VNU-HUS MAT3500: Toán rời rạc

Lý thuyết số cơ bản II

Hoàng Anh Đức

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

Nội dung

Phương trình đồng dư

- Giới thiệu
- Định lý phần dư Trung Hoa
- Định lý Fermat nhỏ

Thuật toán mã hóa RSA

Phương trình đồng dư
Giới thiệu

- 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, ký hiệu a^{-1}, là bất kỳ số nguyên nào thỏa mãn $a^{-1}a \equiv 1 \pmod{m}$
  - Đôi khi ta cũng dùng ký hiệu $\overline{a}$ thay vì a^{-1}
  - Chú ý rằng nếu ta có thể tìm được a^{-1} thỏa mãn điều kiện trên, ta có thể giải $ax \equiv b \pmod{m}$ bằng cách nhân cả hai vế với a^{-1}, nghĩa là, $a^{-1}ax \equiv a^{-1}b \pmod{m}$, suy ra $1 \cdot x \equiv a^{-1}b \pmod{m}$, và do đó $x \equiv a^{-1}b \pmod{m}$

Định lý 1

Nếu $\gcd(a, m) = 1$ *và* $m > 1$ *thì tồn tại nghịch đảo* a^{-1} *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 $a^{-1} = s$
- 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 $a \equiv b \pmod{m}$

□

Bài tập 1

Chứng minh rằng nếu $\gcd(a, m) > 1$ *với* a *là số nguyên bất kỳ và* $m > 2$ *là một số nguyên dương thì không tồn tại một nghịch đảo của* a *theo môđun* m

Định lý 1 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 1

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 1, $s = -2$ 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 $5, -9, 12, \ldots$) đều là nghịch đảo của -3 theo môđun 7

Ví dụ 2

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 2

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) $a = 89, m = 232$

(5) $a = 101, m = 4620$

Bài tập 3

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 4

Cho các số nguyên dương $m_1, m_2, \ldots, m_n$ *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* $m = m_1 m_2 \ldots m_n$. (***Gợi ý:*** *Chứng minh với* $n = 2$)

Phương trình đồng dư

Định lý phần dư Trung Hoa

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 2: Định lý phần dư Trung Hoa

Cho các số nguyên dương $m_1, m_2, \ldots, m_n$ *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* $a_1, a_2, \ldots, a_n$. *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 $m = m_1 m_2 \ldots m_n$. *(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 1, 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

□

Bài tập 5

*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 (**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 4 để kết luận rằng $m \mid (x - y)$ trong đó $m = m_1 m_2 \ldots m_n$)*

Ví dụ 3

Giải hệ phương trình

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

- $m = m_1 m_2 m_3 = 3 \cdot 5 \cdot 7 = 105$
- $M_1 = m/m_1 = 35$ 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 4 (Phương pháp thay ngược)

Giải hệ phương trình

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

- 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 6

Giải hệ phương trình sau bằng các phương pháp minh họa trong hai ví dụ trước

$$x \equiv 1 \pmod 5 \quad (4)$$
$$x \equiv 2 \pmod 6 \quad (5)$$
$$x \equiv 3 \pmod 7 \quad (6)$$

Bài tập 7

Giải hệ phương trình sau bằng các phương pháp minh họa trong hai ví dụ trước

$$x \equiv 2 \pmod 3 \quad (7)$$
$$x \equiv 1 \pmod 4 \quad (8)$$
$$x \equiv 3 \pmod 5 \quad (9)$$

Phương trình đồng dư

Định lý phần dư Trung Hoa

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 3: 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 8 (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 5 (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 9

(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* $1001 = 7 \cdot 11 \cdot 13$*)*

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

Thuật toán mã hóa RSA

RSA - Rivest-Shamir-Adleman

Ví dụ 6

- $n = pq = 43 \cdot 59 = 2537$, $k = 42 \cdot 58 = 2436$
- 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

Thuật toán mã hóa RSA

RSA - Rivest-Shamir-Adleman

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 $m^{ed} \equiv m \pmod{pq} \equiv m \pmod{n}$

□