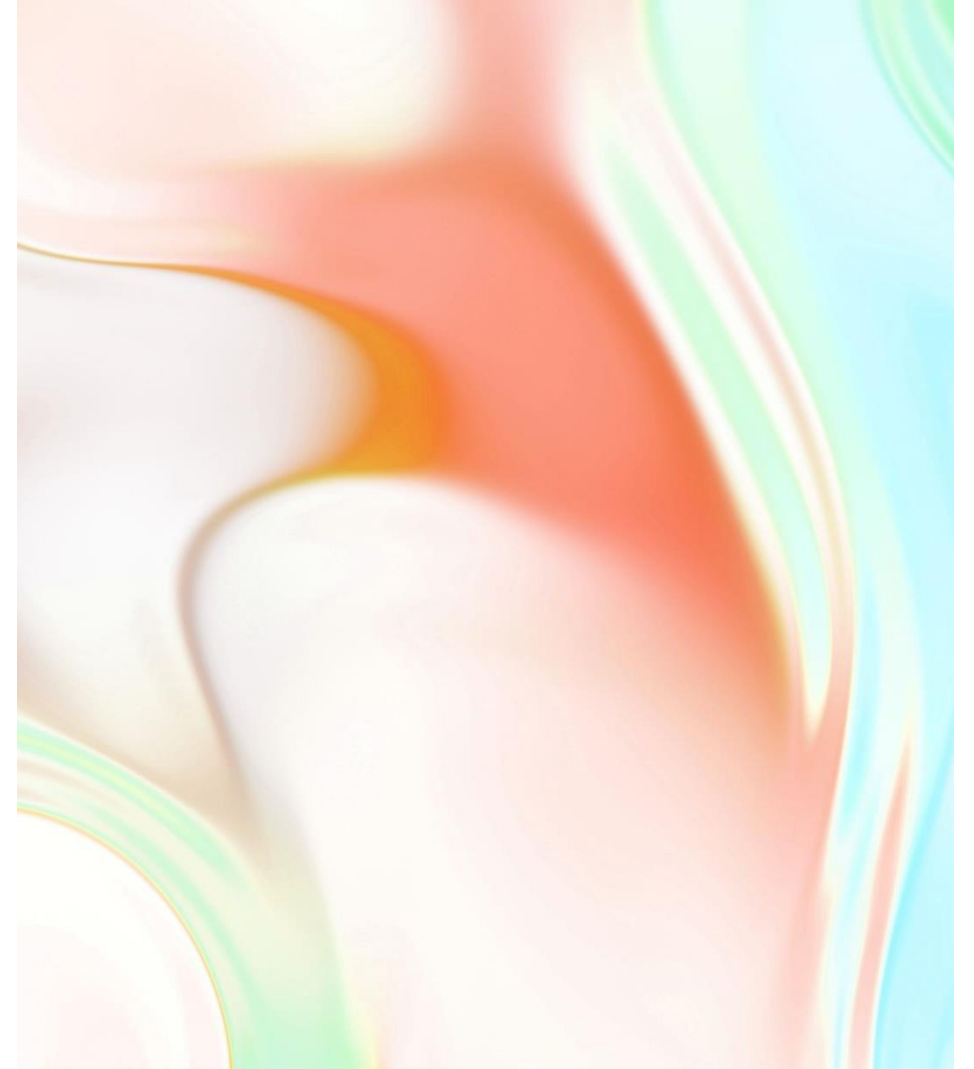


**Discrete Mathematics**  
**Lecture 6**  
**Application of Linear Congruence**

**Lecturer: Kahenya, N.P**



# Introduction to lecture 6



Lecture 6 is a continuation of lecture 5 on *Linear congruences*.



This lecture will introduce some applications of linear congruence.



Linear congruence is applicable in such areas as hashing functions, pseudorandom numbers, check digits, and parity check digits.

# References

---

These lecture notes have been derived from the following sources, Susanna (2003), Rosen (2011), and Rosen (2012).



# Intended learning outcomes

Be

At the end of this lecture, you will be able to;

Apply

Apply linear congruence in check digits.

Apply

Apply Fermat's little theorem.

# Fermat's Little theorem

Fermat's little theorem states that, If  $p$  is prime and  $a$  is an integer not divisible by  $p$ , then

$$a^{p-1} \equiv 1 \pmod{p}$$

Furthermore  $\forall a$  then  $a^p \equiv a \pmod{p}$

Fermat's little theorem helps compute powers of large integers modulo prime numbers

and it is also used in primality test.

This makes it valuable in public-key cryptography.

# Example 1

---

Use Fermat's Little theorem to simplify;  $5^{902} \pmod{31}$

**Solution:** We have;  $5^{30} \equiv 1 \pmod{31}$

Hence our problem becomes;

$$\begin{aligned} & 50^{30 \times 30 + 2} \pmod{31} \\ & (50^{30})^{30} \times 5^2 \pmod{31} \\ & \equiv 1 \times 25 \pmod{31} \\ & \equiv 25 \pmod{31} \end{aligned}$$



## Example 2

□ Simplify;  $7^{276959} \pmod{23}$

$$\begin{aligned}\text{Solution: } 7^{22 \times 12589 + 1} \pmod{23} &= (7^{22})^{12589} \times 7^1 \pmod{23} \\ &= 1 \times 7 \pmod{23} = 7 \pmod{23}\end{aligned}$$

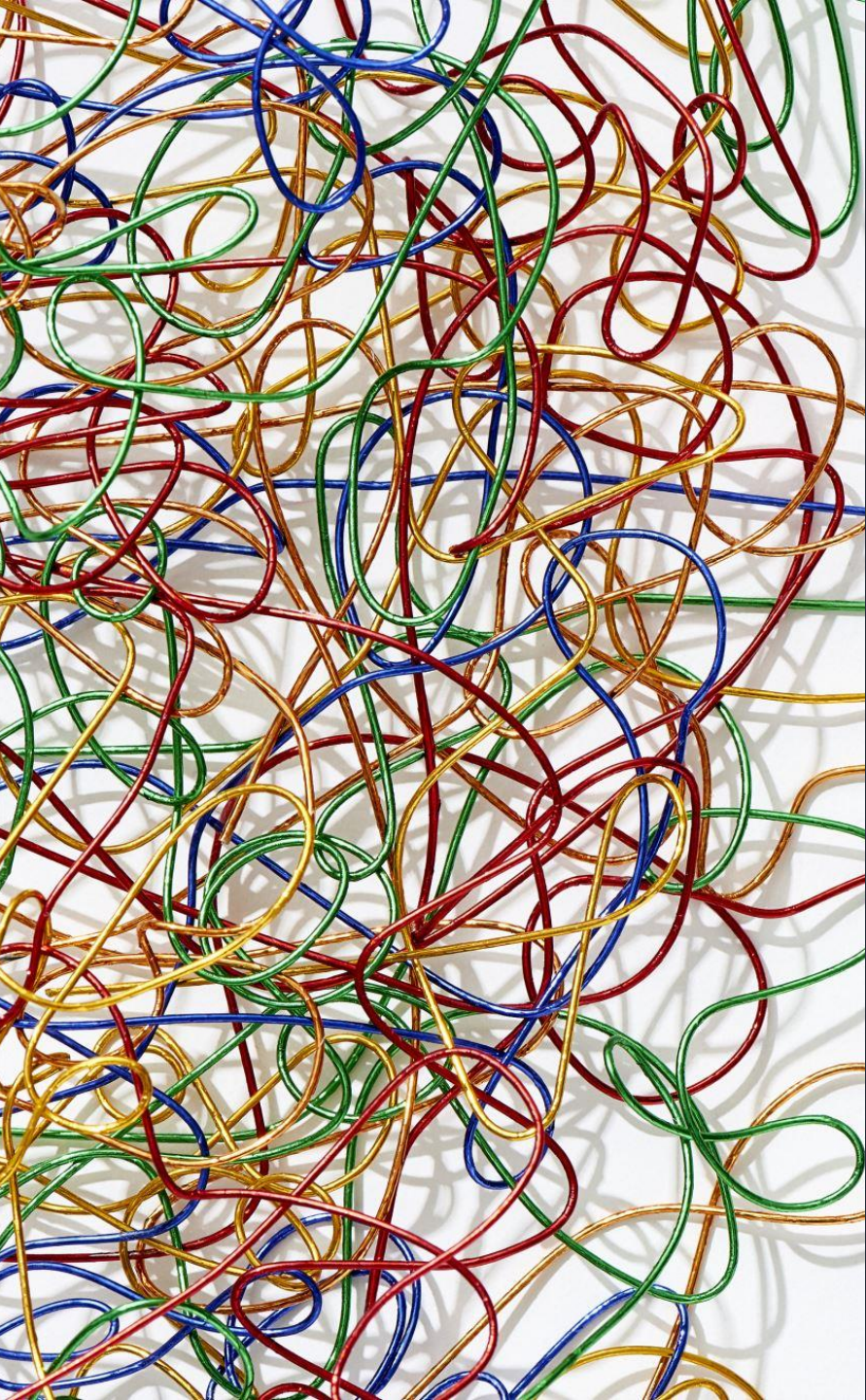
□ Simplify;  $3^{1175} \pmod{19}$

$$\begin{aligned}\text{Solution: } 3^{18 \times 65 + 5} \pmod{19} &= (3^{18})^{65} \times 3^5 \pmod{19} \\ &= 1 \times 3^5 \pmod{19} = 15\end{aligned}$$

# Check digits

---

- ❑ Data may be lost or corrupted when in transmission.
- ❑ The receiving end may get the wrong message contrary to what was initially transmitted.
- ❑ To help solve such problems additional digits are added to the digit strings being transmitted.



- ❑ Linear congruences are applied to determine or check errors in digit strings.
- ❑ There exist different techniques of determining if errors exist in a digit string.
- ❑ The most common technique for detecting errors is to add an extra digit at the end of the string.
- ❑ This last digit is called the check digit.
- ❑ Hence to determine whether a digit string is correct a check is made to determine if the last check digit is correct.

# Parity check digits

- Bit strings can be split into blocks of a certain length.
- An extra bit is added at the end of each block before transmission of the message string.
- This extra bit is called a parity check bit.

---

□ Hence a message string of length  $n$  i.e.,  $x_1, x_2, \dots, x_n$  will have its parity check bit as  $x_{n+1}$ .


□ The linear congruence for the parity check digit is defined by

$$x_{n+1} = x_1 + x_2 + \dots + x_n \pmod{2}$$

# Types of parity digits

- ❑ We have odd and even parity.
- ❑ In odd parity, the total number of 1s (including the parity digit) in the digit string is odd.
- ❑ Similarly for the even parity the total numbers of 1s should be even.
- ❑ **Example of odd parity:** Suppose the signal digit string is 1011000 the parity bit should be 0 for this to be odd.
- ❑ Again, if the signal digit string is 1011011, the parity bit should be 0 for the digit string to be odd.



- 
- ❑ **Even parity:** If there are an even number of 1 bits in the block of  $n$  bits then the parity check digit  $x_{n+1}$  is 0.
  - ❑ If there are an odd number of 1 bits in the block of  $n$  bits then parity check digit  $x_{n+1}$  is 1.
  - ❑ If the parity check digit is wrong, then there is an error in the transmitted message.
  - ❑ If the parity check is correct there may still be an error in the transmitted message.

# Example 3

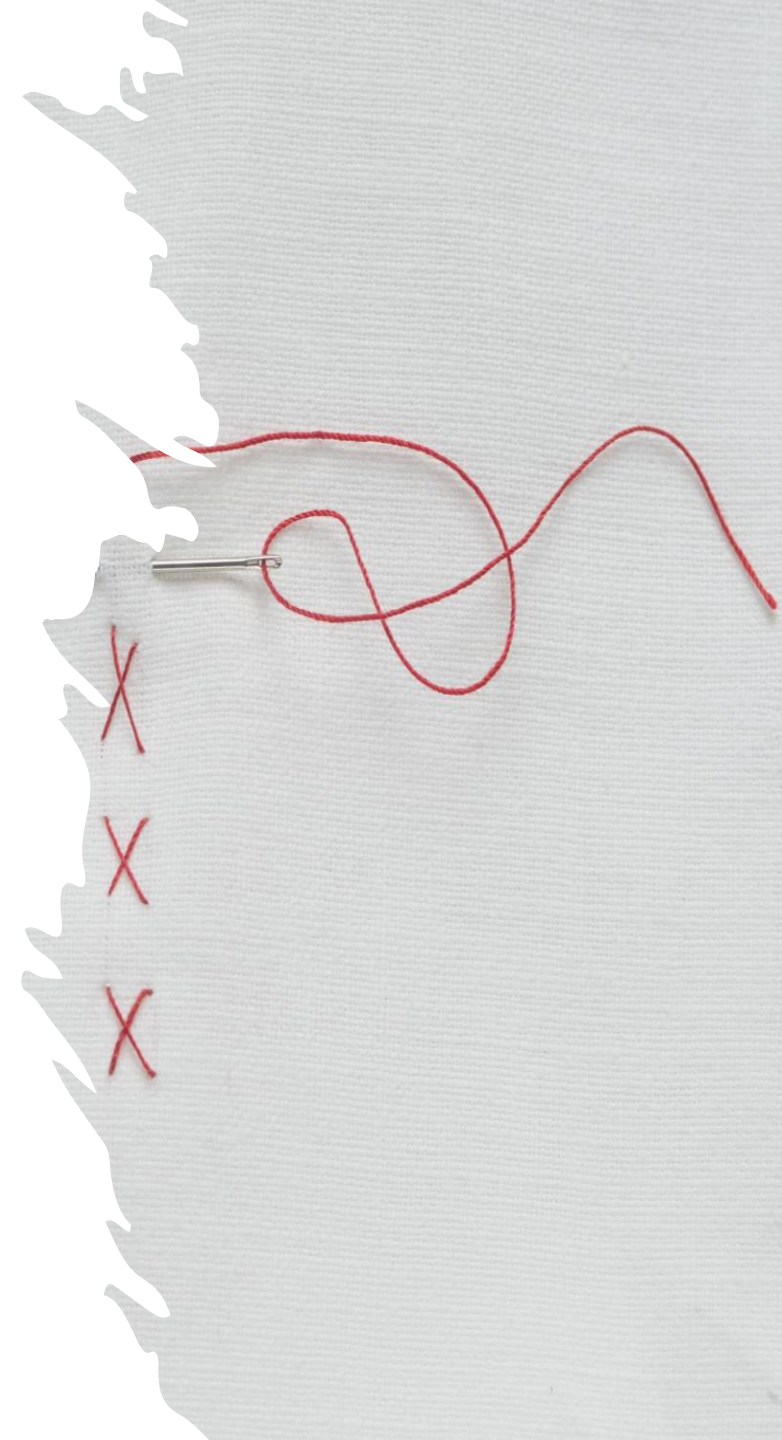
The following odd parity transmission was received; 100110101 that ended with a parity check.

Determine if the bit string should be accepted as correct.

**Solution:** The parity check digit is 1 now

$$1 + 0 + 0 + 1 + 1 + 0 + 1 + 0 + 1 = 1 \pmod{2}.$$

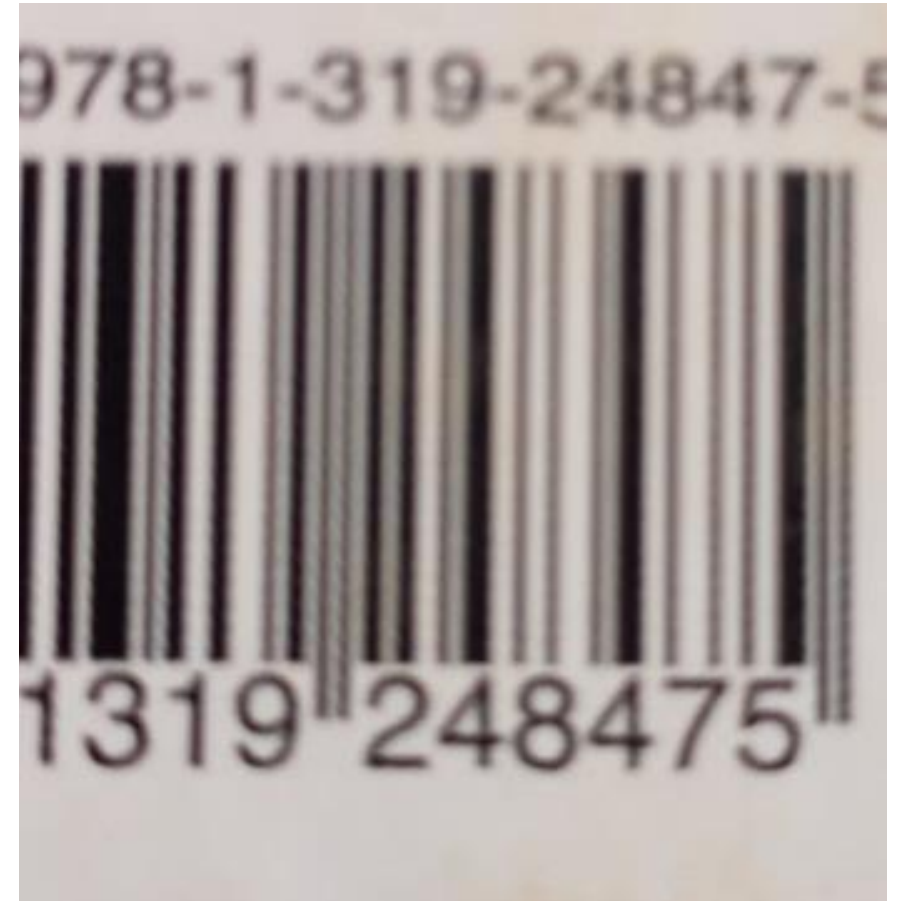
The parity check digit is correct.



# Products Identification numbers

---

- ❑ Check digits are applied to verify the validity of products identification numbers.
- ❑ Products are normally given numbers such as
  - Universal Product Codes UPC
  - International Mobile Equipment Identification IMEI
  - International Standard Book Number ISBN
  - Credit Card Number, and others.



# Universal Product Codes UPC

**Example:** Major retailers use a unique 12-digit number or code to track products as they are sold, shipped, received, and store or in stock.

The digit is called the universal product code UPC.

This number is printed on the product and can be scanned at check-out in supermarkets or other outlets to fast and accurately record a product.

The numbers are critical in inventory control.

---

❑ There exist different types of UPCs. The common UPC has 12 digits:-

❑ The first digit identifies the product category;

❑ The next five digits identify the manufacturer,

❑ The next 5 the specific product,

❑ The last digit is a check digit.

❑ The check digit is determined by the congruence;

$$3x_1 + x_2 + 3x_3 + x_4 + 3x_5 + x_6 + 3x_7 + x_8 + 3x_9 + x_{10} + 3x_{11} + x_{12} \equiv 0 \pmod{10}$$

## Example 4

Determine the check digit for the UPC 23765491601

Solution: we insert the digits in the congruence;

$$3(2) + 3 + 3(7) + 6 + 3(5) + 4 + 3(9) + 1 + 3(6) + 3(1) + x_{12} \equiv 0 \pmod{10}$$

$$6 + 3 + 21 + 6 + 15 + 4 + 27 + 1 + 18 + 0 + 3 + x_{12} = 0 \pmod{10}$$

$$104 + x_{12} = 0 \pmod{m} \Rightarrow x_{12} = 6 \pmod{10}$$

The check digit is 6



# Example 5

---

Determine if the UPC 034578231024 is valid

**Solution:**

$$3(0) + 3 + 3(4) + 5 + 3(7) + 8 + 3(2) + 3 + 3(1) + 0 \\ + 3(2) + 4$$

$$= 0 + 3 + 12 + 5 + 21 + 8 + 6 + 3 + 3 + 0 + 6 + 4 = 71$$

However,  $71 \not\equiv 0 \pmod{10}$

Hence 034578231024 is not a valid code



# International Standard Book Number ISBN

---

- ❑ ISBN -10 is a 10-digit code used to identify all books.
- ❑ The number was developed by the international organization for standardization ISO.
- ❑ The ISBN was first published in 1970 as ISO 2108 ([ISBN, 2023](#)).
- ❑ Currently we have a 13-digit code known as ISBN-13, that came into use in 2007.

# ISBN-10



An ISBN-10 consists of blocks identifying the language, the publisher, the number assigned by the publishing company, a check digit (which can be the letter X for 10).

	Group	Publisher	Title	Check digit
<b>ISBN-10</b>	<b>XX</b>	<b>XXXX</b>	<b>XXX</b>	<b>X</b>

# ISBN-13

	Prefix	Group	Publisher	Title	Check digit
ISBN-13	XXX	XX	XXXX	XXX	X



# Linear congruence

The linear congruence for the check digit for ISBN-10 is;

$$\sum_{i=1}^{10} ix_i = 1x_1 + 2x_2 + 3x_3 + 4x_4 + 5x_5 + 6x_6 + 7x_7 + 8x_8 + 9x_9 + 10x_{10} = 0 \pmod{11}$$

Note that the linear congruence can also be written as;

$$\sum_{i=1}^{10} ix_i = 1x_{10} + 2x_9 + 3x_8 + 4x_7 + 5x_6 + 6x_5 + 7x_4 + 8x_3 + 9x_2 + 10x_1 = 0 \pmod{11}$$

## Example 6

Determine if the following is a valid ISBN-10; 8177583336

**Solution:** We use the linear congruence;

$$\begin{aligned} &1(8) + 2(1) + 3(7) + 4(7) + 5(5) + 6(8) + 7(3) + 8(3) + 9(3) + 10(6) \\ &= 8 + 2 + 21 + 28 + 25 + 48 + 21 + 24 + 27 + 60 \end{aligned}$$

$$= 264 = 0 \pmod{11}$$

It is a valid ISBN-10 i.e., Lay (2003)

# Example 7

The first nine digits of ISBN-10 of a book are 007239848 find the check digit

**Solution:** We determine the check digit by the congruence

---

$$\sum_{i=1}^{10} ix_i = 0 \pmod{11}$$

We insert the digits to get;

$$= 10(0) + 9(0) + 8(7) + 7(2) + 6(3) + 5(9) + 4(8) + 3(4) + 2(8) + x_{10} \equiv 0 \pmod{11}$$

$$= 0 + 0 + 56 + 14 + 18 + 45 + 32 + 12 + 16 + x_{10} \equiv 0 \pmod{11}$$

$$193 + x_{10} \equiv 0 \pmod{11} \Rightarrow x_{10} = 5$$



# Example 8

---

Determine if the following ISBN-13 is valid;  
9788177583335

**Solution:** we can use a table to organize our working as below.

Clearly  $140 \equiv 0 \pmod{10}$  and therefore it is a valid ISBN-13 i.e. Lay (2003).

	9	7	8	8	1	7	7	5	8	3	3	3	5	Total
Weights	1	3	1	3	1	3	1	3	1	3	1	3	1	
Product	9	21	8	24	1	21	7	15	8	9	3	9	5	140

# Example 9

Determine the check digit for ISBN - 13; 978 1 41 65808 3

**Solution:** The linear congruence for ISBN - 13 is

$$x_1 + 3x_2 + x_3 + 3x_4 + x_5 + 3x_6 + x_7 + 3x_8 + x_9 + 3x_{10} + x_{11} + 3x_{12} + x_{13} = 0 \pmod{10}$$

$$9 + 3(7) + 8 + 3(1) + 4 + 3(1) + 6 + 3(5) + 8 + 3(0) + 8 + 3(3) + x_{13} = 0 \pmod{10}$$

$$= 9 + 21 + 8 + 3 + 4 + 3 + 6 + 15 + 8 + 8 + 9 + x_{13} = 0 \pmod{10}$$

$$= 84 + x_{13} = 0 \pmod{10}$$

$$x_{13} = 6$$



# Luhn Algorithm

This congruence is used to verify a variety of identification numbers such as credit card numbers, IMEI numbers, national identification numbers of certain countries, SIM card numbers among others.

The linear congruence for the check digit is a bit complicated as it involves some steps.

---



# Luhn Algorithm...contd...

---

For instance, when validating a 16-digits credit card number, the following steps are essential;

**Step 1:** compute the weighted sum with the weight pattern of 2, 1, 2, 1, 2, and so on. That is the first digit to have a weight of 2, the second digit a weight of 1, the third digit a weight of 2 and so on. Keep alternating the weights between 2 and 1 until you reach the end of the credit card number.

**Step 2:** In case you get a two-digit number after multiplying by 2, add the two digits and record their sum.

**Step 3:** Add up all the resultant numbers.

**Step 4:** If the sum is a multiple of 10 (i.e., modulo 10) then it is a valid credit card number.

# Example 10

Determine if the following is a valid credit card number; 4407 8300 2994 7691

**Solution:** We can use a table to organize our working.

Next, we have;

$$\begin{aligned} &8 + 4 + 0 + 7 + 7 + 3 + 0 + 0 + 8 + 9 + 9 \\ &+ 4 + 5 + 6 + 9 + 1 = 0 \pmod{10} \\ &80 = 0 \pmod{10} \end{aligned}$$

Indeed, it is a valid number.

	4	4	0	7	8	3	0	0	2	9	9	4	7	6	9	1
<b>Weight</b>	2	1	2	1	2	1	2	1	2	1	2	1	2	1	2	1
<b>Product</b>	8	4	0	7	16	3	0	0	4	9	18	4	14	6	18	1
	8	4	0	7	7	3	0	0	8	9	9	4	5	6	9	1

# Example 11

Determine if the following International Mobile Equipment Identity IMEI-15 number is valid; 352178131363200.

**Solution:** This IMEI is a 15-digits number. Using a table, we have;

Clearly  $50 = 0 \pmod{10}$ . It is a valid IMEI-15 number.

	3	5	2	1	7	8	1	3	1	3	6	3	2	0	0	TOTAL
Weight	1	2	1	2	1	2	1	2	1	2	1	2	1	2	1	
Product	3	10	2	2	7	16	1	6	1	6	6	6	2	0	0	
	3	1	2	2	7	7	1	6	1	6	6	6	2	0	0	50

# Example 12

---

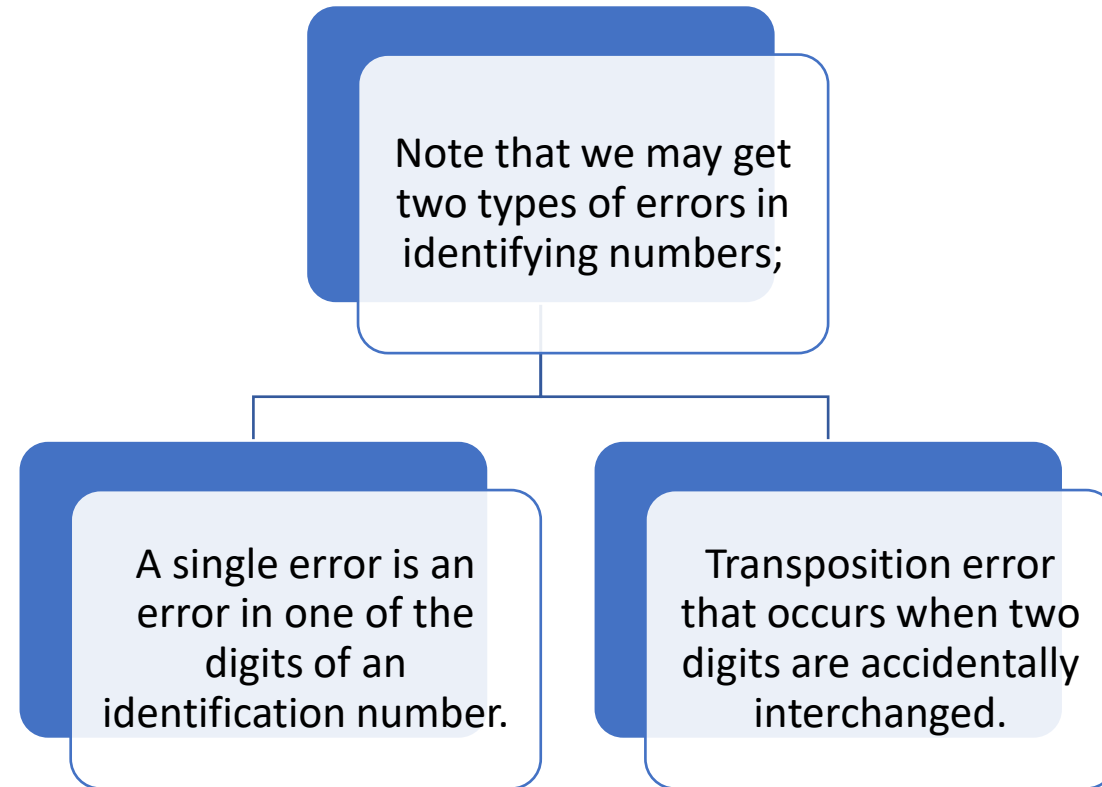
Determine the check digit of the following IMEI-15 number;  
35216275088773X

Next, we have;

$$\begin{aligned} &3 + 1 + 2 + 2 + 6 + 4 + 7 + 1 + 0 + 7 + 8 \\ &+ 5 + 7 + 6 + x \equiv 0 \pmod{10} \\ &59 + x \equiv 0 \pmod{10} \Rightarrow x = 1 \end{aligned}$$

	3	5	2	1	6	2	7	5	0	8	8	7	7	3	X
<b>Weights</b>	1	2	1	2	1	2	1	2	1	2	1	2	1	2	1
<b>Product</b>	3	10	2	2	6	4	7	10	0	16	8	14	7	6	X
	3	1	2	2	6	4	7	1	0	7	8	5	7	6	X

# Remark





# References

---

Lay, D. C. (2003). *Linear Algebra and its Application* (3rd ed.). Pearson Education, Inc.

Rosen, K. (2011). *Elementary Number Theory and Its Application* (6th ed.). Person.

Rosen, K. (2012). *Discrete mathematics and its application* (7th ed.). McGraw-Hill.

Sullivan, M., & Miranda, K. (2019). *Calculus: Early Transcendentals* (second). W.H. Freeman and Company.

Susanna, S. E. (2003). *Discrete Mathematics with Application* (3rd ed.). Brooks Cole.

ISBN, 2023 [About the ISBN standard | ISBN.org](#) retrieved on 2/4/2023.

IBM Handling credit cards [Handling credit cards - IBM Documentation](#) retrieved on 2/4/2023

<https://www.youtube.com/watch?v=pMA-dD-KCWM>