The Integers and Division

Course Code: CSC 1204 Course Title: Discrete Mathematics

Dept. of Computer Science
Faculty of Science and Technology

Lecture No:	**9**	**Week No:**	**5**	**Semester:**	**Summer 2021-2022**
Lecturer:	S.M. Abdur Rouf Bhuiyan (arouf@aiub.edu)				

Lecture Outline

3.4 The Integers and Division

- Division
- The Division Algorithm
- Modular Arithmetic
- Applications of Congruence
- Cryptology – Encryption and Decryption

Objectives and Outcomes

- **Objectives**: To understand integers and division, division algorithm, congruence, applications of congruence, encryption and decryption in cryptology.
- **Outcomes**: Students are expected to be able explain the terms divisor, dividend, quotient, remainder; be able to determine whether two integers are congruent for a certain integer (modulo), be able to encrypt and decrypt messages.

3.4 The Integers and Division

- **Definition 1:** If *a* and *b* are integers with $a \neq 0$, we say that *a divides b* if there is an integer *c* such that $b = ac$. When *a* divides *b* we say that
  - *a* is a *factor* of *b*
  - *b* is a *multiple* of *a*
- The notation $\boldsymbol{a \mid b}$ denotes that ***a*** **divides** ***b***
- We write $\boldsymbol{a \nmid b}$ when **a does not divide b**

Example 1

- Determine whether $3|7$ and whether $3|12$.
- Solution:
- It follows that $3 \nmid 7$, because $7/3$ is not an integer.
- On the other hand, $3|12$, because $12/3 = 4$, which is an integer.

Integer Division: More Examples

Question: Which of the following is true?

1) 77 | 7
2) 7 | 77
3) 24 | 24
4) 0 | 24
5) 24 | 0

Answers

1. 77 | 7: false bigger number can't divide smaller positive number
2. 7 | 77: true because 77 = 7 · 11
3. 24 | 24: true because 24 = 24 · 1
4. 0 | 24: false, only 0 is divisible by 0
5. 24 | 0: true, 0 is divisible by every number (0 = 24 · 0)

Some basic properties of divisibility of Integers

Theorem 1: Let *a, b, c* be integers. Then

(i) if $a|b$ and $a|c$, then $a|(b + c)$

(ii) if $a|b$, then $a|bc$ for all integers c

(iii) if $a|b$ and $b|c$, then $a|c$

For example:

i. If 17|34 and 17|170, then 17|204
ii. If 17|34, then 17|340
iii. If 6|12 and 12|144, then 6 | 144

Corollary 1: If *a, b,* and *c* are integers such that $a|b$ and $a|c$, then $a|mb + nc$ whenever m and n are integers.

The Division Algorithm

- **Theorem 2**: (**The Division Algorithm**) Let *a* be an integer and *d* a positive integer. Then there are unique integers *q* and *r*, with ***0<=r<d***, such that ***a = dq + r***

- **Definition 2**: In the equality given in **the division algorithm**, ***d*** is called the ***divisor***, ***a*** is called the ***dividend***, ***q*** is called the ***quotient***, and ***r*** is called the ***remainder***. This notation is used to express the quotient and remainder:

  q = *a* **div** *d*, *r* = *a* **mod** *d*

Example 3 (p. 216)

- What are the quotient and remainder when 101 is divided by 11?
- Solution: We have

101 = 11.9 + 2

Hence, the quotient when 101 is divided by 11 is

9 = 101 **div** 11, and

the remainder is 2 = 101 **mod** 11

Example 4 (p. 216)

- What are the quotient and remainder when –11 is divided by 3?
- **Solution**: we have, –11 = 3(– 4) + 1

  Hence, the quotient when –11 is divided by 3 is

  – 4 = –11 **div** 3, and the remainder is 1 = –11 **mod** 3

- **Remember,** Remainder cannot be negative (since ***0<=r<d***)

  So, the remainder is not –2, even though

  –11 = 3(–3) –2, Because r = –2 does not satisfy ***0 <=r < 3***

Modular Arithmetic

- **Modular arithmetic** is a system of arithmetic for integers, where numbers "*wrap around*" upon reaching a certain value—the **modulus** (plural **moduli**).
- Modular arithmetic can be handled mathematically by introducing a ***congruence relation*** on the integers that is compatible with the operations on integers: addition, subtraction, and multiplication.
- In some situations we care only about the remainder of an integer when it is divided by some specified positive integers.
  - A familiar use of modular arithmetic is in the 12-hour clock

Applications of Modular Arithmetic

- **Generating pseudorandom numbers**
  - Needed for computer simulation
- **Assigning computer memory locations to files**
  - Hashing Functions
- **Cryptology**
  - Encrypting and decrypting messages

Congruence : Formal Definition

- **Definition 3**: If *a* and *b* are integers and *m* is a positive integer, then *a* is congruent to *b* modulo *m* if *m* divides *a* – *b*
- We use the notation $a \equiv b \pmod{m}$ to indicate that

  a is congruent to *b* modulo *m*
- If *a* and *b* are not congruent modulo *m*, we write

  $a \not\equiv b \pmod{m}$

- **Theorem 3**:Let *a* and *b* be integers, and let *m* be a positive integer. Then $a \equiv b \pmod{m}$ iff *a* **mod** *m* = *b* **mod** *m*

Example 5

- Determine whether 17 is congruent to 5 modulo 6 and whether 24 and 14 are congruent modulo 6.

- **Solution:**

  Because 6 divides $17 - 5 = 12$, $17 \equiv 5$ (**mod** 6)

  Because $24 - 14 = 10$ is not divisible by 6, $24 \not\equiv 14$ (**mod** 6)

Class Work

Question: Which of the following are true?

1) $3 \equiv 3 \pmod{17}$
2) $3 \equiv -3 \pmod{17}$
3) $172 \equiv 177 \pmod{5}$
4) $-13 \equiv 13 \pmod{26}$

Answers

1) $3 \equiv 3 \pmod{17}$ True. Any number is congruent to itself (3 – 3 = 0, divisible by all)
2) $3 \equiv -3 \pmod{17}$ False. (3 – (– 3)) = 6 isn't divisible by 17.
3) $172 \equiv 177 \pmod{5}$ True. 172 – 177 = – 5 is a multiple of 5
4) $-13 \equiv 13 \pmod{26}$ True. – 13 – 13 = – 26 is divisible by 26.

***Question*: List five integers that are congruent to 3 modulo 7.**

Answer: 3, 10, 17, 24, 31

Cryptology

- **Cryptology** is the study of secrete messages.
- One of the earliest known uses of cryptology was by ***Julius Caesar.***
- He made messages secret by shifting each letter three letters forward in the alphabet. For instance, using this scheme the letter *B* is sent to *E* and the letter *X* is sent to *A*.
  - *B* → *E*
  - *X* → *A*
- This is an example of **encryption**, that is the process of making a message secret.

Caesar Cipher

- **Mathematical expression:**

  $f(p) = (p + 3)$ **mod** 26 $0 \leq p \leq 25$

- There are 26 letters in English alphabet.
  - $A = 0$, $B = 1$, …., $K= 10$, …., $Z = 25$

Letter ←→ Number Conversion Table

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Example 9 @ p. 221

- What is the secret message produced from the message "**MEET YOU IN THE PARK**" using the Caesar cipher?

Solution:

- **First replace the letters** in the message **with numbers**. This produces

12 4 4 19   24 14 20   8 13   19 7 4   15 0 17 10

- Now **replace each of these numbers *p*** by ***f(p)* = (*p* + 3) mod 26**. This produces

15 7 7 22   1 17 23   11 16   22 10 7   18 3 20 13

- **Translating this back to letters** produces the **encrypted message**

"PHHW BRX LQ WKH SDUN"

Decryption

- **Question:** How to recover the original message from a secret message encrypted by the Caesar cipher**?**
- To recover the original message from a secret message encrypted by the Caesar cipher, the function f^{-1}, the inverse of *f*, is used.

  The function f^{-1} sends an integer *p* from { 0, 1, 2, …25} to $\boldsymbol{f^{-1}(p) = (p - 3) \bmod 26}$. In other words, to find the original message, each letter is shifted back three letters in the alphabet, with the first three letters sent to the last three letters of the alphabet.
- The process of determining the original message from the encrypted message is called ***decryption***.
- **Homework**: Decrypt the encrypted message **"PHHW BRX LQ WKH SDUN"** (that was encrypted using Caesar cipher) to the original message.

Shift Cipher : Generalization of Caesar Cipher

- There are various ways to generalize the Caesar cipher. For example, instead of shifting each letter by 3,

  we can shift each letter by *k*, so that

  $$f(p) = (p + k) \textbf{ mod } 26$$

  Such a cipher is called a **shift cipher**.

- The decryption can be carried out using

  $$f^{-1}(p) = (p - k) \text{ mod } 26$$

Exercise 31(b) @ page 222-223 [Example of Shift cipher]

- Encrypt the message “**DO NOT PASS GO**” by translating the letters into numbers, applying the encryption function given, and then translating the numbers back into letters.

  $f(p) = (p + 13)$ **mod** 26

- **Solution**: (Answer is in your book!)
- Try it yourself first. If you can not, then SEE next slide for solution.

Solution of Exercise 31(b)

- The message in number is –

  3-14 13-14-19 15-0-18-18 6-14

- Replacing each of these numbers *p* by *f(p)* = (*p* + 13) **mod** 26 produces –

  16-1 0-1-6 2-13-5-5 19-1

- Translating this back into letter produces the **encrypted message “QB ABG CNFF TB”**

Homework: Decrypt the encrypted message **“QB ABG CNFF TB”** which was encrypted using *f(p)* = (*p* + 13) **mod** 26.

Practice @ Home

- **Relevant odd-numbered Exercises** from your text book

Books

1. *Discrete Mathematics and its applications with combinatorics and graph theory (7th edition)* by Kenneth H. Rosen [Indian Adaptation by KAMALA KRITHIVASAN], published by McGraw-Hill

References

1. Discrete Mathematics, *Richard Johnsonbaugh*, Pearson education, Inc.
2. Discrete Mathematical Structures, *Bernard Kolman*, *Robert C. Busby*, *Sharon Ross,* Prentice-Hall, Inc.
3. *SCHAUM'S outlines Discrete Mathematics(2nd edition)*, by *Seymour Lipschutz*, *Marc Lipson*