Thuật toán Euclid

Số nguyên tố (prime)

- **Định nghĩa:** Một số nguyên dương *p* lớn hơn 1 và chỉ chia hết cho 1 và chính nó được gọi là một **số nguyên tố**.
- **Ví dụ:** 2, 3, 5, 7,…

  1|2 và 2|2; 1|3 và 3|3;…

  Số nguyên tố tiếp theo sau 7?

  - 11

  Tiếp theo?

  - 13

Số nguyên tố

- **Định nghĩa:** Một số nguyên dương lớn hơn 1 và không phải là số nguyên tố gọi là **một hợp số (composite number)**.
- **Ví dụ:** 4, 6, 8, 9,…
  Vì sao?
  - 2|4

  Vì sao 6 là hợp số?

Định lý cơ bản của số học (arithmetic)

- **Định lý Cơ bản của Số học:**
  - Bất cứ số nguyên dương lớn hơn 1 nào đều có thể được biểu diễn dưới dạng tích của các số nguyên tố.
- **Ví dụ:**
  - $12 = 2 \times 2 \times 3$
  - $21 = 3 \times 7$
- Quy trình tìm ra các thừa số: **phân tích thừa số (factorization)**

Số nguyên tố và Hợp số

- **Phân tích thừa số nguyên tố của các hợp số:**
  - $100 = 2 \times 2 \times 5 \times 5 = 2^2 \times 5^2$
  - $99 = 3 \times 3 \times 11 = 3^2 \times 11$
- **Câu hỏi quan trọng:**
  - Làm thế nào để xác định một số là số nguyên tố hay hợp số?

Số nguyên tố và Hợp số

- Làm thế nào để xác định một số là số nguyên tố hay hợp số?
- **Phương pháp đơn giản (1):**
  - Để xác định một số n có phải là số nguyên tố không, ta có thể kiểm tra với **một số *x*** nào đó $x < n$ và n chia hết cho x. **Nếu đúng thì nó là hợp số.**
  - Nếu ta kiểm tra hết **tất cả các số** $x < n$ và không tìm thấy một số chia nào thì n là số nguyên tố.
  - **Ví dụ:**
    Giả sử ta muốn kiểm tra 17 có phải là số nguyên tố?
    Phương pháp trên yêu cầu ta phải kiểm tra:
    2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16

Số nguyên tố và Hợp số

- **Ví dụ Phương pháp 1:**
  Giả sử ta muốn kiểm tra 17 có phải là số nguyên tố?
  Phương pháp trên yêu cầu ta phải kiểm tra:
  2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16
- **Đây có phải là cách tốt nhất không?**
  - **Không**. Vấn đề ở đây là chúng ta phải kiểm tra tất cả các số và điều này là không cần thiết.
- **Ý tưởng:**
  - Tất cả các hợp số đều có thể được phân tích thành tích của các thừa số nguyên tố. Do đó, chỉ cần kiểm tra các số nguyên tố $x < n$ để xác định n có phải số nguyên tố hay không.

Số nguyên tố và Hợp số

- Làm thế nào để xác định một số là số nguyên tố hay hợp số?
- **Phương pháp 2:**
  - Để xác định số n có là số nguyên tố hay không, ta có thể kiểm tra có tồn tại **số nguyên tố** $\boldsymbol{x}$ nào đó, $x < n$ và n chia hết cho x hay không. **Nếu có thì** $\boldsymbol{n}$ **là hợp số**.
  - Nếu ta kiểm tra tất cả các **số nguyên tố** $x < n$ và không tìm thấy số chia nào thì $\boldsymbol{n}$ **là số nguyên tố**.
  - **Ví dụ:** 31 có phải số nguyên tố không?
    Kiểm tra nó có chia hết cho 2, 3, 5, 7, 11, 13, 17, 23, 29 không?
    Nó là số nguyên tố.

Số nguyên tố và Hợp số

- **Ví dụ Phương pháp 2:**
  - 91 có phải là số nguyên tố không?
  - Các số nguyên tố dễ biết: 2, 3, 5, 7, 11, 13, 17, 19,…
  - Nhưng có bao nhiêu số nguyên tố nhỏ hơn 91?
- **Lưu ý:**
  - Nếu n tương đối nhỏ, phép kiểm tra là tốt vì ta có thể lặp (ghi nhớ) tất cả những số nguyên tố nhỏ trước nó.
  - Nhưng nếu n lớn thì sẽ có những số nguyên tố lớn hơn và không dễ thấy.

Số nguyên tố và Hợp số

- **Định lý:** Nếu n là hợp số thì n có một số chia là số nguyên tố nhỏ hơn hoặc bằng $\sqrt{n}$.

- **Chứng minh:**
  - Nếu n là hợp số, thì nó có số chia a là số nguyên dương sao cho $1 < a < n$ theo định nghĩa. Điều này có nghĩa là $n = ab$, với b là một số nguyên lớn hơn 1.
  - Giả sử $a > \sqrt{n}$ và $b > \sqrt{n}$. Thì $ab > \sqrt{n}\sqrt{n} = n$, trái với giả thiết. Vì vậy, hoặc là $a \leq \sqrt{n}$ hoặc $b \leq \sqrt{n}$.
  - Do đó, n có số chia nhỏ hơn $\sqrt{n}$.
  - Dựa vào Định lý Cơ bản của Số học, số chia này hoặc là số nguyên tố, hoặc là tích của các số nguyên tố.
    - Trong cả 2 trường hợp, n đều có một số chia là số nguyên tố nhỏ hơn $\sqrt{n}$.

Số nguyên tố và Hợp số

- **Định lý:** Nếu n là hợp số thì n có một số chia là số nguyên tố nhỏ hơn hoặc bằng $\sqrt{n}$.
- **Phương pháp 3:**
  - Để xác định n có phải số nguyên tố hay không, ta có thể kiểm tra có tồn tại số chia x nào đó là số nguyên tố và $x < \sqrt{n}$ hay không.
- **Ví dụ:** 101 có phải là số nguyên tố không?
  - Các số nguyên tố nhỏ hơn $\sqrt{101} = 10.xxx$ là 2, 3, 5, 7
  - 101 không chia hết cho các số trên
  - Do đó, 101 là số nguyên tố
- **Ví dụ:** 91 có phải là số nguyên tố không?
  - Các số nguyên tố nhỏ hơn $\sqrt{91}$ là 2, 3, 5, 7
  - 91 chia hết cho 7
  - Do đó, 91 là hợp số.

Số nguyên tố

- ❑ Câu hỏi đặt ra là có tất cả bao nhiêu số nguyên tố?
- ❑ **Định lý:** Có vô số số nguyên tố.
- ❑ **Chứng minh bởi Euclid:**
  - Chứng minh phản chứng: Giả sử có hữu hạn các số nguyên tố: $p_1, p_2, \dots, p_n$
  - Đặt $Q = p_1 p_2 \dots p_n + 1$ là một số
  - Q không chia hết cho bất cứ số nào trong số $p_1, p_2, \dots, p_n$
  - Điều này là vô lý vì đã giả sử rằng ta đã liệt kê hết các số nguyên tố.

Ước chung lớn nhất

- **Định nghĩa:** Cho a và b là các số nguyên, không đồng thời bằng 0. Số nguyên lớn nhất d sao cho $d|a$ và $d|b$ được gọi là **ước chung lớn nhất** (**greatest common divisor**) của a và b. Ước chung lớn nhất được ký hiệu là $\mathbf{gcd}(\boldsymbol{a}, \boldsymbol{b})$.
- **Ví dụ:**
  - $\gcd(24, 36) = ?$
    Kiểm tra 2, 3, 4, 6, 12 $\Rightarrow \gcd(24, 36) = 12$
  - $\gcd(11, 23) = ?$

Ước chung lớn nhất

❑ Tìm gcd sử dụng phân tích thừa số

- Đặt $a = p_1^{a_1} p_2^{a_2} p_3^{a_3} \dots p_k^{a_k}$ và $b = p_1^{b_1} p_2^{b_2} p_3^{b_3} \dots p_k^{b_k}$
- $\gcd(a, b) = p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} p_3^{\min(a_3,b_3)} \dots p_k^{\min(a_k,b_k)}$

❑ Ví dụ:

- $\gcd(24, 36) = ?$
- $24 = 2 \times 2 \times 2 \times 3 = 2^3 \times 3$
- $36 = 2 \times 2 \times 3 \times 3 = 2^2 \times 3^2$
- $\gcd(24, 36) = 2^2 \times 3 = 12$

Bội chung nhỏ nhất

- **Định nghĩa:** Đặt a và b là các số nguyên dương. **Bội chung nhỏ nhất (least common multipler)** của a và b là số nguyên dương nhỏ nhất chia hết cho cả a và b. Bội chung nhỏ nhất được ký hiệu là **lcm**$(\boldsymbol{a}, \boldsymbol{b})$.
- **Ví dụ:**
  - $lcm(12, 9) = ?$
  - Hãy đưa ra một bội chung: …

Bội chung nhỏ nhất

- **Định nghĩa:** Đặt a và b là các số nguyên dương. **Bội chung nhỏ nhất (least common multipler)** của a và b là số nguyên dương nhỏ nhất chia hết cho cả a và b. Bội chung nhỏ nhất được ký hiệu là $\mathbf{lcm}(\boldsymbol{a},\boldsymbol{b})$.
- **Ví dụ:**
  - $lcm(12,9) = ?$
  - Hãy đưa ra một bội chung: … $12 \times 9 = 108$
  - Ta có thể tìm được số nhỏ hơn không?
  - Có. Thử 36. Cả hai số 12 và 9 đều được chia hết bởi 36.

Bội chung nhỏ nhất

❑ Tìm lcm sử dụng phân tích thừa số

- Đặt $a = p_1^{a_1} p_2^{a_2} p_3^{a_3} \dots p_k^{a_k}$ và $b = p_1^{b_1} p_2^{b_2} p_3^{b_3} \dots p_k^{b_k}$
- $\mathrm{lcm}(a, b) = p_1^{\max(a_1, b_1)} p_2^{\max(a_2, b_2)} p_3^{\max(a_3, b_3)} \dots p_k^{\max(a_k, b_k)}$

❑ Ví dụ:

- $\mathrm{lcm}(12, 9) = ?$
- $12 = 2 \times 2 \times 3 = 2^2 \times 3$
- $9 = 3 \times 3 = 3^2$
- $\mathrm{lcm}(12, 9) = 2^2 \times 3^2 = 4 \times 9 = 36$

Thuật toán Euclid

❑ Tìm ước chung lớn nhất đòi hỏi phân tích thừa số

- $a = p_1^{a_1} p_2^{a_2} p_3^{a_3} \dots p_k^{a_k}$ và $b = p_1^{b_1} p_2^{b_2} p_3^{b_3} \dots p_k^{b_k}$
- $\gcd(a, b) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} p_3^{\min(a_3, b_3)} \dots p_k^{\min(a_k, b_k)}$
- Phân tích thừa số có thể rất tốn thời gian vì ta phải tìm tất cả các thừa số của 2 số nguyên có thể rất lớn.
- May mắn là có một phương pháp hiệu quả hơn để tính gcd, là **thuật toán Euclid**.
  - Phương pháp được biết đến từ xa xưa và được đặt tên theo nhà toán học Hy Lạp Euclid.

Thuật toán Euclid

- **Ta muốn tìm gcd$(\mathbf{287}, \mathbf{91})$.**
  - Đầu tiên, chia số lớn (287) cho số bé (91)
  - Ta có $287 = 3 \times 91 + 14$

1) **Bất cứ số chia nào của 91 và 287 đều là số chia của 14:**
   - $287 - 3 \times 91 = 14$
   - Tại sao? $[ak - cbk] = r \Rightarrow (a - cb)k = r \Rightarrow (a - cb) = \frac{r}{k}$ (phải là số nguyên, vì vậy r chia hết cho k).

2) **Bất cứ số chia nào của 91 và 14 đều là số chia của 287:**
   - Tại sao? $287 = 3bk + dk \Rightarrow 287 = k(3b + d) \Rightarrow \frac{287}{k} = (3b + d) \leftarrow \frac{287}{k}$ là số nguyên.
   - **Do đó,** $\mathbf{gcd}(\mathbf{287}, \mathbf{91}) = \mathbf{gcd}(\mathbf{91}, \mathbf{14})$

Thuật toán Euclid

- **Ta biết rằng $\mathbf{gcd(287, 91) = gcd(91, 14)}$**
- Có thể áp dụng lại cách đó:
  - $\mathrm{gcd}(91, 14)$
  - $91 = 14 \times 6 + 7$
- Vì vậy
  - $\mathrm{gcd}(91, 14) = \mathrm{gcd}(14, 7)$
- Áp dụng 1 lần nữa:
  - $\mathrm{gcd}(14, 7) = 7$
  - Dễ giải
- Kết quả: $\mathrm{gcd}(287, 91) = \mathrm{gcd}(91,14) = \mathrm{gcd}(14, 7) = 7$

Thuật toán Euclid

❑ Ví dụ:

- Tìm ước chung lớn nhất của 666 và 558
- $\gcd(666, 558)$ $\quad 666 = 1 \times 558 + 108$

  $= \gcd(558, 108)$ $\quad 558 = 5 \times 108 + 18$

  $= \gcd(108, 18)$ $\quad 108 = 6 \times 18 + 0 = 18$

Thuật toán Euclid

❑ Ví dụ

- Tìm ước chung lớn nhất của 286 và 503:
- $\gcd(503, 286)$ $\quad 503 = 1 \times 286 + 217$

$= \gcd(286, 217)$ $\quad 286 = 1 \times 217 + 69$

$= \gcd(217, 69)$ $\quad 217 = 3 \times 69 + 10$

$= \gcd(69, 10)$ $\quad 69 = 6 \times 10 + 9$

$= \gcd(10, 9)$ $\quad 10 = 1 \times 9 + 1$

$$= \gcd(9, 1) = 1$$

Phương trình đồng dư và ứng dụng

Số học đồng dư (modular arithmetics)

- Trong khoa học máy tính, chúng ta thường quan tâm đến phần dư (remain) của một số nguyên khi nó chia cho một số nguyên dương nào đó.
- **Bài toán:** Giả sử bây giờ là nửa đêm. Sau 50 giờ nữa là mấy giờ?
- **Đáp án:** 2 giờ sáng
- **Giải thích:**
  - Chia 50 cho 24. Phần dư là thời gian dựa trên khung 24 giờ.
    - $50 = 2 \times 24 + 2$
    - Nên kết quả là 2 giờ sáng.

Đồng dư

- **Định nghĩa:** Nếu a và b là các số nguyên và m là một số nguyên dương thì ***a* đồng dư với *b* mô-đu-lô *m*** nếu $a - b$ chia hết cho m. Ta dùng $\boldsymbol{a} = \boldsymbol{b}(\mathbf{mod}\ \boldsymbol{m})$ để kí hiệu sự đồng dư. Nếu a và b không đồng dư ta viết $a \neq b$ $(\text{mod}\ m)$.
- **Ví dụ:**
  - Xác định 17 có đồng dư với 5 mô-đu-lô 6 không?

Đồng dư

- **Định lý:** Nếu a và b là các số nguyên và m là một số nguyên dương, thì $a = b(\text{mod } m)$ khi và chỉ khi $a \text{ mod } m = b \text{ mod } m$.
- **Ví dụ:**
  - Xác định 17 có đồng dư với 5 mô-đu-lô 6 không?
  - 17 mod 6 = 5
  - 5 mod 6 = 5
  - Do đó, 17 đồng dư với 5 mô-đu-lô 6

Đồng dư

- **Định lý 1:** Đặt m là một số nguyên dương. Các số nguyên a và b đồng dư mô-đu-lô m khi và chỉ khi tồn tại một số nguyên k sao cho $a = b + mk$.

- **Định lý 2:** Đặt m là một số nguyên dương. Nếu $a = b(\text{mod}\, m)$ và $c = d(\text{mod}\, m)$ thì:
  $a + c = b + d(\text{mod}\, m)$ và $ac = bd(\text{mod}\, m)$.

Hệ quả (Corolary)

- Giả sử m là một số nguyên dương và a và b là các số nguyên, khi đó:
  $(a + b) \textbf{ mod } m = \big((a \textbf{ mod } m) + (b \textbf{ mod } m)\big) \textbf{ mod } m$
  $ab \textbf{ mod } m = \big((a \textbf{ mod } m)(b \textbf{ mod } m)\big) \textbf{ mod } m$

- **Chứng minh:**
  - Từ định nghĩa của **mod** m và đồng dư mô-đu-lô m, ta biết rằng $a \equiv (a \textbf{ mod } m)\ (\textbf{mod } m)$ và $b \equiv (b \textbf{ mod } m)\ (\textbf{mod } m)$. Do đó, Đinh lý 5 cho ta thấy:
    $a + b \equiv (a \textbf{ mod } m) + (b \textbf{ mod } m)\ (\textbf{mod } m)$
    và
    $ab \equiv (a \textbf{ mod } m)(b \textbf{ mod } m)\ (\textbf{mod } m)$.
  - Tính chất của hệ quả này được suy ra từ hai phương trình đồng dư cuối cùng ở Định lý 3.

Ứng dung số học đồng dư

- Số học đồng dư được ứng dụng trong Khoa học máy tính:
  - Bộ sinh số giả ngẫu nhiên (pseudo-random)
  - Hàm băm (hash function)
  - Mã hóa (cryptology) RSA

Bộ sinh số giả ngẫu nhiên

- Có một số bài toán lập trình cần giả lập sự lựa chọn ngẫu nhiên.
- **Ví dụ:** tung đồng xu, tung xúc xắc.
- Ta cần một cách để sinh ra các kết quả ngẫu nhiên
- **Bài toán cơ bản:**
  - Giả sử các kết quả: 0, 1, … N
  - Tạo một chuỗi các kết quả ngẫu nhiên
- Bộ sinh số giả ngẫu nhiên cho phép ta tạo ra chuỗi số có vẻ ngẫu nhiên.
- **Tiếp theo:** phương pháp đồng dư tuyến tính

Bộ sinh số giả ngẫu nhiên

❑ Phương pháp đồng dư tuyến tính

- Ta chọn 4 số:
    - Số mô-đu-lô m
    - Số nhận a
    - Số đếm c
    - Hạt giống x_0

  sao cho $2 \leq a < m, 0 \leq c < m, 0 \leq x_0 < m$.
- Tạo một chuỗi các số $x_1, x_2, x_3, \dots, x_n \dots$ sao cho $0 \leq x_n < m$ với mọi n thỏa mãn:

$$x_{n+1} = (a \times x_n + c) \bmod m$$

Bộ sinh số giả ngẫu nhiên

❑ Phương pháp đồng dư tuyến tính

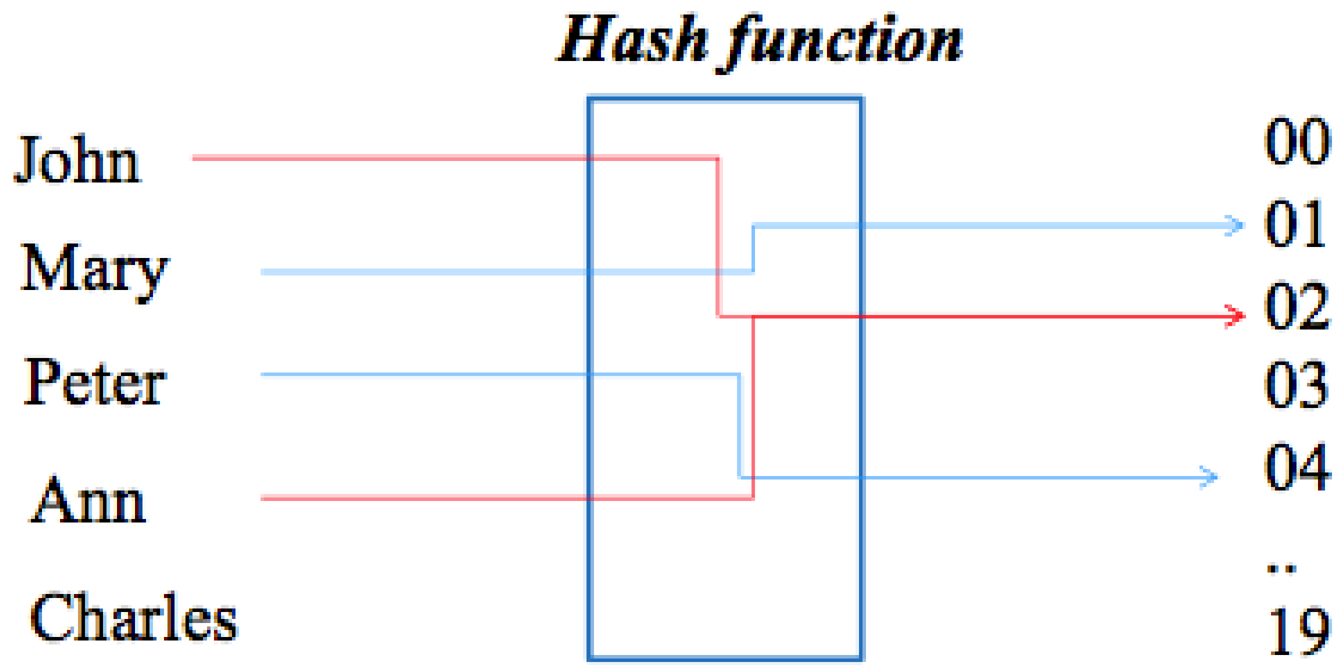
- $x_{n+1} = (a \times x_n + c) \bmod m$

❑ Ví dụ

- Giả sử $m = 9, a = 7, c = 4, x_0 = 3$
  - $x_1 = (7 \times 3 + 4) \bmod 9 = 25 \bmod 9 = 7$
  - $x_2 = 53 \bmod 9 = 8$
  - $x_3 = 60 \bmod 9 = 6$
  - $x_4 = 46 \bmod 9 = 1$
  - $x_5 = 11 \bmod 9 = 2$
  - $x_6 = 18 \bmod 9 = 0$
  - $\ldots$

Hàm băm

- Một hàm băm là một thuật toán ánh xạ dữ liệu có độ dài bất kì sang dự liệu có độ dài cố định.
- Giá trị trả về từ hàm băm gọi là giá trị băm hoặc mã băm.
- **Ví dụ:**



Hàm băm

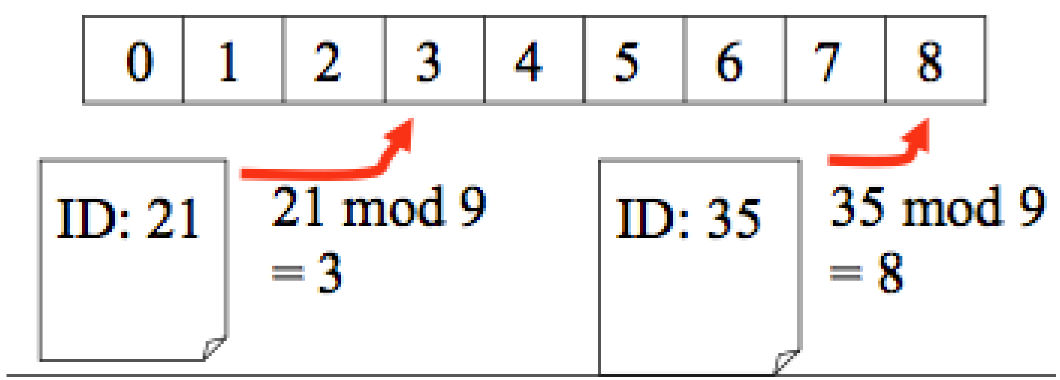
- Một ví dụ về hàm băm ánh xạ các số nguyên (bao gồm cả số lớn) sang một tập con $0, 1, \ldots, m-1$ là:

$$\boldsymbol{h(k) = k \bmod m}$$

- **Ví dụ:** Giả sử ta có một cơ sở dữ liệu các nhân viên, mỗi người có một ID duy nhất – số CMTND gồm 8 chữ số. Ta muốn lưu trữ các bản ghi vào một bảng nhỏ với m mục.
  - Sử dụng hàm $h(k)$, ta có thể ánh xạ số an ninh trong cơ sở dữ liệu nhân viên sang số thứ tự của bảng.
    - Giả sử: $h(k) = k \bmod 111$. Thì:
      $h(064212848) = 064212848 \bmod 111 = 14$
      $h(037149212) = 037149212 \bmod 111 = 65$

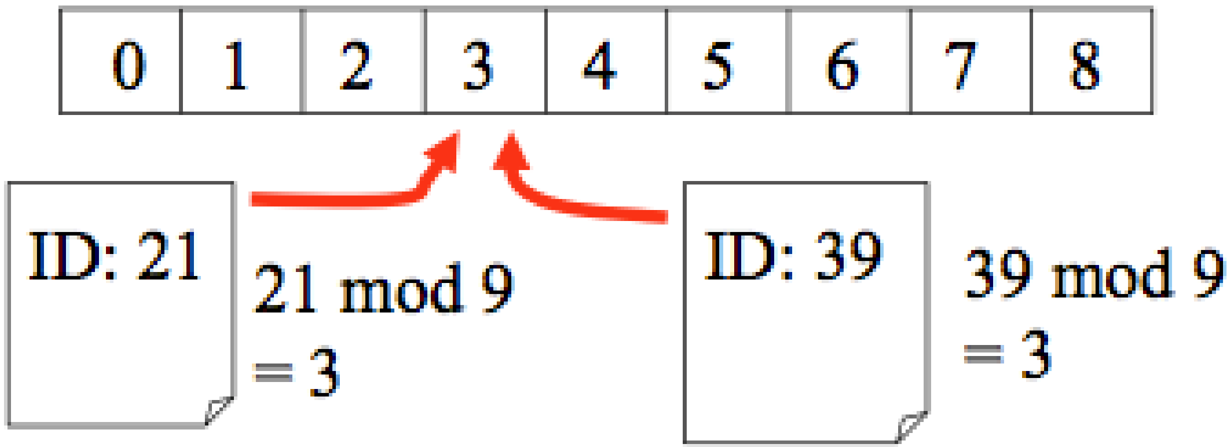
Hàm băm

- **Bài toán:** Cho tập các bản ghi lớn, làm thế nào để lưu và tìm kiếm nhanh một bản ghi?
- **Giải pháp:** Sử dụng hàm băm để tính ra vị trí của bản ghi dựa vào ID của nó.
- **Ví dụ:** Một hàm băm thông dụng là $h(k) = k \bmod n$, với n là số vị trí lưu trữ có sẵn.



Hàm băm

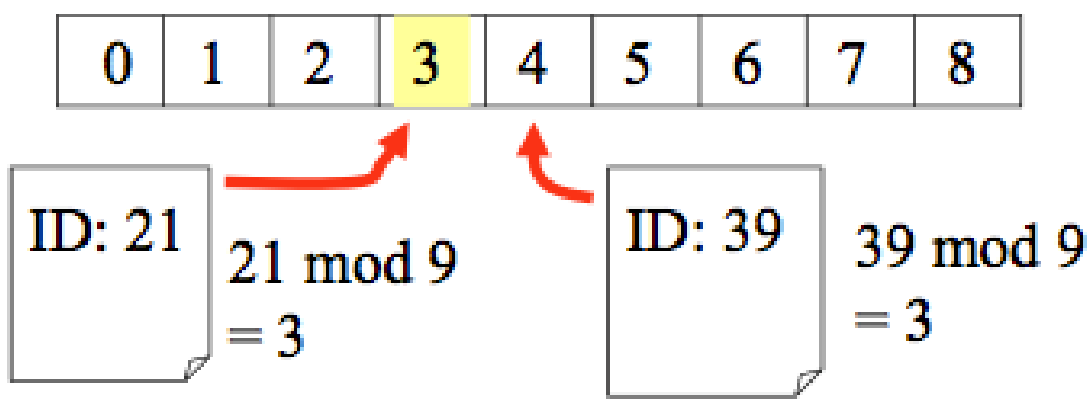
- **Bài toán:** hai bản ghi được ánh xạ đến cùng một vị trí



Hàm băm

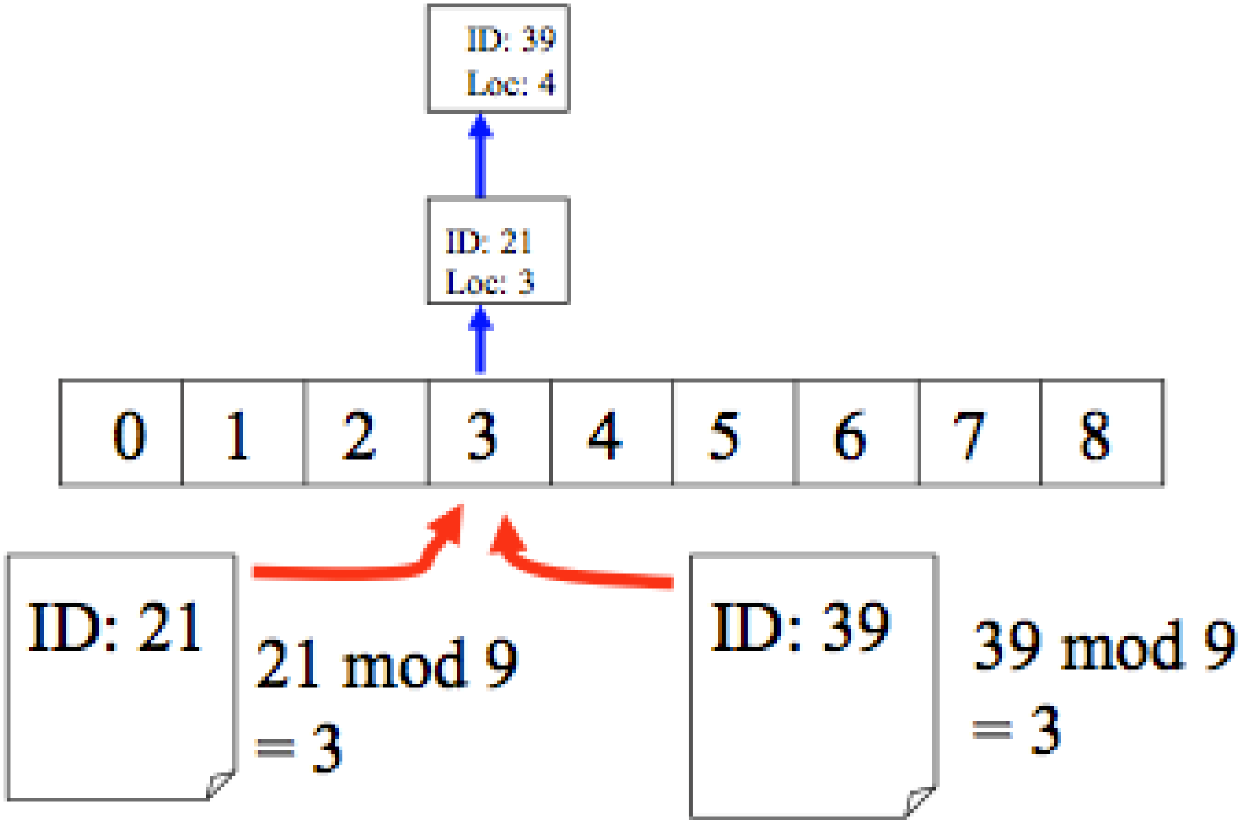
- **Giải pháp 1:** di chuyển đến vị trí trống tiếp theo.
  - Phương pháp được biểu diễn bởi một chuỗi các hàm băm để thử

$$h_0(k) = k \bmod n$$
$$h_1(k) = (k+1) \bmod n$$
$$\dots$$
$$h_m(k) = (k+m) \bmod n$$



Hàm băm

- **Giải pháp 2:** ghi nhớ chính xác vị trí trong cấu trúc thứ hai được tìm kiếm tuần tự.



Đồng dư ứng dụng trong mã hóa RSA

- Biểu diễn tuyến tính của ước chung lớn nhất
  - **Định lý Bézout:** Nếu a và b là các số nguyên dương, thì tồn tại các số nguyên s và t sao cho $\gcd(a, b) = sa + tb$.
  - **Ví dụ 1:**
    - Biểu diễn $\gcd(252, 198) = 18$ dưới dạng một biểu thức tuyến tính của 252 và 198.
  - **Đáp án:**
    - Để cho thấy $\gcd(252, 198) = 18$, thuật toán Euclidean sử dụng các phép chia sau:

$$252 = 1 \cdot 198 + 54$$
$$198 = 3 \cdot 54 + 36$$
$$54 = 1 \cdot 36 + 18$$
$$36 = 2 \cdot 18$$

    - Sử dụng phép chia tiếp-đến-cuối (next-to-last), ta có thể biểu diễn $\gcd(252, 198) = 18$ dưới dạng một kết hợp tuyến tính của 54 và 36. Ta thấy:

$$18 = 54 - 1 \cdot 36$$

      Phép chia thứ hai cho ta thấy:

$$36 = 198 - 3 \cdot 54$$

    - Thay biểu thức này cho 36 trong biểu thức trước, ta có thể biểu diễn 18 dưới dạng một kết hợp tuyến tính của 54 và 198. Ta có
      $18 = 54 - 1 \cdot 36 = 54 - 1 \cdot (198 - 3 \cdot 54) = 4 \cdot 54 - 1 \cdot 198$

Ước chung lớn nhất

- Nếu a, b, và c là các số nguyên dương sao cho $\gcd(a, b) = 1$ và $a \mid bc$, thì $a \mid c$.
- **Chứng minh:**
  - Vì $\gcd(a, b) = 1$, từ **Định lý Bézout,** tồn tại các số nguyên s và t sao cho:
    $$sa + tb = 1$$
  - Nhân hai vế của đẳng thức với c, ta có:
    $$sac + tbc = c$$
  - Sử dụng **Định lý 1** trong Phần 4.1 để suy ra $a \mid c$.
    - Từ phần (ii) của định lý đó, $a \mid tbc$. Vì $a \mid sac$ và $a \mid tbc$, từ phần (i) của định lý đó, ta kết luận rằng $sac + tbc$ chia hết cho a. Vì $sac + tbc = c$, ta kết luận rằng $a \mid c$ (đpcm).

Ước chung lớn nhất

- Cho m là một số nguyên dương và a, b, và c là các số nguyên. Nếu $ac \equiv bc(\mathbf{mod}\, m)$ và $\gcd(c, m) = 1$, thì $a \equiv b(\mathbf{mod}\, m)$.

- **Chứng minh:**
  - Vì $ac \equiv bc(\mathbf{mod}\, m)$, $m \mid ac - bc = c(a - b)$. Từ **Bổ đề 2**, vì $\gcd(c, m) = 1$, suy ra $m \mid a - b$.
  - Từ đó ta có $a \equiv b(\mathbf{mod}\, m)$.

Phương trình Đồng dư Tuyến tính

- Nếu a và m là các số nguyên tố và $m > 1$, thì tồn tại nghịch đảo của a theo mô-đu-lô m, ký hiệu là $\bar{a} < m$, sao cho $a\bar{a} = 1\ (mod\ m)$
  - Nghịch đảo này là duy nhất.
  - Mọi nghịch đảo khác của a ($\mathbf{mod}\ m$) đều là đồng dư của $\bar{a}$ theo mô-đu-lô m).
- **Chứng minh:**
  - Từ **Định lý 6** phần 4.3, vì $\gcd(a, m) = 1$, tồn tại các số nguyên s và t sao cho:
  $$sa + tm = 1$$
  - Điều này nghĩa là:
  $$sa + tm \equiv 1(\mathbf{mod}\ m)$$
  - Vì $tm \equiv 0(\mathbf{mod}\ m)$, suy ra
  $$sa \equiv 1(\mathbf{mod}\ m)$$
  - Từ đó, s là nghịch đảo của a $\mathbf{mod}\ m$ (đpcm).
  - (Chứng minh nghịch đảo này là duy nhất là một bài tập).

Căn nguyên thủy và Lô-ga-rít rời rạc

- Cho p là một số nguyên tố, một căn nguyên thủy mô-đu-lô p là một số nguyên r thuộc $\mathbb{Z}_p$ sao cho mọi phần tử khác 0 của $\mathbb{Z}_p$ đều là lũy thừa của r mô-đu-lô p.
- **Ví dụ:** Xác định 2 và 3 có là căn nguyên thủy của mô-đu-lô 11 hay không.
  - **Đáp án:**
    - Khi ta tính các lũy thừa của 2 trong $\mathbb{Z}_{11}$, ta thu được $2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 = 5, 2^5 = 10, 2^6 = 9, 2^7 = 7, 2^8 = 3, 2^9 = 6, 2^{10} = 1$. Vì mọi phần tử của $\mathbb{Z}_{11}$ là lũy thừa của 2, 2 là căn nguyên thủy của 11.
    - Khi ta tính các lũy thừa của 3 mô-đu-lô 11, ta thu được $3^1 = 3, 3^2 = 9, 3^3 = 5, 3^4 = 4, 3^5 = 1$. Ta thấy rằng quy luật này lặp lại khi tính các lũy thừa lớn hơn của 3. Vì không phải mọi phần tử của $\mathbb{Z}_{11}$ là lũy thừa của 3, ta kết luận rằng 3 không là căn nguyên thủy của 11.

Căn nguyên thủy và Lô-ga-rít rời rạc

- Giả sử p là một số nguyên tố, r là một căn nguyên thủy mô-đu-lô p, và a là một số nguyên trong khoảng 1 và $p - 1$.
  - Nếu $r^e \ \mathbf{mod}\ p = a$ và $0 \leq e \leq p - 1$, ta nói e là lô-ga-rít rời rạc cơ số r của $a \ \mathbf{mod}\ p$
    - Ký hiệu là: $\log_r a = e$ (số nguyên tố p được ngầm hiểu).
- **Ví dụ 3:** Tìm lô-ga-rít rời rạc cơ số 2 của 3 và 5 mô-đu-lô 11.
  - **Đáp án:**
    - Khi ta tính được các lũy thừa của 2 mô-đu-lô 11 trong **Ví dụ 2**, ta thấy $2^8 = 3$ và $2^4 = 5$ trong $\mathbb{Z}_{11}$. Do đó lô-ga-rít rời rạc cơ số 2 của 3 và 5 mô-đu-lô 11 lần lượt là 8 và 4 (Đây là các lũy thừa của 2 mà lần lượt bằng 3 và 5 trong $\mathbb{Z}_{11}$). Ta viết $\log_2 3 = 8$ và $\log_2 5 = 4$ (với mô-đu-lô 11 được ngầm hiểu).

Kết thúc nội dung chương!