Chapter 4: Number Theory and Crytography

Trần Hòa Phú

Ngày 29 tháng 5 năm 2023

Divisibility and Modular Arithmetic

Definition

• If a and b are integers with $a \neq 0$, we say that a divides b ($a|b$) if there is an integer c such that $b = ac$, or equivalently, if $\dfrac{b}{a}$ is an integer.

• When a divides b we say that a is a factor or divisor of b, and that b is a multiple of a.

Example : $2|4, \quad 5|25, \quad -7|14.$

$2 \nmid 5, \quad 3 \nmid 11$

Theorem

Let a, b and c be integers, where $a \neq 0$. 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 $a|c$.

Chứng minh.

(i) $a|b \Rightarrow \exists s \in \mathbb{Z} : b = s.a$
$a|c \Rightarrow \exists t \in \mathbb{Z} : c = t.a$
Therefore $b + c = s.a + t.a = (s+t).a$ □

(ii),(iii): **Exercise**!

The Division Algorithm

Theorem

Let a be an integer and d a positive integer.
Then there are unique integers q and r, with $0 \leq r < d$, such that $a = dq + r$.
*q: quotient. Notation $q = a$ **div** d*
*r : remainder. Notation $r = a$ **mod** d*
***Note** r must not be negative.*

NO OK $-11 = 3 \times (-3) - 2 \Rightarrow q = -3, r = -2$

Example

What are the quotient and remainder when 101 is divided by 11?

Solution

$101 = 11.9 + 2$

quotient is 9 and remainder is 2.

$9 = 101 \text{ div } 11$

$2 = 101 \bmod 11.$

Exercise

Evaluate these quantities.

$13 \mod 3$

$-120 \text{ div } 7$

$27 \mod 4$

$39 \text{ div } 15$

Modular Arithmetic

Definition

- If a and b are integers and m is a positive integer, then **a is congruent to b modulo m** if $m|a-b$.
- if $m|(a-b)$, we write $a \equiv b \pmod{m}$.
- if $m \nmid a-b$, we write $a \not\equiv b \pmod{m}$.

Example 1:

$3 \equiv 7 \pmod{2}$, $-10 \equiv 4 \pmod{7}$, $20 \not\equiv 3 \pmod{8}$

Exercise

Decide whether each of these integers is congruent to 5 modulo 17.

$80 \quad 103 \quad -29 \quad -122$

Modular Arithmetic

Theorem 3

a,b: integers, m: positive integer

$a \equiv b \pmod{m} \leftrightarrow a \bmod m = b \bmod m$

Proof

(1) $a \equiv b \pmod{m} \rightarrow a \bmod m = b \bmod m$

$a \equiv b \pmod{m} \rightarrow m \mid a-b \rightarrow a-b = km \rightarrow a = b + km$

$\rightarrow a \bmod m = (b + km) \bmod m$

$\rightarrow a \bmod m = b \bmod m \quad \{ km \bmod m = 0 \}$

(2) $a \bmod m = b \bmod m \rightarrow a \equiv b \pmod{m}$

$a = k1m + c \wedge b = k2m + c \rightarrow a-b = (k1-k2)\, m$ { suppose $a>b$)

Theorem

Let m be a positive integer.
If $a \equiv b \pmod m$ and $c \equiv d \pmod m$, then

$$ac \equiv bd(\text{mod } m) \tag{1}$$

$$a + c \equiv b + d(\text{mod } m) \tag{2}$$

Example 1

$7 \equiv 2(\text{mod } 5), \quad 11 \equiv 1(\text{mod } 5)$

Therefore

$11 + 7 \equiv 2 + 1(\text{mod } 5)$ and $11.7 \equiv 2.1(\text{mod } 5)$

Exercise

Suppose that a and b are integers, $a \equiv 4 \pmod{13}$, and $b \equiv 9 \pmod{13}$. Find the integer c with $0 \leq c \leq 12$ such that

a) $c \equiv 9a \pmod{13}$.

b) $c \equiv 11b \pmod{13}$.

c) $c \equiv a + b \pmod{13}$.

d) $c \equiv 2a + 3b \pmod{13}$.

e) $c \equiv a^2 + b^2 \pmod{13}$.

f) $c \equiv a^3 - b^3 \pmod{13}$.

Representations of Integers

Theorem

Let b be an integer greater than 1. Then if n is a positive integer, it can be expressed uniquely in the form

$$\mathbf{n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_1 b + a_0}$$
$$\mathbf{(n = (a_k a_{k-1} \ldots a_1 a_0)_b)}$$

where k is a nonnegative integer, $a_0, a_1, \ldots, a_k$ are nonnegative integers less than b and $a_k \neq 0$.

Example 1: $165 = 2.8^2 + 4.8 + 5 = (245)_8$

Example 2: $5 = 1.2^2 + 0.2^1 + 1 = (101)_2$

$$325 = 325_{10} = 5.10^0 + 2.10^1 + 3.10^2$$
$$1232 = 1232_{10} = 2.10^0 + 3.10^1 + 2.10^2 + 1.10^3$$
$$(234)_5 = 4.5^0 + 3.5^1 + 2.5^2 = 69$$
$$(1001)_2 = 1.2^0 + 0.2^1 + 0.2^2 + 1.2^3 = 9$$
$$(30071)_8 = ?$$

Base Conversion

Example 1: Find the octal expansion of $(12345)_{10}$.

Solution

Computing $12345 : 8 \Rightarrow q = 1543,\ r = 1$

Computing $1543 : 8 \Rightarrow q = 192,\ r = 7$

Computing $192 : 8 \Rightarrow q = 24,\ r = 0$

Computing $24 : 8 \Rightarrow q = 3, r = 0.$

Computing $3 : 8 \Rightarrow q = 0, r = 3.$

Then $(12345)_{10} = (30071)_8$

Exercise

11. Convert each of the following expansions to **decimal expansion**.

a) $(1021)_3$ b) $(325)_7$ c) $(A3)_{12}$ d) $(401)_5$ e) $(12B7)_{13}$

12. Convert 69 to

a) a binary expansion b) a base 6 expansion c) a base 9 expansion

ALGORITHM 1 Constructing Base b Expansions.

procedure *base b expansion*(n, b: positive integers with $b > 1$)
$q := n$
$k := 0$
while $q \neq 0$
    $a_k := q$ **mod** b
    $q := q$ **div** b
    $k := k + 1$
return $(a_{k-1}, \ldots, a_1, a_0)$ $\{(a_{k-1} \ldots a_1 a_0)_b$ is the base b expansion of $n\}$

Algorithms for Integer Operations

- Addition integers in binary format
- Multiplying integers in binary format

Algorithm 1: Adding of integers in binary format

Quy tắc cộng 2 số trong hệ nhị phân:

$\mathbf{1} + \mathbf{0} = \mathbf{1}$

$\mathbf{0} + \mathbf{1} = \mathbf{1}$

$\mathbf{1} + \mathbf{1} = \mathbf{10}$ (ghi 0, nhớ 1)

Ví dụ 1: $(0111)_2 + (1110)_2$

Ví dụ 2: $(100011)_2 + (1110)_2$

ALGORITHM 2 Addition of Integers.

procedure *add*(a, b: positive integers)
{the binary expansions of a and b are $(a_{n-1}a_{n-2}\dots a_1a_0)_2$
and $(b_{n-1}b_{n-2}\dots b_1b_0)_2$, respectively}
$c := 0$
for $j := 0$ **to** $n-1$
    $d := \lfloor (a_j + b_j + c)/2 \rfloor$
    $s_j := a_j + b_j + c - 2d$
    $c := d$
$s_n := c$
return $(s_0, s_1, \dots, s_n)$ {the binary expansion of the sum is $(s_n s_{n-1} \dots s_0)_2$}

Algorithm 2: Multiplying integers in binary format

Quy tắc nhân 2 số nhị phân: $1 \times 1 = 1$

```
        1 0 1 1
      × 1 0 1 0
        -------
       0 0 0 0
     1 0 1 1
   0 0 0 0
 1 0 1 1
```

ALGORITHM 3 Multiplication of Integers.

procedure *multiply*(a, b: positive integers)
{the binary expansions of a and b are $(a_{n-1}a_{n-2}\ldots a_1a_0)_2$
  and $(b_{n-1}b_{n-2}\ldots b_1b_0)_2$, respectively}
for $j := 0$ **to** $n - 1$
    if $b_j = 1$ **then** $c_j := a$ shifted j places
    else $c_j := 0$
{$c_0, c_1, \ldots, c_{n-1}$ are the partial products}
$p := 0$
for $j := 0$ **to** $n - 1$
    $p := p + c_j$
return p {p is the value of ab}

Prime and Greatest Common Divisors

Definition

- An integer p greater than 1 is called a prime if the only positive factors of p are 1 and p.
- A positive integer that is greater than 1 and is not prime is called composite.

Example

$2, 5, 7, 29$ are primes

$9, 15, 26$ are composites.

Theorem 1- The fundamental theorem of arithmetic:

Every positive integer greater than 1 can be written uniquely as a prime or as the product of two or more primes where the prime factors are written in order of nondecreasing size

Examples:

Primes: 37

Composite: $100 = 2.2.5.5 = 2^2 5^2$

$999 = 3.3.3.37 = 3^3 37$

Exercise

Find the prime factorization of 10!

Greatest Common Divisors and Least Common Multiples

Definition 2:

Let a, b be integers, not both zero. The largest integer d such that d|a and d|b is called the *greatest common divisor* of a and b.

Notation: gcd(a,b)

Example: gcd(24,36)=?

Divisors of 24: 2 3 4 6 8 12 = $2^3 3^1$

Divisors of 36: 2 3 4 6 9 12 18 = $2^2 3^2$

gcd(24,36)=12 = $2^2 3^1$ // Get factors having minimum power

Theorem

$a = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}$ *where* $a_1, \dots, a_n$ *are nonnegative integer.*

$b = p_1^{b_1} p_2^{b_2} \dots p_n^{b_n}$ *where* $b_1, \dots, b_n$ *are nonnegative integer.*

Then

$\gcd(a, b) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \dots p_n^{\min(a_n, b_n)}$

Example

$180 = 2^2.3^2.5$

$24 = 2^3.3$

$\gcd(180, 24) = 2^2.3 = 12$

Greatest Common Divisors and Least Common Multiples

Definition 3:

The integers a, b are ***relatively prime*** if their greatest common divisor is 1

Example:

gcd(3,7)=1 → 3,7 are relatively prime

gcd (17,22)=1 → 17,22 are relatively prime

gcd(17,34) = 17 → 17, 34 are **not** relatively prime

Exercise

Which positive integers less than 30 are relatively prime to 30?

Euclidean Algorithm

Theorem If
$\mathbf{a = bq + r}$ **with** $\mathbf{a, b, q, r \in Z} \Rightarrow \gcd(\mathbf{a}, \mathbf{b}) = \gcd(\mathbf{b}, \mathbf{r})$.
In other words, $\gcd(\mathbf{a}, \mathbf{b}) = \gcd(\mathbf{b}, \mathbf{a} \mod \mathbf{b})$

Example

Find the greatest common divisor of 441 and 662?

662 chia 441, dư 221

441 chia 221, dư 220

221 chia 220, dư 1

220 chia 1, dư 0

$\gcd(662, 441) = 1$

Euclidean Algorithm

ALGORITHM 1 The Euclidean Algorithm.

procedure *gcd*(a, b: positive integers)
$x := a$
$y := b$
while $y \neq 0$
    $r := x$ **mod** y
    $x := y$
    $y := r$
return $x\{\gcd(a, b) \text{ is } x\}$

Exercise

Use the Euclidean algorithm to find

a) gcd(14,28)

b) gcd(8,28)

c) gcd(28,35)

Greatest Common Divisors and Least Common Multiples

Definition 5:

The Least common multiple of the positive integer a and b is the smallest integer that is divisible by both a and b

Notation: lcm(a,b)

Example:

lcm(12,36) = 36 lcm(7,11) = 77

$\text{lcm}\,(2^3 3^5 7^2,\ 2^4 3^3) = 2^4 3^5 7^2$

Theorem

$a = p_1^{a_1} p_2^{a_2} \ldots p_n^{a_n}$ *where* $a_1, \ldots, a_n$ *are nonnegative integer.*

$b = p_1^{b_1} p_2^{b_2} \ldots p_n^{b_n}$ *where* $b_1, \ldots, b_n$ *are nonnegative integer.*

Then

$lcm(a, b) = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \ldots p_n^{\max(a_n,b_n)}$

Find $lcm(2^3.\underline{3^5}.7^2, \underline{2}^4.3^3)$

Greatest Common Divisors and Least Common Multiples

Theorem 5:

Let a, b be positive integers then

ab= gcd(a,b). lcm(a,b)

Example: gcd(8, 12) = 4 lcm(8,12)=24 ➔ 8.12 = 4.24

Proof: Based on analyzing a, b to prime factors to get gcd(a,b) and lcm(a,b)

➔ ab=gcd(a,b). lcm(a,b)

Applications of Congruences: Hasing functions

Bài toán

Giả sử ta có 10 cái hộp được đánh số từ 1,2,...,10 và có các thẻ được đánh số từ 1 đến 100. Ta muốn phân bố đều các thẻ này vào các hộp. Hãy mô tả mô hình toán học cho bài toán này.

Hashing Function: $H(k) = k \bmod m$

Using in searching data tin memory.

k: data searched, m : memory block

Examples:

$H(064212848) \bmod 111 = 14$

$H(037149212) \bmod 111 = 65$

Collision: $H(k_1) = H(k_2)$. For example, $H(107405723) = 14$

Q8. Suppose that a computer has only the memory locations 0,1,2,...,19. Use the hashing function h where $h(x) = (x + 5)$ **mod** 20 to determine the memory locations in which 57, 32, and 97 are stored.

Exercise

Which memory locations are assigned by the hasing function $h(k) = k \mod 101$ to the recoreds of insurance company customers with these Social Security Numbers?

a) 104578690 b) 432222187

Pseudorandom Numbers
(Số giả ngẫu nhiên)

Randomly chosen numbers are often needed for computer simulations.

Definition

Pseudo-random numbers $\mathbf{x_{n+1} = ax_n + c \bmod m}$

$2 \leq a < m \quad 0 \leq c < m, \quad 0 \leq x_0 < m$

Example Choosing $m = 9, a = 7, c = 4, x_0 = 3$ we have

$x_{n+1} = (7x_n + 4) \bmod 9$ with $x_0 = 3$.

$x_1 = 7x_0 + 4 \bmod 9 = 25 \bmod 9 = 7$

$x_2 = 7x_1 + 4 \bmod 9 = 53 \bmod 9 = 8$

Similarly $x_3 = 6, x_4 = 1, x_5 = 2, x_6 = 0, x_7 = 4.$

Exercise

1) Suppose

$$x_{n+1} = 3x_n + 11 \bmod 13$$

If $x_3 = 5$, find x_2 and x_4.

$x_2 = 11$

$\cdot)\ x_4 = 3x_3 + 11$

$= 26 \bmod 13 = 0$

$\cdot)\ x_3 = 3x_2 + 11 \bmod 13$

$5 = 3x_2 + 11 \pmod{13} \rightarrow 33 \equiv 3x_2 \pmod{13}$

$-6 \equiv 3x_2$

cộng nhiều lần với 13 / chia để cho vế phải để tìm x_2 và $x_2 <$ số chia (13)

Exercise

A pseudorandom number sequence is generated as follows

$$x_0 = 2, x_n = (3x_{n-1} + 2) \mod 11$$

Find x_3.

A.3 B.4 C.5 D.8

Cryptography

Classical Cryptography

Julius Caeser cipher: shifting each letters forward in the alphabet.

Example $A \rightarrow D, B \rightarrow E, ..., X \rightarrow A, ...$

Problem: How to model Caeser cipher mathematically ?

Answer $Z_{26} = \{0, 1, 2, ..., 25\}$, each element in Z_{26} is assigned to each letter.

Example : $0 \equiv A$, $1 \equiv B$, $2 \equiv C$,...,$25 \equiv Z$.

Then consider the function f

$f(p) = p + 3 \bmod 26$ and $f^{-1}(p) = p - 3 \pmod{26}$

encrypt decrypt

Cryptography: letter 1 $\longrightarrow$ letter 2

Examples: shift cipher with k, $f(p) = (p+k) \bmod 26$

$\rightarrow$ $f^{-1}(p) = (p-k) \bmod 26$

Sender: (encoding)

Message: "ABC" , k=3

Using $f(p) = (p+3) \bmod 26$ // 26 characters

ABC ➔ 0 1 2 ➔ 3 4 5 ➔ DEF

+3

Receiver: (decoding)

DEF ➔ 3 4 5

Using $f^{-1}(p) = (p-3) \bmod 26$

3 4 5 ➔ 0 1 2 ➔ ABC

−3

Exercise

Using the function $f(x) = (x + 10) \bmod 26$ to encrypt messages. Answer each of these questions.

a) Encrypt the message STOP.

b) Decrypt the message LEI.

Exercise

Explaining why $f(x) = 2x \pmod{26}$ is not a good coding function.

$$\mathrm{lcm}(a,b) = 2^3 . 3^4 . 5^7 . 7^2$$

Exercise

What is the greatest common divisor of

$$a = 2^3.3^2.5^7, \quad b = 3^4.5^3.7^2$$

A.225 B. 1125 C. 375 D.2250 E.None

$$3^2 . 5^3$$

$$\mathrm{gcd} \neq \frac{a \cdot b}{\mathrm{lcm}} = 1125$$

Exercise

Find the sum 101111 + 110111 in binary representation

A. 1100110 B. 1100111

C. 1000101 D. 1010110

Exercise

How many numbers in the set $(80, 90, -80, -90)$ are congruent to 5 modulo 17?

A.0 B.1 C.2 D.3 E.4

so nao dong du voi 5 khi chia lay du voi 7
Tips: lay x - 5 va check xem co chia het cho 17 ko

Exercise

Find the greatest common divisor of $2^3.3^2.5.7$ and $2^4.5^2.11^3$

A.360 B.2310 C.40 D.120

Exercise

Given the Euclidean Algorithm

```
procedure gcd(a,b: positive integers)
x=a
y=b
while y>0
    r:= x mod y
    x:=y
    y:= r
return x
```

If $a = 16, b = 573$, then before performing step 3 of the loop

$A.x = 35, y = 13$ $\quad$ $B.x = 13, \cancel{y = 3}$

$C.x = 35, y = \cancel{16}$ $\quad$ $D.x = 16, y = 13$ (R)

573 mod 16 - R

15 : F

10 :

Exercise

Find the hexa-decimal expansion of $(1101111011)_2$

A. $(6EB)_{16}$ *B.* $(6FB)_{16}$ *C.* $(6FA)_{16}$ *D.* $(6FC)_{16}$

6 :

11 = B

Exercise

How many primes are in $(89, 111, 103, 205)$?

A.2 B.3 C.4 D.1 E.None

Exercise

Find the decimal expansion of the binary number 101011

A. 53 B. 49 C. 47 D. 43 E. None

43

Exercise

Given three sets of integers

i) $\{5, 12, 18\}$

ii) $\{4, 9, 25, 49\}$

iii) $\{12, 17, 23, 21, 35\}$

Which set consists of pairwise relative prime?

A. i B. ii C. iii D. None

Exercise

Consider an encryption scheme using the function

$$f(p) = 7p + 3 \mod 26$$

Encrypt the message "NO"

A.QB B.QX C.ZX D.DB E.DH

Exercise

Let a= 131 div 29, b= -131 div 29. Find a+b

A. -1 B. 29 C. 0 D. 8

4 + (-5)

Exercise

Suppose a message has been encrypted using the function $f(p) = p + 9 \mod 26$. If the encoded message is UE, decrypt the message.

A. OK B. LV C. CK D. DG

p-9

20 4

11 21

mod 26 U - 11 21

L V

Exercise

Suppose that a computer has only the memory locations $0, 1, 2, ..., 29$. Use the hasing function h where $h(k) = k$ mod 30 to determine the locations in which 197 are stored.

A.17 B. 13 C.7 D.23