VNU-HUS MAT3500: Toán rời rạc

Lý thuyết số cơ bản

Hoàng Anh Đức

Bộ môn Tin học, Khoa Toán-Cơ-Tin học
Đại học KHTN, ĐHQG Hà Nội
hoanganhduc@hus.edu.vn

Nội dung

Giới thiệu

- *Lý thuyết số (number theory)* nghiên cứu các tính chất và mối liên hệ giữa các loại số
  - quan trọng nhất là *các số nguyên dương (positive integers)*
  - đặc biệt là *các số nguyên tố (prime numbers)*

- Cho các số nguyên a và b với $a \neq 0$. Ta nói b *chia hết cho* a, ký hiệu $b \,\vdots\, a$, nếu tồn tại một số nguyên c sao cho $b = ac$.
- Trong trường hợp này, ta cũng nói a là *ước (factor)* của b hay b là *bội (multiple)* của a và ký hiệu $a \mid b$.
- Ta lần lượt sử dụng các ký hiệu $b \not\vdots\, a$ và $a \nmid b$ để chỉ b không chia hết cho a và a không là ước của b

Định lý 1

(1) *Nếu* $a \mid b$ *và* $a \mid c$, *thì* $a \mid (b + c)$

(2) *Nếu* $a \mid b$, *thì* $a \mid bc$

(3) *Nếu* $a \mid b$ *và* $b \mid c$, *thì* $a \mid c$

Bài tập 1

Chứng minh Định lý 1

Định lý 2

Với $a \in \mathbb{Z}$ và $d \in \mathbb{Z}^+$, tồn tại duy nhất các số nguyên q và r, với $0 \leq r < d$, thỏa mãn $a = dq + r$

Chứng minh.

- Tồn tại các số nguyên q và r với $0 \leq r < d$ thỏa mãn $a = dq + r$
  - Chọn q là số nguyên lớn nhất thỏa mãn $dq \leq a$
  - Chọn $r = a - dq$. Ta có $0 \leq r < d$ (Tại sao?)
- Giả sử tồn tại các cặp số nguyên q_1, r_1 và q_2, r_2 thỏa mãn $a = dq_1 + r_1$ và $a = dq_2 + r_2$, với $0 \leq r_1 \leq r_2 < d$ và $(q_1, r_1) \neq (q_2, r_2)$
  - Nếu $q_1 = q_2$ thì $r_1 = a - dq_1 = a - dq_2 = r_2$
  - Do đó, $q_1 \neq q_2$. Theo giả thiết $a = dq_1 + r_1 = dq_2 + r_2$ và do đó $d = (r_2 - r_1)/(q_1 - q_2)$. Do $0 \leq r_1 \leq r_2 < d$, ta có $0 \leq r_2 - r_1 < d = (r_2 - r_1)/(q_1 - q_2)$. Do đó, $0 \leq q_1 - q_2 < 1$. Đây là một mâu thuẫn (Tại sao?)

□

- Trong Định lý 2, a là *số bị chia (dividend)*, d là *số chia (divisor)*, q là *thương (quotient)*, và r là *số dư (remainder)*
- Ta cũng viết $q = a \operatorname{div} d$ và $r = a \bmod d$. Chú ý rằng với d cố định, $a \operatorname{div} d$ và $a \bmod d$ là các hàm từ $\mathbb{Z}$ đến $\mathbb{Z}$
- Ta có $q = \lfloor a/d \rfloor$ và $r = a - dq = a - d\lfloor a/d \rfloor$

Ví dụ 1

- $101 \operatorname{div} 11 = 9$ và $101 \bmod 11 = 2$
- $-11 \operatorname{div} 3 = -4$ và $-11 \bmod 3 = 1$
  (Chú ý rằng mặc dù $-11 = 3(-3) - 2$ nhưng *số dư của phép chia $a = -11$ cho $d = 3$ không bằng -2* do $r = -2$ không thỏa mãn $0 \leq r < d$)

Thuật toán 1: Tìm thương và số dư

Input: $a \in \mathbb{Z}$, $d \in \mathbb{Z}^+$
Output: Thương q và số dư r của phép chia a cho d

procedure `div-mod`(a, d):
  $q := 0$
  $r := |a|$
  while $r \geq d$ **do** `// Tiếp tục trừ` d `từ` r `và tăng` q `cho đến khi` $r < d$
    $r := r - d$
    $q := q + 1$
  if $a < 0$ *và* $r > 0$ **then** `// Trường hợp` a `âm`
    $r := d - r$
    $q := -(q + 1)$
  return (q, r) `//` $q = a$ `div` d `là thương,` $r = a \bmod d$ `là số dư`

- Với $a, b \in \mathbb{Z}$ và $m \in \mathbb{Z}^+$, *a đồng dư với b (theo) môđun m*, ký hiệu $a \equiv b \pmod{m}$, khi và chỉ khi $m \mid (a - b)$

Định lý 3

Với $a, b \in \mathbb{Z}$ và $m \in \mathbb{Z}^+$, $a \equiv b \pmod{m}$ khi và chỉ khi $a \bmod m = b \bmod m$

Chứng minh.

($\Rightarrow$) Giả sử $a \equiv b \pmod{m}$. Giả sử $a = q_1 m + r_1$ và $b = q_2 m + r_2$ với $q_1, q_2 \in \mathbb{Z}$, $0 \leq r_1 < m$, và $0 \leq r_2 < m$. Ta chứng minh $a \bmod m = r_1 = r_2 = b \bmod m$

- Do $a \equiv b \pmod{m}$, ta có $m \mid (a - b)$
- Suy ra $m \mid ((q_1 - q_2)m + (r_1 - r_2))$. Do đó $m \mid (r_1 - r_2)$, nghĩa là $r_1 - r_2 = mp$ với $p \in \mathbb{Z}$
- Do $0 \leq r_1, r_2 < m$ nên $-m < r_1 - r_2 < m$
- Suy ra $-m < mp < m$ và do đó $p = 0$, nghĩa là $r_1 = r_2$

($\Leftarrow$) Giả sử $a \bmod m = b \bmod m = r$. Suy ra $a = q_1 m + r$ và $b = q_2 m + r$ với $q_1, q_2 \in \mathbb{Z}$. Do đó, $a - b = (q_1 - q_2)m$, nghĩa là $m \mid (a - b)$

Bài tập 2

Chứng minh rằng quan hệ đồng dư theo môđun m "$\equiv \pmod m$" là một quan hệ tương đương trên tập các số nguyên

Định lý 4

Với $a, b \in \mathbb{Z}$ và $m \in \mathbb{Z}^+$, $a \equiv b \pmod m$ khi và chỉ khi tồn tại $k \in \mathbb{Z}$ sao cho $a = b + km$

Chứng minh.

($\Rightarrow$) Giả sử $a \equiv b \pmod m$. Theo định nghĩa, $m \mid (a - b)$, nghĩa là tồn tại $k \in \mathbb{Z}$ sao cho $a - b = km$ hay $a = b + km$

($\Leftarrow$) Giả sử tồn tại $k \in \mathbb{Z}$ sao cho $a = b + km$. Suy ra $a - b = km$ và do đó $m \mid (a - b)$. Theo định nghĩa, $a \equiv b \pmod m$

$\square$

Định lý 5

Với $a, b, c, d \in \mathbb{Z}$ *và* $m \in \mathbb{Z}^+$*, nếu* $a \equiv b \pmod{m}$ *và* $c \equiv d \pmod{m}$ *thì* $a + c \equiv b + d \pmod{m}$ *và* $ac \equiv bd \pmod{m}$

Chứng minh.

Giả sử $a \equiv b \pmod{m}$ và $c \equiv d \pmod{m}$. Theo Định lý 4, tồn tại $s, t \in \mathbb{Z}$ thỏa mãn $a = b + sm$ và $c = d + tm$. Do đó, $a + c = (b + d) + (s + t)m$ và $ac = (b + sm)(d + tm) = bd + (bt + sd + stm)m$. Theo Định lý 4, $a + c \equiv b + d \pmod{m}$ và $ac \equiv bd \pmod{m}$ □

Hệ quả 6

- $(a + b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$
- $ab \bmod m = ((a \bmod m)(b \bmod m)) \bmod m$

Bài tập 3

Chứng minh rằng nếu $a \equiv b \pmod{m}$ *và* $c \equiv d \pmod{m}$, *trong đó* $a, b, c, d \in \mathbb{Z}$ *và* $m \in \mathbb{Z}$ *thỏa mãn* $m \geq 2$, *thì* $a - c \equiv b - d \pmod{m}$

Bài tập 4

Tính các biểu thức sau

(a) $(-133 \bmod 23 + 261 \bmod 23) \bmod 23$

(b) $((457 \bmod 23) \cdot (182 \bmod 23)) \bmod 23$

(c) $(99^2 \bmod 32)^3 \bmod 15$

(d) $(3^4 \bmod 17)^2 \bmod 11$

Bài tập 5

Chứng minh rằng tích của ba số nguyên liên tiếp bất kỳ chia hết cho 6

- Thông thường, chúng ta biểu diễn các số theo *hệ cơ số (base)* 10, sử dụng các *chữ số (digit)* từ 0 đến 9
- Trên thực tế, ta có thể biểu diễn các số theo hệ cơ số $b > 1$ bất kỳ
- Với mọi $n, b \in \mathbb{Z}^+$, tồn tại duy nhất một dãy $a_k a_{k-1} \dots a_1 a_0$ gồm các *chữ số* $a_i < b$ $(0 \leq i \leq k)$ thỏa mãn

  $$n = a_k b^k + a_{k-1} b^{k-1} + a_{k-2} b^{k-2} + \cdots + a_1 b^1 + a_0 = \sum_{i=0}^{k} a_i b^i$$

  Ta cũng ký hiệu $n = (a_k a_{k-1} \dots a_2 a_1 a_0)_b$
- Một số hệ cơ số phổ biến
  - **Hệ cơ số 10 (hệ thập phân (decimal)):** sử dụng 10 chữ số $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$ (do chúng ta có 10 ngón tay)
  - **Hệ cơ số 2 (nhị phân (binary)):** sử dụng 2 chữ số $0, 1$ (dùng trong tất cả các hệ thống máy tính hiện đại)
  - **Hệ cơ số 8 (hệ bát phân (octal)):** sử dụng 8 chữ số $0, 1, 2, 3, 4, 5, 6, 7$ (tương ứng với các nhóm 3 bit)
  - **Hệ cơ số 16 (hệ thập lục phân (hexadecimal)):** sử dụng 16 chữ số $0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F$ (tương ứng với các nhóm 4 bit)

Ví dụ 2 (Phân quyền tệp tin (file permission))

Ký hiệu số trong hệ bát phân sử dụng để biểu diễn *phân quyền tệp tin trong các hệ điều hành Linux*

Thông tin tệp trong Linux

```
-rw-r--r-- 1 hoanganhduc hoanganhduc 1085121 Oct 21 15:17 Basic_Number_Theory.pdf
```

Thông tin thư mục trong Linux

```
drwxr-xr-x  3 hoanganhduc hoanganhduc 4096 Oct 21 15:24 Basic_Number_Theory
```

Loại	Phân quyền owner	Phân quyền group	Phân quyền public
-	r w -	r - -	r - -
d	r w x	r - x	r - x

Ký hiệu số tương ứng của các quyền r (read, đọc), w (write, ghi), x (execute, thực thi)		
Phân quyền owner	Phân quyền group	Phân quyền public
r w x 400 200 100	r w x 40 20 10	r w x 4 2 1

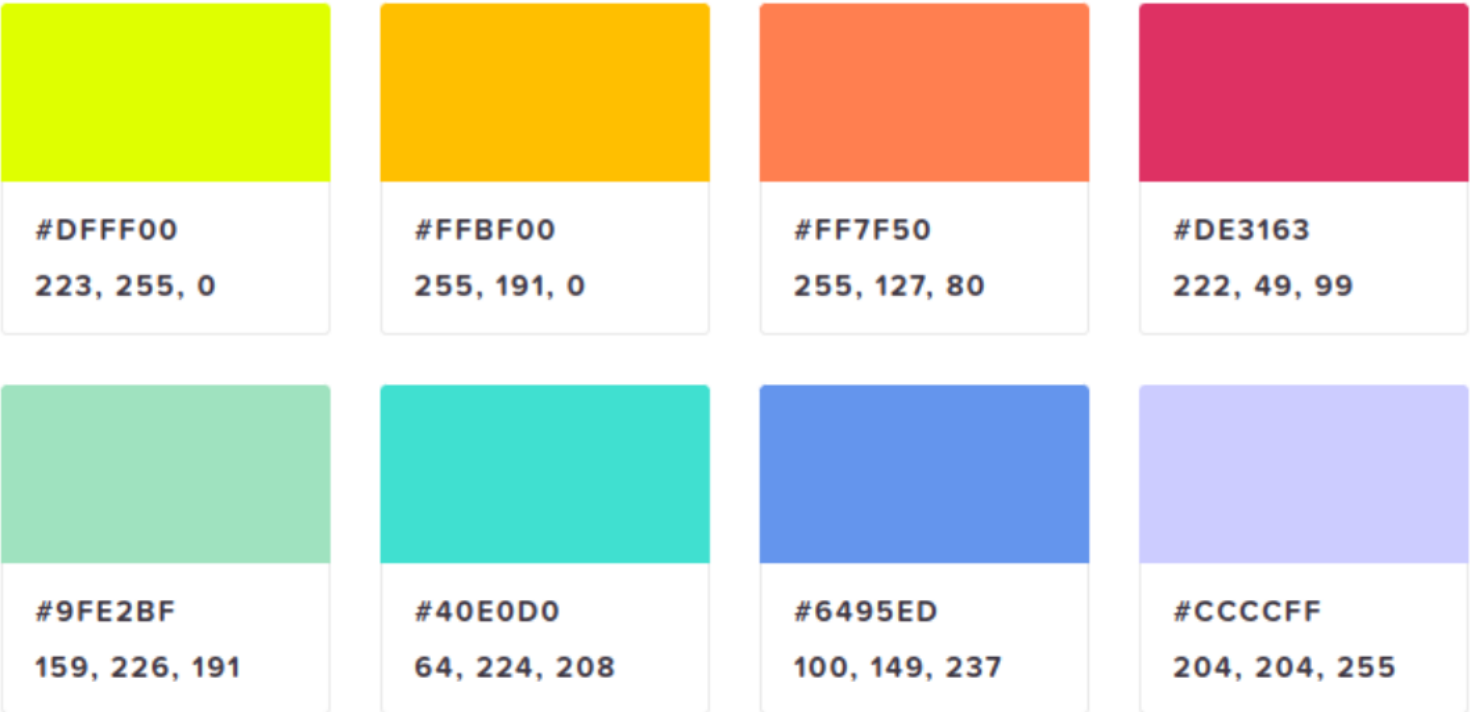
`rw-r--r--` $\Longleftrightarrow$ 644

`rwxr-xr-x` $\Longleftrightarrow$ 755

Biểu diễn số nguyên
Biểu diễn theo hệ b-phân

Ví dụ 3 (Mã màu)

Các số trong hệ thập lục phân được sử dụng để biểu diễn *mã màu (color code)* (nhằm đảm bảo các màu sắc được sử dụng một cách chính xác)



Hình: Một số mã màu từ trang `https://htmlcolorcodes.com/`

Chuyển số từ hệ b-phân sang hệ thập phân ($b \in \mathbb{Z}^+$)

$$(a_k a_{k-1} \dots a_1 a_0)_b = \sum_{i=0}^{k} a_i b^i$$

- $(101011111)_2 = 1 \cdot 2^8 + 0 \cdot 2^7 + 1 \cdot 2^6 + 0 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 351$
- $(2AE0B)_{16} = 2 \cdot 16^4 + 10 \cdot 16^3 + 14 \cdot 16^2 + 0 \cdot 16^1 + 11 \cdot 16^0 = 175627$

Chuyển số từ hệ thập phân sang hệ b-phân ($b \in \mathbb{Z}^+$)

(1) Tìm giá trị của chữ số ngoài cùng bên phải bằng cách tính $n \bmod b$

(2) Gán $n := n \operatorname{div} b$

(3) Lặp lại các bước (1) và (2) cho đến khi $n = 0$

$$
\begin{aligned}
n &= bq_0 + a_0 && n := q_0 \\
&= b(bq_1 + a_1) + a_0 \\
&= b^2 q_1 + ba_1 + a_0 && n := q_1 \\
&\vdots && \vdots \\
&= b^k(0 + a_k) + b^{k-1}a_{k-1} + \dots b^3 a_3 + b^2 a_2 + ba_1 + a_0 && n := 0 \\
&= b^k a_k + b^{k-1}a_{k-1} + \dots b^3 a_3 + b^2 a_2 + ba_1 + a_0
\end{aligned}
$$

Bài tập 6

Mô tả thuật toán trên bằng giả mã

Ví dụ 4

$$(12345)_{10} = (?)_8$$

$$\begin{aligned} 12345 &= 8 \cdot 1543 + 1 \\ 1543 &= 8 \cdot 192 + 7 \\ 192 &= 8 \cdot 24 + 0 \\ 24 &= 8 \cdot 3 + 0 \\ 3 &= 8 \cdot 0 + 3 \end{aligned}$$

Do đó, $(12345)_{10} = (30071)_8$

Bài tập 7

(a) $(177130)_{10} = (?)_2$

(b) $(177130)_{10} = (?)_8$

(c) $(177130)_{10} = (?)_{16}$

Chuyển đổi giữa hệ nhị phân và bát/thập lục phân

- Mỗi chữ số trong hệ bát phân tương ứng với một khối 3 bit trong biểu diễn nhị phân
- Mỗi chữ số trong hệ thập lục phân tương ứng với một khối 4 bit trong biểu diễn nhị phân

Thập phân	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Thập lục phân	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Bát phân	0	1	2	3	4	5	6	7	10	11	12	13	14	15	16	17
Nhị phân	0	1	10	11	100	101	110	111	1000	1001	1010	1011	1100	1101	1110	1111

$$(\underline{11}\ \underline{1110}\ \underline{1011}\ \underline{1111})_2 = (3EBF)_{16}$$

$$(\underline{A}\underline{3}\underline{D})_{16} = (1010\ 0011\ 1101)_2$$

Bài tập 8

(a) $(111110101111100)_2 = (?)_8$

(b) $(111110101111100)_2 = (?)_{16}$

(c) $(765)_8 = (?)_2$

(d) $(A8D)_{16} = (?)_2$

Biểu diễn số nguyên

Cộng và nhân các số nhị phân

Để cộng hai số nhị phân $a = (a_{n-1}a_{n-2}\dots a_1a_0)_2$ và $b = (b_{n-1}b_{n-2}\dots b_1b_0)_2$

- Cộng hai chữ số nhị phân ngoài cùng bên phải
$$a_0 + b_0 = c_0 \cdot 2 + s_0,$$
trong đó s_0 là chữ số ngoài cùng bên phải trong biểu diễn nhị phân của tổng $a+b$ và *nhớ (carry)* c_0
- Cộng hai chữ số nhị phân tiếp theo và nhớ
$$a_1 + b_1 + c_0 = c_1 \cdot 2 + s_1,$$
trong đó s_1 là chữ số tiếp theo (tính từ bên phải) trong biểu diễn nhị phân của tổng $a+b$ và nhớ c_1
- Tiếp tục cộng hai chữ số nhị phân tiếp theo và nhớ để xác định chữ số tiếp theo (tính từ bên phải) trong biểu diễn nhị phân của tổng $a+b$ và nhớ
- Ở bước cuối cùng, tính
$$a_{n-1} + b_{n-1} + c_{n-2} = c_{n-1} \cdot 2 + s_{n-1},$$
và chữ số đầu tiên trong biểu diễn nhị phân của tổng $a+b$ là $s_n = c_{n-1}$

Thuật toán trên cho ta $a + b = (s_ns_{n-1}\dots s_1s_0)_2$

Thuật toán 2: Cộng hai số nhị phân

Input: $a = (a_{n-1} \dots a_0)_2, b = (b_{n-1} \dots b_0)_2$: biểu diễn nhị phân của các số nguyên dương a, b

Output: $s = (s_n s_{n-1} \dots s_0)$: biểu diễn nhị phân của $s = a + b$

```
procedure add(a, b):
    c := 0
    for j := 0 to n − 1 do
        d := ⌊(a_j + b_j + c)/2⌋
        s_j = a_j + b_j + c − 2d
        c := d
    s_n := c
    return (s_0, s_1, ..., s_n)
```

Ví dụ 5

Cộng hai số $a = (10111)_2$ và $b = (11100)_2$

$$\begin{array}{r} 10111 \\ +\ 11100 \\ \hline 1 \end{array} \quad \text{nhớ } 0 \qquad \begin{array}{r} 10111 \\ +\ 11100 \\ \hline 11 \end{array} \quad \text{nhớ } 0 \qquad \begin{array}{r} 10111 \\ +\ 11100 \\ \hline 011 \end{array} \quad \text{nhớ } 1$$

$$\begin{array}{r} 10111 \\ +\ 11100 \\ \hline 0011 \end{array} \quad \text{nhớ } 1 \qquad \begin{array}{r} 10111 \\ +\ 11100 \\ \hline 110011 \end{array} \quad \text{nhớ } 1$$

Biểu diễn số nguyên

Cộng và nhân các số nhị phân

Để nhân hai số nhị phân $a = (a_{n-1}a_{n-2}\dots a_1a_0)_2$ và $b = (b_{n-1}b_{n-2}\dots b_1b_0)_2$, chú ý rằng

$$\begin{aligned} ab &= a(b_0 2^0 + b_1 2^1 + \dots + b_{n-1}2^{n-1}) \\ &= a(b_0 2^0) + a(b_1 2^1) + \dots + a(b_{n-1}2^{n-1}) \end{aligned}$$

Phương trình này cho ta cách tính ab:

- Chú ý rằng $ab_j = a$ nếu $b_j = 1$ và $ab_j = 0$ nếu $b_j = 0$
- Mỗi lần nhân một số hạng với 2, ta dịch chuyển biểu diễn nhị phân của số đó sang trái một đơn vị và thêm 0 vào đuôi của biểu diễn. Nói cách khác, ta có thể thu được biểu diễn nhị phân của $(ab_j)2^j$ bằng cách dịch chuyển biểu diễn nhị phân của ab_j sang trái j đơn vị và thêm j số 0 vào đuôi của biểu diễn
- Cuối cùng, ta nhận được ab bằng cách cộng biểu diễn nhị phân của n số $(ab_j)2^j$ với $j \in \{0, \dots, n-1\}$

Thuật toán 3: Nhân hai số nhị phân

Input: $a = (a_{n-1} \dots a_0)_2, b = (b_{n-1} \dots b_0)_2$: biểu diễn nhị phân của các số nguyên dương a, b

Output: biểu diễn nhị phân của $p = ab$

procedure `multiply(`a`, `b`)`**:**

  for $j := 0$ **to** $n - 1$ **do**

    if $b_j = 1$ **then**

      $c_j := a$ sau khi di chuyển j đơn vị sang trái

    else

      $c_j := 0$

    `//` $c_0, \dots, c_{n-1}$ `là các tích thành phần`

    $p := 0$

    for $j := 0$ **to** $n - 1$ **do**

      $p :=$ `add(`p`, `c_j`)`

  return p

Ví dụ 6

Nhân hai số $a = (110)_2$ và $b = (101)_2$

$$\begin{array}{r} 110 \\ \times\ 101 \\ \hline 110 \end{array} \qquad \begin{array}{r} 110 \\ \times\ 101 \\ \hline 110 \\ 0000 \end{array} \qquad \begin{array}{r} 110 \\ \times\ 101 \\ \hline 110 \\ +\ 0000 \\ 11000 \\ \hline 11110 \end{array}$$

Bài tập 9

Tính tổng và tích các số nhị phân sau

(a) $(1000111)_2$ *và* $(1110111)_2$

- ***Kết quả:*** *Tổng* = $(10111110)_2$, *Tích* = $(10000100000001)_2$

(b) $(11101111)_2$ *và* $(10111101)_2$

- ***Kết quả:*** *Tổng* = $(110101100)_2$, *Tích* = $(1011000001110011)_2$

Biểu diễn số nguyên

Biểu diễn các số nguyên âm theo hệ nhị phân

- Trong thực hành, chúng ta cần biểu diễn không chỉ các số dương (positive integers) mà cả các số âm (negative integers)
- Khi sử dụng “giấy và bút”, các số âm được thể hiện bằng cách thêm dấu “$-$” đằng trước
- Khi sử dụng máy tính, tất cả các loại dữ liệu đều được biểu diễn trong hệ nhị phân

Biểu diễn thông qua *định dạng dấu-lượng (sign-magnitude format)*

- Bit ngoài cùng bên trái dùng để biểu diễn dấu (0 là dương, 1 là âm)
- Phần còn lại biểu diễn độ lớn (hay trị tuyệt đối) của số
- Một chuỗi nhị phân n bit có thể biểu diễn bất kỳ số nguyên i nào thỏa mãn $-(2^{n-1} - 1) \leq i \leq 2^{n-1} - 1$
- **Ví dụ:** biểu diễn nhị phân của 93 là 01011101 và biểu diễn nhị phân của -93 là 11011101
- **Hạn chế:** Số 0 có hai biểu diễn nhị phân: $000\dots00$ (biểu diễn $+0$) và $100\dots00$ (biểu diễn -0)

Biểu diễn thông qua *ký hiệu phần bù một (one's complement notation)*

- Bit ngoài cùng bên trái dùng để biểu diễn dấu (0 là dương, 1 là âm)
- Khi biểu diễn bằng ký hiệu phần bù một, nếu $+a = (a_{n-1} \dots a_0)_2$ thì $-a = (\overline{a_{n-1} \dots a_0})_2$, trong đó $\overline{a_{n-1} \dots a_0}$ là phần bù của $a_{n-1} \dots a_0$ thu được thông qua tính toán bằng toán tử lôgic $^-$ (phủ định) theo từng bit
- Một chuỗi nhị phân n bit có thể biểu diễn bất kỳ số nguyên i nào thỏa mãn $-(2^{n-1} - 1) \leq i \leq 2^{n-1} - 1$
- **Ví dụ:** biểu diễn nhị phân của 93 là 01011101 và biểu diễn nhị phân của -93 là 10100010
- **Hạn chế:** Số 0 có hai biểu diễn nhị phân: $00 \dots 00$ (biểu diễn $+0$) và $11 \dots 11$ (biểu diễn -0)

Biểu diễn thông qua *ký hiệu phần bù hai (two's complement notation)*

- Bit ngoài cùng bên trái dùng để biểu diễn dấu (0 là dương, 1 là âm)
- Khi biểu diễn bằng ký hiệu phần bù hai, nếu $a = (a_{n-1} \dots a_0)_2$ thì $-a = (\overline{a_{n-1} \dots a_0})_2 + 1$, trong đó $\overline{a_{n-1} \dots a_0}$ là phần bù của $a_{n-1} \dots a_0$ thu được thông qua tính toán bằng toán tử lôgic $\overline{}$ (phủ định) theo từng bit
- Trong trường hợp này, một chuỗi nhị phân n bit có thể biểu diễn bất kỳ số nguyên i nào thỏa mãn $-2^{n-1} \leq i < 2^{n-1}$

Ví dụ 7 (Với $n = 3$)

Giá trị	Chuỗi 3-bit	Giá trị	Chuỗi 3-bit
3	011	-3	101
2	010	-2	110
1	001	-1	111
0	000	-4	100

- Trong các thuật toán mã hóa hiện đại, một bài toán quan trọng là *tính $b^n \bmod m$ một cách hiệu quả* mà không cần sử dụng quá nhiều bộ nhớ, đặc biệt là *khi b, n, m là các số nguyên lớn*
- Việc tính b^n rồi tìm số dư khi chia nó cho m là không thực tế, do b^n có thể cực lớn và ta sẽ cần một lượng lớn bộ nhớ chỉ để lưu giá trị của b^n
- Ta có thể tính $b^n \bmod m$ bằng cách lần lượt tính $b^k \bmod m$ cho $k = 1, 2, \dots, n$, sử dụng tính chất $b^{k+1} \bmod m = b(b^k \bmod m) \bmod m$. Tuy nhiên, hướng tiếp cận này cũng không thực tế, do ta cần thực hiện $n - 1$ phép nhân các số nguyên và n có thể rất lớn
- Ta trình bày một hướng tiếp cận hiệu quả *dựa trên biểu diễn nhị phân của n*

- Chú ý rằng

$$
\begin{aligned}
b^n &= b^{\overbrace{a_{k-1}2^{k-1}+a_{k-2}2^{k-2}+\cdots+a_1 2^1+a_0 2^0}^{\text{Biểu diễn nhị phân của } n}} \\
&= (b^{2^{k-1}})^{a_{k-1}} \times (b^{2^{k-2}})^{a_{k-2}} \times \cdots \times (b^{2^1})^{a_1} \times (b^{2^0})^{a_0}
\end{aligned}
$$

- Chúng ta có thể tính các giá trị b^{2^j} bằng cách *liên tục bình phương*
- Sau đó ta chỉ cần nhân các giá trị này với nhau để tạo thành một tích thành phần, tùy thuộc vào a_j có bằng 1 hay không
- Quan trọng là, sau mỗi bước nhân, để tăng tính hiệu quả và tiết kiệm bộ nhớ, ta *có thể lấy* $\bmod m$ *của kết quả để tiếp tục thực hiện tính toán*

Ví dụ 8

Ta tính $3^{644} \bmod 645$

$$
\begin{aligned}
644 &= 1 \times 2^9 + 0 \times 2^8 + 1 \times 2^7 + 0 \times 2^6 + 0 \times 2^5 + 0 \times 2^4 \\
&\quad + 0 \times 2^3 + 1 \times 2^2 + 0 \times 2^1 + 0 \times 2^0 \\
3^{644} &= {\color{red}(3^{2^9})^1} \times (3^{2^8})^0 \times {\color{green}(3^{2^7})^1} \times (3^{2^6})^0 \times (3^{2^5})^0 \times (3^{2^4})^0 \\
&\quad \times (3^{2^3})^0 \times {\color{blue}(3^{2^2})^1} \times (3^{2^1})^0
\end{aligned}
$$

Ta tính các giá trị $3^{2^j} \mod 645$ $(1 \leq j \leq 9)$ bằng cách liên tục bình phương và lấy $\mod 645$

$$3^{2^1} \mod 645 = 9$$

$$3^{2^2} \mod 645 = (3^{2^1})^2 \mod 645 = (3^{2^1} \mod 645)^2 \mod 645 = 81$$

$$3^{2^3} \mod 645 = (3^{2^2})^2 \mod 645 = (3^{2^2} \mod 645)^2 \mod 645 = 111$$

$$3^{2^4} \mod 645 = (3^{2^3})^2 \mod 645 = (3^{2^3} \mod 645)^2 \mod 645 = 66$$

$$3^{2^5} \mod 645 = (3^{2^4})^2 \mod 645 = (3^{2^4} \mod 645)^2 \mod 645 = 486$$

$$3^{2^6} \mod 645 = (3^{2^5})^2 \mod 645 = (3^{2^5} \mod 645)^2 \mod 645 = 126$$

$$3^{2^7} \mod 645 = (3^{2^6})^2 \mod 645 = (3^{2^6} \mod 645)^2 \mod 645 = 396$$

$$3^{2^8} \mod 645 = (3^{2^7})^2 \mod 645 = (3^{2^7} \mod 645)^2 \mod 645 = 81$$

$$3^{2^9} \mod 645 = (3^{2^8})^2 \mod 645 = (3^{2^8} \mod 645)^2 \mod 645 = 111$$

Do đó,

$$
\begin{aligned}
3^{644} \bmod 645 &= (3^{2^2} \times 3^{2^7} \times 3^{2^9}) \bmod 645 \\
&= ((((3^{2^2} \bmod 645) \times (3^{2^7} \bmod 645)) \bmod 645) \\
&\times (3^{2^9} \bmod 645)) \bmod 645 \\
&= (((81 \times 396) \bmod 45) \times 111) \bmod 645 \\
&= (471 \times 111) \bmod 645 \\
&= 36
\end{aligned}
$$

Thuật toán 4: Tính lũy thừa môđun nhanh

Input: b: số nguyên, $n = (a_{k-1}a_{k-2}\dots a_1a_0)_2$: biểu diễn nhị phân của số nguyên dương n, m: số nguyên dương

Output: $b^n \bmod m$

$x := 1$ // để lưu trữ kết quả

$b2i := b \bmod m$ // b^{2^i}, đầu tiên $i = 0$

for $i := 0$ **to** $k-1$ **do** // xét tất cả k bit của n

  if $a_i = 1$ **then**

    $x := (x \cdot b2i) \bmod m$

  $b2i := (b2i \cdot b2i) \bmod m$ // $b^{2^{i+1}} = (b^{2^i}) \cdot (b^{2^i})$

return x

Bài tập 10

Sử dụng thuật toán tính $b^n \bmod m$ thông qua biểu diễn nhị phân của n đã mô tả ở trên để tính $7^{644} \bmod 645$

- Một số nguyên $p > 1$ là một *số nguyên tố (prime number)* nếu các ước số dương duy nhất của p là 1 và chính nó
  - Ví dụ: $2, 3, 5, 11, \dots$
- Các số nguyên lớn hơn 1 và không phải là số nguyên tố được gọi là các *hợp số (composite number)*

Bài tập 11

*Chứng minh rằng nếu p là một số nguyên tố và $p \mid ab$ với $a, b \in \mathbb{Z}^+$ thì $p \mid a$ hoặc $p \mid b$. (**Gợi ý:** Giả sử $p \nmid a$, chứng minh $p \mid b$. Sử dụng Định lý Bézout (Định lý 12)) sẽ đề cập ở phần sau.) Phát biểu trên có đúng với p là hợp số hay không? Tại sao?*

Bài tập 12

Sử dụng quy nạp, hãy chứng minh phát biểu tổng quát: nếu p là một số nguyên tố và $p \mid a_1a_2 \dots a_n$, trong đó $a_i \in \mathbb{Z}$ với $1 \leq i \leq n$, thì $p \mid a_j$ với j nào đó ($1 \leq j \leq n$)

Định lý 7: Định lý cơ bản của số học

Mọi số nguyên dương lớn hơn 1 có thể được viết một cách duy nhất dưới dạng một số nguyên tố hoặc một tích của các ước nguyên tố của nó theo thứ tự tăng dần

Gợi ý.

- Ta đã chứng minh bằng phương pháp quy nạp: nếu $n > 1$ là một số nguyên thì n có thể được biểu diễn dưới dạng tích của các số nguyên tố
- Để chỉ ra tính "duy nhất", ta chứng minh bằng phản chứng: giả sử số nguyên dương $n > 1$ có thể được biểu diễn dưới dạng tích các số nguyên tố theo hai cách, ví dụ như $n = p_1 p_2 \dots p_s$ và $n = q_1 q_2 \dots q_t$, trong đó mỗi p_i $(1 \leq i \leq s)$ và q_j $(1 \leq j \leq t)$ là một số nguyên tố thỏa mãn $p_1 \leq p_2 \leq \cdots \leq p_s$ và $q_1 \leq q_2 \leq \cdots \leq q_t$. Sử dụng Bài tập 12 để chỉ ra mâu thuẫn

Định lý 8

Nếu $n \in \mathbb{Z}^+$ là một hợp số, thì n có một ước nguyên tố nhỏ hơn hoặc bằng $\sqrt{n}$

Chứng minh.

- Theo giả thiết, $n \in \mathbb{Z}^+$ là hợp số, do đó n có một ước số a thỏa mãn $1 < a < n$. Do đó, tồn tại số nguyên $b > 1$ sao cho $n = ab$.
- Ta chứng minh $a \leq \sqrt{n}$ hoặc $b \leq \sqrt{n}$. Thật vậy, giả sử $a > \sqrt{n}$ và $b > \sqrt{n}$. Suy ra, $ab > \sqrt{n} \cdot \sqrt{n} = n$, mâu thuẫn với định nghĩa của a, b. Do đó $a \leq \sqrt{n}$ hoặc $b \leq \sqrt{n}$, nghĩa là, n có một ước số lớn hơn 1 và không vượt quá $\sqrt{n}$ (a hoặc b)
- Theo Định lý cơ bản của số học, ước số này là một số nguyên tố hoặc có một ước nguyên tố nhỏ hơn nó. Trong cả hai trường hợp, n có một ước nguyên tố nhỏ hơn hoặc bằng $\sqrt{n}$

- Mệnh đề phản đảo của Định lý 8: Một số nguyên $n > 1$ là số nguyên tố nếu nó không chia hết cho bất kỳ số nguyên tố nào nhỏ hơn hoặc bằng $\sqrt{n}$
- Tìm các số nguyên tố giữa 2 và n bằng *Sàng Eratosthenes (The Sieve of Eratosthenes)*
  (1) Viết các số $2, \dots, n$ vào một danh sách. Gán $i := 2$
  (2) Bỏ đi tất cả các bội của i trừ chính nó khỏi danh sách
  (3) Gọi k là số nhỏ nhất hiện có trong danh sách thỏa mãn $k > i$. Gán $i := k$
  (4) Nếu $i > \sqrt{n}$ thì dừng lại, ngược lại thì quay lại bước (2)
- Việc kiểm tra xem một số có phải là số nguyên tố hay không có thể được thực hiện trong thời gian đa thức [Agrawal, Kayal, and Saxena 2004] (đa thức của số bit sử dụng để mô tả số đầu vào)

Định lý 9

Có vô hạn số nguyên tố

Chứng minh (theo Euclid).

- Giả sử chỉ có hữu hạn các số nguyên tố $p_1, p_2, \ldots, p_n$. Đặt $Q = p_1 p_2 \ldots p_n + 1$
- Theo Định lý cơ bản của số học, (a) Q là một số nguyên tố hoặc (b) Q có thể được viết thành tích của ít nhất hai số nguyên tố
- **(a) đúng:** Do đó, Q là số nguyên tố. Theo định nghĩa, $Q \notin \{p_1, \ldots, p_n\}$, mâu thuẫn với giả thiết toàn bộ các số nguyên tố là $p_1, \ldots, p_n$
- **(b) đúng:** Do đó, tồn tại j thỏa mãn $p_j \mid Q$ với $1 \leq j \leq n$. Chú ý rằng $p_j \mid (p_1 p_2 \ldots p_n)$, và do đó $p_j \mid (Q - p_1 p_2 \ldots p_n)$, suy ra $p_j \mid 1$, mâu thuẫn với giả thiết p_j là số nguyên tố

Số nguyên tố và Ước chung lớn nhất

Ước chung lớn nhất

- Cho $a, b \in \mathbb{Z}$ và a, b không đồng thời bằng 0. *Ước chung lớn nhất (greatest common divisor)* của a và b, ký hiệu $\gcd(a, b)$, là số nguyên lớn nhất d thỏa mãn $d \mid a$ và $d \mid b$
- Các số nguyên a và b được gọi là *nguyên tố cùng nhau (relatively prime hoặc coprime)* khi và chỉ khi $\gcd(a, b) = 1$
- Một tập các số nguyên $\{a_1, a_2, a_3, \dots, a_n\}$ được gọi là *đôi một nguyên tố cùng nhau (pairwise relatively prime)* nếu mọi cặp a_i, a_j với $1 \leq i < j \leq n$ là nguyên tố cùng nhau
- Nếu các số nguyên dương a và b được phân tích thành tích các số nguyên tố

$$a = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n} \qquad b = p_1^{b_1} p_2^{b_2} \dots p_n^{b_n}$$

trong đó các số mũ là các số nguyên không âm (có thể bằng 0), thì

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

- Cho $a, b \in \mathbb{Z}^+$. *Bội chung nhỏ nhất (least common multiple)* của a và b, ký hiệu $\mathrm{lcm}(a, b)$, là số nguyên nhỏ nhất d thỏa mãn $a \mid d$ và $b \mid d$
  - Tập các bội chung của a và b có ít nhất một phần tử ab
  - **Tính sắp thứ tự tốt:** Mọi tập con khác rỗng của $\mathbb{Z}^+$ có phần tử nhỏ nhất
- Nếu a và b được phân tích thành tích các số nguyên tố

$$a = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n} \qquad b = p_1^{b_1} p_2^{b_2} \dots p_n^{b_n}$$

trong đó các số mũ là các số nguyên không âm (có thể bằng 0), thì

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

Định lý 10

Với $a, b \in \mathbb{Z}^+$, $ab = \gcd(a, b) \cdot \mathrm{lcm}(a, b)$

Bài tập 14

Chứng minh Định lý 10

Bổ đề 11

Cho $a = bq + r$ với a, b, q, r là các số nguyên. Ta có $\gcd(a, b) = \gcd(b, r)$. Do đó, ta cũng có $\gcd(a, b) = \gcd(b, (a \bmod b))$

Chứng minh.

- Gọi D_{ab} là tập các ước số chung của a và b, với các số nguyên a, b bất kỳ. Ta chứng minh $D_{ab} = D_{br}$
- $D_{ab} \subseteq D_{br}$: Giả sử $x \in D_{ab}$. Theo định nghĩa, $x \mid a$ và $x \mid b$. Theo Định lý 1, $x \mid (a - bq)$ và do đó $x \mid r$, suy ra $x \in D_{br}$
- $D_{br} \subseteq D_{ab}$: Giả sử $x \in D_{br}$. Theo định nghĩa, $x \mid b$ và $x \mid r$. Theo Định lý 1, $x \mid (bq + r)$ và do đó $x \mid a$, suy ra $x \in D_{ab}$
- Từ $D_{ab} = D_{br}$, ta có $\gcd(a, b) = \gcd(b, r)$

$\square$

Thuật toán Euclid

Ý tưởng: Sử dụng đẳng thức $\gcd(a, b) = \gcd(b, (a \bmod b))$

Ví dụ 9 (Thuật toán Euclid)

Tìm $\gcd(372, 164)$

$$\begin{aligned}
\gcd(372, 164) &= \gcd(164, 372 \bmod 164) = \gcd(164, 44) \\
&= \gcd(44, 164 \bmod 44) = \gcd(44, 32) \\
&= \gcd(32, 44 \bmod 32) = \gcd(32, 12) \\
&= \gcd(12, 32 \bmod 12) = \gcd(12, 8) \\
&= \gcd(8, 12 \bmod 8) = \gcd(8, 4) \\
&= \gcd(4, 8 \bmod 4) = \gcd(4, 0) \\
&= 4
\end{aligned}$$

Số nguyên tố và Ước chung lớn nhất
Thuật toán Euclid

Thuật toán 5: Thuật toán Euclid

Input: a, b: các số nguyên dương
Output: $\gcd(a, b)$

```
x := a
y := b
while y ≠ 0 do
    r := x mod y
    x := y
    y := r
return x                                    // x = gcd(a, b)
```

Bài tập 15

Sử dụng thuật toán Euclid để tìm

(a) $\gcd(12, 18)$

(b) $\gcd(111, 201)$

(c) $\gcd(1001, 1331)$

Bài tập 16

Chứng minh rằng nếu a, b, m *là các số nguyên với* $m \geq 2$ *và* $a \equiv b \pmod{m}$ *thì* $\gcd(a, m) = \gcd(b, m)$. *(**Gợi ý:** Chứng minh tập các ước chung của* a *và* m *bằng với tập các ước chung của* b *và* m.*)*

Định lý 12: Định lý Bézout

Cho các số nguyên dương a, b. Tồn tại các số nguyên s, t sao cho $\gcd(a, b) = sa + tb$

- Các số nguyên s, t thỏa mãn Định lý Bézout được gọi là các *hệ số Bézout (Bézout's coefficients)* của a và b
- Phương trình $\gcd(a, b) = sa + tb$ được gọi là *đẳng thức Bézout (Bézout's identity)*

Chú ý:

- Chúng ta không trình bày chứng minh của Định lý Bézout
- Chúng ta sẽ đề cập hai phương pháp để tìm một tổ hợp tuyến tính của hai số nguyên bằng với ước chung lớn nhất của chúng (Trong phần này, ta luôn giả thiết các tổ hợp tuyến tính chỉ có hệ số nguyên)
  (1) Đi ngược lại theo các phép chia của thuật toán Euclid
  (2) Thuật toán Euclid mở rộng (The extended Euclidean algorithm)

Ví dụ 10

Biểu diễn $\gcd(252, 198) = 18$ dưới dạng tổ hợp tuyến tính của 252 và 198

- Thuật toán Euclid sử dụng các phép chia như sau
  - $252 = 1 \cdot 198 + 54$
  - $198 = 3 \cdot 54 + 36$
  - $54 = 1 \cdot 36 + 18$
  - $36 = 2 \cdot 18 + 0$
- Ta có

$$\begin{aligned}
18 &= 54 - 1 \cdot 36 \\
&= 54 - 1 \cdot (198 - 3 \cdot 54) \\
&= 4 \cdot 54 - 1 \cdot 198 \\
&= 4 \cdot (252 - 1 \cdot 198) - 1 \cdot 198 \\
&= 4 \cdot 252 - 5 \cdot 198
\end{aligned}$$

Thuật toán 6: Thuật toán Euclid mở rộng

Input: a, b: các số nguyên dương

Output: (d, s, t): $d = \gcd(a, b)$ và s, t thỏa mãn $d = sa + tb$

procedure `ExtEuclid`(a, b):

  if $b = 0$ **then**

    return $(a, 1, 0)$

  $(d_1, s_1, t_1) :=$ `ExtEuclid`$(b, a \bmod b)$

  $d := d_1$

  $s := t_1$

  $t := s_1 - (a \operatorname{div} b) \cdot t_1$

  return (d, s, t)

Ví dụ 11

$\texttt{ExtEuclid}(252, 198) = (18, 4, -5)$

Gọi $\texttt{ExtEuclid}(\cdot, \cdot)$	a	b	d	s	t
1	252	198	18	4	-5
2	198	54	18	-1	4
3	54	36	18	1	-1
4	36	18	18	0	1
5	18	0	18	1	0

Bài tập 17

Biểu diễn ước chung lớn nhất của các cặp số sau dưới dạng tổ hợp tuyến tính của chúng

(a) $10, 11$

(b) $21, 44$

(c) $36, 48$

(d) $34, 55$

(e) $117, 213$

(f) $1023, 36$

Định lý 13

Cho các số nguyên dương a, b, c *thỏa mãn* $\gcd(a, b) = 1$ *và* $a \mid bc$. *Ta có* $a \mid c$

Chứng minh.

- Theo Định lý Bézout, tồn tại các số nguyên s, t thỏa mãn $\gcd(a, b) = 1 = sa + tb$
- Do $a \mid bc$, ta cũng có $a \mid tbc$
- Mặt khác, $a \mid sac$
- Suy ra, $a \mid (tb + sa)c$, hay $a \mid c$

□

Định lý 14

Cho số nguyên dương m *và các số nguyên* a, b, c. *Nếu* $ac \equiv bc \pmod{m}$ *và* $\gcd(c, m) = 1$, *thì* $a \equiv b \pmod{m}$

Chứng minh.

- Theo định nghĩa, do $ac \equiv bc \pmod{m}$, ta có $m \mid (a - b)c$
- Kết hợp với $\gcd(c, m) = 1$ và Định lý 13, ta có $m \mid (a - b)$, nghĩa là $a \equiv b \pmod{m}$

$\square$

- Một *phương trình đồng dư (congruence)* có dạng

$$ax \equiv b \pmod{m}$$

với $a, b \in \mathbb{Z}$, $m \in \mathbb{Z}^+$, và x là một biến, được gọi là một *phương trình đồng dư tuyến tính (linear congruence)*

  - Việc *giải* phương trình đồng dư nghĩa là tìm giá trị của x thỏa mãn phương trình đó
- Một *nghịch đảo (inverse)* của a theo môđun m là bất kỳ số nguyên s nào thỏa mãn $sa \equiv 1 \pmod{m}$
  - Ví dụ, 5 là một nghịch đảo của 3 theo môđun 7, vì $5 \cdot 3 \equiv 1 \pmod{7}$
  - Đôi khi ta cũng dùng ký hiệu $\overline{a}$ hoặc a^{-1} để chỉ một nghịch đảo của a
  - Chú ý rằng nếu ta có thể tìm được s thỏa mãn điều kiện trên, ta có thể giải $ax \equiv b \pmod{m}$ bằng cách nhân cả hai vế với s, nghĩa là, $sax \equiv sb \pmod{m}$, suy ra $x \equiv sb \pmod{m}$

Phương trình đồng dư

Giới thiệu

Định lý 15

Nếu $\gcd(a, m) = 1$ và $m > 1$ thì tồn tại nghịch đảo s của a. Thêm vào đó, nghịch đảo này là duy nhất theo môđun m

Chứng minh.

- Tồn tại số nguyên s thỏa mãn $sa \equiv 1 \pmod{m}$
    - Theo định lý Bézout, tồn tại các số nguyên s, t thỏa mãn $sa + tm = 1$. Do đó $sa + tm \equiv 1 \pmod{m}$
    - Do $tm \equiv 0 \pmod{m}$, ta có $sa \equiv 1 \pmod{m}$, và do đó s là một nghịch đảo của a theo môđun m
- Nếu tồn tại hai số nguyên s, r thỏa mãn $sa \equiv 1 \pmod{m}$ và $ra \equiv 1 \pmod{m}$ thì $s \equiv r \pmod{m}$
    - **Nhắc lại:** Với các số nguyên a, b, c và số nguyên dương m, nếu $ac \equiv bc \pmod{m}$ và $\gcd(c, m) = 1$ thì $a \equiv b \pmod{m}$

$\square$

Bài tập 18

Chứng minh rằng nếu $\gcd(a, m) > 1$ với $a \in \mathbb{Z}$ bất kỳ và $m > 2$ thì không tồn tại một nghịch đảo của a theo môđun m

Định lý 15 cho ta một phương pháp tìm một nghịch đảo của $a \in \mathbb{Z}$ theo môđun $m \in \mathbb{Z}^+$ khi $\gcd(a, m) = 1$ và $m > 1$

Ví dụ 12

Tìm một nghịch đảo của 3 theo môđun 7

(1) Tìm các số nguyên s, t thỏa mãn $1 = s \cdot 3 + t \cdot 7$

- Thuật toán Euclid tìm ước chung lớn nhất của 3 và 7 bằng cách sử dụng phương trình

$$7 = 2 \cdot 3 + 1$$

- Từ phương trình trên, ta có

$$1 = -2 \cdot 3 + 1 \cdot 7$$

nghĩa là $s = -2$ và $t = 1$

(2) Theo Định lý 15, $s = -2$ là một nghịch đảo của 3 theo môđun 7. Chú ý rằng mọi số nguyên t thỏa mãn $t \equiv -2 \pmod 7$ (ví dụ như $5, -9, 12, \dots$) đều là nghịch đảo của 3 theo môđun 7

Ví dụ 13

Giải phương trình $3x \equiv 4 \pmod 7$

- Từ ví dụ trước, ta biết rằng -2 là một nghịch đảo của 3 theo môđun 7. Nhân cả hai vế của phương trình với -2, ta có
$$-2 \cdot 3x \equiv -2 \cdot 4 \pmod 7$$
- Do $-6 \equiv 1 \pmod 7$ và $-8 \equiv 6 \pmod 7$, nếu x là nghiệm của phương trình thì $x \equiv 6 \pmod 7$
- Thật vậy, với mọi x thỏa mãn $x \equiv 6 \pmod 7$
$$3x \equiv 3 \cdot 6 = 18 \equiv 4 \pmod 7$$

Bài tập 19

Tìm nghịch đảo của a theo môđun m với

(1) $a = 4, m = 9$

(2) $a = 19, m = 141$

(3) $a = 55, m = 89$

(4) $a = 89, m = 232$

Bài tập 20

Giải các phương trình đồng dư

(1) $4x \equiv 5 \pmod{9}$

(2) $19x \equiv 4 \pmod{141}$

(3) $55x \equiv 34 \pmod{89}$

(4) $89x \equiv 2 \pmod{232}$

Bài tập 21

*Cho các số nguyên dương $m_1, m_2, \dots, m_n$ thỏa mãn $m_i \geq 2$ và $\gcd(m_i, m_j) = 1$ với mọi $i \neq j$ và $1 \leq i, j \leq n$. Chứng minh rằng nếu $a \equiv b \pmod{m_i}$ với mọi $1 \leq i \leq n$, thì $a \equiv b \pmod{m}$ với $m = m_1 m_2 \dots m_n$. (**Gợi ý:** Chứng minh với $n = 2$)*

Định lý phần dư Trung Hoa (The Chinese Remainder Theorem) nói rằng nếu các môđun của một hệ các phương trình đồng dư tuyến tính là đôi một nguyên tố cùng nhau thì hệ phương trình có nghiệm duy nhất theo môđun tích của các môđun của từng phương trình

Định lý 16: Định lý phần dư Trung Hoa

Cho các số nguyên dương $m_1, m_2, \dots, m_n$ thỏa mãn $m_i \geq 2$ và $\gcd(m_i, m_j) = 1$ với mọi $i \neq j$ và $1 \leq i, j \leq n$. Cho các số nguyên bất kỳ $a_1, a_2, \dots, a_n$. Hệ phương trình

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

có nghiệm duy nhất theo môđun $m = m_1 m_2 \dots m_n$. (Nghĩa là, tồn tại một nghiệm x với $0 \leq x < m$, và tất cả các nghiệm khác đồng dư với x theo môđun m)

Chứng minh (tồn tại).

- Đặt $M_i = m/m_i$ $(1 \leq i \leq n)$. Do đó $\gcd(M_i, m_i) = 1$
- Theo Định lý 15, tồn tại số nguyên y_i sao cho $y_i M_i \equiv 1 \pmod{m_i}$
- Đặt $x = \sum_{i=1}^{n} a_i y_i M_i = a_1 y_1 M_1 + a_2 y_2 M_2 + \cdots + a_n y_n M_n$
- Do $m_i \mid M_k$ với mọi $k \neq i$, $M_k \equiv 0 \pmod{m_i}$, do đó $x \equiv a_i y_i M_i \equiv a_i \pmod{m_i}$ với mọi i. Do đó x là nghiệm của hệ phương trình đã cho

$\square$

Bài tập 22

*Hoàn thành Chứng minh của Định lý phần dư Trung Hoa bằng cách chỉ ra nghiệm x của hệ phương trình đã cho là duy nhất theo môđun $m = m_1 m_2 \dots m_n$ (**Gợi ý:** Giả sử x và y là hai nghiệm phân biệt của hệ phương trình đã cho. Chứng minh rằng $m_i \mid (x - y)$ với mọi $1 \leq i \leq n$. Sử dụng Bài tập 21 để kết luận rằng $m \mid (x - y)$)*

Ví dụ 14 (Sử dụng Chứng minh của Định lý Phần dư Trung Hoa)

Giải hệ phương trình

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \\ x &\equiv 5 \pmod 7 \end{aligned}$$

Chú ý: $3, 5, 7$ là dãy các số nguyên ≥ 2 và đôi một nguyên tố cùng nhau

- $m = m_1 m_2 m_3 = 3 \cdot 5 \cdot 7 = 105$
- $M_1 = m/m_1 = 35$ và $y_1 = 2$ là một nghịch đảo của M_1 theo môđun $m_1 = 3$
- $M_2 = m/m_2 = 21$ và $y_2 = 1$ là một nghịch đảo của M_2 theo môđun $m_2 = 5$
- $M_3 = m/m_3 = 15$ và $y_3 = 1$ là một nghịch đảo của M_3 theo môđun $m_2 = 7$
- $x = \sum_{i=1}^{3} a_i y_i M_i = 2 \cdot 2 \cdot 35 + 3 \cdot 1 \cdot 21 + 5 \cdot 1 \cdot 15 = 278 \equiv 68 \pmod{105}$

Ví dụ 15 (Phương pháp thay ngược)

Giải hệ phương trình

$$x \equiv 2 \pmod 3 \qquad (1)$$
$$x \equiv 3 \pmod 5 \qquad (2)$$
$$x \equiv 5 \pmod 7 \qquad (3)$$

- Từ (1), tồn tại $t \in \mathbb{Z}$ sao cho $x = 3t + 2$
- Thay vào (2), ta có $3t + 2 \equiv 3 \pmod 5$, suy ra $3t \equiv 1 \pmod 5$, do đó $t \equiv 2 \pmod 5$. Do đó, tồn tại $u \in \mathbb{Z}$ sao cho $t = 5u + 2$. Suy ra, $x = 3t + 2 = 3(5u + 2) + 2 = 15u + 8$
- Thay vào (3), ta có $15u + 8 \equiv 5 \pmod 7$, suy ra $15u \equiv -3 \pmod 7$, do đó $u \equiv 4 \pmod 7$. Do đó, tồn tại $v \in \mathbb{Z}$ sao cho $u = 7v + 4$
- Suy ra $x = 15u + 8 = 15(7v + 4) + 8 = 105v + 68$. Do đó, $x \equiv 68 \pmod{105}$

Bài tập 23

Giải hệ phương trình sau bằng các phương pháp đã đề cập

$$x \equiv 1 \pmod{5} \tag{4}$$
$$x \equiv 2 \pmod{6} \tag{5}$$
$$x \equiv 3 \pmod{7} \tag{6}$$

Bài tập 24

Giải hệ phương trình sau bằng các phương pháp đã đề cập

$$x \equiv 2 \pmod{3} \tag{7}$$
$$x \equiv 1 \pmod{4} \tag{8}$$
$$x \equiv 3 \pmod{5} \tag{9}$$

Bài tập 25

Giải hệ phương trình sau bằng các phương pháp đã đề cập

$$x \equiv 1 \pmod 2 \tag{10}$$
$$x \equiv 2 \pmod 3 \tag{11}$$
$$x \equiv 3 \pmod 5 \tag{12}$$
$$x \equiv 4 \pmod{11} \tag{13}$$

Bài tập 26

Những số nguyên nào chia 2 dư 1 và chia 3 cũng dư 1?

Bài tập 27 ($\star$)

Giải hệ phương trình

$$x \equiv 5 \pmod{6} \tag{14}$$
$$x \equiv 3 \pmod{10} \tag{15}$$
$$x \equiv 8 \pmod{15} \tag{16}$$

Chú ý: 6, 10, *và* 15 *không đôi một nguyên tố cùng nhau*

Định lý phần dư Trung Hoa cho ta một cách thực hiện các tính toán số học với các số nguyên lớn

- Theo Định lý, một số nguyên a với $0 \leq a < m = m_1 m_2 \dots m_n$ trong đó $\gcd(m_i, m_j) = 1$ với mọi $i \neq j$, $1 \leq i, j \leq n$, có thể được biểu diễn thông qua bộ $(a \bmod m_1, a \bmod m_2, \dots, a \bmod m_n)$
- Để thực hiện tính toán với các số nguyên lớn được biểu diễn theo cách này
  - Thực hiện tính toán riêng biệt cho từng bộ
  - Mỗi tính toán có thể được thực hiện trong cùng một máy tính hoặc thực hiện song song
  - Xuất kết quả đầu ra bằng cách giải hệ phương trình đồng dư
  - Có thể thực hiện khi m luôn lớn hơn kết quả đầu ra mong muốn

Định lý 17: Định lý Fermat nhỏ

Nếu p là một số nguyên tố và a là một số nguyên không chia hết cho p, thì $a^{p-1} \equiv 1 \pmod{p}$. Thêm vào đó, với mọi số nguyên a, ta có $a^p \equiv a \pmod{p}$

Bài tập 28 (Chứng minh Định lý Fermat nhỏ)

Nhắc lại: *Với các số nguyên a, b, c và số nguyên dương m, nếu $ac \equiv bc \pmod{m}$ và $\gcd(c, m) = 1$ thì $a \equiv b \pmod{m}$.*

(a) *Giả sử a không chia hết cho p. Chứng minh rằng không có hai số nguyên nào trong số các số $1 \cdot a, 2 \cdot a, \ldots, (p-1) \cdot a$ là đồng dư theo môđun p*

(b) *Từ phần (a), kết luận rằng tích các số $1, 2, \ldots, p-1$ đồng dư với tích các số $a, 2a, \ldots, (p-1)a$ theo môđun p. Sử dụng điều này để chứng minh rằng $(p-1)! \equiv a^{p-1}(p-1)! \pmod{p}$*

(c) *Chỉ ra từ phần (b) rằng $a^{p-1} \equiv 1 \pmod{p}$ nếu a không chia hết cho p. (**Gợi ý:** Xem lại phần chứng minh Định lý cơ bản của số học. Chứng minh $p \nmid (p-1)!$ và áp dụng mệnh đề trên)*

Ví dụ 16 (Tìm số dư của phép chia cho số nguyên tố)

Tìm $7^{222} \bmod 11$

- Theo Định lý Fermat nhỏ, ta có $7^{10} \equiv 1 \pmod{11}$
- Do đó, $(7^{10})^k \equiv 1 \pmod{11}$ với mọi $k \in \mathbb{Z}$
- Mặt khác, $7^{222} = 7^{10\cdot 22+2} = (7^{10})^{22} \cdot 7^2 \equiv 49 \equiv 5 \pmod{11}$

Bài tập 29

Sử dụng Định lý Fermat nhỏ để tính

(a) $7^{121} \bmod 13$

(b) $23^{1002} \bmod 41$

(c) *nghịch đảo của* 5^{39} *theo môđun* 41

Bài tập 30

(a) *Sử dụng Định lý Fermat nhỏ để tính* $5^{2003} \bmod 7$, $5^{2003} \bmod 11$, *và* $5^{2003} \bmod 13$

(b) *Sử dụng kết quả từ phần (a) và Định lý phần dư Trung Hoa để tính* $5^{2003} \bmod 1001$ *(Chú ý rằng* $1001 = 7 \cdot 11 \cdot 13$*)*

Bài tập 31

Sử dụng sự trợ giúp từ Định lý Fermat nhỏ, hãy chứng minh rằng 42 *là ước của* $n^7 - n$

Thuật toán mã hóa RSA

Mật mã khóa công khai

- Trong *mật mã khóa bí mật (private key cryptography)*, một khóa bí mật được sử dụng cả trong việc mã hóa lẫn giải mã các thông điệp
  - Một vấn đề đặt ra là làm sao để *chia sẻ khóa bí mật một cách an toàn*
- Trong *mật mã khóa công khai (public key cryptography)*, hai khóa được sử dụng: một để mã hóa và một để giải mã
  - Thông tin gửi đến có thể được mã hóa bởi bất kỳ ai có khóa công khai, nhưng chỉ có thể được giải mã bởi người sở hữu khóa bí mật
  - Người sở hữu khóa bí mật có thể mã hóa thông tin với khóa bí mật của mình, và bất kỳ ai cũng có thể giải mã thông tin này bằng khóa công khai, và biết rằng chỉ có duy nhất người sở hữu khóa bí mật có thể mã hóa thông tin đó. (Đây là cơ sở của chữ ký điện tử)
- Hệ mã khóa công khai được biết đến nhiều nhất là RSA

Thuật toán mã hóa RSA

RSA - Rivest-Shamir-Adleman

- Chọn hai số nguyên tố lớn phân biệt p, q
- Đặt $n = pq$ và $k = (p-1)(q-1)$
- Chọn số nguyên e thỏa mãn $1 < e < k$ và $\gcd(e, k) = 1$
- Tính nghịch đảo d của e theo môđun k, nghĩa là $de \equiv 1 \pmod{k}$
- **Khóa công khai:** (n, e)
- **Khóa bí mật:** (n, d)
- **Mã hóa:**
  - Chuyển thông điệp M cần mã hóa thành số nguyên m, $0 \leq m < n$
  - Thông điệp mã hóa c được tính bằng $c = m^e \bmod n$ (Việc này có thể được thực hiện một cách hiệu quả. Xem bài giảng trước)
- **Giải mã:**
  - Tính $m = c^d \bmod n$
  - Chuyển m từ số nguyên sang thông điệp M ban đầu

Ví dụ 17

- $n = pq = 43 \cdot 59 = 2537$, $k = 42 \cdot 58 = 2436$
- Chọn $e = 13$: $1 < e < k$ và $\gcd(13, 2436) = 1$
- $d = 937$ là nghịch đảo của 13 theo môđun 2436
- **Khóa công khai:** $(2537, 13)$
- **Khóa bí mật:** $(2537, 937)$

Mã hóa và Giải mã

- Chuyển thông điệp $M =$ STOP gồm các chữ cái thành số nguyên bằng cách gán mỗi chữ cái bằng thứ tự trong bảng chữ cái tiếng Anh trừ đi 1: ST $\Rightarrow 1819$ và OP $\Rightarrow 1415$
- $1819^{13} \bmod 2537 = 2081$ và $1415^{13} \bmod 2537 = 2182$
- Thông điệp mã hóa là $2081\,2182$
- Ví dụ nếu nhận được thông điệp $0981\,0461$
- $0981^{937} \bmod 2537 = 0704$ và $0461^{937} \bmod 2537 = 1115$
- Thông điệp giải mã là HELP

Tính đúng đắn của quá trình giải mã.

Ta chứng minh nếu $c = m^e \bmod n$ thì $m = c^d \bmod n$.

- Ta có $c^d = (m^e)^d \equiv m^{ed} \pmod{n}$
- Theo cách xây dựng, $ed \equiv 1 \pmod{k}$ với $k = (p-1)(q-1)$. Do đó tồn tại số nguyên h thỏa mãn $ed - 1 = h(p-1)(q-1)$
- Ta xét $m^{ed} \bmod p$. Nếu $p \nmid m$ thì theo Định lý Fermat nhỏ, ta có

$$\begin{aligned} m^{ed} &= m^{h(p-1)(q-1)}m = (m^{p-1})^{h(q-1)}m \\ &\equiv 1^{h(q-1)}m \equiv m \pmod{p} \end{aligned}$$

  Nếu $p \mid m$, ta có $m^{ed} \equiv 0 \equiv m \pmod{p}$. Tóm lại, $m^{ed} \equiv m \pmod{p}$. Tương tự, ta có $m^{ed} \equiv m \pmod{q}$
- Do $\gcd(p,q) = 1$, sử dụng Định lý phần dư Trung Hoa, ta có $m^{ed} \equiv m \pmod{pq}$
  - Do $\gcd(p,q) = 1$, theo Định lý Bézout, tồn tại $s, t \in \mathbb{Z}$ thỏa mãn $sp + tq = 1$. Đặt $x = m \cdot sp + m \cdot tq$ thì $x \bmod p = (m \cdot sp + m \cdot (1 - sp)) \bmod p = m \bmod p$. Suy ra $x \equiv m \pmod{p}$. Tương tự, $x \equiv m \pmod{q}$
  - Theo Định lý phần dư Trung Hoa, $x \equiv m^{ed} \pmod{pq}$, hay $m^{ed} \equiv m \pmod{pq} \equiv m \pmod{n}$

□

Tài liệu tham khảo

Agrawal, Manindra, Neeraj Kayal, and Nitin Saxena (2004). "PRIMES is in P". In: *Annals of Mathematics* 160.2, pp. 781–793. DOI: 10.4007/annals.2004.160.781.