Discrete Math for Computing

Ch 4.1 Divisibility and Modular Arithmetic

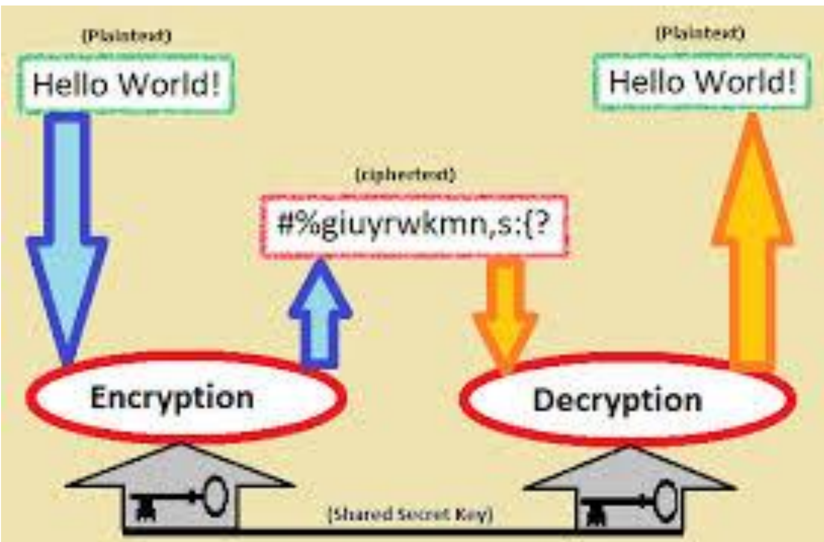
- Number Theory – Part of mathematics involving the integers and their properties
- Divisibility

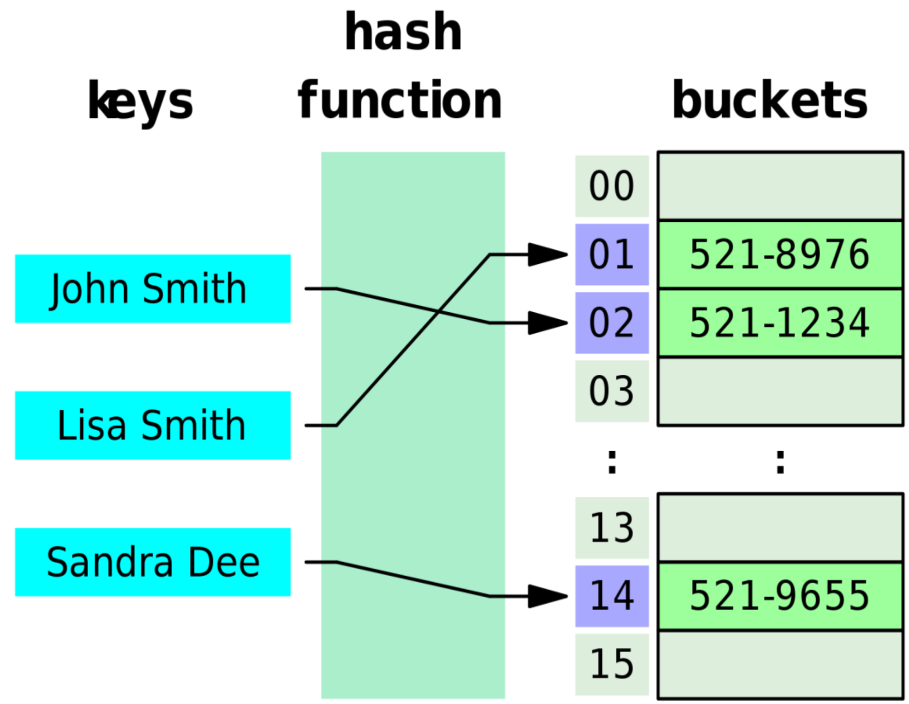
  Division of an integer by a positive integer

  Quotient, Remainder

  Modular Arithmetic

Practical examples





- Applications

  Cryptography – Encryption, Decryption

  Assigning Computer memory locations to files

The Integers and Division

- If ‘a’ and ‘b’ are integers with $a \neq 0$
- a divides b if there is an integer c such that $b = ac$

  a is the factor of b

  b is a multiple of a
- Denoted by $a \mid b$ - a divides b
- $a \nmid b$ denotes a does not divide b
- $a \mid b$ can also be denoted as $\exists c(ac = b)$

  domain is the set of integers

The Integers and Division

- Example: Determine whether $3 \mid 7$.
- Is $7/3$ an integer?
- No => $3 \nmid 7$

- Determine whether $3 \mid 12$.
- Is $12/3$ an integer?
- Yes => $3 \mid 12$

The Integers and Division

- Example: Show that if a is an integer other than 0, then

  a) 1 divides a

  b) a divides 0

a) $1 \mid a$ since $a = 1 \cdot a$

b) $a \mid 0$ since $0 = a \cdot 0$

Properties of Divisibility of Integers

- If 'a', 'b', and 'c' are integers

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

  ii) if $a \mid b$, then $a \mid bc$ for all integers c

  iii) if $a \mid b$ and $b \mid c$, then $a \mid c$

- If 'a', 'b', and 'c' are integers

  such that $a \mid b$ and $a \mid c$ then

  $a \mid mb + nc$, m and n are integers

The Integers and Division

- Direct Proof: If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$

  Assume that $a \mid b$ and $a \mid c$

  From definition of divisibility,

  There exist integers s and t such that

  $b = as$ 1)

  $c = at$ 2)

  Adding 1) and 2),

  $b + c = as + at = a(s + t)$

  $\therefore$ a divides $b + c$ or $a \mid (b + c)$

The Integers and Division

- Example: Show that if a, b, and c are integers with $c \neq 0$, such that $ac \mid bc$, then $a \mid b$.
- Since $ac \mid bc$

  $\Rightarrow bc = (ac)t$ for some integer t

  Since $c \neq 0$, we divide both sides by t

  $\Rightarrow b = at$

  $\therefore a \mid b$

The Integers and Division

- The Division Algorithm

  When an integer is divided by a positive integer,

  There is a quotient and a remainder

  Let ‘a’ be an integer and ‘d’ a positive integer

  Then there exist unique integers ‘q’ and ‘r’

  with $0 \leq r < d$

  such that $a = dq + r$

The Integers and Division

- The Division Algorithm

$$a = dq + r$$

d - divisor

a - dividend

q - quotient

r - remainder

Mathematical notation

$q = a \text{ div } d, r = a \bmod d$

The Integers and Division

- Example: What are the quotient and remainder when 101 is divided by 11?
- 101 = 11 . 9 + 2
- Quotient = **9**, 101 div 9
- Remainder = **2** = 101 mod 11

Example: What are the quotient and remainder when -11 is divided by 3?

- -11 = 3 . (-4) + 1
- Quotient = **-4**, -11 div 3
- Remainder = **1** = -11 mod 3

The Integers and Division

Example: What are the quotient and remainder when -11 is divided by 3?

- $-11 = 3 \,.\, (-3) - 2$
- Remainder = -2
- Is this correct?
- No, because r = -2 does not satisfy $0 \leq r < 3$
- Remainder cannot be negative
- Try $-11 = 3\,(-4) + r$
- Remainder = 1, r is positive, this is correct

Modular Arithmetic

-6	-5	-4	-3	-2	-1	0	1	2	3	***4***	5	6

Let’s find 5 mod 2.
What is the largest number *less than* 5 divisible by 2?   ***4***
What *positive* number do we have to add to this number to get 5?   ***1***

Let’s find -5 mod 2.
What is the largest number *less than* -5 divisible by 2?   ***-6***
What *positive* number do we have to add to this number to get -5?   ***1***

Modular Arithmetic

- If a is an integer and m a positive integer, a **mod** m is the remainder when a is divided by m.
- If $a = qm + r$ and $0 \leq r < m$, then

  a **mod** $m = r$
- Example: Find 17 **mod** 5.
- Example: Find –133 **mod** 9.

Modular Arithmetic

- Example: Find 17 **mod** 5.

  $a = dq + r$

  $17 = 5(q) + r$

  We know 17 / 5 = 3.4, so set q to 3

  $17 = 5(3) + r$

  $17 = 15 + r$

  $17 = 15 + 2$, so $r = 2$ and 17 **mod** 5 = 2.

UTD

Modular Arithmetic

- Example: Find –133 **mod** 9.

  $a = dq + r$

  $-133 = 9(q) + r$

  We know -133 / 9 = -14.7. Choosing q = -14 isn't going to work, because 9 • -14 = -126, and we can't add a positive remainder r to -126 to get -133. So choose q = -15.

  $-133 = 9(-15) + r$

  $-133 = -135 + r$, so $r = 2$, and –133 **mod** 9 = 2.

The Integers and Division

- **Modular Arithmetic**
- Only Remainder is important
- If 'a' and 'b' are integers and 'm' is a positive integer
- 'a' is congruent to 'b modulo m'

  if 'm' divides a - b
- Notation $a \equiv b \pmod{m}$
- Notation $a \not\equiv b \pmod{m}$

  if a and b are not 'congruent modulo m'

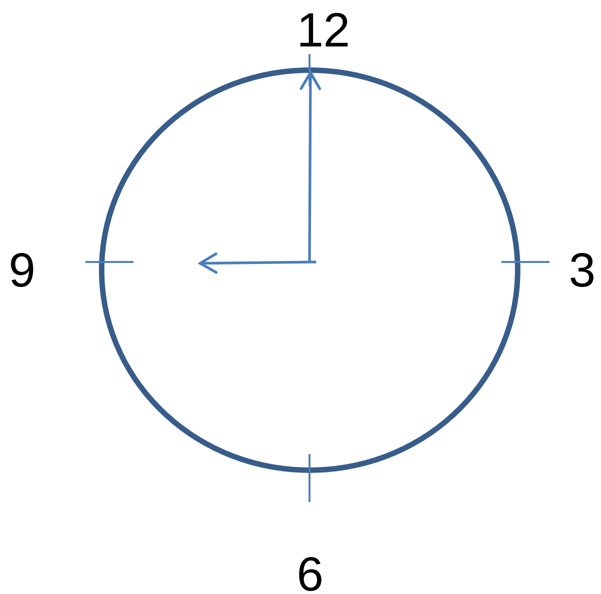
The Integers and Division

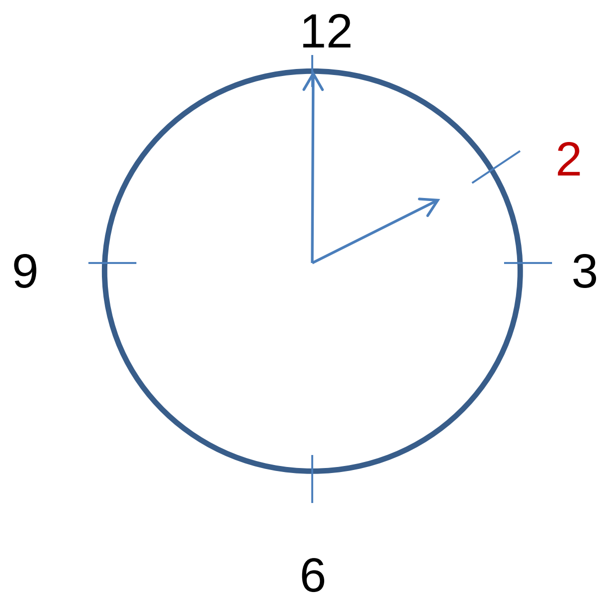
- **Modular Arithmetic**
- If ‘a’ and ‘b’ are integers

  and ‘m’ is a positive integer
- $a \equiv b \pmod{m}$
- if and only if
- a mod m = b mod m
- Congruences – German mathematician Friedrich Gauss, end of eighteenth century

The Integers and Division

- **Modular Arithmetic**
- Also called "Clock Arithmetic"
- What is 9 + 5?





The Integers and Division

- Example: Determine whether 17 is congruent to 5 modulo 6

  $17 - 5 = 12$

  $\because$ 6 divides 12, 17 is congruent to 5 modulo 6

  or $17 \equiv 5 \pmod{6}$

- Determine whether 24 and 14 are congruent modulo 6

  $24 - 14 = 10$

  $\because$ 10 not divisible by 6, $24 \not\equiv 14 \pmod{6}$

The Integers and Division

- Let ‘m’ be a positive integer
- Integers ‘a’ and ‘b’ are congruent modulo m, if and only if there is an integer k such that

$$a = b + km$$

- Let ‘m’ be a positive integer

If $a \equiv b \pmod{m}$

and $c \equiv d \pmod{m}$ then

$a + c \equiv b + d \pmod{m}$

and $ac \equiv bd \pmod{m}$

The Integers and Division

- Example: Given $7 \equiv 2 \pmod 5$ and $11 \equiv 1 \pmod 5$, what is the sum and product of 7 and 11 for congruences?
- $7 + 11 \equiv 2 + 1 \pmod 5$

=> $18 \equiv 3 \pmod 5$ -> SUM

- $7 . 11 \equiv 2 . 1 \pmod 5$

=> $77 \equiv 2 \pmod 5$ -> PRODUCT