Division Algorithm

We start with a fundamental fact about the integers, the set $\{\dots -4, -3, -2, -1, 0, 1, 2, 3, 4, \dots\}$. Division algorithm:

If n is an integer and m is a positive integer, then n can be expressed in the form,

n = qm + r, where $0 \le r < m$,

for unique integers q (quotient) and r (remainder).

Example

If n = 38 and m = 7,

 $38 = 5 \times 7 + 3$

where 5 is the quotient and 3 is the remainder. Alternatively, we sometimes write $38 \div 7 = 5 \text{ R } 3.$

Congruence modulo m

Let x and y be integers.

We say x is congruent to y modulo m, $x \equiv y \pmod{m}$,

if x - y is an integer multiple of m.

E.g., $66 \equiv 38 \pmod{7}$, since $66 - 38 = 28 = 4 \times 7$. If $x \equiv y \pmod{m}$, then *x* and *y* have the same remainder when divided by *m*:

> $66 \div 7 = 9 \text{ R } 3$ $38 \div 7 = 5 \text{ R } 3$

and both are equivalent to the remainder: $66 \equiv 3 \equiv 38$.

Examples

- Twelve hour clocks keep track of time modulo 12. So, for example, 29 hours after 2 o'clock, the clock will show $2 + 29 = 31 \equiv 7 \pmod{12}$, or 7 o'clock.
- Congruence modulo 2 determines parity (whether an integer is even or odd). If an integer $x \equiv 0 \pmod{2}$, *x* is even. If $x \equiv 1 \pmod{2}$, *x* is odd.
- When we express a positive integer in base 10, that integer is congruent modulo 10 to its last digit:
 2857 ≡ 7 (mod 10).

Congruence classes

When we consider congruence modulo *m*, the integers break down into groups called **congruence classes**.

Two integers are in the same congruence class if they are congruent modulo *m*.

We write [x] for the congruence class containing x, that is, the set of integers congruent to x modulo m.

For example, for congruence modulo 3, the congruence class [2] is the set of integers $\{..., -4, -1, 2, 5, 8, ...\}$.

Z_m

Note that if $x \equiv y \pmod{m}$ then the congruence classes [x] and [y] are the same sets.

For example, for congruence modulo 3, [5] = [11], and both equal [2], since 2 is the remainder when dividing by 3. The class can be represented with any of these values, but we will usually choose the value between 0 and m - 1. For congruence modulo 3, there are only three different congruence classes: [0], [1], and [2], but each has many representations.

The set of congruence classes mod *m* are denoted by Z_m . Z_m consists of *m* distinct classes: [0], [1], [2], ..., [m - 1].

Modular arithmetic

Suppose $x \equiv x' \pmod{m}$ and $y \equiv y' \pmod{m}$. Then (a) $x + y \equiv x' + y' \pmod{m}$; (b) $x y \equiv x' y' \pmod{m}$.

We can define for the congruence classes in Z_m :

(a) [x] + [y] = [x + y](b) [x] [y] = [x y]

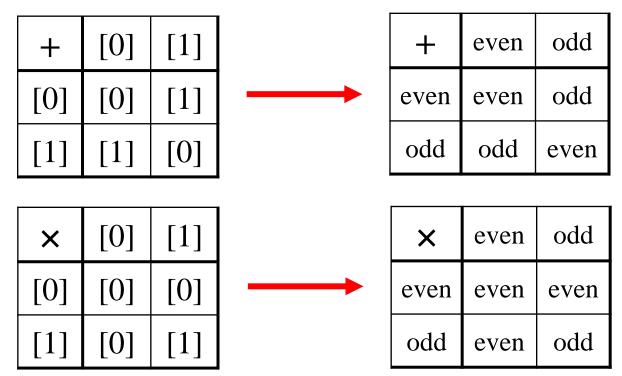
In Z_{11} , [37] + [19] = [37 + 19] = [56] = [1], or [4] + [8] = [4 + 8] = [12] = [1], since $37 \equiv 4 \pmod{11}$, $19 \equiv 8 \pmod{11}$, and $12 \equiv 1 \pmod{11}$.

Parity and Z₂

 Z_2 has two congruence classes:

$$[0] = \{..., -4, -2, 0, 2, 4, ...\}$$
 (even integers)
 $[1] = \{..., -3, -1, 1, 3, 5, ...\}$ (odd integers)

Addition and multiplication can be expressed in terms of parity:



Identification Numbers

Modern identification numbers have at least two functions:

- identify the person or thing to which it is associated.
- have a "self-checking" mechanism for the number

Many frequently used types of error-detecting codes for identification numbers include an extra digit (usually the last digit) called a check digit. Different types of identification numbers use different schemes.

Example: Federal Express tracking numbers

Federal Express packages carry a 10-digit identification number. The tenth digit is a check digit that equals the remainder when the nine-digit number made from the other digits is divided by 7.

For example, for the tracking number, 9157549236, the last digit is found by dividing 915754923 by 7:

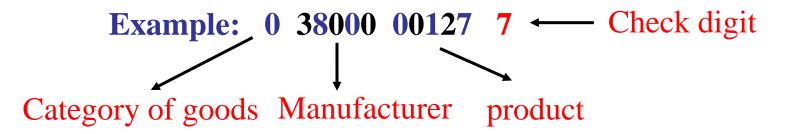
 $915754923 = 130822131 \times 7 + 6$.

<u>130822131</u> 7) 915754923

915754917

Example Universal Product Code (UPC)

The UPC is used to identify many products.



To find the check digit for the UPC:

- Sum the digits in the odd positions and multiply that sum by 3.
- Add to that the sum of the digits in the even positions.
- When the check digit is added, the total must be a multiple of 10.

$(0+8+0+0+1+7) \times 3 + (3+0+0+0+2) + 7 = 60$

(odd positions)

(even positions)

The sum is a number ending in 0.

The International Standard Book Number (ISBN)

A 10-digit ISBN $a_1a_2 \cdots a_{10}$ has the property that $10a_1 + 9a_2 + 8a_3 + 7a_4 + 6a_5 + 5a_6 + 4a_7 + 3a_8 + 2a_9 + a_{10}$

is evenly divisible by 11; that is, $\equiv 0 \pmod{11}$.

Example: the ISBN-10 of our main textbook is 1-256-76447-7.

The initial digit 1 indicates that the book is published in an English-speaking country. The next block 256 identifies the publisher. The third block 76447 is assigned by the publisher and identifies this book. The last digit, 7, is the check digit.

 $10 \times 1 + 9 \times 2 + 8 \times 5 + 7 \times 6 + 6 \times 7 + 5 \times 6 + 4 \times 4 + 3 \times 4 + 2 \times 7 + 1 \times 7 = 231$

Note: $231 = 11 \times 21$, so $231 \equiv 0 \pmod{11}$.

About ISBN

- Since ISBN-10 uses congruence modulo 11, the check "digit" could be 0, 1, 2, ..., or 10. Since 10 is not a digit, publishers use "X" for 10 as a check digit.
- The check digit scheme for the ISBN-10 is very effective at detecting the most common errors in reading and entering these numbers.
- To include books in a system including other types of products, the ISBN-13 was introduced. The ISBN-13 uses a check digit scheme similar to the UPC.

Practice Question

Determine the check digit which should be appended to ISBN 0-7167-9811.

 $10 \times 0 + 9 \times 7 + 8 \times 1 + 7 \times 6 + 6 \times 7 + 5 \times 9$ $+ 4 \times 8 + 3 \times 1 + 2 \times 1 + 1 \times x = 237 + x$

 $237 \equiv 6 \pmod{11}$ since $237 \equiv 21 \times 11 + 6$

To get $6 + x \equiv 0 \pmod{11}$, choose x = 5.

D) 8

C) 6

A) 2

Error Detection with ISBN

Example: suppose an ISBN-10 is **1-4292-4580-8**.

 $10 \times 1 + 9 \times 4 + 8 \times 2 + 7 \times 9 + 6 \times 2 + 5 \times 4 + 4 \times 5 + 3 \times 8 + 2 \times 0 + 1 \times 8 = 209$

Suppose the fourth digit is incorrectly read as 6. Then the weighted sum of all of the digits will differ by $(9 - 6) \times 7 = 21$, which is not a multiple of 11. Thus

 $10 \times 1 + 9 \times 4 + 8 \times 2 + 7 \times 6 + 6 \times 2 + 5 \times 4 + 4 \times 5 + 3 \times 8 + 2 \times 0 + 1 \times 8 = 188$

and 188 is not a multiple of 11 indicating an error. In fact no single digit error can produce a difference which is a multiple of 11 and thus every single digit error will be detected!

Transposition Error and ISBN

Example: suppose an ISBN-10 is **1-4292-4580-8**.

 $10 \times 1 + 9 \times 4 + 8 \times 2 + 7 \times 9 + 6 \times 2 + 5 \times 4 + 4 \times 5 + 3 \times 8 + 2 \times 0 + 1 \times 8 = 209$

If the fourth and fifth digits are transposed **1-4229-4580-8**. Then the weighted sum of all of the digits will be less by

$$(7 \times 9 + 6 \times 2) - (7 \times 2 + 6 \times 9) = 7 \times (9 - 2) - 6 \times (9 - 2)$$
$$= (7 - 6) \times (9 - 2) = 1 \times 7,$$

which is not a multiple of 11. Thus

 $10 \times 1 + 9 \times 4 + 8 \times 2 + 7 \times 2 + 6 \times 9 + 5 \times 4 + 4 \times 5 + 3 \times 8 + 2 \times 0 + 1 \times 8 = 202$

and 202 is not a multiple of 11 indicating an error. In fact no transposition error can produce a difference which is a multiple of 11 and thus all transposition errors will be detected!