Số học

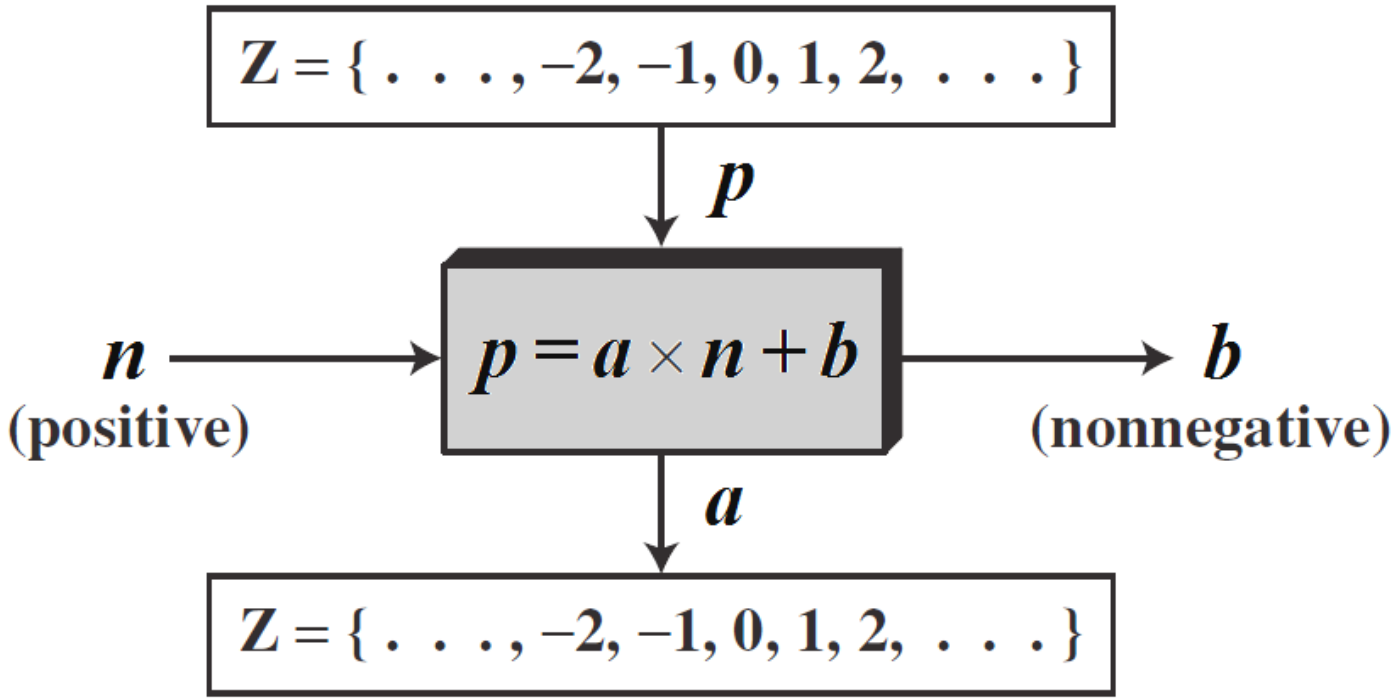
Khoa CNTT

Trường Đại học Phenikaa

Số học (4 tiết)

1. Số nguyên và Phép chia
2. Số học modular (mô-đun) và ứng dụng
3. Biểu diễn số nguyên

1. Số nguyên và Phép chia



1.1. Số nguyên

- Lý thuyết số là một nhánh của toán học. Trong đó, chúng ta tìm hiểu về số nguyên và các đặc điểm của chúng.
- Tập hợp số nguyên được kí hiệu là $\mathbb{Z}$, bao gồm các số $\{..., -2, -1, 0, 1, 2, ...\}$. Tập hợp số nguyên dương được kí hiệu là $\mathbb{Z}^+$, bao gồm các số $\{1, 2, ...\}$.
- Lý thuyết số có nhiều ứng dụng trong ngành CNTT:
  - Indexing (đánh chỉ số) - Lưu trữ và tổ chức dữ liệu
  - Encryption (mã hóa) - Bảo mật thông tin

1.2. Phép chia hết

- **Định nghĩa:**
  Cho 2 số nguyên a và b, sao cho $a \neq 0$. Ta nói rằng, a **chia hết** b (hoặc b **chia hết cho** a) nếu tồn tại một số nguyên c sao cho $b = ac$. Khi đó,
  - a là ước số (gọi tắt là **ước**) của b và b là bội số (gọi tắt là **bội**) của a.
  - kí hiệu là $a \mid b$.

    Ví dụ:
    - $4 \mid 24 \rightarrow$ Đúng
      4 là ước của 24
      24 là bội của 4
    - $3 \mid 7 \rightarrow$ Sai

1.2. Phép chia hết

- **Các tính chất của phép chia:**
  Cho 3 số nguyên a, b và c. Khi đó,
  1. Nếu $a \mid b$ và $a \mid c$ thì $a \mid (b + c)$.
     Chứng minh 1:
     Từ định nghĩa của phép chia ta có: $b = au$ và $c = av$, với u, v là hai số nguyên.
     $\Longrightarrow$ $b + c = au + av = a(u + v)$
     $\Longrightarrow$ a chia hết $b + c$

1.2. Phép chia hết

- **Các tính chất của phép chia:**
  Cho 3 số nguyên a, b và c. Khi đó,
  1. Nếu $a \mid b$ và $a \mid c$ thì $a \mid (b + c)$.
  2. Nếu $a \mid b$ thì $a \mid bc$ với mọi số nguyên c.
     Chứng minh 2:
     ...

1.2. Phép chia hết

- **Các tính chất của phép chia:**
  Cho 3 số nguyên a, b và c. Khi đó,
  1. Nếu $a \mid b$ và $a \mid c$ thì $a \mid (b + c)$.
  2. Nếu $a \mid b$ thì $a \mid bc$ với mọi số nguyên c.
  3. Nếu $a \mid b$ và $b \mid c$ thì $a \mid c$.

     Chứng minh 3:

     ...

1.3. Số nguyên tố và Hợp số

- **Định nghĩa:**
  - Số nguyên dương lớn hơn 1 và chỉ chia hết cho 1 và chính nó được gọi là **số nguyên tố**.
    Ví dụ: 2, 3, 5, 7, 11, 13, ...
  - Số nguyên dương lớn hơn 1 mà không phải là số nguyên tố được gọi là **hợp số**.
    Ví dụ: 4, 6, 8, 9, 10, 12, ...

- **Phân tích một số nguyên ra thừa số nguyên tố:**

Định lý 2.1

Mọi số nguyên dương lớn hơn 1 đều có thể biểu diễn được dưới dạng một tích các số nguyên tố.

Ví dụ:

$12 = 2 \times 2 \times 3 = 2^2 \times 3$

$21 = 3 \times 7$

$100 = 2 \times 2 \times 5 \times 5 = 2^2 \times 5^2$

$99 = 3 \times 3 \times 11 = 3^2 \times 11$

1.3. Số nguyên tố và Hợp số

- **Xác định một số là số nguyên tố hay hợp số:**
  1. Xét số nguyên n. Để xác định xem n có phải số nguyên tố hay không, ta có thể xét phép chia n cho các **số nguyên** $x \in (1, n)$.
     - Nếu n chia hết cho một số x nào đó thì n là hợp số.
     - Nếu n không chia hết cho bất cứ số x nào thì n là số nguyên tố.

     Ví dụ:
     Để kiểm tra xem 17 có phải là số nguyên tố hay không, ta cần phải xét phép chia của 17 cho các số 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16.

1.3. Số nguyên tố và Hợp số

- **Xác định một số là số nguyên tố hay hợp số:**
  1. Xét số nguyên n. Để xác định xem n có phải số nguyên tố hay không, ta có thể xét phép chia n cho các **số nguyên** $x \in (1, n)$.
     - Nếu n chia hết cho một số x nào đó thì n là hợp số.
     - Nếu n không chia hết cho bất cứ số x nào thì n là số nguyên tố.

Thảo luận

- Đây đã phải cách nhanh nhất chưa?
- Có nhất thiết phải xét tất cả các số $1 < x < n$?
- Có cách nào khác nhanh hơn không?

1.3. Số nguyên tố và Hợp số

- **Xác định một số là số nguyên tố hay hợp số:**
  1. Xét số nguyên n. Để xác định xem n có phải số nguyên tố hay không, ta có thể xét phép chia n cho các **số nguyên** $x \in (1, n)$.

  2. Xét số nguyên n. Để xác định xem n có phải số nguyên tố hay không, ta có thể xét phép chia n cho các **số nguyên tố** $x < n$.
     Ví dụ:
     Để kiểm tra xem 17 có phải là số nguyên tố hay không, ta cần phải xét phép chia của 17 cho các số 2,3,5,7,11,13.

1.3. Số nguyên tố và Hợp số

- **Xác định một số là số nguyên tố hay hợp số:**
  1. Xét số nguyên n. Để xác định xem n có phải số nguyên tố hay không, ta có thể xét phép chia n cho các **số nguyên** $1 < x < n$.
  2. Xét số nguyên n. Để xác định xem n có phải số nguyên tố hay không, ta có thể xét phép chia n cho các **số nguyên tố** $x < n$.

Thảo luận

- Có bao nhiêu số nguyên tố $x < n$?
- Việc tìm tất cả các số nguyên tố x khi n là một số rất lớn phức tạp như thế nào?
- Có cách nào khác nhanh hơn không?

Định lý 2.2

Nếu n là hợp số thì n có một ước nguyên tố nhỏ hơn hoặc bằng $\sqrt{n}$.

Định lý 2.2

Nếu n là hợp số thì n có một ước nguyên tố nhỏ hơn hoặc bằng $\sqrt{n}$.

Chứng minh:

Nếu n là hợp số thì n có một ước a sao cho $1 < a < n$. Nghĩa là, $n = ab$, với b là một số nguyên lớn hơn 1.

Nếu $a > \sqrt{n}$ và $b > \sqrt{n}$ thì $ab > \sqrt{n} \times \sqrt{n} = n \implies$ Vô lý. Vậy $a \leq \sqrt{n}$ hoặc $b \leq \sqrt{n}$.

$\implies$ n có một ước nhỏ hơn $\sqrt{n}$. Giả sử là a.

- a là số nguyên tố $\implies$ Điều phải chứng minh.
- a là hợp số. Theo Định lý 1.1, a có thể phân tích được thành tích số nguyên tố nhỏ hơn nó. Và các ước nguyên tố của a cũng chính là ước nguyên tố của n $\implies$ Điều phải chứng minh.

1.3. Số nguyên tố và Hợp số

- **Xác định một số là số nguyên tố hay hợp số:**
  1. Xét số nguyên n. Để xác định xem n có phải số nguyên tố hay không, ta có thể xét phép chia n cho các **số nguyên** $x \in (1, n)$.
  2. Xét số nguyên n. Để xác định xem n có phải số nguyên tố hay không, ta có thể xét phép chia n cho các **số nguyên tố** $x < n$.
  3. Xét số nguyên n. Để xác định xem n có phải số nguyên tố hay không, ta có thể xét phép chia n cho các **số nguyên tố** $x < \sqrt{n}$.
     Ví dụ:
     Để kiểm tra xem 17 có phải là số nguyên tố hay không, ta cần phải xét phép chia của 17 cho các số 2,3 vì $\sqrt{17} = 4.xx$.
     $\Longrightarrow$ 17 là số nguyên tố.
     Để kiểm tra xem 101 có phải là số nguyên tố hay không, ta cần phải xét phép chia của 101 cho các số 2,3,5,7 vì $\sqrt{101} = 10.xx$.
     $\Longrightarrow$ 101 là số nguyên tố.

1.3. Số nguyên tố và Hợp số

Thảo luận

- Có bao nhiêu số nguyên tố?
- Số nguyên tố lớn nhất là số nào?

1.3. Số nguyên tố và Hợp số

Thảo luận

- Có bao nhiêu số nguyên tố?
- Số nguyên tố lớn nhất là số nào?

Định lý 2.3

Có vô số số nguyên tố.

Định lý 2.3

Có vô số số nguyên tố.

Chứng minh:

Giả sử có hữu hạn số nguyên tố là: $p_1, p_2, ..., p_n$ và p_n là số nguyên tố lớn nhất.

Xét số nguyên $Q = p_1 p_2 ... p_n + 1$. Hiển nhiên, $Q > p_n$.

Theo giả thiết, Q không là số nguyên tố.

Tuy nhiên, Q không chia hết cho bất kỳ số nguyên tố nào trong tập hợp hữu hạn các số nguyên tố $\{p_1, p_2, ..., p_n\}$.

$\Longrightarrow$ Q là số nguyên tố.

$\Longrightarrow$ Mâu thuẫn

$\Longrightarrow$ Giả sử ban đầu sai.

1.4. Phép chia có dư

Cho a là một số nguyên và b là một số nguyên dương. Khi đó, tồn tại duy nhất số nguyên q và số nguyên r, sao cho $0 \leq r < b$, sao cho:

$$a = bq + r$$

- **Định nghĩa:**
  - a được gọi là **số bị chia**.
  - b được gọi là **số chia**.
  - q được gọi là **thương**.
  - r được gọi là **số dư**.
- **Kí hiệu:**
  - $q = a \div b$
  - $r = a \mod b$

1.5. Ước chung lớn nhất

- **Định nghĩa:**
  Cho a và b là các số nguyên, a, b không cùng bằng 0. Số nguyên lớn nhất d sao cho $d \mid a$ và $d \mid b$ được gọi là **ước chung lớn nhất** của a và b.
- **Kí hiệu:**
  Ước chung lớn nhất của a và b được kí hiệu là: $\gcd(a, b)$.

Thảo luận

Cho 2 số nguyên a và b. Tìm $\gcd(a, b)$.

Ví dụ:

$\gcd(24, 36) = ?$

Thảo luận

Cho 2 số nguyên a và b. Tìm $\gcd(a, b)$.

- **Tìm ước chung lớn nhất của 2 số:**
  1. Liệt kê các ước của từng số và tìm ra ước số giống nhau lớn nhất:
     Ví dụ:
     Các ước của 24 là: 2,3,4,6,12
     Các ước của 36 là: 2,3,4,6,9,12
     $\Longrightarrow \gcd(24, 36) = 12$

1.5. Ước chung lớn nhất

- **Tìm ước chung lớn nhất của 2 số:**
  1. Liệt kê các ước của từng số và tìm ra ước số giống nhau lớn nhất.
  2. Phân tích 2 số đã cho thành tích các thừa số nguyên tố:
     Giả sử $a = p_1^{a_1} p_2^{a_2} p_3^{a_3} ... p_k^{a_k}$ và $b = p_1^{b_1} p_2^{b_2} p_3^{b_3} ... p_k^{b_k}$
     với $p_1, p_2, ..., p_k$ là các số nguyên tố.
     $\Longrightarrow \gcd(a, b) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} p_3^{\min(a_3, b_3)} ... p_k^{\min(a_k, b_k)}$
     Ví dụ:
     $24 = 2^3 \times 3$
     $36 = 2^2 \times 3^2$
     $\gcd(24, 36) = 2^2 \times 3 = 12$

Thảo luận

Khi 2 số nguyên a và b rất lớn thì việc tìm $\gcd(a, b)$ bằng cách liệt kê các ước của a và b, hoặc phân tích a và b thành tích các thừa số nguyên tố có khả quan hay không?

1.5. Ước chung lớn nhất

- **Tìm ước chung lớn nhất của 2 số:**
  1. Liệt kê các ước của từng số và tìm ra ước số giống nhau lớn nhất.
  2. Phân tích 2 số đã cho thành tích các thừa số nguyên tố.
  3. Thuật toán Euclid:

     Ví dụ:

     Tìm $\gcd(287, 91)$.
     - $287 = 91 \times 3 + 14$

       Giả sử a là ước chung của 287 và 91, b là ước chung của 91 và 14.

       $a \mid 287$ và $a \mid (91 \times 3) \implies a$ là ước của 14. (1)

       $b \mid 14$ và $b \mid (91 \times 3) \implies b$ là ước của 287. (2)

       (1) và (2) $\implies$ mọi ước chung của 287 và 91 đều là ước chung của 91 và 14 và ngược lại.

       $\implies \gcd(287, 91) = \gcd(91, 14)$
     - $91 = 14 \times 6 + 7$

       Tương tự ta có: $\implies \gcd(287, 91) = \gcd(91, 14) = \gcd(14, 7)$
     - $14 = 7 \times 2 + 0$

       Tương tự ta có:

       $\implies \gcd(287, 91) = \gcd(91, 14) = \gcd(14, 7) = \gcd(7, 0) = 7$

1.5. Ước chung lớn nhất

- **Tìm ước chung lớn nhất của 2 số:**
  1. Liệt kê các ước của từng số và tìm ra ước số giống nhau lớn nhất.
  2. Phân tích 2 số đã cho thành tích các thừa số nguyên tố.
  3. Thuật toán Euclid:

     Bài tập 2.1:

     1. Tìm gcd(666,558) bằng 2 cách vừa học.
     2. Tìm gcd(286,503) bằng 2 cách vừa học.

1.6. Bội chung nhỏ nhất

- **Định nghĩa:**
  Cho a và b là các số nguyên dương. Số nguyên nhỏ nhất d sao cho $a \mid d$ và $b \mid d$ được gọi là **bội chung nhỏ nhất** của a và b.
- **Kí hiệu:**
  Bội chung nhỏ nhất của a và b được kí hiệu là: $\text{lcm}(a, b)$.

1.6. Bội chung nhỏ nhất

- **Tìm bội chung nhỏ nhất của 2 số:**
  1. Phân tích 2 số đã cho thành tích các thừa số nguyên tố:
     Giả sử $a = p_1^{a_1} p_2^{a_2} p_3^{a_3} ... p_k^{a_k}$ và $b = p_1^{b_1} p_2^{b_2} p_3^{b_3} ... p_k^{b_k}$
     với $p_1, p_2, ..., p_k$ là các số nguyên tố.
     $\Longrightarrow \text{lcm}(a, b) = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} p_3^{\max(a_3,b_3)} ... p_k^{\max(a_k,b_k)}$
     Ví dụ:
     $24 = 2^3 \times 3$
     $36 = 2^2 \times 3^2$
     $\text{lcm}(24, 36) = 2^3 \times 3^2 = 72$

1.6. Bội chung nhỏ nhất

- **Tìm bội chung nhỏ nhất của 2 số:**
  1. Phân tích 2 số đã cho thành tích các thừa số nguyên tố.
  2. Sử dụng thuật toán Euclid để tìm Ước chung lớn nhất rồi áp dụng công thức:
     $\text{lcm}(a, b) = \frac{ab}{\gcd(a,b)}$

2. Số học modular (mô-đun) và ứng dụng

Trong đời sống, đặc biệt là trong ngành CNTT, đôi khi chúng ta thường quan tâm tới số dư trong phép chia một số nguyên cho một số nguyên (khác 0) hơn là thương của phép chia đó.

Ví dụ:

Hỏi: Giả sử bây giờ là nửa đêm. Sau 50 giờ nữa là mấy giờ?

Đáp: 2 giờ sáng.

2 chính là số dư trong phép chia 50 cho 24. Và ở câu hỏi này, người hỏi không quan tâm thương là bao nhiêu.

2.1. Phép đồng dư

- **Định nghĩa:**
  Cho a và b là các số nguyên, m là một số nguyên dương. Ta nói: "a **đồng dư với** b **theo modulo** m" nếu $a - b$ chia hết cho m.
  Ví dụ: 17 đồng dư với 5 theo modulo 6 vì 6 | (17-5).
- **Kí hiệu:**
  - $a = b \pmod{m}$ nếu a và b đồng dư theo modulo m.
  - $a \neq b \pmod{m}$ nếu a và b không đồng dư theo modulo m.
    Ví dụ:
    $17 = 5 \pmod{6}$
    $23 \neq 5 \pmod{4}$

Định lý 2.4

Cho a và b là các số nguyên, m là một số nguyên dương.
$a = b \pmod{m}$ khi và chỉ khi $a \mod m = b \mod m$.

Định lý 2.4

Cho a và b là các số nguyên, m là một số nguyên dương.
$a = b \pmod{m}$ khi và chỉ khi $a \mod m = b \mod m$.

Chứng minh:

- $a = b \pmod{m} \rightarrow a \mod m = b \mod m$
  Theo định nghĩa, $a = b \pmod{m}$ nên $m \mid (a - b)$.
  Giả sử $a - b = mk$ và $a = mu + r$, với $0 \leq r < m$.
  $\Longrightarrow b = a - mk = (mu + r) - mk = (mu - mk) + r = m(u - k) + r$
  $\Longrightarrow a \mod m = b \mod m (= r)$

Định lý 2.4

Cho a và b là các số nguyên, m là một số nguyên dương.
$a = b \pmod{m}$ khi và chỉ khi $a \mod m = b \mod m$.

Chứng minh:

- $a = b \pmod{m} \rightarrow a \mod m = b \mod m$
  Theo định nghĩa, $a = b \pmod{m}$ nên $m \mid (a - b)$.
  Giả sử $a - b = mk$ và $a = mu + r$, với $0 \leq r < m$.
  $\Longrightarrow b = a - mk = (mu + r) - mk = (mu - mk) + r = m(u - k) + r$
  $\Longrightarrow a \mod m = b \mod m (= r)$
- $a = b \pmod{m} \leftarrow a \mod m = b \mod m$
  Giả sử $a = mu + r$ và $b = mv + r$ với $0 \leq r < m$.
  $\Longrightarrow a - b = (mu + r) - (mv + r) = m(u - v)$
  $\Longrightarrow m \mid (a - b)$
  $\Longrightarrow a = b \pmod{m}$

Định lý 2.5

Cho m là một số nguyên dương. Hai số nguyên a và b đồng dư với nhau theo modulo m khi và chỉ khi tồn tại một số nguyên k sao cho $a = b + mk$.

Bài tập 2.2:
Chứng minh Định lý 2.5

Định lý 2.6

Cho m là một số nguyên dương. Nếu $a = b \pmod{m}$ và $c = d \pmod{m}$ thì:
$a + c = b + d \pmod{m}$ và $ac = bd \pmod{m}$

Bài tập 2.3:
Chứng minh Định lý 2.6

Hệ quả 2.1

Cho m là một số nguyên dương và a, b là các số nguyên.
$(a + b) \mod m = ((a \mod m) + (b \mod m)) \mod m$
$ab \mod m = ((a \mod m)(b \mod m)) \mod m$

Bài tập 2.4:
Chứng minh Hệ quả 2.1

2.2. Ứng dụng số học modular trong CNTT

Số học modular và đồng dư có rất nhiều ứng dụng trong ngành CNTT:

1. Bộ sinh số ngẫu nhiên (Pseudorandom number generators)
2. Hàm băm (Hash function)
3. Mật mã học (Cryptology)

2.2.1 Bộ sinh số ngẫu nhiên (Pseudorandom number generators)

- Kết quả ngẫu nhiên là một phần không thể thiếu trong đời sống thường ngày.
  Ví dụ: kết quả nhận được của các lần tung đồng xu hoặc xúc xắc, kết quả xổ số hàng ngày, những lá bài bạn nhận được trong mỗi ván bài,...
- Rất nhiều vấn đề đòi hỏi chương trình máy tính mô phỏng lại sự lựa chọn ngẫu nhiên. Tuy nhiên, mô phỏng lại sự ngẫu nhiên của thực tế cuộc sống là không thể. Bởi nếu có cách để tạo ra một kết quả mà ta cho rằng đó là ngẫu nhiên thì kết quả đó không phải là ngẫu nhiên.
- Bộ sinh ngẫu nhiên cung cấp cho chúng ta các kết quả "nhìn có vẻ" ngẫu nhiên.
  Ví dụ: mật khẩu được TTCNTT cấp để vào email Phenikaa, mật khẩu được gợi ý bởi Google khi tạo một tài khoản Gmail mới,...

2.2.1 Bộ sinh số ngẫu nhiên (Pseudorandom number generators)

Thảo luận

- Giả sử rằng sau mỗi lần lựa chọn, giá trị trả về là một số nguyên nào đó trong tập $\{0, 1, ..., m\}$.
- Làm sao để tạo ra một dãy kết quả "nhìn có vẻ" ngẫu nhiên sau k lần lựa chọn.

2.2.1 Bộ sinh số ngẫu nhiên (Pseudorandom number generators)

Phương pháp đồng dư tuyến tính:
Đây là thuật toán sinh ngẫu nhiên cổ điển nhất và phổ biến nhất được sử dụng. Thuật toán này được tích hợp sẵn trong các thư viện sinh ngẫu nhiên của các ngôn ngữ lập trình như Pascal, C/C++, Java và C#.

Phương pháp bao gồm 4 tham số chính:

- $m, 0 < m$: modulo, thường là một số lớn.
- $a, 2 \leq a < m$: hằng số nhân.
- $c, 0 \leq a < m$: hằng số cộng thêm.
- $x_0, 0 \leq x_0 < m$: giá trị khởi tạo.

2.2.1 Bộ sinh số ngẫu nhiên (Pseudorandom number generators)

Phương pháp đồng dư tuyến tính:

Các số $x_1, x_2, x_3, ..., x_k \in [0, m-1]$ được tạo ra bằng cách sử dụng công thức đồng dư:

$$x_{k+1} = (ax_k + c) \mod m$$

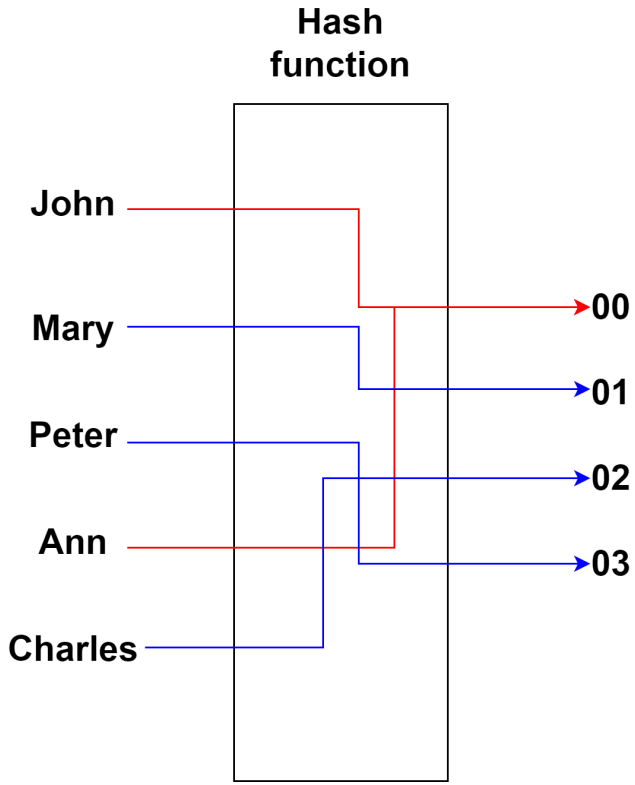
Ví dụ:

Chọn: $m = 9, a = 7, c = 4, x_0 = 3$

- $x_1 = 7 \times 3 + 4 \mod 9 = 25 \mod 9 = 7$
- $x_2 = 7 \times 7 + 4 \mod 9 = 53 \mod 9 = 8$
- $x_3 = 7 \times 8 + 4 \mod 9 = 60 \mod 9 = 6$
- $x_4 = 7 \times 6 + 4 \mod 9 = 46 \mod 9 = 1$
- $x_5 = 7 \times 1 + 4 \mod 9 = 11 \mod 9 = 2$
- $x_6 = 7 \times 2 + 4 \mod 9 = 18 \mod 9 = 0$
- ...

2.2.2 Hàm băm (Hash function)

- Hàm băm là một thuật toán dùng để ánh xạ một tập dữ liệu có độ dài tùy ý thành một tập dữ liệu có độ dài xác định.
- Giá trị trả về bởi hàm băm được gọi là giá trị băm (hash values hoặc hash codes).



2.2.2 Hàm băm (Hash function)

Xét số nguyên k rất lớn và tập các số nguyên $\{0, 1, 2, ..., m-1\}$.

Hàm băm:

$$h(k) = k \mod m$$

ánh xạ số nguyên k tới một giá trị trong tập $\{0, 1, 2, ..., m-1\}$ và giá trị này nhỏ hơn nó rất nhiều.

2.2.2 Hàm băm (Hash function)

Ví dụ:
Giả sử ta có rất nhiều bộ hồ sơ nhập học của sinh viên trường ĐH Phenikaa. Mỗi sinh viên được xác định duy nhất bởi một mã số - dãy số gồm 8 chữ số. Ta muốn lưu trữ các bộ hồ sơ dựa trên mã số này trong một tủ có số lượng ngăn kéo nhất định (không chiếc tủ nào có đủ ngăn kéo để đựng mỗi bộ hồ sơ một ngăn). Sử dụng hàm $h(k)$ nêu trên, ta có thể ánh xạ một mã số với số thứ tự của một ngăn tủ nào đó.

Với $m = 111$, ta có: $h(k) = k \mod 111$
Mã số: 064212848 $\Longrightarrow$ $h(064212848) = 064212848 \mod 111 = 14$
Mã số: 037149212 $\Longrightarrow$ $h(037149212) = 037149212 \mod 111 = 65$

2.2.2 Hàm băm (Hash function)

Thảo luận

Nếu có một bộ hồ sơ mới được cất vào trong một ngăn tủ đã có các bộ hồ sơ khác thì sắp xếp chúng như thế nào để tìm kiếm thuận lợi?

Giải pháp:

1. **Phương pháp dò tuyến tính**: cố gắng tìm ra một ngăn tủ gần nhất còn trống nào đó.
   $h_0(k) = k \mod m$
   $h_1(k) = (k+1) \mod m$
   ...
   $h_n(k) = (k+n) \mod m$

2.2.2 Hàm băm (Hash function)

Thảo luận

Nếu có một bộ hồ sơ mới được cất vào trong một ngăn tủ đã có bộ hồ sơ khác thì sắp xếp chúng như thế nào để tìm kiếm thuận lợi?

Giải pháp:

1. **Phương pháp dò tuyến tính**: cố gắng tìm ra một ngăn tủ gần nhất còn trống nào đó.
2. **Phương pháp nối kết**: ứng với mỗi địa chỉ của ngăn tủ, ta có một danh sách liên kết chứa mã số của các bộ hồ sơ khác nhau.

2.2.3 Mật mã học (Cryptology)

- Trong bảo mật thông tin, các gói tin cần được mã hóa để tránh bị tấn công trong quá trình gửi/nhận giữa các người dùng.
- **Mã Ceasar** là một trong những kỹ thuật mã hóa đơn giản và phổ biến nhất. Đây là dạng mật mã thay thế, trong đó mỗi ký tự trên văn bản gốc sẽ được thay bằng một ký tự khác, có vị trí cách nó một khoảng xác định trong bảng ký tự.

2.2.3 Mật mã học (Cryptology)

Giả sử bảng kí tự có m phần tử. Chúng được sắp xếp theo một trật tự nào đó và ta đánh số thứ tự vị trí của chúng từ 0 đến $m-1$.
Ta có thể sử dụng hàm:

$$f(p) = (p+n) \mod m$$

để mã hóa một văn bản chỉ chứa các kí tự trong tập nêu trên. Trong đó, $p \in \{0, 1, ..., m-1\}$ là thứ tự của kí tự trong tập kí tự gốc, n là khoảng cách dịch chuyển.

Bài tập 2.5:
Giả sử chọn $n = 3$ và xét tập các chữ cái tiếng Anh. Viết kết quả khi mã hóa câu:
I LIKE DISCRETE MATH

3. Biểu diễn số nguyên

- Trong cuộc sống hiện tại, chúng ta sử dụng **hệ thập phân** (hay **cơ số 10**), để biểu diễn số nguyên.
  Ví dụ:
  Ta viết số 965, nghĩa là: $9 \times 10^2 + 6 \times 10^1 + 5 \times 10^0$.
- Chúng ta có thể biểu diễn các số nguyên bằng bất kỳ một hệ cơ số b nào đó, với $b \in \mathbb{Z}, b > 1$.
- Các hệ cơ số $b = 2$ (**nhị phân/binary**), $b = 8$ (**bát phân/octal**) và $b = 16$ (**hexadecimal**) là các hệ cơ số quan trọng được sử dụng trong máy tính.
- Fun fact: Người Maya cổ đại sử dụng hệ cơ số 20 và người Babylon sử dụng hệ đếm cơ số 60.

3. Biểu diễn số nguyên

- Chúng ta có thể biểu diễn các số nguyên bằng bất kỳ một hệ cơ số b nào đó, với $b \in \mathbb{Z}, b > 1$.

Định lý 2.7

Cho b là một số nguyên dương lớn hơn 1. Nếu n là một số nguyên dương thì n có thể được biểu diễn một cách duy nhất dưới dạng sau:

$$n = a_k b^k + a_{k-1} b^{k-1} + ... + a_1 b + a_0$$

trong đó: k là số nguyên không âm, $a_0, a_1, ..., a_k$ là số nguyên không âm nhỏ hơn b và $a_k \neq 0$. Ta gọi a_j, với $(j = 0, ..., k)$, là các chữ số theo hệ cơ số b trong biểu diễn số n.

- Số n sau khi phân tích theo Định lý 2.7 được ký hiệu là: $(a_k a_{k-1} ... a_1 a_0)_b$.

3.1. Hệ nhị phân

Phần lớn máy tính hiện nay biểu diễn số nguyên và tính toán bằng hệ nhị phân. Trong hệ cơ số này, chỉ có 2 chữ số 0 và 1 được sử dụng.

Ví dụ:

Tìm biểu diễn thập phân của số sau: $(11011)_2$.

3.2. Hệ bát phân/octal

Trong hệ cơ số này, các số được biểu diễn bởi các chữ số $\{0, 1, 2, 3, 4, 5, 6, 7\}$.

Ví dụ:

Tìm biểu diễn thập phân của số sau: $(7016)_8$.

3.2. Hệ bát phân/octal

Trong hệ cơ số này, các số được biểu diễn bởi các chữ số $\{0, 1, 2, 3, 4, 5, 6, 7\}$.

Ví dụ:

Tìm biểu diễn thập phân của số sau: $(7016)_8$.

Giải:

$(7016)_8 = 7 \times 8^3 + 0 \times 8^2 + 1 \times 8^1 + 6 \times 8^0 = 3598$

Bài tập 2.7:

Tìm biểu diễn thập phân của số sau: $(16372)_8$

3.3. Hệ cơ số 16/hexadecimal

Trong hệ cơ số này, các số được biểu diễn bởi các chữ số, chữ cái $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F\}$.
Trong đó, A đến F biểu diễn các số 10 đến 15.

Ví dụ:

Tìm biểu diễn thập phân của số sau: $(2AE0B)_{16}$.

3.3. Hệ cơ số 16/hexadecimal

Trong hệ cơ số này, các số được biểu diễn bởi các chữ số, chữ cái $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F\}$.
Trong đó, A đến F biểu diễn các số 10 đến 15.

Ví dụ:

Tìm biểu diễn thập phân của số sau: $(2AE0B)_{16}$.

Giải:

$(2AE0B)_{16} = 2 \times 16^4 + 10 \times 16^3 + 14 \times 16^2 + 0 \times 16^1 + 11 \times 16^0 = 175627$

Bài tập 2.8:

Tìm biểu diễn thập phân của số sau: $(C5F1D2)_{16}$

3.4. Chuyển đổi hệ cơ số

Để chuyển đổi một số thập phân n sang hệ cơ số b nào đó, ta làm như sau:

- Chia n cho b để lấy thương và số dư.
  $n = bq_0 + a_0 \quad (0 \leq a_0 < b)$
- Số dư a_0 sẽ là chữ số tận cùng bên phải của số n trong biểu diễn cơ số b. Tiếp theo, chia q_0 cho b.
  $q_0 = bq_1 + a_1 \quad (0 \leq a_1 < b)$
- Số dư a_1 sẽ là chữ số thứ hai tính từ phải sang của số n trong biểu diễn cơ số b. Tiếp theo, chia q_1 cho b.

  ...
- Tiếp tục lấy thương chia cho b và lấy số dư thêm vào biểu diễn cơ số b của n (theo chiều từ phải sang trái) cho tới khi thương bằng 0 thì dừng lại.

Ví dụ:
Biểu diễn số 12345 theo hệ cơ số 8.
Giải:
$12345 = 8 \times 1543 + 1$
$1543 = 8 \times 192 + 7$
$192 = 8 \times 24 + 0$
$24 = 8 \times 3 + 0$
$3 = 8 \times 0 + 3$
$\Longrightarrow (12345)_{10} = (30071)_8$