

Example-

What is the check digit for united parcel service pick up record number 768113999?

Since

$$768113999 = 7 \times 109730571 + 2$$
$$\therefore 768113999 \equiv 2 \; mod \; 7$$
$$so \; the \; check \; digit \; is \; 2.$$

Avis Car Rental

Example-

Determine the check digit for the Avis rental car with identification number
540047
Here we use modulo 7 values of identification number to assign check digit. Here the check digit is 4 since

$$540047 = 7 \times 77149 + 4$$
$$\therefore 540047 \equiv 4 \, mod \, 7$$

The method used by the postal service and the airline companies do not detect all single digit errors. However, detection of all single-digit errors, as well as nearly all errors involving the transposition of two adjacent digits is easily achieved. One method that does this is the one used to assign the so called Universal Product Code (UPC) to most retail items. A UPC identification number has 12 digits. The first six digits identify the manufacturer, the next five identify the product, and the last is a check.

The dot product notation for two k-tuples is introduced to calculate the check digit:

$$(a_1, a_2, a_3, \dots \dots \dots a_{12}).(w_1, w_2, w_3 \dots \dots \dots . . w_k)$$
$$= a_1 w_1 + a_2 w_2 + \cdots \dots \dots \dots + a_k w_k$$

An item with the UPC identification number

$a_1, a_2, a_3, \dots \dots \dots a_{12}$ Satisfies the condition

$$(a_1, a_2, a_3, \dots \dots \dots a_{12}).(3,1,3,1 \dots \dots \dots 3,1) mod \, 10 = 0$$

The fixed k-tuple used in the calculation of check digits is called the weighting vector. The advantage of the UPC scheme is that it will detect nearly all errors involving the transposition of two adjacent digits as well as all errors involving one digit.

Remark- if the transposition error has the form

$$a_1 a_2, \dots \dots a_i a_{i+1} \dots \dots a_{12} \rightarrow a_1, a_2, \dots \dots a_{i+1} a_i \dots \dots a_{12}$$

Is undetected if and only if

$$(a_{1,}a_{2,}\ldots\ldots a_{i+1,}a_i \ldots\ldots a_{12}).(3,1,3,1,\ldots\ldots\ldots,3,1)\ mod\ 10 = 0$$

That is the error is undetected if and only if

$$(a_{1,}a_{2,}\ldots\ldots a_{i+1,}a_i \ldots\ldots a_{12}).(3,1,3,1,\ldots\ldots\ldots,3,1)\ mod\ 10$$

$$= (a_{1,}a_{2,}\ldots\ldots a_{i,}a_{i+1} \ldots\ldots a_{12}).(3,1,3,1,\ldots\ldots\ldots,3,1)\ mod\ 10$$

This equality simplifies to either

$$(3a_{i+1} + a_i) mod\ 10 = (3a_i + a_{i+1}) mod\ 10$$

Or

$$(a_{i+1} + 3a_i) mod\ 10 = (a_i + 3a_{i+1}) mod\ 10$$

Depending on whether i is even or odd. Both cases reduces to

$2(a_{i+1} - a_i) mod\ 10 = 0$. It follows that $|a_{i+1} - a_i| = 5, if$

$$a_{i+1} \neq a_{i.}$$

Example-

Use UPC scheme to determine the check digit for the number 07312400508.

Since

(0, 7, 3, 1, 2, 4, 0, 0, 5, 0, 8,).(3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3)

= 0.3+7.1+3.3+1.1+2.3+4.1+0.3+0.1+5.3+0.1+8.3

= 66

But 66 mod 10=0 gives us

(66+4) mod 10 = 70 mod 10 =0

So check digit is 4.

Application –ISBN

The International Standard Book Number (ISBN)

$a_1\ a_2\ a_3\ a_4 a_5 a_6\ a_7\ a_8\ a_9\ a_{10}$ has the property

$$(a_1, a_2, a_3 \dots\dots\dots a_{10}).(10,9,8,7,6,5,4,3,2,1) mod 11 = 0$$

The digit a_{10} is the check digit. When a_{10} is required to be 10 to make the dot product 0, the character X is used as the check digit.

Example- What is the check digit for ISBN of

0-306-40615-?

Since $(0,3,0,6,4,0,6,1,5,a_{10}).(10,9,8,7,6,5,4,3,2,1)\ mod\ 11$

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

$$= (0 + 27 + 0 + 42 + 24 + 0 + 24 + 3 + 10 + a_{10}) mod\ 11$$

$= (130+a_{10}) mod\ 11 = 9.$

Check digit a_{10} is the value needed to add to the sum 130 to make it divisible 11. So (130+2) = 132mod 11= 0. Hence check digit is 2 and the valid ISBN is 0306406152.

Remark-

if 10 being the value needed to add to the sum, we use X as the check digit instead of 10.

Example: The ISBN 0-669-03925-4 is the result of transposition of two adjacent digits not involving the first or last digit. Determine the correct ISBN.
Since$(0,6,6,9,0,3,9,2,5,\ 4).(10,9,8,7,6,5,4,3,2,1)\ mod\ 11$

$$= (0 + 54 + 48 + 63 + 0 + 15 + 36 + 6 + 10 + 4) mod\ 11$$

$= 236\ mod 11$

$= 5 \neq 0$

Now check for the transposition of two adjacent digits except 0 and 4. The transposition of 3 and 9 gives

$$242\ mod\ 11 = 0$$

The correct ISBN is 0-669-09325-4.

CONCLUSION

Worked out examples are more efficient for learning. Learning from worked out examples is a faster way of learning which plays an important role in the education process. It also develops the reasoning process of the learner.

REFERENCES

[1] Contemporary Abstract Algebra, Joseph A. Gallian.

[2] Modular Theory in Operator Algebras, Serban Valentin Stratila.

[3] Algebra, Michael Artin.

[4] Modular Arithmetics, Sumit Ramasamy, Mohan K. Pathak.

[5] A Course in Arithmetic, Jean-Pierrr Serre (springer)